10.6326/NDJ.202012_35(4).0002

# 美國與中共網路戰略及其對臺灣可能的影響

# Cyber Strategy of the U.S. and China and Its Possible Implications for Taiwan

林正義 (Cheng-Yi Lin)

中央研究院研究員

## 摘　　要

隨著中共與美國關係進入戰略競爭和不確定性時期，網路安全已成爲兩國互爭優勢的領域。美國前總統歐巴馬在與中共的國防安全關係上，採取低調、防禦性的網路安全政策。川普總統則採取了積極主動的進攻姿態，遏制中共網路作戰能力的提升。北京很少辯論其對美國網路作戰的進攻思想，承諾採取非對抗性的網路安全途徑，但加速建立能打贏不對稱戰爭概念下的「戰略支援部隊」。北京的網路攻擊能力不僅限於美國，也意圖嚇阻、拖延和擊敗美國在臺灣海峽的軍事干預行動。在美國軍事軟硬體的協助下，臺灣致力建立與軍事行動相搭配的網路任務部隊。臺灣與中共和美國一樣，不僅注重網路防禦能力，而且不排除採取攻勢戰略。

**關鍵詞：**網路安全、不對稱作戰、網路戰略、關鍵基礎設施、美中臺關係

## Abstract

As China and the United States enter a strategic competition and uncertainty period, cybersecurity has become a competitive domain for supremacy. President Barack Obama adopted a low key defensive cyber security strategy vis-a-vis China. In contrast, President Donald Trump has adopted a pro-active and offensive posture when facing a surge of Chinese cyber operations. Beijing has seldom debated its offensive thinking of cyber operations against the U.S. and pledged a non-confrontational cyber approach. However, it has expedited building a Strategic Support Force capable of victory in an asymmetric conflict. Beijing's cyber defense capabilities are not in place to defend against the United States only, for China also wishes to deter, delay, and defeat U.S. military intervention efforts in the Taiwan Strait. With assistance from the U.S. in military hardware and software, Taiwan is devoted to creating a formidable cyber defense mission force working closely with its military operations. Like China and the U.S., Taiwan is focusing on hardening cyber defense capabilities and building an offensive strategy.

**Keywords:** Cyber Security, Asymmetric Warfare, Cyber Strategy, Critical Infrastructure, US-China-Taiwan Relations

* 本文為科技部專題研究計畫《美中臺關係的網路安全因素：以歐巴馬政府為例》(MOST 105-2410-H-001-018-MY2) 部分研究成果。

## 壹、前　　言

美國與中共關係自歐巴馬(Barack Obama)、習近平相繼執政以來，至川普(Donald Trump)任內，對網路安全(cybersecurity)的重視為前所未有。美國、中共除國防部之外，有其上位的美國國家安全會議或中共國家安全委員會指導網路戰略。美國白宮、國防部、國土安全部均發表網路戰略相關報告，各有不同的職權、議題視角。中共國防部雖沒有單獨針對網路安全出版報告，但外交部、國家互聯網信息辦公室分別發表《網絡空間國際合作戰略》、《國家網絡空間安全戰略》。[1]本文首先檢視美中兩國的網路戰略報告，其次分析如何評估對方的網路戰略，最後討論對臺灣的可能的影響。

根據美國2015年美國《國防部網路戰略》(DOD Cyber Strategy)，所欲達成的「網路安全」目標，包括：政府資訊分享與跨部門協調、建立與民間私部門的聯繫橋樑、建立與盟邦及友好夥伴的合作關係，既涵蓋國防部網路、系統、資訊的防護，也保護國家免於重大後果的網路攻擊，更可支援作戰與應變計畫。[2]「網路安全」層次較高、範圍更廣，涵蓋非軍事層面的「網路犯罪」(Cyber Crime)、「網路間諜」(Cyber Espionage)的打擊，更需仰賴有國防意涵的「資訊（信息）戰」(Information Warfare)、「網路戰」(Cyber Warfare)及軍事階層的「資訊作戰」(Information Operations)、「網路作戰」(Cyber Operations)的支援，方能確保目標的達成。[3]本文礙於篇幅，不討論網路及電腦技術性等問題，如「電腦網路攻擊」(Computer Network Attack)、「中斷服務常式」(Interrupt Service Routine)及「網路蓄意破壞」(Cyber Vandalism) [4]。2015年，美中針對「網路犯罪」、「網路間諜」問題，達成的五項共識，

