EH-01_張凱銘.tpf-1

川普政府時期的美國國家網路戰略之研究：從威脅平衡理論分析

張凱銘
（臺中科技大學通識教育中心助理教授）

摘　要

本文回顧了川普政府就任以來的網路戰略規畫與實踐狀態，並援引國際關係學界中的威脅平衡理論進行分析。研究結果顯示美國當前的國家網路戰略以因應威脅為主軸，對內積極建設網路攻防能力，對外則與友好國家開展跨國網路安全合作，藉以平衡來自中國和俄羅斯等競爭對手的挑戰。惟部分戰略內容因具有較突出的單邊主義特質，在實踐過程中已引起諸多爭議，對於國際網路政治的穩定運作及網際網路發展前景或將造成更多變數。

關鍵詞：網路安全、美國國家網路戰略、美國外交政策、國際網路政治、防禦推進

壹、前言

自 2017 年以來，川普總統(Donald J. Trump)治下的美國政府展露了較其前任更為大膽進取的為政作風。回顧過往三年間的治理脈絡，可發現除影響廣泛的貿易戰和情勢多變的朝鮮半島問題外，網路安全顯然是川普政府當前高度關注的重點政策領域。川普總統本人與其團隊成員無論在競選期間或正式執政後，都曾多次對外發言強調保障國家網路安全的重要性，聯邦政府各級部門也陸續發表多項網路政策文

EH-01_張凱銘.tpf-2

件，呈現緊湊綿密的戰略布局節奏。檢閱相關發言與文件內容，可發現網路科技在川普政府的認知中既是應用廣泛且極具潛力的科學技術，也和國家安全、經濟繁榮及文化價值的維護息息相關。更重要的是，川普政府的網路戰略論述尤其強調美國網路安全面臨的各種威脅及強化攻防能力的重要性，進而提出一系列涉及行政改革、國防建設與外交政策的行動方針並逐一落實中。

本文以川普政府第一任期的國家網路戰略規畫為研究主題，文中回顧了美國在 2017 年至 2019 年中旬間的相關政策文件及網路施政狀況，援引國際關係現實主義學派(Realism)的威脅平衡理論(Balance of Threat Theory)，分析川普政府的網路戰略建構動因，以及其如何在實踐層面同步運用內部平衡(Internal Balancing)與外部平衡(External Balancing)策略設法制約威脅，俾有效維護美國在網路空間中的安全與利益。

貳、川普政府的國家網路戰略論述

源於美國的網路科技本係冷戰時代核子戰爭陰影下形成的軍事通訊技術，隨著軟硬體設備轉入學研機構，在 1980 年代後受惠於多方參與研發而迅速演進，並和個人電腦普及趨勢相匯集，全面滲入政經體系與民眾日常生活。美國政府也在過程中漸進完善網路法令制訂及資訊基礎設施安全防護等工作。[1]

進入 21 世紀後，網路科技的戰略價值在其應用範疇持續拓展下大幅上升，世界各國在致力網路技術研發和設施布建之外亦高度重視網路安全問題。譬如美國歐巴馬(Barack H. Obama)政府便將網路安全升格至國家安全層次，強調網路空間的和平穩定，與美國的軍事防務、民生經濟及國土安全密切相關，並在《網路空間政策評估》(*Cyber-*

1. 關於網路科技的演進軌跡，請見 Johnny Ryan, *A History of the Internet and the Digital Future* (London: Reaktion Books, 2010), pp. 23-104。

EH-01_張凱銘.tpf-3

space Policy Review)和《網路空間國際戰略》(*International Strategy for Cyberspace*)等文件中指出，鑑於網路空間安全情勢日益惡化的趨向，美國應加強本國網路系統安全並積極參與國際網路政治，以應對網路惡意活動及來自戰略競爭對手的挑戰。[2]

2017 年後執政的川普總統及其團隊部分成員早在競選期間，便於媒體訪談和公開演說等場合中屢屢表達對網路安全問題的關切，當時雖為部分媒體視作虛浮的選舉語言，[3] 但由美國於 2017 年後的網路施政情況來看，川普總統對網路安全的重視並非僅是用以吸引選民的口號，其領導的政府團隊正積極籌畫國家網路戰略並加以實踐。

美國國防部國防科學委員會(Defense Science Board)在川普政府就任伊始便發表《網路嚇阻的工作組報告》(*Cyber Deterrence Task Force*)，敦促新任政府盡速建立足以嚇阻外部威脅的網路防務能力。[4] 隨後面世的新版《國家安全戰略》(*National Security Strategy, NSS*)

2. The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: The White House, 2009), pp. 1-2; The White House, *International Strategy for Cyberspace* (Washington, D.C.: The White House, 2011), pp. 8-11.
3. 有關川普總統與其團隊成員在競選過程中關於網路議題的發言，請見"Transcript: Donald Trump on NATO, Turkey's Coup Attempt and the World," *The New York Times*, July 21, 2016, <https://www.nytimes.com/2016/07/22/us/politics/donald-trump-foreign-policy-interview.html>；Adrienne LaFrance, "Trump's Incoherent Ideas About 'the Cyber,'" *The Atlantic*, September 27, 2016, <https://www.theatlantic.com/technology/archive/2016/09/trumps-incoherent-ideas-about-the-cyber/501839/>；Dustin Volz & Mark Hosenball, "Trump Cyber Security Team, Policy Slow to Take Shape: Officials," *Reuters*, November 17, 2016, <https://www.reuters.com/article/us-usa-trump-cyber-idUSKBN13B2VI>。
4. U.S. Defense Science Board, *Cyber Deterrence Task Force* (Washington, D.C.: Office of the Secretary of Defense, 2017), pp. 1-16.

EH-01_張凱銘.tpf-4

中，川普政府除闡述美國當前的宏觀戰略架構，根據「美國優先」(America First)理念提出「保護美國民眾、國土與美國的生活方式」、「促進美國的繁榮」、「以實力保障和平」及「強化美國的影響力」等四項核心目標外，更以相當篇幅說明美國對於網路科技及資安議題的關切。網路(Cyber)一詞在這份報告中出現高達 46 次，為前兩版《國家安全戰略》的一倍有餘。川普政府強調來自國際間的大量網路惡意活動已構成重大安全威脅，美國須致力提升網路攻防能力，在平時發揮嚇阻功用，並於衝突發生時成功挫敗對手。川普政府也承諾將積極查緝他國對美國發起的網路間諜及侵權活動，以保護本國資訊產業，並鞏固美國在數位經濟方面的領先地位。美國同時將積極參與國際網路政治，增進與友邦間的外交協調，以保障網際網路的自由和秩序不受侵擾。[5]

2018 年 9 月，川普政府正式發表《國家網路戰略》(*National Cyber Strategy, NCS*)，除奠立美國在網路領域的總體戰略指導，亦再度確認網路科技在美國國家安全戰略中的核心地位，外界可透過這份報告一覽川普政府的網路戰略藍圖。整體而言，報告內容以網路安全問題為主軸，直指美國正面臨來自中國、俄羅斯、伊朗、北韓與部分非國家行為體造成的網路威脅，並在回應威脅的理路下逐步鋪展出涵蓋安全、經濟與外交等三大面向的戰略框架。[6]

在安全方面，川普政府認為除發展網路戰力以嚇阻及反制對手外，亦有必要於國內外採取各種資安保障措施。國內部分，美國將盡快汰換陳舊過時的資訊基礎設施，並在政府內建立跨部門的網路風險問責及協調制度以防堵資安漏洞，同時加強與民間企業合作，共同開

5. The White House, *National Security Strategy* (Washington, D.C.: The White House, 2017), pp. 12-13, 31-32.
6. The White House, *National Cyber Strategy* (Washington, D.C.: The White House, 2018), pp. 1-3.

EH-01_張凱銘.tpf-5

發即時偵測與反溯網路惡意活動的技術能力。國際部分，美國將與友邦建立網路安全合作機制以因應各類威脅，並透過聯合國等平臺促進多邊協調，以期建立網路空間國家行為準則。在經濟方面，川普政府宣示將加強偵辦網路間諜活動，為資訊產業創造安全營運環境，同時以政策手段促進專業人才培育和高階技術創新，為下一階段的數位經濟成長創造條件。在外交方面，美國將經由雙邊與多邊途徑擴大與各國在網路領域的交流，包含數位經濟合作、針對低度開發國家的網路技術援助，以及推廣網路自由價值觀等，藉此拓展美國在國際網路政治中的影響力，並維繫網際網路的自由開放。[7]

根據《國家安全戰略》與《國家網路戰略》的指導，部分聯邦部門也在應對網路威脅的脈絡下提出業務範圍內的政策規畫。例如美國國務院先後發表《有關嚇阻敵人與更好地保護美國人民免於網路威脅的建議》(*Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*)及《關於透過國際參與保護美國網路利益與嚇阻網路威脅的建議》(*Recommendations to the President on Securing America's Cyber Interests and Deterring Cyber Threats through International Engagement*)等文件，指出美國應對位處動武門檻之下(Below the Threshold of the Use of Force)的網路攻擊提出嚇阻方案並發展多元反制能力，同時透過國際合作建設網路空間國家行為準則及網路信心建立措施(Cyber Confidence Building Measures, CCBM)，以保障網際網路的和平穩定。[8]

美國行政管理與預算局(Office of Management and Budget)發表的《聯邦網路安全評估報告暨行動計畫》(*Federal Cybersecurity Risk*

7. The White House, *National Cyber Strategy*, pp. 6-26.

8. U.S. Department of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*

EH-01_張凱銘.tpf-6

Determination Report and Action Plan)批評許多政府部門對於網路安全風險欠缺理解、不具備感知威脅並反制惡意活動的能力，亦未建立有效的資安問責制度，並提出多項改革倡議。[9]美國商務部(Department of Commerce)與國土安全部(Department of Homeland Security)共同發表的《有關強化網際網路與通訊生態系統韌性以應對殭屍網路與其他自動化分散性威脅的報告》(*A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*)與《有關支持國家網路安全人力資源發展與維持的報告》(*A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce*)兩份文件，除提出加強資訊基礎設施與網路服務安全性等方案，也建議政府向教育體系擴大投入資源以培養專業人才，並與企業及高等教育機構合作建立培訓機制，藉此緩解當前資安人力資源短缺的問題。[10]

美國國防部於 2018 年 9 月發表的《2018 年國防部網路戰略摘要》(*Summary of the 2018 Department of Defense Cyber Strategy*)中宣

(Washington, D.C.: U.S. Department of State, 2018), pp. 1-3; U.S. Department of State, *Recommendations to the President on Securing America's Cyber Interests and Deterring Cyber Threats through International Engagement* (Washington, D.C.: U.S. Department of State, 2018), pp. 1-4.

9. U.S. Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan* (Washington, D.C.: Office of Management and Budget, 2018), pp. 1-18.

10. U.S. Department of Commerce & U.S. Department of Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* (Washington, D.C.: U.S. Department of Commerce & U.S. Department of Homeland Security, 2018), pp. 9-46; U.S. Department of Commerce & U.S. Department of Homeland Security, *A Report to the President on*

EH-01_張凱銘.tpf-7

示將強化與國內外學研機構及資安產業合作，以加速軍用網路技術研發進程，並強調美軍對網路戰力的運用不僅止於嚇阻或反制網路攻擊，在預先察知潛在威脅時更可能逕行發動先制打擊。[11] 在同年稍晚發表的《國防部雲端戰略》(*DoD Cloud Strategy*)中，美國國防部指出美軍將於日常防務擴大運用雲端運算工具，並加強參與雲端安全防護技術開發工作，期望透過雲端技術提升數據蒐集和行政管理效率，並藉由高速的情資分析傳遞功能為前線人員提供支持。[12]

時序進入 2019 年後，川普政府對於網路戰略的籌畫步調同樣緊湊。2019 年 1 月，美國情報總監辦公室(U.S. Office of the Director of National Intelligence)在 2019 年版《國家情報戰略》(*National Intelligence Strategy 2019*)中點出，網路威脅的升高已嚴重危害到美國國家安全與社會大眾對於政府治理能力的信心，美國的情報體系為此將擴大蒐集涉及網路惡意活動的情資，協助相關部門即時偵測並反制各種網路威脅。[13] 當年五月，美國國防部公布了向國會提交的 2019 年版《關於中華人民共和國的軍事與安全力量發展報告》(*Military and Security Developments. Involving the People's Republic of China 2019*)，報告中指出中國不僅利用大量網路間諜活動竊取他國科學知識與商業技術，其國安單位更暗中支持駭客組織向許多國家發起網路攻

Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (Washington, D.C.: U.S. Department of Commerce & U.S. Department of Homeland Security, 2018), pp. 1-20.

11. U.S. Department of Defense, *Summary of the 2018 Department of Defense Cyber Strategy* (Washington, D.C.: U.S. Department of Defense, 2018), pp. 1-7.
12. U.S. Department of Defense, *DoD Cloud Strategy* (Washington, D.C.: U.S. Department of Defense, 2018), pp. 1-11.
13. U.S. Office of the Director of National Intelligence, *National Intelligence Strategy 2019* (Washington, D.C.: U.S. Office of the Director of National Intelligence, 2019), p. 11.

EH-01_張凱銘.tpf-8

擊，藉以取得關於商業、科學與防務方面的機敏情資。[14]美國政府問責署(Government Accountability Office, GAO)在同年 8 月發表的報告《關鍵基礎設施保障：因應電網系統面臨重大網路安全風險的必要措施》(*Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*)，文中警示美國電網系統的網路安全防護並不充分，極易遭遇來自外國勢力、駭客組織與犯罪份子發動的網路襲擊，進而間接導致工業控制系統、物聯網系統與全球定位系統等陷入風險之中，並呼籲能源部與國土安全部等單位儘速採取必要應對措施。[15]2019 年 12 月時，美國國家科學技術委員會(National Science and Technology Council)發表了 2019 年版的《聯邦網路空間安全研究暨發展戰略計畫》(*2019 Federal Cybersecurity Research and Development Strategic Plan*)，宣示聯邦政府將持續鎖定「防護」(Protect)、「嚇阻」(Deter)、「偵測」(Detect)與「回應」(Respond)四個面向發展更為成熟可靠的網路安全能力，並擴大對人工智慧、量子計算與人力資源培育等領域的投資，以保持美國的科技領導優勢。[16]

本文透過表 1 羅列了自 2017 年 2 月至 2019 年 12 月間，美國聯邦政府部門所發表關於國家網路政策的重要文件，觀察者可從中察見川

14. U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2019* (Washington, D.C.: U.S. Department of Defense, 2019), pp. 9-10.
15. U.S. Government Accountability Office, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid* (Washington, D.C.: U.S. Government Accountability Office, 2019), pp. 5-53.
16. U.S. National Science and Technology Council, *2019 Federal Cybersecurity Research and Development Strategic Plan* (Washington, D.C.: U.S. National Science and Technology Council, 2019), pp. 6-23.