1「Cyber」、「Internet」及「Network」在中國大陸譯為「互聯網」或「網絡」，臺灣稱為「網際網路」或「網路」。

2 U.S. Department of Defense, *The DOD Cyber Strategy* (Washington, DC: U.S. Department of Defense, 2015), pp. 13-15, <https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod _cyber_ strategy_ for_web.pdf>（檢索日期：2020年7月23日）

3 根據美國蘭德公司資深研究員李畢基(Martin C. Libicki)的分類，「資訊戰」(Information Warfare)涵蓋面較廣，包括指揮管制戰、情報戰、電子戰、心理戰、駭客戰、經濟資訊戰、網路戰。請參見Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), pp. 16-17；「資訊作戰」指的是「在軍事作戰整合運用資訊相關能力(information-related capabilities)，並協同其他作戰線，來影響、破壞、惡化、侵佔對手及潛在對手的決策，並保護自己本身」。「資訊相關能力」包括：戰略溝通、跨部門協調小組、公共事務、軍民聯戰、網路空間作戰（網路作戰）、資訊掌握、太空作戰、軍事資訊支援作戰、情報、軍事欺敵、作業安全、特殊技術戰、聯合電磁脈衝戰、關鍵領導接觸等14項。請參見Joint Chiefs of Staff, "Information Operations," in Joint Chiefs of Staff, ed., *Joint Publication 3-13* (Washington, DC: Joint Chiefs of Staff, 2014), pp. II 5-13.

4「電腦網路攻擊」乃利用電腦網絡破壞、阻絕、降級、摧毀儲存於電腦或電腦網絡資訊。此類攻擊行動包括：訊息竄改、服務阻斷、連線截奪、竊聽、通訊分析等。「中斷服務常式」指的是電腦系統負責處理中斷來源的一種專用服務程式，使用時間多寡對「執行緒排程」(thread scheduling)有很大影響。「網路蓄意破壞」如植入病毒或移走磁碟驅動器，讓電腦系統或關鍵基礎設施無法運作。

隨後也進行多輪網路安全對話，本文也不予以探討。[5]

## 貳、歐巴馬與川普政府的網路戰略

911事件後，小布希總統在2003年頒布白宮《確保網路空間的國家戰略》(*The National Strategy to Secure Cyberspace*)，展現對網路安全的重視，其中，國防工業基地是屬於國防部防護的關鍵基礎設施。[6] 2008年，小布希政府時期的「國家情報總監」(Director of National Intelligence)麥康奈爾(John Michael McConnell)建議時任國防部長的蓋茲(Robert M. Gates)，創立一個作戰司令部專責處理網路威脅。蓋茲接受此建議，先在2009年在位於馬里蘭州的「國家安全局」(National Security Agency)總部籌備，隨後要求該局局長亞歷山大將軍(General Keith Alexander)設立「網路指揮部」(Cyber Command)，2010年歐巴馬任內正式開始運作，以因應有關國防安全的網路威脅。[7] 網路資安的案例則早在此之前被證實，2008年，中共軍隊駭客入侵洛克馬丁(Lockheed Martin)竊取F-35戰機藍圖，美國總統歐巴馬競選網站亦被入侵；2010年10月，美國與以色列為阻止伊朗發展核武，使用一種名為「震網」(Stuxnet)的電腦蠕蟲，秘密地對伊朗核設施發動網路攻擊，成功延遲伊朗的核計畫。[8] 川普政府除提升網路戰略報告的層級外，集中在對中共的貿易談判與資訊、通信科技的圍堵。

### 一、歐巴馬政府網路戰略報告

歐巴馬政府任內先後通過多項有關網路安全的官方文書（如表1）。歐巴馬總統上台之後第一本《國家安全戰略》(*National Security Strategy*)（2010年5月）明顯提高對網路議題的關注度。由於太空與網路在美國軍事運作扮演重要角色，容易遭受外來攻擊。面對這種不對稱的威脅，美國必須全面強化網路國防安全。[9] 前白宮反恐、網路空

5 美中五點共識包括：就惡意網路活動，協助提供資訊；不從事或支持網路竊取智慧財產權；承諾推動國際社會網路空間合適的國家行為準則；維持「打擊網路犯罪及相關事項高層聯合對話」機制；就網路安全意外事件加強執法溝通。「網路犯罪」可透過「網路釣魚」取得個人、特定公司與組織盜竊帳戶、智慧財產權、企業機密；涉及駭入政府機關，如間諜取得機敏資訊，可稱之為「網路間諜」活動。The White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>（檢索日期：2020年9月19日）；U.S. Department of Justice, "Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," December 8, 2016, <https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues>（檢索日期：2020年9月19日）

6 The White House, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, 2003), p. 16, <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>（檢索日期：2020年7月23日）

7 Robert M. Gates, *Duty: Memoirs of a Secretary at War* (New York: Alfred A. Knopf, 2014), pp. 449-450.

8 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Broadway Books, 2018), pp. 7-8, 18-19.