EH-01_張凱銘.tpf-9

普政府的網路戰略構想，不僅止於理念陳述，而是在來自層峰的宏觀指導之下，由各部門就業管範圍提出更為細膩的籌畫，漸進勾勒出一幅周密而可行的戰略藍圖，並體現三項重要特質：首先，川普政府雖與其前任在諸多事項上意見不一，但對網路治理的看法十分相近，同將網路科技定位於國家戰略層級，視之為保障國家安全和利益的關鍵，強調鞏固既有技術優勢的重要性。[17] 其次，川普政府的網路戰略論述雖亦有觸及民生經濟層面，但網路安全才是首要關切，相關文件之篇幅多數用於討論美國面臨的網路威脅及回應方式。[18] 最後，在《國家安全戰略》與《國家網路戰略》等高階政策文件外，聯邦政府各部門亦就所轄業務陸續發表施政計畫，顯示川普政府的網路戰略建構已跨越宏觀的原則性論述，進一步形成具體實踐方案。[19] 事實上，若回顧美國近期在網路領域的諸多作為如升格網路司令部、簽發資安行政指令和組建國際網路工作組等，皆顯示川普政府正在逐步落實其戰略構想。

17. The White House, *National Cyber Strategy*, p. 15.

18. U.S. National Science and Technology Council, *2019 Federal Cybersecurity Research and Development Strategic Plan*, pp. 6-10.

19. U.S. Department of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*, pp. 1-3; U.S. Department of State, *Recommendations to the President on Securing America's Cyber Interests and Deterring Cyber Threats through International Engagement*, pp. 1-4; U.S. Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, pp. 1-18; U.S. Department of Commerce & U.S. Department of Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, pp. 9-46; U.S. Department of Commerce & U.S. Department of Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce*, pp. 1-20.

EH-01_張凱銘.tpf-10

對於當前美國國家網路戰略的探討，將導引出兩個值得深入思考的問題：第一，國力雄厚且在網路領域掌握技術優勢的美國，為何如此擔憂自身的網路安全？第二，川普政府提出的戰略論述及實踐舉措中，是否存在可理解的一致性因果脈絡？為解釋這兩個問題，本文將援用國際關係現實主義學派的威脅平衡理論進行分析，檢視川普政府積極籌畫國家網路戰略的深層動因及其具體施政作為中蘊含的平衡意義。

表 1　川普政府之國家網路戰略相關政策文件一覽

發表單位	時間	文件名稱	內容概要
國防部國防科學委員會	2017 年 2 月	《網路嚇阻的工作組報告》	報告警示中國與俄羅斯的網路戰力建設使美國的安全壓力日趨沈重。伊朗與北韓透過對外採購技術設備，也已具備向美國關鍵基礎設施發動網路攻擊的能力。故報告呼籲新任政府盡速採取行動，對現行國家網路防務態勢進行完整評估，並建立強大且全面的網路嚇阻能力。
白宮	2017 年 12 月	《國家安全戰略》	報告闡述了現任政府的總體國安戰略架構，提出「保護美國民眾、國土與美國的生活方式、「促進美國的繁榮」、「以實力保障和平」及「強化美國的影響力」四項核心目標。文中賦予網路安全問題高度重視，指出來自網路空間的大量惡意活動已對國家安全構成危害，聯邦政府未來將強化網路攻防能力、提升資安防護標準，並擴大國際合作以維護國家網路系統安全並促進數位經濟增長。
國務院	2018 年 5 月	《有關嚇阻敵人與更好地保護美國人民免於網路威脅的建議》	報告指出美國既有的網路嚇阻能力仍然不足，尤其是未能有效因應未達動武門檻的各類惡意活動。報告建議聯邦政府建立多層次反制清單，並發展與民間機構及其他國家的資安協作機制，建構周密有效的網路嚇阻能力。
國務院	2018 年 5 月	《關於透過國際參與保護美國網路利益與嚇阻網路威脅的建議》	報告建議美國政府加強與其他國家的資安合作，在國際交流中探索構築網路信心建立措施，以及制訂網路空間國家行為準則等規範的可能性。
行政管理與預算局	2018 年 5 月	《聯邦網路安全評估報告暨行動計畫》	報告警示聯邦政府長期以來對網路威脅的重視不足，未建立可靠的資安防護與問責機制，亦無法即時掌握政府網路系統安全動態並反制惡意活動。報告提出多項具體改革建議，呼籲各部門盡速啟動內部資安整頓工作。

EH-01_張凱銘.tpf-11

商務部與國土安全部	2018 年 5 月	《有關強化網際網路與通訊生態系統韌性以應對殭屍網路與其他自動化分散性威脅的報告》	報告指出數量龐大且型態多元的網路惡意活動為資安防護帶來巨大挑戰。聯邦政府未來的網路施政除須設法嚇阻並抵禦外部威脅，也應強化國內網路系統的韌性，提升其承受損害並迅速回復正常運作的能力。
商務部與國土安全部	2018 年 5 月	《有關支持國家網路安全人力資源發展與維持的報告》	報告建議聯邦政府制訂相關教育政策，以擴大培養資訊科技領域的人力資源，同時設計更為開放的招聘制度，以延攬學術界與產業界的高階專業人才。
白宮	2018 年 9 月	《國家網路戰略》	報告說明現任政府的總體網路戰略藍圖，以《國家安全戰略》的四項核心目標為基礎，提出安全、經濟與外交層面的戰略規畫。在安全方面強調改善內部資安防護與提升網路戰力，和民間企業共同開發創新資安技術以反制外部威脅。在經濟方面著重查緝網路間諜活動以保障資訊產業競爭優勢，同時以政策手段推動人才培育及前瞻技術領域的投資與研發工作。在外交方面則將以雙邊及多邊形式持續拓展國際網路合作，與友邦共同維護網際網路空間的自由與秩序，並鞏固美國的領導地位。
國防部	2018 年 9 月	《2018 年國防部網路戰略摘要》	報告檢視了來自中國、俄羅斯、伊朗與北韓等國家的網路威脅，宣示美軍將與學研機構和民間企業合作，加速推動網路防務技術及數位軍備的開發更新工作。報告同時提出「防禦推進」(Defending Forward)概念，指出美軍未來將在外部網路威脅尚未成形前便主動出擊，藉以預先消弭隱患。
國防部	2018 年 12 月	《國防部雲端戰略》	報告指出雲端運算技術具有高度防務價值，美軍將積極投入相關技術的研發工作，並在日常防務中擴大運用，以期改善數據蒐集分析效能，為前線人員提供即時且精確的情報資訊。
情報總監辦公室	2019 年 1 月	《國家情報戰略》	報告指出網路威脅已嚴重危害美國國家安全與大眾對政府治理能力的信心，情報體系將擴大蒐集網路惡意活動情資，協助相關部門即時偵測並反制各種網路威脅。
國防部	2019 年 5 月	《關於中華人民共和國的軍事與安全力量發展報告》	報告指出中國利用大量網路間諜活動竊取他國科學知識與商業技術，其國安單位暗中支持駭客組織向多國發起網路攻擊以取得商業、科學與防務方面的機敏情資。
政府問責署	2019 年 8 月	《關鍵基礎設施保障：因應電網系統面臨重大網路安全風險的必要措施》	報告警示美國電網系統的網路安全防護不足，易遭遇外國勢力、駭客組織與犯罪份子發動的網路襲擊，進而導致工業控制系統、物聯網系統與全球定位系統陷入風險，並呼籲能源部與國土安全部等單位盡速採取應對措施。

EH-01_張凱銘.tpf-12

國家科學技術委員會	2019 年 12 月	《聯邦網路空間安全研究暨發展戰略計畫》	報告宣示聯邦政府將持續鎖定「防護」、「嚇阻」、「偵測」與「回應」等四個面向發展更成熟可靠的網路安全能力，並擴大投資人工智慧、量子計算與人力資源培育等領域，以保持美國的科技領導優勢。

資料來源：作者整理自 U.S. Defense Science Board, *Cyber Deterrence Task Force*, pp. 1-16；The White House, *National Security Strategy*, pp. 12-13；U.S. Department of State, *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*, pp. 1-3；U.S. Department of State, *Recommendations to the President on Securing America's Cyber Interests and Deterring Cyber Threats through International Engagement*, pp. 1-4；U.S. Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, pp. 1-18；U.S. Department of Commerce & U.S. Department of Homeland Security, *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, pp. 9-46；U.S. Department of Commerce & U.S. Department of Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce*, pp. 1-20；The White House, *National Cyber Strategy*, pp. 1-26；U.S. Department of Defense, *Summary of the 2018 Department of Defense Cyber Strategy*, pp. 1-7；U.S. Department of Defense, *DoD Cloud Strategy*, pp. 1-11；U.S. Office of the Director of National Intelligence, *National Intelligence Strategy 2019*, p. 11；U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2019*, pp. 9-10；U.S. Government Accountability Office, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, pp. 5-53；U.S. National Science and Technology Council, *2019 Federal Cybersecurity Research and Development Strategic Plan*, pp. 6-23。

參、威脅平衡視角下的美國國家網路戰略：威脅動因的評估

一、國際關係研究中的威脅平衡理論

當代國際關係學界的現實主義學派認為，由於長期處於無政府狀態(Anarchy)的國際社會不存在超越主權國家的更高權威可維護秩序與公義，作為理性行為體(Rational Actor)的國家將在其間奉行自助原則(Self-help)以確保安全與生存。現實主義學者們由此推導出平衡理論，

EH-01_張凱銘.tpf-13

指出理性自助的國家行為體對於生存環境的安全狀態將保持警惕，在情勢出現危險變化時設法平衡造成負面影響的他國。[20]

平衡理論的代表性論述當為華爾茲(Kenneth N. Waltz)提出的權力平衡理論(Balance of Power Theory)，其修正了傳統的人性歸因觀點，主張促使國家對他國採取平衡作為的關鍵動因是國際權力分配狀態(Distribution of Power)。華爾茲指出，當國際社會中的權力配置失衡時，國家將設法制約掌握過多權力的他國以免生存遭受危害，可能舉措則包含以提升本國實力為主的內部平衡和以締建國際同盟為主的外部平衡兩種主要類型。[21]此後部分學者在權力平衡的基礎上進行修正，導入其他平衡動因假設，如安全威脅與利益企求等，使平衡理論的內涵更趨豐富。[22]至若冷戰後期以降的國際政經變遷，雖使平衡理論的解釋力一度遭受質疑，但該理論在各方學者持續論辯交流之下，不僅未遭否定，反而在過程中逐漸衍發出多項新興分支，如柔性平衡(Soft Balancing)和制度平衡(Institutional Balancing)以適應全球化時代的國際情勢轉變，展現了理論研究的適應能力。[23]

在平衡理論的演化過程中，由哈佛大學教授華特(Stephen M. Walt)提出的威脅平衡理論具有突出的重要性。華特接受了平衡理論的立論基礎，即理性國家行為體在遭逢外部安全情勢變化時，會設法平衡他

---

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

21. Kenneth N. Waltz, *Theory of International Politics*, pp. 116-128.

22. 鄭端耀，〈搶救權力平衡理論〉，包宗和主編，《國際關係理論》（臺北：五南，2011 年），頁 69-83。

23. Robert A. Pape, "Soft Balancing Against the United States," *International Security*, Vol. 30, No. 1, Summer 2005, pp. 7-45; Stephen M. Walt, *Taming American Power: The Global Response to U.S. Primacy* (New York: Norton, 2005), p. 25; Kai He, *Institutional Balancing in the Asia Pacific, Economic Interdependence and China's Rise* (New York: Routledge, 2009), p. 10.

EH-01_張凱銘.tpf-14

國以圖自保，並透過外交案例分析論證在國際關係中，平衡確實是較扈從強者(Bandwagoning)更為常見且合理的政策反應。但他也注意到權力平衡理論的論述存在盲點，譬如後冷戰時期握有巨大權力的美國未曾引起國際社會聯手抵制，而二戰期間實際上並未掌握超強權力的德國，卻帶動了一個強大的對抗性同盟，凡此事例似乎都和權力平衡理論的主張有所矛盾。華特認為這些經驗說明了在國際政治中觸發國家平衡反應的關鍵動因並非權力分配狀態，而是安全威脅的形成。[24]

威脅平衡理論所稱的威脅係由四項要件共構而成的產物。首先是綜合國力(Aggregate Power)，即國家的總體物質資源如人口數量、產業發展、防務規模和科技水準等；其次是地緣鄰近性(Geographic Proximity)，由於地理距離遠近與國家投射軍事力量的能力密切相關，一般來說鄰近國家較相距遙遠的國家更可能構成威脅；再次是進攻實力(Offensive Power)，意指將綜合國力和地緣位置等要件綜合轉換為可用於攻擊他國的資源的能力；最後則為侵略意圖(Aggressive Intentions)，即運用物質實力對他國發動侵略的主觀意向。華特強調一國握有的物質實力本質上是客觀中性的存在，重點仍在於國家將如何加以運用，因此侵略意圖往往是威脅構成的關鍵。[25]

透過將平衡動因的思考由權力分配轉向安全威脅，並釐清威脅的基本構成要件，威脅平衡理論得以對過去被視為反常現象的外交案例提出合理解釋：由於物質性權力僅是威脅組成的部分要件，一個綜合國力強大的國家可能因未積極發展進攻實力或未曾表露侵略意圖而不致被他國視作威脅，成功避免遭受平衡的風險。相反的，一個權勢有限的國家也可能因對外展現強烈侵略意圖，而引起其他國家的強力抵制。由此，威脅平衡的觀點在平衡理論研究中發揮了承上啟下的關鍵

24. Stephen M. Walt, *The Origins of Alliances* (New York: Cornell University, 1987), pp. 263-266.

25. Stephen M. Walt, *The Origins of Alliances*, pp. 22-28.

EH-01_張凱銘.tpf-15

作用，既有效修正權力平衡論述的不足之處，也為後繼研究提供了可靠的知識基礎。

對於以美國國家網路戰略為研究主題的本文而言，威脅平衡當為值得借鑑的理論途徑。如上文所述，觀察川普政府自 2017 年以來提出的各項網路施政規畫，雖然在內容上涵蓋數位經濟、資訊基礎建設與技術創新等多元面向，但對於網路安全的高度關注顯然是前述各政策文件的共通特點。尤其是作為國家網路戰略總體藍圖的 2018 年版《國家網路戰略》，更是近乎於一份尖銳的網路威脅敘事。這份戰略報告中通篇有 26 處出現「惡意」(malicious)，37 處出現「威脅」(threat)等用語，反覆闡述源自中國、俄羅斯、伊朗與北韓等國家的網路惡意活動，已對美國的國家安全造成嚴峻威脅，從而提出各種加強資安防護與反制對手的構想。[26]在這一背景下，援引威脅平衡理論作為分析當前美國國家網路戰略規畫的研究途徑，一方面可與川普政府關切網路威脅與服膺現實主義理念的治理思路相互對應，[27]另一方面則可以更具系統性的角度審視川普政府近期推出的各項具體政策，揭示蘊含於龐雜政令背後的平衡意涵。

二、美國國家網路戰略的威脅動因探討

檢閱相關政策文件，相較於駭客與犯罪集團等非國家行為體，川普政府關切的網路威脅來源仍以中國、俄羅斯、伊朗與北韓等對立國家為主。[28]為了解相關國家如何對美國的網路安全構成挑戰，下文將按威脅平衡理論的威脅構成要件進行檢視。必須說明地是，在探討網路威脅構成問題時，鑑於網路空間不受地理局限的技術特徵，前述要件中的地緣鄰近性一項於此應可暫行忽略，而針對其他三項要件的評

26. The White House, *National Cyber Strategy*, pp. 1-2.
27. The White House, *National Security Strategy*, p. 1.
28. The White House, *National Cyber Strategy*, p. 2.

EH-01_張凱銘.tpf-16

估，亦須一併考慮網路環境與現實世界間的差異。

(一) 綜合國力

威脅平衡理論所稱的綜合國力係指對總體國家實力的概括式評估，亦即彙集經濟發展、人口數量、產業規模、社會建設等要素後得到的評估結果。綜合國力雖無法直接用以危害他國安全，卻是經營進攻實力與實踐侵略意圖的根基所在，是以在其他因素不變的前提下，一國的綜合國力越強大，對他國造成威脅的可能性就越高。由於此處的探討焦點是網路威脅，在衡量總體國力之外，亦有必要檢視相關國家的網路科技及資訊產業發展情形。

在總體國力部分，遭川普政府點名的四個國家中，伊朗與北韓顯然和美國之間存在巨大實力落差，即便是被外界普遍認知為強權國家的中國及俄羅斯，與美國間也仍有一定的實力差距。以澳洲智庫羅伊研究所(Lowy Institute)發表的《2018 年亞洲權力指數》(*Asia Power Index 2018*)來看，經過綜合計算亞太各國的經濟產業、防務建設、外交影響及文化吸引力等多重指標後，美國以 85 分列名首席強國，中國以 75.5 的得分居次，排名第 5 的俄羅斯得分則僅 33.3。[29] 若將含有更多非物質要素在內的軟實力(Soft Power)納入考量，美國的優勢將倍加明顯。美國南加州大學公眾外交中心(USC Center on Public Diplomacy)的研究報告《軟實力 30：2018 年全球軟實力統計》(*The Soft Power 30: A Global Ranking of Soft Power 2018*) 顯示，美國的軟實力排名高居全球第四，遠勝於排名第 27 位的中國與 28 位的俄羅斯。[30]

美國的優勢在網路領域同樣明顯：首先，由國內網路普及程度來看，美國的網路用戶數量超越俄羅斯、伊朗、北韓，但不及中國，惟

29. Lowy Institute, *Asia Power Index 2018* (Sydney: Lowy Institute, 2018), p. 8.
30. USC Center on Public Diplomacy, *The Soft Power 30: A Global Ranking of Soft Power 2018* (Los Angeles: USC Center on Public Diplomacy, 2018), pp. 42-43.

EH-01_張凱銘.tpf-17

若納入人均網路使用率(Individuals Using the Internet)和寬頻固網訂購量(Fixed Broadband Subscriptions)等更精確的指標綜合觀察，美國仍是全球網路民生應用水準最高的國家之一。[31] 其次，在產業發展部分，當前具全球影響力的軟硬體設備、網站服務及社群媒體等產品泰半源自美國企業。[32] 中國與俄羅斯的資訊產業近年雖有明顯成長，並開發多項頗受國內市場歡迎的網路產品如搜尋引擎百度、Yandex，或社群媒體如微博、VK等，但相關產品多具高度本土特質，在國際市場的影響力和商業版圖較為有限。[33] 最後，美國在網路領域最大亦是最根本的優勢在於完善的研發環境。自由開放的社會文化不僅有益於創意發想，專業人才資源也在產官學界間相互流通。[34] 而遭美國點名為網路威

31. 相關資訊可參考世界銀行(The World Bank)數據庫，北韓部分由於缺乏可靠的統計資訊而無法納入比對，但其民間的網路使用及產業營運迄今仍受到政府嚴格管制，請見 The World Bank, "Individuals using the Internet (% of population)," December 25, 2019(Accessed), *The World Bank*, <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=IR-US-CN-KP-RU>；The World Bank, "Fixed Broadband Subscriptions (per 100 people)," December 25, 2019(Accessed), *The World Bank*, <https://data.worldbank.org/indicator/IT.NET.BBND.P2?locations=KP-US-RU-CN-IR>；Freedom House, "Freedom in the World in 2019: North Korea," December 25, 2019 (Accessed), *Freedom House*, <https://freedomhouse.org/report/freedom-world/2019/north-korea>。

32. U.S. House of Representatives, "Maintaining U.S. Leadership in Science and Technology: Testimony before the Congress of the United States House of Representatives Committee on Science, Space and Technology," March 6, 2019, *U.S. House of Representatives*, <https://docs.house.gov/meetings/SY/SY00/20190306/109030/HHRG-116-SY00-Wstate-KhanM-20190306.pdf>.

33. Dal Yong Jin, "The Construction of Platform Imperialism in the Globalisation Era," in Christian Fuchs & Vincent Mosco, eds., *Marx in the Age of Digital Capitalism* (Leiden: Brill, 2016), pp. 334-335.

EH-01_張凱銘.tpf-18

脅的幾個國家，受到政治管制、網路隔離與高等教育水準等因素影響，迄未形成如美國一樣良好的網路科技生態系統。

(二) 進攻實力

自 1990 年代以來，許多國家皆體認到網路科技的軍事價值並積極推動相關防務建設。川普政府關注的幾個國家中，中國和俄羅斯已公開有關本國網路軍事部門的訊息。例如中國國防部早在 2011 年時便對外承認已建立正規網軍，[35] 部分資安企業調查亦顯示解放軍轄下設有多支活躍的網路間諜部隊。[36] 中國軍方在 2015 年後的國防組織改造中更進一步設立「戰略支援部隊」，以加強統合網軍及其他「新型作戰力量」的運作。[37] 俄羅斯國防部在 2017 年時宣示已設立網軍部隊，[38] 部分學者也注意到網路戰力在俄羅斯近年防務規畫中的比重正迅速上升。[39] 而北韓與伊朗政府雖對本國網軍發展現況諱莫如深，但來自資安

34. Frederic Martel 著，林幼嵐譯，《全球網路戰爭》(*Smart: Enquête sur les Internets*)（新北：稻田，2016 年），頁 18-29。

35.〈國防部證實建網上藍軍稱為提高部隊網絡防護〉，《人民網》，2011 年 5 月 26 日，<http://politics.people.com.cn/BIG5/1027/14740509.html>。

36. Mandiant Corporation, *APT1: Exposing One of China's Cyber Espionage Units* (Washington D.C.: Mandiant Corporation, 2013), pp. 2-4; Mark A. Stokes, *The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398* (Arlington: Project 2049 Institute, 2015), pp. 3-14; CrowdStrike, "Hat-tribution to PLA Unit 61486," June 9, 2014, *CrowdStrike*, <https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/>; Jonathan Racicot, "The Past, Present and Future of Chinese Cyber Operations," *Canadian Military Journal*, Vol. 14, No. 3, Summer 2014, p. 29.

37. John Costello, "The Strategic Support Force: China's Information Warfare Service," *China Brief*, Vol. 16, No. 3, February 2016, pp. 15-19.

38."Russian Military Admits Significant Cyber-War Effort," *BBC News*, February 23, 2017, <https://www.bbc.com/news/world-europe-39062663>.

EH-01_張凱銘.tpf-19

企業和學研機構的研究顯示兩國不僅建有一定規模的網路作戰部隊，更積極用於各類惡意活動之中。[40]

美國政府更注意到網路空間中的進攻實力構建較現實世界更為容易：如美中俄一般具有龐大內需市場和產業生態支撐的大國，固然有能力建立強盛的網軍戰力，但即便是北韓與伊朗這類因外部制裁或國內政治管制，而不具備蓬勃資訊產業的國家，透過對外採購技術設備等方式，仍可組建起規模較小的網路部隊。縱使未必能在正規網路戰爭中和強權國家直接對抗，但透過在平時開展各類隱蔽的惡意活動，仍能以不對稱的戰力條件為對手帶來嚴重資安危害。[41]

另一方面，網路的匿名特質促使國家可能更傾向以正規編制外的駭客團體從事惡意活動，以便在遭到外界指控時得以迴避責任。相關研究指出，近年涉入重大國際資安事件的部分駭客團體如「奇幻熊」(Fancy Bear)、「舒適熊」(Cozy Bear)、「拉薩路斯」(Lazarus)和「思想家」(Tarh　Andishan)等，背後都有某些國家暗中運作的痕跡（請見表 2）。[42] 換言之，對於特定國家網路進攻實力的評估往往不易得到精確結果。在這種情況下，國家勢將採取較現實世界中更為寬泛的料敵標準。

---

39. Keir Giles, *The Next Phase of Russian Information Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2015), pp. 2-3.
40. Cylance, *Operation Cleaver* (Irvine: Cylance, 2014), pp. 18-30; Emma Chanlett-Avery et al., *North Korean Cyber Capabilities: In Brief* (Washington, D.C.: Congressional Research Service, 2017), pp. 2-9.
41. U.S. Defense Science Board, *Cyber Deterrence Task Force*, p. 4.
42. Lilly Pijnenburg Muller, Lars Gjesvik, & Karsten Friis, *Cyber-weapons in International Politics* (Oslo: Norwegian Institute of International Affairs, 2018), pp. 11-19.

EH-01_張凱銘.tpf-20

表 2 主要駭客團體與疑似關連國家一覽

駭客團體名稱	疑似關連國家	主要針對國家
舒適熊(Cozy Bear)	俄羅斯	美國
惡毒熊(Venomous Bear)		歐美及中東國家
蜻蜓(Dragonfl)		美國、土耳其、瑞士
黑能源(BlackEnergy)		烏克蘭
奇幻熊(Fancy Bear)		美國、英國、德國
伏都熊(Voodoo Bear)		烏克蘭
野馬貓熊 (Mustang Panda)	中國	德國、蒙古、緬甸、巴基斯坦、越南
薊馬(Thrip)		美國
石貓熊(Stone Panda)		歐美國家
潑婦貓熊(Vixen Panda)		英國
代理犬(Deputy Dog)		美國
網路破解程式駭客組織(NCPH Group)		美國
臨時潛望鏡(TEMP.Periscope)		美國、加拿大、東南亞國家
滴答(Tick)		日本、南韓
武士貓熊(Samurai Panda)		美國
新聞播報員團隊(Newscaster Team)	伊朗	美國
迷人小貓(Charming Kitten)		美國
濁水(MuddyWater)		伊拉克、庫德族團體
金龜子(Chafer)		以色列、約旦、沙烏地阿拉伯
石油鑽探機(OilRig)		美國、沙烏地阿拉伯、土耳其
優雅小貓(Refined Kitten)		美國、沙烏地阿拉伯
螺旋小貓(Helix Kitten)		美國、英國
思想者(Tarh Andishan)		歐美及中東國家
拉薩路斯(Lazarus)	北韓	歐美及亞太各國
暗黑飯店(DarkHotel)		南韓、中國、俄羅斯、日本
安達利爾(Andariel)		南韓
收割者(Reaper)		南韓、日本、中東國家
金壽基(Kimsuky)		南韓、美國

資料來源：作者整理自 CrowdStrike, “Two Birds, One Stone Panda,” August 30, 2018, *CrowdStrike*, <https://www.crowdstrike.com/blog/two-birds-one-stone-panda/>；Global Cyber Security Company, “Hi-Tech Crime Trends 2018,” October 1, 2018, *Group-IB*, <https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf>；Adam Meyers, “Meet CrowdStrike’s Adversary of the Month for November: Helix Kitten,”

EH-01_張凱銘.tpf-21

November 27, 2018, *CrowdStrike*, <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/>；CrowdStrike, "Meet the Threat Actors-Who are your Cyber Adversaries?" February 24, 2019, *CrowdStrike*, <https://www.crowdstrike.com/blog/meet-the-adversaries/>；Pierluigi Paganini, "China-Linked APT15 Group is Using a Previously Undocumented Backdoor," July 24, 2019, *Security Affairs*, <https://securityaffairs.co/wordpress/88824/apt/apt15-okrum-backdoor.html#top>；CrowdStrike, "Who is Refined Kitten?" December 12, 2019, *CrowdStrike*, <https://www.crowdstrike.com/blog/who-is-refined-kitten/>；The MITRE Corporation, "JUST RELEASED: ATT&CK for Industrial Control Systems," January 9, 2020, *The MITRE Corporation*, <https://attack.mitre.org/groups/>。

(三) 侵略意圖

侵略意圖指國家運用物質資源打擊他國的主觀意向。華特認為在威脅的組成上，意圖因素比綜合國力和進攻實力等物質因素更為關鍵，當國家被外界認定具侵略意圖時，即使並未掌握客觀的實力優勢，仍可能遭他國判定為安全威脅並加以平衡。

一般來說，針對特定國家的侵略意圖分析，多來自對其政策文件、領導人發言、軍事部署態勢等外部資訊的綜合估算，這種由客觀事跡推論主觀思維的作法雖為不得不然，但在準確度上必然存在一定的模糊空間。[43]尤有甚者，在網路領域判斷他國的侵略意圖將比現實環境更加艱難，原因是網路的技術特性使得進攻方易於隱匿身分以致受害方無法準確歸責。在這種情況下，有意以網路手段打擊他國的國家將更有隱藏真實想法以迴避追究的動機。換言之，要從其他國家的官方發言或政策文件等資訊中推斷其網路侵略意圖並非易事。

不過網路空間的技術性質也意味著伴隨科技創新升級，深入分析資安事件中遺留的電子跡證以反溯行為者身分，並推論其有無惡意仍然可能。例如在 2014 年發生的索尼影視娛樂公司(SONY Pictures Entertainment, Inc., SPE)遭駭事件中，資安企業卡巴斯基實驗室(Kaspersky

43. Robert J. Art, "Striking the Balance," *International Security*, Vol. 30, No. 3, Winter 2005-2006, pp. 178-180.

EH-01_張凱銘.tpf-22

Lab)經由分析駭客活動時區與惡意程式編碼的韓語元素等細節，推導出發起該次攻擊的駭客團體「拉薩路斯」與北韓政府間存在聯繫。[44]另一資安企業賽門鐵克公司(Symantec Corporation)也曾利用解構電子跡證的方式，破解多起網路金融竊案的犯罪者身分。[45]此即美國政府在戰略規畫中強調提升網路溯源能力的重要性，並將其列入施政要項的原因：掌握先進的反向溯源能力，將使國家可精準辨識每次網路惡意活動的行為者身分，進而研判對方的侵略意圖並加以回應。[46]

透過情資與電子跡證分析，美國自歐巴馬政府第二任期起，對於中國、俄羅斯、伊朗與北韓的網路活動表現出高度關切。2016年2月，時任美國國家情報總監(Director of National Intelligence, DNI)克拉柏(James R. Clapper)在參議院情報特別委員會(Senate Select Committee on Intelligence)的發言中，公開點名上述四國不僅積極構建自身的網路戰力，亦向美國發動為數甚多且牽連廣泛的網路惡意活動，嚴重危害美國國家安全。[47]川普政府的看法與其前任相同，2018 年版的《國家

44. Kate Kochetkova, "What is Known about the Lazarus Group: Sony Hack, Military Espionage, Attacks on Korean Banks and other Crimes," February 24, 2016, *Kaspersky Lab*, <https://www.kaspersky.com/blog/operation-blockbuster/11407/>.