9 The White House, *National Security Strategy* (Washington, DC: The White House, 2010), pp. 4, 17, <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>（檢索日期：2020年7月23日）

表1　歐巴馬政府公布的網路戰略報告

| 公布機關 | 時間 | 報告名稱 |
|---|---|---|
| 白宮 | 2011年5月 | 《網路空間國際戰略：網路世界的繁榮、安全與開放》(International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World) |
| 國防部 | 2011年7月 | 《國防部網路空間行動戰略》(Department of Defense Strategy for Operating Cyberspace) |
| 美國總統行政辦公室(Executive Office of the President of the United States) | 2013年2月 | 《降低美國貿易機密偷竊的行政策略》(Administration Strategy on Mitigating the Theft of U.S. Trade Secrets) |
| 國防部 | 2015年4月 | 《國防部網路戰略》(The Department of Defense Cyber Strategy) |

資料來源：作者整理自公開資訊。

間的顧問克拉克(Richard A. Clarke)在2010年出版的《網路戰爭：下一個國安威脅及因應之道》(*Cyber War: The Next threat to National Security and What to Do About It*)，指出中共在2003年已成立「網路戰」單位，準備好在戰爭時使用不對稱的網路攻擊，來克服傳統武器的弱勢。中共在「網路戰」至少具備10種武器與技術：埋設資訊地雷、遂行資訊偵察、修改網路資料、釋放資訊炸彈、傾倒資訊垃圾、散佈宣傳文宣、運用資訊欺敵、釋放仿製資訊、組織資訊防禦、建立網路間諜站。中共網路攻擊能力輸給美國，但防禦能力遠勝於美國，對網路依賴度也低於美國。[10]

2011年5月，白宮公布《網路空間國際戰略》(*International Strategy for Cyberspace*)，主要內容分為四部分，「制定網路空間政策」、「網路空間的未來」、「政策重點」及「策進未來」。在「政策重點」一節，歐巴馬政府列出在網路安全的七大政策重點，與本文探討焦點最直接相關的是第四點，它提到「在軍事領域與盟友通力合作，提高盟友因應網路威脅的能力，並確保美國軍用網路的安全」。[11] 2011年7月美國國防部發布《國防部執行網路空間戰略》(*Department of Defense Strategy for Operating Cyberspace*)，扼要明列五大「戰略倡議」(Strategic Initiatives)，包括：一、要求國防部充分利用網路空間的潛

10 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Haper Collins Publishers, 2010), pp. 57-58, 148.

11 其他六點分別為：一、在經濟領域加強接觸，確保網路為全球繁榮和科技創新做出貢獻，並加大保護智慧財產權；二、網路安全領域增進合作，增強美國及全球互聯網的安全性、可靠性及靈活性；三、在執法領域加強網路立法和執行力度，提高全球打擊網絡犯罪的能力；四、在網際網路管理領域加強與各國間的溝通交流，保障全球網絡系統的穩定和安全；五、在國際發展領域援助合作夥伴構建「數位基礎設施」(digital infrastructure)，協助它們提高抵禦網路威脅的能力；六、加強保護隱私，促進網路表達自由、集會自由及結社自由。The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, 2011), pp. 3-25, <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_ cyberspace.pdf>（檢索日期：2020年7月23日）

力，將網路空間列為軍事行動領域，建構軍事行動保護網路、組織、訓練和執行網路任務裝備的部隊；二、運用新的主動、積極性防衛概念，保護國防部網路與系統，包括運用傳感器（感測器）、軟體和網路簽名，以阻止惡意代碼的攻擊；三、美國政府、民間部門結為夥伴，合作維護電網、運輸系統、金融業等關鍵基礎設施的安全；四、美國與盟邦建造堅強的關係，強化集體網路安全；五、利用科技快速革新、優勢網路人力、國家創造力，加強網路安全人員的培訓，降低網路空間匿名與駭客攻擊的威脅。[12]

在《紐約時報》遭中國大陸駭客入侵後，2013年2月，美國總統行政辦公室公布的《降低美國貿易機密偷竊的行政策略》(*Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*)，提出的「戰略行動項目」(Strategy Action Items)，主要在保護對外貿易機密、企業機密，針對美國智慧財產遭到中共解放軍上海61398部隊駭客攻擊意有所指。美國「人事管理局」(Office of Personnel Management)在2013～2014年亦遭中共網軍持續入侵，引起美國政府的全面警覺。[13] 在歐巴馬政府加強宣導網路威脅、鼓勵民間企業防範、外交上強調保護海外商業機密、修訂合宜商業間諜法令、優先調查並起訴盜取公司及國有商業機密案件之後，美國民眾對中共與俄羅斯駭客的威脅認知增強，預防駭客的經費也擴增，但駭客事件仍層出不窮。[14]

2015年4月《國防部網路戰略》(*The DOD Cyber Strategy*)，是歐巴馬政府有關網路安全的最重要文獻，規範未來5年的網路戰略與執行，提到國防部內部各單位、美國政府部門、美國政府與私人企業、美國政府與外國政府的合作。同時指出中共、俄羅斯、伊朗、北韓是主要的網路威脅來源，連「伊斯蘭國」(Islamic State of Iraq and Syria, ISIS)也運用網路招募人員分送情資。美國網路的國際合作特別將重心置於中東、亞太、北約盟邦。此一文獻揭示美國政府在網路戰略的五大戰略目標與搭配的執行目標，列出美網路戰略的「行動」、「防護」與「合作」等三大主線。在「行動」上，提到：「網路任務部隊」(Cyber Mission Force, CMF)正式建立，以可行的行動方案與計畫實施網路行動，基調從重於防禦，轉為在必要時可主動攻擊。在「防護」上，不止國防部門之內，與企業、外國政府要加強合作，以因應網路攻擊的危害。在「合作」上，強調建立全面的國際合作夥伴關係（如表2）。[15]

2015年《國防部網路戰略》，指出

12 U.S. Department of Defense, *Department of Defense Strategy for Operating Cyberspace* (Washington, DC: U.S. Department of Defense, 2011), pp. 5-12, <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>（檢索日期：2020年7月23日）

13 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, pp. 111-117.

14 歐巴馬政府宣導網路威脅、鼓勵民間企業防範、外交保護海外商業機密、修訂合宜商業間諜法令、優先調查並起訴盜取企業機密案件之後，美國民眾對中國與俄羅斯駭客認知轉而增強，預防駭客的經費也增加。Executive Office of the President of the United States, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, February, 2013, <https://www.justice.gov/criminal-ccips/file/938321/download>（檢索日期：2020年7月23日）