45. Lucian Constantin, "Recent Malware Attacks on Polish Banks Tied to Wider Hacking Campaign," *Network World*, February 13, 2017, <https://www.networkworld.com/article/3169409/security/recent-malware-attacks-on-polish-banks-tied-to-wider-hacking-campaign.html>; Symantec Corporation, *Internet Security Threat Report No. 22*, April 2017, p. 44, *Symantec Corporation*, <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>.

46. The White House, *National Security Strategy*, pp. 31-32.

47. U.S. Office of the Director of National Intelligence, "Remarks as Delivered by The Honorable James R. Clapper Director of National Intelligence, Senate Select Committee on Intelligence – IC's Worldwide Threat Assessment Opening Statement," February 9, 2016, *U.S. Office of the Director of*

EH-01_張凱銘.tpf-23

網路戰略》於開篇處便嚴厲指責俄羅斯、伊朗與北韓對美國發起許多魯莽的(Reckless)網路攻擊，源自中國的大量網路間諜活動則嚴重傷害了美國的數位經濟與智慧財產權利保障。[48]於此同時，來自資安企業的許多技術性分析結果，也顯示上述四國對美國及其友邦實施的網路惡意活動，在數量及頻率方面皆呈現增長態勢且攻擊手法不斷進化。[49]這些情形顯然足以支持美國政府做出侵略意圖的判斷，認定相關行為體確有利用網路科技危害美國國家安全的意向。

綜上所述，可發現美國雖在網路領域保有綜合國力方面的優勢，但出於以下兩項原因，使其仍對網路威脅深感憂慮：其一為網路進攻實力的建構與不對稱運用未必需要龐大國力支撐，且可透過編制外的駭客團體暗中運作，是以對其他國家的進攻實力評估須採取較寬鬆的認定標準；其二為電子跡證溯源分析顯示相關國家曾涉入大量網路惡意活動，反映出對美國的侵略意圖。換言之，進攻實力和侵略意圖兩項要件的交互作用，解釋了川普政府將中國、俄羅斯、伊朗與北韓等國家視作主要網路威脅的考量及其戰略規畫深層動因。

肆、威脅平衡視角下的美國國家網路戰略：平衡舉措的觀察

參與平衡理論研究的學者們將國家制約他國的具體舉措概要劃分

National Intelligence, <https://www.dni.gov/files/documents/2016-02-09SSCI_open_threat_hearing_transcript.pdf>.

48. The White House, *National Cyber Strategy*, pp. 1-3.

49. Charles Hymas, "China is ahead of Russia as 'biggest state sponsor of cyber-attacks on the West,'" October 9, 2018, *The Telegraph*, <https://www.telegraph.co.uk/technology/2018/10/09/china-ahead-russia-biggest-state-sponsor-cyber-attacks-west/>; Michael Busselen, "Key Trends from the CrowdStrike 2019 Global Threat Report," March 28, 2019, *CrowdStrike*, <https://www.crowdstrike.com/blog/2019-global-threat-report-key-trends/>.

EH-01_張凱銘.tpf-24

為內部平衡和外部平衡兩種主要類型。前者指國家透過強化綜合國力與國防建設等方式增加對手發動侵略的成本及難度，藉此產生平衡效果；後者則指國家經由外交途徑，在國際間籌建同盟體系或非正式安全合作陣線，以此嚇阻對手並削弱其相對優勢。高度關切網路威脅的川普政府，就任以來的種種施政作為，在相當程度上也反映出內外部平衡的戰略考量。

一、內部平衡

在內部平衡方面，川普政府的作為可大致劃分為兩項，第一是從根本上鞏固美國的網路科技實力與資安防護水準，第二是試圖發展強大攻防能力及採用更具攻勢(Offensive)意涵的防務思維。

(一)鞏固基礎實力

過往數十年間引領全球資訊革命浪潮的美國，憑藉著突出的技術優勢和產業格局，在國際網路政治及數位經濟中長期占據主導地位。面對部分強權國家近年急起直追的態勢，川普政府認為美國必須穩固自身的基礎實力，例如提升行政效率和研發創新能量，以及加速完善國內網路系統的硬體建置和資安防護等。

對此，川普政府首先著眼於聯邦政府部門間的職掌調整，透過縱向與橫向的事權統合改進治理效能。從近年發表的政策文件及〈2019財年預算案〉(Fiscal Year 2019 Budget Proposal)中涉及網路事務的資源配置來看，國土安全部及其下設的網路安全與基礎安全署(Cybersecurity and Infrastructure Security Agency，CISA)將在國內網路治理方面扮演重要角色，和國防部分別主導資安監管及戰力建設工作。[50]

50. Phil Goldstein, "Cybersecurity Funding Would Jump in Trump's 2019 Budget," February 15, 2018, *FedTech*, <https://fedtechmagazine.com/article/2018/02/cybersecurity-funding-would-jump-trumps-2019-budget>; U.S. Office of Management and Budget, "Budget of the United States, Fiscal

EH-01_張凱銘.tpf-25

由國土安全部負責的「持續診斷與緩和計畫」(Continuous Diagnostics and Mitigation, CDM)，更已成為改善政府網路系統防護能力的重點施政項目。[51] 而各部門設置的首席資訊官(Chief Informational Officer, CIO)將被賦予更多權責，在行政管理與預算局和聯邦首席資訊官辦公室(Office of Chief Information Officer, OCIO)協調下，制訂跨單位的資訊產品採購標準、危機應變流程及資安風險問責制度。[52]

為促進技術交流並提升創新能量，川普政府試圖擴大與民間部門合作，規畫以政策手段引導企業投入具戰略前瞻性的事業領域如資安技術、雲端運算、人工智慧(Artificial Intelligence, AI)及量子計算(Quantum Computation)等，利用專案採購及策略性投資等方式支持民間研發工作並優先收穫創新成果。[53] 聯邦政府也將自基礎教育階段起，配合「科學、科技、工程和數學教育計畫」(Science, Technology, Engineering, and Math, STEM)推展，逐步加強資訊教學以培育人力資源，並在產官學界間建立暢通的人事流動渠道，使高階人才的價值得到充分運用。[54]

Year 2019: Efficient, Effective, Accountable — An American Budget," February 1, 2018, *The White House*, <https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf>.

51. 有關該計畫的詳細內容，請見 Cybersecurity and Infrastructure Security Agency, "Continuous Diagnostics and Mitigation," December 25, 2019 (Accessed), *U.S. Department of Homeland Security*, <https://www.us-cert.gov/cdm/home>。

52. U.S. Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, pp. 6-18.

53. Executive Office of the President of the United States, *Science & Technology Highlights in the Second Year of the Trump Administration* (Washington, D.C.: Executive Office of the President of the United States, 2019), pp. 2-18.

54. The White House, "Presidential Memorandum for the Secretary of Education," September 25, 2017, *The White House*, <https://www.whitehouse.gov/presidential-

EH-01_張凱銘.tpf-26

在硬體建設部分，川普政府認為美國的資訊基礎設施布建受到地理位置和區域產業結構差異等因素影響而存在顯著落差，導致網路科技在國內社會的應用潛力未能充分發揮。為此，川普總統於 2018 年 1 月簽發的〈第 13821 號行政命令〉(Executive Order 13821)中要求有關部門簡化行政流程，全面加速農業地區寬頻網路鋪設，在國內建立綿密、穩定且價格合宜的網路服務環境，以支持經濟發展並滿足民生需求。[55]

另一方面，川普總統在〈第 13800 號行政命令〉(Executive Order 13800)中責成聯邦政府部門盡速汰換過時資訊產品，依據 2013 年公布的〈第 21 號總統政策指令〉(Presidential Policy Directive 21, PPD21)，逐一評估關鍵設施的資安風險並加以修補。[56]考量到政府機構與民間企業互動密切，相關政策文件同時指示各部門重新審視資訊供應鏈和承包商的資安水準，篩選出存在安全漏洞的企業及產品並排除在未來合作範圍之外。[57]各部門也應加強與資安企業合作，持續導入先進技術以

actions/presidential-memorandum-secretary-education/>; U.S. Department of Commerce & U.S. Department of Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce*, pp. 35-47.

55. The White House, "Presidential Executive Order on Streamlining and Expediting Requests to Locate Broadband Facilities in Rural America," January 8, 2018, *The White House*, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-streamlining-expediting-requests-locate-broadband-facilities-rural-america/>.

56. The White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, *The White House*, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.

57. U.S. Department of Commerce & U.S. Department of Homeland Security,

EH-01_張凱銘.tpf-27

確保網路系統的防護力，並運用黑客松(Hackathon)及漏洞回報獎勵機制(Bug Bounty)，藉助民間力量即時掌握並修復隱藏的系統缺陷。[58]

(二)發展安全能力

鑑於當前美國政經體系與社會大眾對網路科技的高度依賴，以及外部網路威脅持續增生等情勢，川普政府認為網路安全已不僅是資訊技術領域的專業課題，更是國家安全的核心組成部分，美國應全面強化網路防務體系，建構充足的安全能力並善加運用。

川普政府就任後將網路司令部(Cyber Command)升格為聯合作戰司令部(Unified Combatant Command, UCC)，輔以持續改良的戰力部署設計與動態任務編組精進網路部隊作戰技能。[59]美國國防部則規畫在開發網路武器的過程中擴大導入商用現貨軟體(Commercial Off-The-Shelf, COTS)以加速軍備更新速度。[60]而自 2006 年起每兩年舉行一次的「網路風暴」演習(Cyber Storm Exercise)規模亦有所擴增，2018 年 4 月啟動的第六屆演習邀請了關鍵基礎設施的生產營運廠商，以及參與投票系統監管作業的七個州加入，[61]與聯邦政府共同模擬網路系統遭受

A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, pp. 39-49.

58. Ben Haseltine, "Pentagon's Bug Bounty Program Identifies Defense Travel System Vulnerabilities," June 5, 2018, *GovernmentCIO Media & Research*, <https://www.governmentciomedia.com/pentagons-bug-bounty-program-identifies-defense-travel-system-vulnerabilities-0>.

59. U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority* (Fort Meade: U.S. Cyber Command, 2018), pp. 6-10; Katie Lange, "Cybercom Becomes DoD's 10th Unified Combatant Command," May 3, 2018, *DoD Live*, <http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/>.

60. U.S. Department of Defense, *Summary of the 2018 Department of Defense Cyber Strategy*, p. 4.

EH-01_張凱銘.tpf-28

攻擊時的跨單位應變流程，以加強關鍵基礎設施和國內選務工作的資安防護。[62]

在防務建設工作外，川普政府的高階官員如時任國家安全顧問波頓(John R. Bolton)、國家安全局長兼網路司令部司令官中曾根(Paul M. Nakasone)等人，皆批評美國過去的網路防務思維過於保守，導致競爭對手認為對美國發起網路攻擊不會招致嚴重後果。[63]為改變這一情形，川普總統於 2018 年 8 月時簽署命令，正式推翻歐巴馬政府頒布的〈第 20 號總統政策指令〉(Presidential Policy Directive 20, PPD20)。該指令對網路戰力的使用施以嚴格限制，要求防務部門發起網路軍事行動前，須通過跨部門審核並獲總統批准。[64]川普政府認為其對網路防務構成不必要的束縛，故以〈第 13 號國家安全總統備忘錄〉(National Security Presidential Memorandum 13, NSPM 13)替代，大幅簡化採

61. 分別為：德州、科羅拉多州、德拉瓦州、愛荷華州、維吉尼亞州、華盛頓州及蒙大拿州，請見 Sean Lyngaas, "DHS 'Cyber Storm' Exercise Tests Manufacturing and Transportation Sectors," *Cyberscoop*, April 10, 2018, <https://www.cyberscoop.com/dhs-cyber-storm-jeanette-manfra-critical-infrastructure/>.

62. 關於演習活動詳細資訊，請見U.S. Department of Homeland Security, "Cyber Storm VI: National Cyber Exercise," December 25, 2019(Accessed), *U.S. Department of Homeland Security*, <https://www.dhs.gov/cisa/cyber-storm-vi>.

63. U.S. Senate Committee on Armed Services, "Nominations – Nakasone-Park-White," *U.S. Senate Committee on Armed Services*, March 1, 2018, <https://www.armed-services.senate.gov/hearings/18-03-01-nominations_--nakasone---park---white>; Jeff Seldin, "US Prepared to Strike in Cyberspace," *Voice of America*, September 20, 2018, <https://www.voanews.com/usa/us-politics/us-prepared-strike-cyberspace>.

64. Sean Lyngaas, "PPD-20 Elimination Opens Arguments over How U.S. Should Conduct Offensive Hacking Operations," August 16, 2018, *Cyberscoop*, <https://www.cyberscoop.com/ppd-20-eliminated-cyber-war-donald-trump-mike-rounds/>.