表2　2015年歐巴馬政府《國防部網路戰略》

| 戰略指導 | 執行目標 |
| --- | --- |
| 一、建立及維持立即可用的6,200名「網路任務部隊」，區分爲各地區作戰司令部負責整合的「網路防護部隊」(Cyber Protection Forces)與「作戰任務部隊」(Combat Mission Forces)，及由「網路指揮部」(Cyber Command)負責執行的「國家任務部隊」(National Mission Forces)。 | 第一，策進「網路任務部隊」訓練環境、升遷管道、發展與私部門的交流計畫、支持國家網路教育倡議；建立網路運作的技術能力(Technical Capabilities for Cyber Operations)；確保網路行動指揮與管制機制的調適力、有效發揮；與情報社群合作，建立網路演算、模式、模擬的能力；評估網軍的任務能量。 |
| 二、防護國防部資訊網路，確保國防部資料庫安全，減低國防部的任務風險。 | 建立單一安全架構的聯合資訊環境(Joint Information Environment)，網路防衛焦點從軍種，轉向確保國防部網路安全；整建國防部網路安全架構，找出漏洞及威脅；確保國防部資訊網路聯軍總部(Joint Force Headquarters for DoD Information Network)有效性；評估易毀性、防禦力、效率、恢復能力；提供「國防支援民事當局Defense Support of Civil Authorities」運作；建立採購、情報、反情報、執法之間合作，降低資料流失；支援整個政府反制偷竊智慧財產權。 |
| 三、進行防衛美國國土與重大生存利益，免於破壞性的網路攻擊，造成嚴重後果。 | 發展情報、預警能力以預知威脅、防護國家；建立政府部門間夥伴關係；保護重大基礎設施；建立資訊自動分享工具；評估國防部網路嚇阻態勢與戰略(Cyber Deterrence Posture and Strategy)，建立「國防工業委員會的網路嚇阻小組」(Defense Science Board's Task Force on Cyber Deterrence)、戰略指揮部、參謀首長聯席會議、國防部長辦公室之間合作。 |
| 四、建立及維持可行的網路選項與計畫，控制衝突升高、形塑各個階段的衝突環境。 | 將網路選項、需求，整合爲計畫，聯合參謀、戰略指揮部需同步進行，提供參謀首長聯席會議主席在網軍的聯盟、配置、指定與派任。 |
| 五、與其他國家合作維持國際聯盟、夥伴關係，嚇阻共同威脅及增加國際安全的穩定。 | 美國需在關鍵地區建立夥伴，如強化中東、東北亞地區夥伴的網路及系統，在亞太地區建立戰略夥伴關係，落實國防部的「國際網路安全合作綱領」(International Cyberspace Security Cooperation Guideline)；與北約盟邦合作降低國防部與美國國家利益的風險；尋求解決方案，反制惡意病毒碼擴散；與有能力的國際夥伴一起計畫、訓練網路行動；強化美國與中國大陸的網路對話，維持戰略穩定。 |

資料來源：整理自Department of Defense, *Department of Defense Cyber Strategy*, April 2015, pp. 18-30.

《2004年國防授權法案》(National Defense Authorization Act of 2004)建議在國防部長之下設立「首席網路顧問」(Principal Cyber Advisor)，負責管理國防部網路空間政策與戰略的發展，評估「網路任務部隊」(Cyber Mission Force)、網路攻擊與防衛的行動，

15 U.S. Department of Defense, *The DOD Cyber Strategy* (Washington, DC: U.S. Department of Defense, 2015), pp. 17-31. <https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf>（檢索日期：2020年7月23日）

但不能影響到負責採購、政策、情報、人士與後勤等業務國防次長的職責，也不能干預軍事指揮鏈。「首席網路顧問」透過「網路投資與管理委員會」(Cyber Investment and Management Board)之下「資深行政論壇」(senior executive forum)在關鍵網路議題先行協調。「網路投資與管理委員會」除改善網路預算管理，亦須發展一套網路情報行動政策架構、執行國防部端對端(end-to-end)網路能力評估。[16]

美國國防部在2015年與2011年公布的網路安全戰略最大的不同是，2011年沒有提到中共，2015年卻有9次提及中共，而且強調中共的網路威脅與能力，竊取美國智慧財產權、商業機密與資訊等。它亦指出，美中可透過「國防諮商會談」(Defense Consultation Talks)、「戰略與經濟對話」(U.S.-China Strategic and Economic Dialogue)之下的「網路工作小組」(Cyber Working Group)來加以協商，希望與中方強化「信心建立措施」(Confidence-Building Measures)，降低誤解、誤判，維持兩國的戰略穩定關係。[17] 2015年6月歐巴馬政府揭露美國「人事管理局」個資遭中共竊取。9月，習近平訪美與歐巴馬達成網路安全問題的5項共識，兩人雖承諾推動國際網路空間合適的國家行為準則，卻無重大進展。

2015年《國防部網路戰略》公布之際，當時國防部長卡特(Ashton Carter)在史丹佛大學演講，說明美國在何種情況下，可以使用網路武器來對付攻擊者，並且列出美國自認最大威脅的國家依序為：中共、俄羅斯、伊朗和北韓等。卡特提到，美國國防部在網路安全方面有三大使命：一是防衛國防部的網路、系統和資訊；二是保衛美國國土及國家利益不受重大網路襲擊活動的侵犯；三是集中網路軍隊力量，支援軍事行動和應急計畫。卡特指出，應付網路安全威脅與因應傳統威脅的做法很相似，網路威懾(cyber deterrence)能力是關鍵，企圖阻止惡意攻擊的發生，希望阻止任何入侵行動，並精確追蹤攻擊來源。美國政府與網路安全企業「火眼」(FireEye)、「群擊」(CrowdStrike)、「惠普」(Hewlett-Packard)等，必須建立密切的夥伴關係，以提高美國國防部的因應能力。[18]