EH-01_張凱銘.tpf-29

取網路行動的行政程序，賦予國防部更多自主空間。[65]美國新任國防部長艾思博(Mark T. Esper)論及此事時指出，授權流程的精簡將使美國的網路戰力得以充分發揮，有效嚇阻並反制外部威脅。[66]

伴隨行政管制放寬，美國國防部在 2011 年版網路戰略報告中提出的「積極性網路防禦」(Active Cyber Defense)概念似乎也被 2018 年版報告中的「防禦推進」概念取代。[67]和著重察覺並消除威脅的前者相比，「防禦推進」更強調在危害成形前主動出擊以預先解除風險。[68]由近期時事動向來看，這一概念可能已得到具體落實。例如在 2019 年 6 月時，美國媒體《紐約時報》(*The New York Times*)報導美國已在俄羅斯的電力網路系統中植入惡意程式，作為必要時進行網路攻防的籌碼。[69]同月下旬，多家美國媒體引述政府消息來源，指出川普總統已批准對多次向美國發起網路惡意活動並擊落美軍無人機的伊朗採取網路攻擊，並一度癱瘓該國計畫用於油輪攻擊行動的電腦系統。[70]

---

65. Sydney J. Freedberg Jr., "Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff," *Breaking Defense*, September 17, 2018, <https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/>.
66. Mark Pomerleau, "What Good are 'Exceptional' Cyber Capabilities without Authority?" *Fifth Domain*, July 16, 2019, <https://www.fifthdomain.com/dod/2019/07/16/what-good-are-exceptional-cyber-capabilities-without-authority/>.
67. U.S. Department of Defense, *Department of Defense Cyberspace Policy Report* (Washington, D.C.: U.S. Department of Defense, 2011), p. 1.
68. U.S. Department of Defense, *Summary of the 2018 Department of Defense Cyber Strategy*, p. 4.
69. David E. Sanger & Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019, <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.
70. Ellen Nakashima, "Trump Approved Cyber-Strikes Against Iranian Computer Database Used to Plan Attacks on Oil Tankers," *The Washington Post*, June 23, 2019, <https://www.washingtonpost.com/world/national-security/with-

EH-01_張凱銘.tpf-30

另一方面，川普政府認為有必要在網路防務體系外進一步運用其他政策領域資源，發展更廣泛的嚇阻戰略(Broader Deterrence Strategy)，諸如經濟制裁、行政管制或司法控訴等手段都可應用，藉以形塑周延的嚇阻效力。[71] 循此，川普政府近年在完善國家網路戰略，強化網路防務建設之外，針對網路犯罪案件的司法偵辦步調亦越趨積極：第一，美國司法部在 2017 年後，陸續偵辦並起訴多起涉及網路間諜及非法數位入侵的案件，其中部分案件起訴人數甚眾且對象包含了中國與俄羅斯等國家的現任情報官員；第二，美國國務卿蓬佩奧(Michael R. Pompeo)與聯邦調查局局長瑞伊(Christopher A. Wray)等高階首長，在部分司法案件中親自站上第一線，發表聲明譴責外國勢力對美國網路安全造成的嚴重危害；第三，縱使將對美中關係造成衝擊，川普政府仍透過司法途徑查辦起訴了華為公司這一頗具代表性的中國資訊企業。相關跡象顯示，司法部門在美國目前的國家網路戰略架構中，扮演著頗具重要性的角色，兼有嚇阻與反制網路威脅的功能（相關事例請見表 3）。

trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html>.

71. The White House, *National Cyber Strategy*, pp. 8-11.

EH-01_張凱銘.tpf-31

表 3　美國近期起訴網路犯罪活動事例一覽

時　間	說　明
2017 年 3 月	美國司法部以涉嫌非法入侵雅虎公司(Yahoo!　Inc.)網路系統為由，起訴四名俄羅斯籍人士，其中包含兩名隸屬俄羅斯聯邦安全局(Russian Federal Security Service, FSB)的情報官員。
2017 年 8 月	美國司法部以涉嫌開發惡意程式、串連駭客入侵聯邦人事管理局(The Office of Personnel Management, OPM)網站竊取資料的理由，逮捕一名中國籍人士。
2017 年 11 月	美國司法部以涉嫌非法入侵西門子(Siemens Inc.)和穆迪分析公司(Moodys Analytics)等企業網路系統的理由起訴三名中國籍人士。
2017 年 11 月	美國司法部以涉嫌非法入侵家庭票房公司(Home Box Office, HBO)網路系統的理由起訴一名伊朗籍人士。
2018 年 7 月	美國司法部大規模起訴 12 名俄羅斯軍事情報局(Main Directorate of the General Staff of the Armed Forces of the Russian Federation, GRU)人員，指控其涉嫌於 2016 年美國總統大選期間入侵民主黨全國委員會(Democratic National Committee, DNC)的網路系統。
2018 年 9 月	美國司法部以涉及非法入侵索尼影視娛樂公司網路系統、孟加拉央行數位金融竊案與散播 WannaCry 病毒等事件的理由起訴一名北韓籍人士。
2018 年 10 月	美國司法部以涉嫌入侵多間歐美航空企業網路系統的理由起訴 10 名中國籍人士，其中包含兩名隸屬江蘇省國家安全廳的情報官員。
2018 年 12 月	美國司法部以涉嫌參與駭客團體，入侵多國政府與企業網路系統的理由起訴兩名中國籍人士。美國國務卿蓬佩奧、聯邦調查局局長瑞伊與時任國土安全部長尼爾森(Kirstjen M. Nielsen)對此發表公開聲明，指責中國政府贊助的網路間諜活動嚴重危害國際經濟秩序與美國的國家利益。
2019 年 1 月	美國司法部以涉嫌非法入侵美國證券交易委員會(U.S. Securities and Exchange Commission, SEC)網站竊取資訊並進行內線交易的理由，起訴了來自烏克蘭、俄羅斯及美國國內等地的 10 名人士。
2019 年 1 月	美國司法部以涉嫌竊取商業機密、電信詐欺與妨礙司法等理由，起訴中國企業華為公司與其首席財務官孟晚舟。
2019 年 5 月	美國司法部以涉嫌入侵安森公司(Anthem Inc.)網路系統竊取商業機密與個人資訊的理由起訴兩名中國籍人士。
2019 年 7 月	美國司法部以涉嫌透過企業網路系統為中國竊取美國列車工程商業機密的理由起訴一名美籍華裔人士。

資料來源：作者自行整理自 U.S. Department of Justice, “U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts,” March 15, 2017, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions>；Joseph Menn, “Chinese National Arrested in Los Angeles on U.S. Hacking Charge,” *Reuters*, August 25, 2017, <https://www.reuters.com/article/us-usa-cyber-opm/chinese-national-arrested-in-los-angeles-on-u-s-hacking-charge-idUSKCN1B42RM>；U.S. De-

EH-01_張凱銘.tpf-32

partment of Justice, "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," November 27, 2017, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations>；U.S. Department of Justice, "Acting Manhattan U.S. Attorney Announces Charges against Iranian National for Conducting Cyber Attack And $6 Million Extortion Scheme against HBO," November 21, 2017, *U.S. Department of Justice*, <https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting>；U.S. Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," July 13, 2018, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>；U.S. Department of Justice, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," September 6, 2018, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>；U.S. Department of Justice, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," October 30, 2018, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal>；U.S. Department of Justice, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," December 20, 2018, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion>；U.S. Federal Bureau of Investigation, "FBI Director Christopher Wray's Remarks Regarding Indictment of Chinese Hackers," December 20, 2018, *U.S. Federal Bureau of Investigation*, <https://www.fbi.gov/news/pressrel/press-releases/fbi-director-christopher-wrays-remarks-regarding-indictment-of-chinese-hackers>；U.S. Department of State, "Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers," December 20, 2018, *U.S. Department of State*, <https://www.ait.org.tw/joint-statement-by-dos-sec-pompeo-and-dhs-sec-nielsen/>；U.S. Securities and Exchange Commission, "SEC Brings Charges in Edgar Hacking Case, Litigation Release No. 24381," January 17, 2019, *U.S. Securities and Exchange Commission*, <https://www.sec.gov/litigation/litreleases/2019/lr24381.htm>；U.S. Department of Justice, "Two Ukrainian Nationals Indicted in Computer Hacking and Securities Fraud Scheme Targeting U.S. Securities and Exchange Commission," January 15, 2019, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/two-ukrainian-nationals-indicted-computer-hacking-and-securities-fraud-scheme-targeting-

EH-01_張凱銘.tpf-33

us>；U.S. Department of Justice, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," January 28, 2019, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial>；U.S. Department of Justice, "Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People," May 9, 2019, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including>；U.S. Department of Justice, "Newly Unsealed Federal Indictment Charges Software Engineer with Taking Stolen Trade Secrets to China," July 11, 2019, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china>。

二、外部平衡

傳統平衡理論研究對於外部平衡的界定多聚焦於國家透過組建同盟應對安全威脅與權力失衡狀態的作法，晚近的研究則更具彈性，認為在正式締結盟約之外，國家間的防務交流、安全合作及非正式外交協調，都可被視作外部平衡的表現型態。[72]為因應日益惡化的網路安全情勢，川普政府不僅提出各種強化網路防務實力的構想，也主張美國應透過外交合作鞏固自身在國際網路政治中的領導地位，並和友邦攜手應對網路惡意活動等挑戰。過去數年間，美國積極推動跨國網路交流，展現以外部平衡手段消弭威脅的意向，對此可由以下兩個層面觀察：

(一) 多邊層面的規範建構努力

2009 年以前，小布希(George W. Bush)時期的美國對於透過聯合國等多邊機制制訂網路空間國家行為準則一事存有疑慮。由於受到單

72. Robert A. Pape, "Soft Balancing Against the United States," pp. 36-37; Stephen M. Walt, *Taming American Power: The Global Response to U.S. Primacy*, pp. 126-132.

EH-01_張凱銘.tpf-34

邊主義(Unilateralism)思維影響，以及懷疑中國與俄羅斯等競爭對手意圖利用國際法規束縛美國的行動自由，當時的美國不僅未在國際磋商中發揮積極作用，甚至試圖抵制相關決議。[73] 歐巴馬政府執政後著手重置(Reset)美國外交政策，對於建設國際網路規範的態度轉趨開放，在「聯合國政府專家工作組」(United Nations Governmental Group of Expert, UNGGE)等平臺內與其他國家開啟協商。[74] 而川普政府的外交風格雖不時表露對於多邊機制效用的質疑，但在制訂網路規範一事上卻大抵沿襲前任方針，繼續推進多邊協商工作。2018 年版的《國家網路戰略》明確指出美國將持續參與多邊論壇，「尋求建立以國際法為基礎的網路空間國家行為責任規範，……提升網際網路環境的可預測性和穩定度。」[75]

在內容上，川普政府仍秉承美國長期的政策主張，要求將現行國際法規直接適用於網路空間，以之約束國家行為並確保網際網路的秩序穩定。此間重點在於將《武裝衝突法》(*Law of Armed Conflict, LOAC*)和《聯合國憲章》(*Charter of the United Nations*)第 51 條導入網路空間的爭議。川普政府認為在特定情況下，網路攻擊應被視同於現實世界中的武裝衝突，遭受攻擊的國家不僅有權採取自衛措施，更可使用傳統軍事力量加以回應。[76] 這一看法在 2017 年 4 月的七大工業國集團峰會(G7 Summit)中獲得肯定，各國領導人在會後發表的〈七大

73. Tim Maurer, *Cyber Norm Emergence at the United Nations* (Cambridge: Harvard Kennedy School, 2011), pp. 19-21.

74. 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.

75. The White House, *National Cyber Strategy*, p. 20.

76. Arun M. Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" July 4, 2017, *The Lawfare Institute*, <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.

EH-01_張凱銘.tpf-35

工業國集團關於網路空間國家行為規範的宣言〉(G7 Declaration on Responsible States Behavior in Cyberspace)中申明支持將特定網路攻擊視作武裝攻擊，並依據現行國際法規進行反制的作法。[77]

同年六至七月間舉行的第五屆「聯合國政府專家工作組」會議中，川普政府將上述論點列入決議草案，卻因遭到部分國家強力反對，最終致使工作組會議未能達成結論。反對國家認為《聯合國憲章》第 51 條的本意係指國家在遭受傳統武裝攻擊時方能以軍事手段自衛，由於網路攻擊並不在此處規範範圍內，國家不應以傳統武力反擊網路惡意活動，以免導致網路空間的軍事化。[78]

事實上，川普政府在聯合國等多邊機制內推動網路空間國家行為準則規範建設的努力，不僅是為了保障網路空間的安全與秩序，更蘊有為本國網路戰略爭取國際支持和合法性等考量。川普政府認為將網路攻擊與現實武裝攻擊掛鉤的作法能更有效地嚇阻網路威脅，使美國在網路安全事務中掌握更多元的行動選項。因此，該提案雖在多邊協調框架內受挫，但美國仍固守立場，轉而利用國內政策規畫與雙邊外交途徑繼續推動其理念。[79]

---

77. G7 Summit, "G7 Declaration on Responsible States Behavior in Cyberspace," April 11, 2017, *Ministry of Foreign Affairs of Japan*, <https://www.mofa.go.jp/files/000246367.pdf>.

78. Owen Bowcott, "Dispute along Cold War Lines Led to Collapse of UN Cyberwarfare Talks," *The Guardian*, August 23, 2017, <https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges>.

79. David E. Sanger & William J. Broad, "Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms," *The New York Times*, January 16, 2018, <https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html?_ga=2.182743974.1450541312.1564318121-1345450338.1537238599>; U.S. Department of State, "Joint Statement of

EH-01_張凱銘.tpf-36

(二) 雙邊與有限多邊層面的網路安全合作

相較於多邊磋商，川普政府的網路外交更偏好簡捷明快且能讓美國掌握主導優勢的雙邊與有限多邊合作。譬如在 2017 年 5 月時，川普政府表示鑑於先前進駐南韓的「戰區高空防衛系統」(Terminal High Altitude Area Defense, THAAD)高度仰賴網路傳輸技術，而周邊國家如中國、俄羅斯及北韓等不僅反對該系統設置，且皆具備相當的網路攻擊能力，因此美國已派遣網路安全團隊進駐南韓，以強化美軍在朝鮮半島的戰力部署。[80]同年六月，川普政府宣布與以色列共建雙邊網路工作組，邀集兩國資訊專家及軍方、司法和外交官員共同參與，以深化網路安全合作並反制各類惡意活動的危害。[81]美國國會近期更通過了《增進美國—以色列合作與區域安全法案》(*United States-Israel Co-operation Enhancement and Regional Security Act, H.R.1837*)，授權行政部門進一步擴大美以網路合作範疇。[82]

2018 年 7 月，美國國務卿蓬佩奧在華府舉行的「印太商業論壇」(Indo-Pacific Business Forum)中發表了「數位連結與網路安全夥伴關

---

the Security Consultative Committee," April 19, 2019, *U.S. Department of State*, <https://www.state.gov/u-s-japan-joint-press-statement/>.

80. 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/>; Peter Pella, *The Continuing Quest for Missile Defense: When Lofty Goals Confront Reality* (San Rafael: Morgan & Claypool Publishers, 2018), p. 5/3.

81. 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>.

82. U.S. 116th Congress, "H.R.1837 - United States-Israel Cooperation Enhancement and Regional Security Act," July 24, 2019, *U.S. Library of Congress*, <https://www.congress.gov/bill/116th-congress/house-bill/1837>.

EH-01_張凱銘.tpf-37

係計畫」(Digital Connectivity and Cybersecurity Partnership)，宣布美國將投入資金協助友好國家完善資訊基礎建設、提升網路安全能力，並廣泛發展官方與民間的網路事務合作。[83]同年九月，美國與印度在外交及國防部長 2+2 對話(U.S.-India 2+2 Ministerial Dialogue)中簽訂《通訊相容與安全協議》(*Communications Compatibility and Security Agreement*, COMCASA)，授權美印軍方共用機密通訊協定，加強兩軍在軍事通訊和關鍵防務系統方面的操作互通性，並允許印度軍方登入美軍關鍵通訊網路取用機敏數據。[84]

美國副總統彭斯(Michael R. Pence)於 2018 年 11 月出席第六屆「美國—東協高峰會」(U.S.-ASEAN Summit)時，與東協國家共同發表〈東協—美國領袖關於網路安全合作的宣言〉(ASEAN-United States Leaders' Statement on Cybersecurity Cooperation)，宣示美國將與東南亞各國進一步加強網路合作並共同應對各類安全挑戰。[85]美國與新加坡同時簽署了網路安全合作意向書，使星國網路安全局(Cyber Security Agency of Singapore, CSA)的「東協網路能力計畫」(ASEAN Cyber Capacity Programme, ACCP)與美國的「數位連結與網路安全夥伴關係計畫」相互銜接，共同改善東協國家的資訊建設與網路安全能力。[86]

---

83. U.S. Department of State, "Remarks on America's Indo-Pacific Economic Vision," July 30, 2018, *U.S. Department of State*, <https://www.state.gov/remarks-on-americas-indo-pacific-economic-vision/>.

84. Ankit Panda, "What the Recently Concluded US-India COMCASA Means," *The Diplomat*, September 9, 2018, <https://thediplomat.com/2018/09/what-the-recently-concluded-us-india-comcasa-means/>.

85. ASEAN, "ASEAN-United States Leaders' Statement on Cybersecurity Cooperation," November 15, 2018, *Association of South East Asia Nations*, <https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf>.

86. Cyber Security Agency of Singapore, "Singapore and the United States

EH-01_張凱銘.tpf-38

2019 年 3 月，與美國在網路及 5G 通訊系統安全議題上存有分歧的歐洲聯盟(European Union, EU)調整了政策立場，在歐洲聯盟執行委員會(European Commission)發表的報告《歐洲聯盟與中國：一個戰略展望》(*EU-China – A Strategic Outlook*)中採取了與川普政府相近的態度，將中國定位為「戰略競爭者」(Strategic Competitor)，同時要求歐盟成員國未來在管理關鍵資訊基礎設施與布建 5G 通訊系統時須將資安風險列為優先考量。[87] 同年四月，美國與日本在外交及國防部長共同參與的「安全磋商會議」(Security Consultative Committee)中達成共識，確認將持續加強雙邊網路安全合作，除提升協作水準與嚇阻能力外，更宣布把特定情況下的網路攻擊納入《美日安保條約》(*Treaty of Mutual Cooperation and Security between the United States and Japan*)第五條範疇之中，[88] 並共同推動國際法規在網路空間中的適用。[89]

Sign Declaration of Intent on Cybersecurity Technical Assistance Programme," November 16, 2018, *Cyber Security Agency of Singapore*, <https://www.csa.gov.sg/news/press-releases/singapore-and-the-us-sign-doi-on-cybersecurity-technical-assistance-programme>；關於新加坡「東協網路能力計畫」的內容請見 Cyber Security Agency of Singapore, "Factsheet on ASEAN Cyber Capacity Programme," April 2017, *Cyber Security Agency of Singapore*, <https://www.csa.gov.sg/news/speeches/media/3bfa3b0aaf264a41b8f7a31551baf2b4.ashx>。

87. European Commission, *EU-China – A Strategic Outlook* (Brussels: European Commission, 2019), pp. 5-11.

88. 該條文的主旨係授權美日兩國採取行動應對在日本治理領土上發生的武裝攻擊與共同危險，美日兩國並未詳細解釋何種網路攻擊將被納入此條文範疇，亦未說明雙方將以何種形式回應。條文內容請見 Headquarters U.S. Forces, Japan, "Treaty of Mutual Cooperation and Security between the United States and Japan," January 19, 1960, *U.S. Central Intelligence Agency*, <https://www.cia.gov/library/readingroom/docs/CIA-RDP07-00469R000100950001-2.pdf>。

89. Ministry of Foreign Affairs of Japan, "Joint Statement of the Security

EH-01_張凱銘.tpf-39

2019年5月，美國與我國及日本在「全球合作暨訓練架構」(Global Cooperation and Training Framework, GCTF)下合作籌辦「網路安全與新興科技國際研習營」(The Workshop on Network Security and Emerging Technologies)，並邀集印太地區多國官員共同參與「印太資安聯盟成立暨戰略對話」(Indo-Pacific Cyber Security Dialogue & Inauguration of the Indo-Pacific Cyber Security Alliance)，向與會國家分享美國的網路自由理念，並呼籲各國從行政與立法層面加強跨國資安合作。[90]

由上述事例來看，川普政府的網路外交大抵仍以傳統同盟體系和安全合作夥伴等既有網絡為基礎，除透過推廣網路自由等價值觀爭取相關國家支持，「安全」與「發展」兩者更是川普政府的主要著力點，既透過突出網路威脅帶來的種種風險，向各國強調加強對美合作的必要性；復針對經濟發展程度較低、網路建設短缺的國家提出資訊援助計畫，藉以尋求其在國際網路政治中的支持。

伍、對於美國國家網路戰略現況及前景的思考

上述事例顯示川普政府自就任以來迄今，已對網路科技領域展露積極治理意向，在回應威脅的思路指導下漸進形塑總體戰略架構，並採取諸多具有平衡意涵的政策舉措。在內部平衡層面，川普政府的施

Consultative Committee," April 19, 2019, *Ministry of Foreign Affairs of Japan*, <https://www.mofa.go.jp/files/000470738.pdf>.

90. American Institute in Taiwan, "Remarks by AIT Deputy Director Raymond Greene at Opening Ceremony of GCTF on Network Security and Emerging Technologies," May 28, 2019, *American Institute in Taiwan*, <https://www.ait.org.tw/remarks-by-ait-deputy-director-greene-at-opening-ceremony-of-gctf-on-network-security-and-emerging-technologies/>；〈印太資安聯盟成立 AIT：資安不只是政治議題〉，《中央廣播電臺》，2019年5月30日，<https://www.rti.org.tw/news/view/id/2022452>。

EH-01_張凱銘.tpf-40

政重點包含「鞏固基礎實力」與「發展安全能力」，強化內部資安防護水準與推進前瞻技術研發等工作之餘，更致力提升網路攻防戰力，並推出放寬採取網路軍事行動的行政管制，以及以「防禦推進」方式消弭潛在威脅等作法。在外部平衡層面，川普政府一方面推動多邊層面的廣泛交流，探尋將國際法中的自衛權規範導入網路空間，以及制訂網路空間國家行為準則的可能，另一方面則與友好國家加強資安合作，協調彼此在網際網路治理事務上的政策立場，並建立緊密的網路安全及防務合作機制（請見圖 1）。

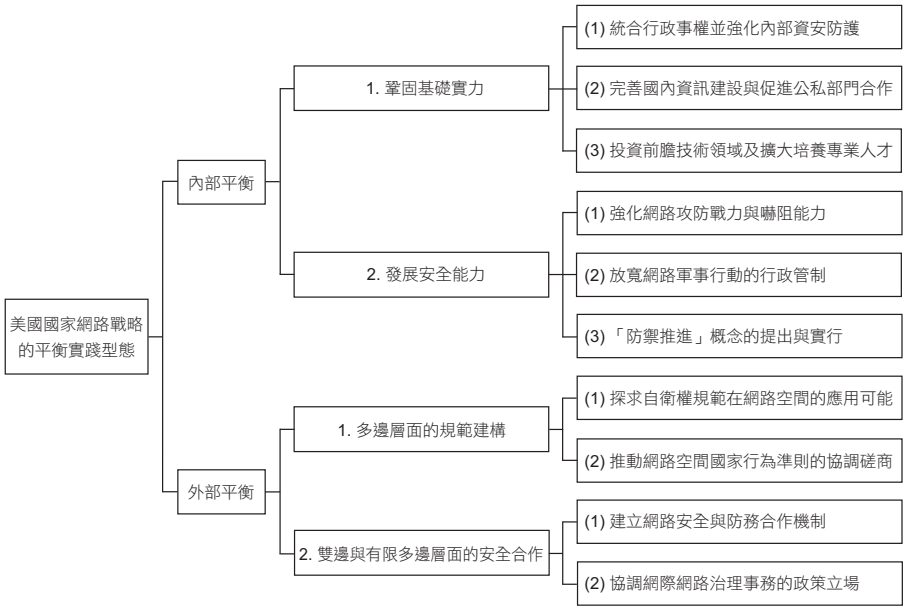

圖 1　美國國家網路戰略的平衡實踐型態

資料來源：作者自製。

在前文討論的基礎上，可進一步對美國國家網路戰略的現況與前景提出以下幾點更為深入的思考：

EH-01_張凱銘.tpf-41

一、國內政策與行政監管方面的檢討必要

川普政府對於國家網路戰略的積極籌畫，反映出美國當前對於網路安全情勢的高度焦慮。然若推原論始，美國目前面臨的網路威脅與相關挑戰，相當程度上與自身施政與行政監管方面的漏失有關。

首先，作為網路科技發源地，美國自 1990 年代後期起便較他國更早也更為充分地經歷了相關技術創新帶來的諸多便利，以及數位經濟推動的繁榮景氣。然而在享受各種紅利的同時，美國卻未同步建立起足夠完善的網路治理體系與資安防護機制，對於網路科技在應用過程中可能衍生的負面影響亦未備妥應對之策。[91] 前文提及川普政府近年的網路施政涵蓋了一系列行政體系內部改革，以及對於資訊基礎設施防護能力的修補，在在顯示美國過去在網路監管方面的不足。

其次，部分遭美國指名為主要網路威脅來源的國家，其網路科技與攻防能力的發展，實際上與美國自身的出口管制不周有關。例如美國在全球反恐戰爭(Global War on Terror)期間，由於視中國為重要戰略夥伴，並覬覦其充滿潛力的國內市場，因而大幅放寬對中國的出口管制，許多高階科技與電子產品隨之流出，為中國後續的資訊技術進步提供了巨大助力。[92] 資安企業「記錄未來」公司(Recorded Future)的調查亦顯示北韓網軍部隊使用的電腦及相關資訊設備，多為美國科技企業製造的產品。[93] 換言之，出口管制周密度的不足，已抵銷部分美國在維護國家網路安全方面的努力。

---

91. Johnny Ryan, *A History of the Internet and the Digital Future*, pp. 178-195.
92. Glenn J. McLoughlin & Ian F. Fergusson, *High Performance Computers and Export Control Policy: Issues for Congress* (Washington, D.C.: Congressional Research Service, 2003), pp. 10-20.
93. Kim Youngnam, "North Korea Uses US Tech for 'Destructive Cyber Operations,'" *Voice of America*, June 8, 2018, <https://www.voanews.com/a/north-korea-us-tech-destructive-cyber-operations/4429922.html>.

EH-01_張凱銘.tpf-42

最後，雖然川普政府積極強化美國的內部資安防護與網路攻防戰力，惟由近年環繞著網路武器「永恆之藍」(EternalBlue)的一系列事件來看，美國在這方面的施政仍有許多改善空間。這項以入侵並利用網路系統漏洞見長的網路武器係由美國國家安全局(National Security Agency, NSA)開發而成，在 2017 年後遭駭客團體「陰影掮客」(The Shadow Brokers)竊取外流，為各方用於新型惡意軟體製作，並開發出Petya和WannaCry等著名網路病毒，[94] 不僅在全球造成大規模資安危機，美國國內多處城市也先後遭逢與「永恆之藍」相關的網路攻擊。[95] 此一事例說明美國的網路安全體系仍存在許多漏洞，在這一情況下研發的網路戰力縱使威力強大，也可能因監管不力而遭對手竊取並反噬自身。

二、外部安全環境進一步惡化的潛在風險

川普政府提出的部分網路戰略規畫雖著眼於保障國家網路安全，但在執行過程中卻可能面臨外部阻力及致使安全環境進一步惡化的風險。

首先，亟於因應網路威脅的川普政府正逐漸放寬動用網路戰力的限制，雖然美國過去在「震網病毒」(Stuxnet)等事件中亦有使用網路武器打擊對手的經驗，但川普政府不僅進一步簡化發起網路軍事行動的行政流程，更提出「防禦推進」概念，強調在威脅成形前便主動出擊以預先弭患。這種頗具攻勢意涵的防務思維，以及近期有關美國對伊

94. 關於相關病毒之間的技術共通性，請見Maxat Akbanov, Vassilios G. Vassilakis, & Michael D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," *Journal of Telecommunications and Information Technology*, No. 1, January 2019, pp. 113-124。

95. Nicole Perlroth & Scott Shane, "In Baltimore and Beyond, a Stolen N.S. A. Tool Wreaks Havoc," *The New York Times*, May 25, 2019, <https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html>.

EH-01_張凱銘.tpf-43

朗和俄羅斯等國家發動網路攻擊的報導，勢必對其競爭對手造成更大的安全壓力，國際間的網路軍備競賽恐將進一步加劇。為防止國際網路政治陷入霍布斯式(Hobbesian)的鬥爭狀態，美國在發展運用本國網路戰力之餘，或應加速推進國際網路軍備控制協議的建設工作。[96]

其次，從美國以網路入侵和投放病毒等手段打擊伊朗的核能發展計畫，與報復其擊落美軍無人機等事例來看，網路戰力已成為華府處理國際安全爭端時的行動選項之一。與此同時，正如波頓在介紹新版《國家網路戰略》時提到的看法：「並非對於所有的網路攻擊都只能在網路空間中進行回應」，[97]川普政府認為必要時可以傳統軍事手段報復網路惡意活動，並強調這麼做將使美國強大的常規武力得以投射至網路空間，更有效地嚇阻潛在敵人。[98]這類打破網路空間與現實世界分際的防務思維，固可為當前的美國網路安全保障創造便利，但長程而言也不無促使各國濫用網路武器，甚或因網路紛爭觸發實體軍事衝突的風險。

此外，由於無法在國際社會中建立共識，美國對網路空間國家行為準則的推動已漸陷入停滯，川普政府遂更加倚賴以雙邊或有限多邊形式，和傳統盟邦及安全夥伴發展跨國網路安全合作。然而相關國家與美國間雖有密切的政經聯繫和防務交流，但無論是部分歐洲國家先前對於美國排拒華為公司參與 5G 網路建設一事的保留態度，[99]或是印

96. Joseph S. Nye, "Rules of the cyber road for America and Russia," March 11, 2019, *The Strategist*, <https://www.aspistrategist.org.au/rules-of-the-cyber-road-for-america-and-russia/>.

97. Jacqueline Thomsen, "US to Prioritize Attacks Against Foreign Adversaries under new Cyber Strategy," *The Hill*, September 20, 2018, <https://thehill.com/policy/cybersecurity/407670-us-to-launch-offensive-attacks-against-foreign-adversaries-under-new>.

98. Jeff Seldin, "US Prepared to Strike in Cyberspace."

99. Katharina Buchholz, "Which Countries Have Banned Huawei?" August 19,

EH-01_張凱銘.tpf-44

度政府近期限縮國民網路自由的作法，[100] 皆顯示美國與其友邦對於網路治理問題的觀點未必全然相同。這種現象不僅意味著美國政府在試圖將現實安全合作體系移轉至網路空間的過程中，必須投入更多心力與資源於跨國協調，更代表相關國家在特定議題上可能會採取與華府不同的政策立場。[101]

三、美國國家網路戰略的實施前景

值得注意地是，若深入思考美國國家網路戰略的實施前景，可發現其間仍存在部分值得關注的變數：

首先，考量到網路戰略本質上仍是總體國家安全戰略的一部分，兩者之間存在連動關係，中國、俄羅斯、伊朗與北韓等國家雖為川普政府視作國家網路安全的主要威脅來源，然若相關國家未來與美國在國家安全戰略方面的矛盾有所緩和，隨著外交方針的調整，彼此在網路領域的互動狀態也將連帶出現變化。

其次，為應對網路空間中日見嚴峻的安全情勢，川普政府透過加強資安管制、開發新型資安技術等作法試圖提升美國的網路防護能力。但隨著各類監管的增加，相關舉措在加強防護時不免將損及網路

2019, *Statista*, <https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/>.

100. Vindu Goel, "India Proposes Chinese-Style Internet Censorship," *The New York Times*, February 14, 2019, <https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html>.

101. 例如作為美國盟邦的南韓在 2012 年「國際電信大會」(World Conference on International Telecommunications, WCIT)中，針對修改「國際電信規則」(International Telecommunication Regulations, ITRs)，承認各國對本國網路空間管轄權限的議案表決過程中，便採取了與美國不同的態度，請見 Kevin Reed, "Global Split Over Telecom Treaty," December 28, 2012, *World Socialist Web Site*, <https://www.wsws.org/en/articles/2012/12/28/wcit-d28.html>。

EH-01_張凱銘.tpf-45

空間的開放與用戶隱私保障，此與美國長年以來主張的網路自由理念勢將產生某種程度的衝突，[102] 如何調和這種內在衝突，當為川普政府後續網路施政中無可迴避的重要課題。

最後，川普政府試圖修訂國際法規，使其可以正當自衛名義動用飛彈等常規軍械報復網路惡意活動的作法，固可使美國的強大軍事實力得以投射至網路空間，進而產生更強烈的嚇阻效用，但相關訴求迄未獲得國際社會廣泛接納，且在執行上可能衍生傷害程度不對等等道德爭議；部分與美國間存在戰略競爭關係的國家，亦恐將加強自身防務建設以因應安全壓力，其結果或將推動國際軍備競賽升級與網路軍事化趨向加速等連帶效應，對美國的國家安全造成負面影響。

另一方面，對於安全的憂慮往往是人類文明進步的重要動力，一如冷戰期間的核戰爭威脅間接促成了網路科技問世，川普政府對各類網路威脅的關切及相應戰略規畫，長遠來看亦可能為網際網路發展前景帶來正面效益。譬如美國近年在強化內部網路防護時，特別著重開發針對網路惡意活動來源及行為者身分的辨識溯源能力，並以政策手段鼓勵學術機構和民間企業研發先進資安產品。相關努力成果不僅可協助美國與其他國家抵禦網路威脅，也將為資安科技的創新突破提供支持，從而改善網際網路環境的安全狀態。

陸、結論

高度重視網路科技領域是川普政府顯著的施政特徵之一。自 2017 年以來，除了《國家安全戰略》與《國家網路戰略》等高階報告外，美國聯邦政府各部門亦陸續發表多份以網路治理為主軸的政策文件，逐步構建起全面性的國家網路戰略框架。

檢視川普政府的網路戰略論述，可察見網路安全為其戰略規畫主軸，聚焦於美國面臨的外部威脅，以及改善資安防護水準的可行作

102. The White House, *National Cyber Strategy*, pp. 24-25.

EH-01_張凱銘.tpf-46

法。為了解在網路科技領域長期保持領先優勢的美國為何對自身的網路安全處境備感焦慮，並探討其龐雜的政策法令背後是否存在一致性的共通脈絡，本文援引了國際關係研究中的威脅平衡理論作為分析途徑。

根據威脅平衡理論的內容，本文首先由威脅要件的角度探討美國當前面臨的網路安全態勢。研究結果顯示美國雖在綜合國力方面持有優勢，但中國、俄羅斯、伊朗與北韓等國家，近年皆發展出規模不等的網路進攻實力，且自相關國家對美國發起的大量網路惡意活動中亦可窺見其侵略意圖，從而使川普政府產生明確的威脅感知。

關於具體的平衡舉措，川普政府在內部平衡層面透過行政改革、鼓勵研發創新與擴大培育人才等方式，力求鞏固美國的基礎網路實力。同時以強化網路防務建設、放寬網路軍事行動管制，與倡議「防禦推進」概念等作法，建設更強大的網路安全力量。在外部平衡層面，川普政府近年於國際交流中試圖將現行國際法的自衛權規範導入網路領域，並主張制訂網路空間國家行為準則以保障網際網路有序運作，而美國與傳統盟邦及安全夥伴間的網路安全合作近期亦持續深化。

在透過威脅平衡理論檢視美國國家網路戰略的基礎上，本文指出美國目前面臨的網路安全威脅，與其內部治理及行政監管的嚴謹度不足有關，此即川普政府的網路戰略規畫包含多項行政改革措施的主因，相關舉措雖在各層級部門協作下漸次開展，但對於網路空間的監管強化，會否損及其自由程度當為後續值得注意之處。而美國近期在網路防務方面的諸多攻勢作為，如提倡「防禦推進」概念、放寬網路軍事行動管制，以及意圖運用常規軍事力量報復網路攻擊等，固然對其資安防護有直接助益，但在實踐上仍可能引發國際法規適用爭議及加劇軍備競賽和網路空間軍事化風險等效應。此外，雖然美國與其友邦間的網路安全合作漸次開展，但相關事例顯示各國對於網路治理議題的看法仍不盡一致，川普政府未來在國際網路交流中，恐須投入更

EH-01_張凱銘.tpf-47

多精力與資源於協調折衝之上。

（收件：2019 年 9 月 1 日；修正：2020 年 1 月 6 日；採用：2020 年 1 月 13 日）

EH-01_張凱銘.tpf-48

參考文獻

中文部分

專書譯著

Martel, Frederic 著，林幼嵐譯，2016。《全球網路戰爭》(*Smart: Enquête sur les Internets*)。新北：稻田。

專書論文

鄭端耀，2011。〈搶救權力平衡理論〉，包宗和主編，《國際關係理論》。臺北：五南。頁 69-83。

網際網路

2011/5/26。〈國防部證實建網上藍軍稱為提高部隊網絡防護〉，《人民網》，<http://politics.people.com.cn/BIG5/1027/14740509.html>。

2019/5/30。〈印太資安聯盟成立 AIT：資安不只是政治議題〉，《中央廣播電臺》，<https://www.rti.org.tw/news/view/id/2022452>。

英文部分

專書

Chanlett-Avery, Emma et al., 2017. *North Korean Cyber Capabilities: In Brief*. Washington D.C.: Congressional Research Service.

Cylance, 2014. *Operation Cleaver*. Irvine: Cylance.

Giles, Keir, 2015. *The Next Phase of Russian Information Warfare*. Riga: NATO Strategic Communications Centre of Excellence.

He, Kai, 2009. *Institutional Balancing in the Asia Pacific, Economic Interdependence and China's Rise*. New York: Routledge.

Lowy Institute, 2018. *Asia Power Index 2018*. Sydney: Lowy Institute.

EH-01_張凱銘.tpf-49

Mandiant Corporation, 2013. *APT1: Exposing One of China's Cyber Espionage Units*. Washington, D.C.: Mandiant Corporation.

Maurer, Tim, 2011. *Cyber Norm Emergence at the United Nations*. Cambridge: Harvard Kennedy School.

McLoughlin, Glenn J. & Ian F. Fergusson, 2003. *High Performance Computers and Export Control Policy: Issues for Congress*. Washington, D.C.: Congressional Research Service.

Muller, Lilly Pijnenburg, Lars Gjesvik, & Karsten Friis, 2018. *Cyber-weapons in International Politics*. Oslo: Norwegian Institute of International Affairs.

Pella, Peter, 2018. *The Continuing Quest for Missile Defense: When Lofty Goals Confront Reality*. San Rafael: Morgan & Claypool Publishers.

Ryan, Johnny, 2010. *A History of the Internet and the Digital Future*. London: Reaktion Books.

Stokes, Mark A., 2015. *The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398*. Arlington: Project 2049 Institute.

Tikk-Ringas, Eneken, 2012. *Developments in the Field of Information and Telecommunications in the Context of International Security*. Geneva: ICT for Peace Foundation.

USC Center on Public Diplomacy, 2018. *The Soft Power 30: A Global Ranking of Soft Power 2018*. Los Angeles: USC Center on Public Diplomacy.

Walt, Stephen M., 1987. *The Origins of Alliances*. New York: Cornell University.

Walt, Stephen M., 2005. *Taming American Power: The Global Response to U.S. Primacy*. New York: Norton.

Waltz, Kenneth N., 1979. *Theory of International Politics*. New York:

EH-01_張凱銘.tpf-50

McGraw-Hill.

專書論文

Jin, Dal Yong, 2016. "The Construction of Platform Imperialism in the Globalisation Era," in Christian Fuchs & Vincent Mosco, eds., *Marx in the Age of Digital Capitalism*. Leiden: Brill. pp. 322-349.

期刊論文

Akbanov, Maxat, Vassilios G. Vassilakis, & Michael D. Logothetis, 2019/1. "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," *Journal of Telecommunications and Information Technology*, No. 1, pp. 113-124.

Art, Robert J., 2005/Winter-2006. "Striking the Balance," *International Security*, Vol. 30, No. 3, pp. 178-180.

Costello, John, 2016/2. "The Strategic Support Force: China's Information Warfare Service," *China Brief*, Vol. 16, No. 3, pp. 15-20.

Pape, Robert A., 2005/Summer. "Soft Balancing Against the United States," *International Security*, Vol. 30, No. 1, pp. 7-45.

Racicot, Jonathan, 2014/Summer. "The Past, Present and Future of Chinese Cyber Operations," *Canadian Military Journal*, Vol. 14, No. 3, pp. 26-37.

官方文件

European Commission, 2019. *EU-China – A Strategic Outlook*. Brussels: European Commission.

Executive Office of the President of the United States, 2019. *Science & Technology Highlights in the Second Year of the Trump Administration*. Washington, D.C.: Executive Office of the President of the United States.

U.S. Cyber Command, 2018. *Achieve and Maintain Cyberspace Superiority*.

EH-01_張凱銘.tpf-51

Fort Meade: U.S. Cyber Command.

U.S. Defense Science Board, 2017. *Cyber Deterrence Task Force*. Washington, D.C.: Office of the Secretary of Defense.

U.S. Department of Commerce & U.S. Department of Homeland Security, 2018. *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*. Washington, D.C.: U.S. Department of Commerce & U.S. Department of Homeland Security.

U.S. Department of Commerce & U.S. Department of Homeland Security, 2018. *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce*. Washington, D.C.: U.S. Department of Commerce & U.S. Department of Homeland Security.

U.S. Department of Defense, 2011. *Department of Defense Cyberspace Policy Report*. Washington, D.C.: U.S. Department of Defense.

U.S. Department of Defense, 2018. *DoD Cloud Strategy*. Washington, D.C.: U.S. Department of Defense.

U.S. Department of Defense, 2018. *Summary of the 2018 Department of Defense Cyber Strategy*. Washington, D.C.: U.S. Department of Defense.

U.S. Department of Defense, 2019. *Military and Security Developments Involving the People's Republic of China 2019*. Washington, D.C.: U.S. Department of Defense.

U.S. Department of State, 2018. *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. Washington, D.C.: U.S. Department of State.

U.S. Department of State, 2018. *Recommendations to the President on Securing America's Cyber Interests and Deterring Cyber Threats through International Engagement*. Washington, D.C.: U.S. Department

EH-01_張凱銘.tpf-52

of State.

U.S. Government Accountability Office, 2019. *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*. Washington, D.C.: U.S. Government Accountability Office.

U.S. National Science and Technology Council, 2019. *2019 Federal Cybersecurity Research and Development Strategic Plan*. Washington, D.C.: U.S. National Science and Technology Council.

U.S. Office of the Director of National Intelligence, 2019. *National Intelligence Strategy 2019*. Washington, D.C.: U.S. Office of the Director of National Intelligence.

U.S. Office of Management and Budget, 2018. *Federal Cybersecurity Risk Determination Report and Action Plan*. Washington, D.C.: Office of Management and Budget.

The White House, 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, D.C.: The White House.

The White House, 2011. *International Strategy for Cyberspace*. Washington, D.C.: The White House.

The White House, 2017. *National Security Strategy*. Washington, D.C.: The White House.

The White House, 2018. *National Cyber Strategy*. Washington, D.C.: The White House.

網際網路

2016/7/21. “Transcript: Donald Trump on NATO, Turkey’s Coup Attempt and the World,” *The New York Times*, <https://www.nytimes.com/2016/07/22/us/politics/donald-trump-foreign-policy-interview.

EH-01_張凱銘.tpf-53

html>.

2017/2/23. “Russian Military Admits Significant Cyber-War Effort,” *BBC News*, <https://www.bbc.com/news/world-europe-39062663>.

American Institute in Taiwan, 2019/5/28. “Remarks by AIT Deputy Director Raymond Greene at Opening Ceremony of GCTF on Network Security and Emerging Technologies,” *American Institute in Taiwan*, <https://www.ait.org.tw/remarks-by-ait-deputy-director-greene-at-opening-ceremony-of-gctf-on-network-security-and-emerging-technologies/>.

ASEAN, 2018/11/15. “ASEAN-United States Leaders’ Statement on Cybersecurity Cooperation,” *Association of South East Asia Nations*, <https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf>.

Bowcott, Owen, 2017/8/23. “Dispute along Cold War Lines Led to Collapse of UN Cyberwarfare Talks,” *The Guardian*, <https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges>.

Buchholz, Katharina, 2019/8/19. “Which Countries Have Banned Huawei?” *Statista*, <https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/>.

Busselen, Michael, 2019/3/28. “Key Trends from the CrowdStrike 2019 Global Threat Report,” *CrowdStrike*, <https://www.crowdstrike.com/blog/2019-global-threat-report-key-trends/>.

Constantin, Lucian, 2017/2/13. “Recent Malware Attacks on Polish Banks Tied to Wider Hacking Campaign,” *Network World*, <https://www.networkworld.com/article/3169409/security/recent-malware-attacks-on-polish-banks-tied-to-wider-hacking-campaign.html>.

CrowdStrike, 2014/6/9. “Hat-tribution to PLA Unit 61486,” *CrowdStrike*,

EH-01_張凱銘.tpf-54

<https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/>.

CrowdStrike, 2018/8/30. "Two Birds, One Stone Panda," *CrowdStrike*, <https://www.crowdstrike.com/blog/two-birds-one-stone-panda/>.

CrowdStrike, 2019/2/24. "Meet the Threat Actors-Who are your Cyber Adversaries?" *CrowdStrike*, <https://www.crowdstrike.com/blog/meet-the-adversaries/>.

CrowdStrike, 2019/12/12. "Who is Refined Kitten?" *CrowdStrike*, <https://www.crowdstrike.com/blog/who-is-refined-kitten/>.

Cyber Security Agency of Singapore, 2017/4. "Factsheet on ASEAN Cyber Capacity Programme," *Cyber Security Agency of Singapore*, <https://www.csa.gov.sg/news/speeches/media/3bfa3b0aaf264a41b8f7a31551baf2b4.ashx>.

Cyber Security Agency of Singapore, 2018/11/16. "Singapore and the United States Sign Declaration of Intent on Cybersecurity Technical Assistance Programme," *Cyber Security Agency of Singapore*, <https://www.csa.gov.sg/news/press-releases/singapore-and-the-us-sign-doi-on-cybersecurity-technical-assistance-programme>.

Cybersecurity and Infrastructure Security Agency, 2019/12/25(Accessed). "Continuous Diagnostics and Mitigation," *U.S. Department of Homeland Security*, <https://www.us-cert.gov/cdm/home>.

Freedberg Jr., Sydney J., 2018/9/17. "Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff," *Breaking Defense*, <https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/>.

Freedom House, 2019/12/25(Accessed). "Freedom in the World in 2019: North Korea," *Freedom House*, <https://freedomhouse.org/report/freedom-world/2019/north-korea>.

G7 Summit, 2017/4/11. "G7 Declaration on Responsible States Behavior

EH-01_張凱銘.tpf-55

in Cyberspace," *Ministry of Foreign Affairs of Japan*, <https://www.mofa.go.jp/files/000246367.pdf>.

Global Cyber Security Company, 2018/10/1. "Hi-Tech Crime Trends 2018," *Group-IB*, <https://www.fintechsecurity.com.hk/slides/01.Dmitry-Annual-Group-IB-report-High-Tech-Crime-Trends.pdf>.

Goel, Vindu, 2019/2/14. "India Proposes Chinese-Style Internet Censorship," *The New York Times*, <https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html>.

Goldstein, Phil, 2018/2/15. "Cybersecurity Funding Would Jump in Trump's 2019 Budget," *FedTech*, <https://fedtechmagazine.com/article/2018/02/cybersecurity-funding-would-jump-trumps-2019-budget>.

Haseltine, Ben, 2018/6/5. "Pentagon's Bug Bounty Program Identifies Defense Travel System Vulnerabilities," *GovernmentCIO Media & Research*, <https://www.governmentciomedia.com/pentagons-bug-bounty-program-identifies-defense-travel-system-vulnerabilities-0>.

Headquarters U.S. Forces, Japan, 1960/1/19. "Treaty of Mutual Cooperation and Security between the United States and Japan," *U.S. Central Intelligence Agency*, <https://www.cia.gov/library/readingroom/docs/CIA-RDP07-00469R000100950001-2.pdf>.

Hymas, Charles, 2018/10/9. "China is ahead of Russia as 'biggest state sponsor of cyber-attacks on the West,'" *The Telegraph*, <https://www.telegraph.co.uk/technology/2018/10/09/china-ahead-russia-biggest-state-sponsor-cyber-attacks-west/>.

Kim, Youngnam, 2018/6/8. "North Korea Uses US Tech for 'Destructive Cyber Operations'," *Voice of America*, <https://www.voanews.com/a/north-korea-us-tech-destructive-cyber-operations/4429922.html>.

Kochetkova, Kate, 2016/2/24. "What is Known about the Lazarus Group: Sony Hack, Military Espionage, Attacks on Korean Banks and other

EH-01_張凱銘.tpf-56

Crimes," *Kaspersky Lab*, <https://www.kaspersky.com/blog/operation-blockbuster/11407/>.

LaFrance, Adrienne, 2016/9/27. "Trump's Incoherent Ideas About 'the Cyber,'" *The Atlantic*, <https://www.theatlantic.com/technology/archive/2016/09/trumps-incoherent-ideas-about-the-cyber/501839/>.

Lange, Katie, 2018/5/3. "Cybercom Becomes DoD's 10th Unified Combatant Command," *DoD Live*, <http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/>.

Lyngaas, Sean, 2018/4/10. "DHS 'Cyber Storm' Exercise Tests Manufacturing and Transportation Sectors," *Cyberscoop*, <https://www.cyberscoop.com/dhs-cyber-storm-jeanette-manfra-critical-infrastructure/>.

Lyngaas, Sean, 2018/8/16. "PPD-20 Elimination Opens Arguments over How U.S. Should Conduct Offensive Hacking Operations," *Cyberscoop*, <https://www.cyberscoop.com/ppd-20-eliminated-cyber-war-donald-trump-mike-rounds/>.

Menn, Joseph, 2017/8/25. "Chinese National Arrested in Los Angeles on U.S. Hacking Charge," *Reuters*, <https://www.reuters.com/article/us-usa-cyber-opm/chinese-national-arrested-in-los-angeles-on-u-s-hacking-charge-idUSKCN1B42RM>.

Meyers, Adam, 2018/11/27. "Meet CrowdStrike's Adversary of the Month for November: Helix Kitten," *CrowdStrike*, <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/>.

Ministry of Foreign Affairs of Japan, 2019/4/19. "Joint Statement of the Security Consultative Committee," *Ministry of Foreign Affairs of Japan*, <https://www.mofa.go.jp/files/000470738.pdf>.

The MITRE Corporation, 2020/1/9. "JUST RELEASED: ATT&CK for Industrial Control Systems," *The MITRE Corporation*, <https://attack.

EH-01_張凱銘.tpf-57

mitre.org/groups/>.

Nakashima, Ellen, 2019/6/23. "Trump Approved Cyber-Strikes Against Iranian Computer Database Used to Plan Attacks on Oil Tankers," *The Washington Post*, <https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html>.

Nye, Joseph S., 2019/3/11. "Rules of the cyber road for America and Russia," *The Strategist*, <https://www.aspistrategist.org.au/rules-of-the-cyber-road-for-america-and-russia/>.

Paganini, Pierluigi, 2019/7/24. "China-Linked APT15 Group is Using a Previously Undocumented Backdoor," *Security Affairs*, <https://securityaffairs.co/wordpress/88824/apt/apt15-okrum-backdoor.html#top>.

Panda, Ankit, 2018/9/9. "What the Recently Concluded US-India COMCASA Means," *The Diplomat*, <https://thediplomat.com/2018/09/what-the-recently-concluded-us-india-comcasa-means/>.

Perlroth, Nicole & Scott Shane, 2019/5/25. "In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc," *The New York Times*, <https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html>.

Pomerleau, Mark, 2017/6/1. "Cyber protection teams assigned to THAAD in South Korea," *Fifth Domain*, <https://www.fifthdomain.com/home/2017/06/01/cyber-protection-teams-assigned-to-thaad-in-south-korea/>.

Pomerleau, Mark, 2019/7/16. "What Good are 'Exceptional' Cyber Capabilities without Authority?" *Fifth Domain*, <https://www.fifthdomain.com/dod/2019/07/16/what-good-are-exceptional-cyber-capabilities-without-authority/>.

Reed, Kevin, 2012/12/28. "Global Split Over Telecom Treaty," *World*

EH-01_張凱銘.tpf-58

Socialist Web Site, <https://www.wsws.org/en/articles/2012/12/28/wcit-d28.html>.

Sanger David E. & Nicole Perlroth, 2019/6/15. "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.

Sanger, David E. & William J. Broad, 2018/1/16. "Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms," *The New York Times*, <https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html?_ga=2.182743974.1450541312.1564318121-1345450338.1537238599>.

Scheer, Steven, 2017/6/26. "U.S. to Work with Israel, Seek other Ties to Combat Cyber Attacks," *Reuters*, <https://www.reuters.com/article/us-usa-israel-cyber-idUSKBN19H1KE>.

Seldin, Jeff, 2018/9/20. "US Prepared to Strike in Cyberspace," *Voice of America*, <https://www.voanews.com/usa/us-politics/us-prepared-strike-cyberspace>.

Sukumar, Arun M., 2017/7/4. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *The Lawfare Institute*, <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.

Symantec Corporation, 2017/4. *Internet Security Threat Report No. 22*, pp. 1-75, *Symantec Corporation*, <https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf>.

Thomsen, Jacqueline, 2018/9/20. "US to Prioritize Attacks Against Foreign Adversaries under new Cyber Strategy," *The Hill*, <https://thehill.com/policy/cybersecurity/407670-us-to-launch-offensive-attacks-against-foreign-adversaries-under-new>.

EH-01_張凱銘.tpf-59

U.S. 116th Congress, 2019/7/24. "H.R.1837 - United States-Israel Cooperation Enhancement and Regional Security Act," *U.S. Library of Congress*, <https://www.congress.gov/bill/116th-congress/house-bill/1837>.

U.S. Department of Homeland Security, 2019/12/25(Accessed). "Cyber Storm VI: National Cyber Exercise," *U.S. Department of Homeland Security*, <https://www.dhs.gov/cisa/cyber-storm-vi>.

U.S. Department of Justice, 2017/3/15. "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions>.

U.S. Department of Justice, 2017/11/21. "Acting Manhattan U.S. Attorney Announces Charges against Iranian National for Conducting Cyber Attack And $6 Million Extortion Scheme against HBO," *U.S. Department of Justice*, <https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting>.

U.S. Department of Justice, 2017/11/27. "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations>.

U.S. Department of Justice, 2018/7/13. "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>.

U.S. Department of Justice, 2018/9/6. "North Korean Regime-Backed

EH-01_張凱銘.tpf-60

Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>.

U.S. Department of Justice, 2018/10/30. "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal>.

U.S. Department of Justice, 2018/12/20. "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion>.

U.S. Department of Justice, 2019/1/15. "Two Ukrainian Nationals Indicted in Computer Hacking and Securities Fraud Scheme Targeting U.S. Securities and Exchange Commission," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/two-ukrainian-nationals-indicted-computer-hacking-and-securities-fraud-scheme-targeting-us>.

U.S. Department of Justice, 2019/1/28. "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial>.

U.S. Department of Justice, 2019/5/9. "Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions,

EH-01_張凱銘.tpf-61

Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including>.

U.S. Department of Justice, 2019/7/11. "Newly Unsealed Federal Indictment Charges Software Engineer with Taking Stolen Trade Secrets to China," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china>.

U.S. Department of State, 2018/7/30. "Remarks on America's Indo-Pacific Economic Vision," *U.S. Department of State*, <https://www.state.gov/remarks-on-americas-indo-pacific-economic-vision/>.

U.S. Department of State, 2018/12/20. "Joint Statement by Secretary of State Michael R. Pompeo and Secretary of Homeland Security Kirstjen Nielsen: Chinese Actors Compromise Global Managed Service Providers," *U.S. Department of State*, <https://www.ait.org.tw/joint-statement-by-dos-sec-pompeo-and-dhs-sec-nielsen/>.

U.S. Department of State, 2019/4/19. "Joint Statement of the Security Consultative Committee," *U.S. Department of State*, <https://www.state.gov/u-s-japan-joint-press-statement/>.

U.S. Federal Bureau of Investigation, 2018/12/20. "FBI Director Christopher Wray's Remarks Regarding Indictment of Chinese Hackers," *U.S. Federal Bureau of Investigation*, <https://www.fbi.gov/news/pressrel/press-releases/fbi-director-christopher-wrays-remarks-regarding-indictment-of-chinese-hackers>.

U.S. House of Representatives, 2019/3/6. "Maintaining U.S. Leadership in Science and Technology: Testimony before the Congress of the United States House of Representatives Committee on Science, Space

EH-01_張凱銘.tpf-62

and Technology," *U.S. House of Representatives*, <https://docs.house.gov/meetings/SY/SY00/20190306/109030/HHRG-116-SY00-Wstate-KhanM-20190306.pdf>.

U.S. Office of the Director of National Intelligence, 2016/2/9. "Remarks as Delivered by The Honorable James R. Clapper Director of National Intelligence, Senate Select Committee on Intelligence – IC's Worldwide Threat Assessment Opening Statement," *U.S. Office of the Director of National Intelligence*, <https://www.dni.gov/files/documents/2016-02-09SSCI_open_threat_hearing_transcript.pdf>.

U.S. Office of Management and Budget, 2018/2/1. "Budget of the United States, Fiscal Year 2019: Efficient, Effective, Accountable — An American Budget," *The White House*, <https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf>.

U.S. Securities and Exchange Commission, 2019/1/17. "SEC Brings Charges in Edgar Hacking Case, Litigation Release No. 24381," *U.S. Securities and Exchange Commission*, <https://www.sec.gov/litigation/litreleases/2019/lr24381.htm>.

U.S. Senate Committee on Armed Services, 2018/3/1. "Nominations – Nakasone-Park-White," *U.S. Senate Committee on Armed Services*, <https://www.armed-services.senate.gov/hearings/18-03-01-nominations_--nakasone---park---white>.

The White House, 2017/5/11. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *The White House*, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.

The White House, 2017/9/25. "Presidential Memorandum for the Secretary of Education," *The White House*, <https://www.whitehouse.gov/presid-

EH-01_張凱銘.tpf-63

ential-actions/presidential-memorandum-secretary-education/>.

The White House, 2018/1/8. "Presidential Executive Order on Streamlining and Expediting Requests to Locate Broadband Facilities in Rural America," *The White House*, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-streamlining-expediting-requests-locate-broadband-facilities-rural-america/>.

The World Bank, 2019/12/25(Accessed). "Fixed Broadband Subscriptions (per 100 people)," *The World Bank*, <https://data.worldbank.org/indicator/IT.NET.BBND.P2?locations=KP-US-RU-CN-IR>.

The World Bank, 2019/12/25(Accessed). "Individuals using the Internet (% of population)," *The World Bank*, <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=IR-US-CN-KP-RU>.

Volz, Dustin & Mark Hosenball, 2016/11/17. "Trump Cyber Security Team, Policy Slow to Take Shape: Officials," *Reuters*, <https://www.reuters.com/article/us-usa-trump-cyber-idUSKBN13B2VI>.

EH-01_張凱銘.tpf-64

Study on the U.S. National Cyber Strategy in the Trump Era: From the Perspective of the Balance of Threat Theory

Kai-ming Chang

(Assistant Professor, Center for General Education, National Taichung University of Science and Technology)

Abstract

This article reviews the formulation and practice of the Trump administration's cyber strategy and analyzes it through the Balance of Threat Theory of international relations. The research results show that the current national cyber strategy of the U.S. is aimed to resist security threats. The Trump administration has actively constructed cyber offensive and defensive capabilities internally and developed cross-border cooperation in cybersecurity with friendly countries to balance the challenges from adversaries such as China and Russia. However, the strategy has caused some controversy in the course of its practice because of the obvious unilateral style and could make the future of international cyber politics and the scenario of the Internet more unpredictable.

Keywords: Cybersecurity, The U.S. National Cyber Strategy, The U.S. Foreign Policy, International Cyber Politics, Defending Forward