二、川普政府網路戰略報告

川普總統上任之後，美國國防部在網路安全採取更具攻擊性的政策取向。這可由美國國防部在2017年2月公布的「國防科學董事會」(Defense Science Board)建議看出端倪。該董事會明確指出美國受到網路攻擊來自中共、俄羅斯的主要大國(Major Powers)與伊朗、北韓的次等大國(Lesser Powers)。因此，建議美國國防部：一、規劃及執行針對性的多套量身打造的嚇阻行動(Plan and Conduct

16 DOD, *The DOD Cyber Strategy*, 2015, pp. 29-30.

17 *Ibid*., p. 28.「網路首席顧問」由主管國土防禦與全球安全事務的助理國防部長拉普諾(Kenneth Rapuano)兼任。

18 Ashton Carter, "Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity," *Secretary of Defense Speech, U.S. Department of Defense*, April 23, 2015, <https://www.defense.gov/Newsroom/Speeches/Speech/Article/606666/drell-lecture-rewiring-the-pentagon-charting-a-new-path-on-innovation-and-cyber/>（檢索日期：2020年8月21日）

Tailored Deterrence Campaigns)，包括平時、灰色地帶衝突及戰爭危機；二、創造美國主要攻擊系統（網路、核武、傳統武器長程攻擊載台）同時具備網路復甦、支援關鍵基礎設施的能力，使美國軍力具有第二擊與網路韌性的條件，以確保中、俄大國的網路攻擊，必須付出無法承受的代價；三、美國政府必須強化網路基礎能力，判別網路攻擊來源、軍隊網路韌性、創新科技，以保障最重大基礎設施的安全。[19] 即使網路國防安全政策方向調整為攻擊性，但身兼「國家安全局長」與「網路指揮官」的亞歷山大將軍承認「網路指揮部缺乏明確授權與交戰規則」，以有效執行美國的網路安全政策目標，亦缺乏公私部門共同防衛、有效夥伴關係的機制。[20]

2017年12月，川普政府第一份「國家安全戰略」報告，將中共、俄羅斯定位為「修正主義強權」(Revisionist Powers)、「戰略競爭者」(Strategic Competitors)，指控中共利用「網路遂行經濟戰及其他惡意活動」(Cyber-Enabled Economic Warfare and Other Malicious Activities)取得美國智慧財產權、創新科技。[21] 因此，美國政府在網路時代的安全上，必須採取下列優先行動：判讀及列出風險順序；建立具有防衛能力的政府網路系統；嚇阻及破壞惡意的網路行為者；改進資訊分享與警覺性；部署多層次的網路防衛。[22]

2018年4月，《達成及維持網路空間優勢：美國網路指揮部願景》(*Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*)，指出美國必須增加韌性，採取更靠近對手活動源頭的「向前防衛」(Defend Forward as Close as Possible to the Origin of Adversary Activity)，因為對手持續在武裝衝突的門檻下運作，削弱美國的機構，並在戰略上獲益。美國對手的網路攻擊行動持續增加，是因為機會成本與代價低廉。「網路指揮部」除了是情報社群一環之外，特別需要與「國防資訊系統局」(Defense Information Systems Agency)與「國家安全局」合作，採取主動權，破壞對手的行動自由。[23] 不過，「網路指揮部」的

19 U.S. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Defense Science Board (DSB) Task Force on Cyber Deterrence* (Washington, DC: U.S. Department of Defense, 2017), <https://apps.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>（檢索日期：2020年7月23日）

20 U.S. Congress, *Cyber Strategy and Policy*, Hearing, Committee on Armed Services, U.S. Senate, 115th Congress, First Session, March 2, 2017, <https://www.armed-services.senate.gov/imo/media/doc/Alexander_03-02-17.pdf>（檢索日期：2020年7月23日）

21 The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), pp. 21, 35.

22 *Ibid*., p. 13.

23 U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, April, 2018, <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>（檢索日期：2020年7月23日）；吳俊德、賴達文，〈2011-2018年美國網路戰略沿革〉，《國防安全週報》，第16期，2018年10月5日，頁20-25。

願景沒有明確指出，美國將在網路空間使用「先制」或「攻擊」的用語。

2018年5月，美國《國土安全部網路安全戰略》(*Department of Homeland Security Cybersecurity Strategy*)，提出至2023年的5年願景與5大支柱，其中與國防相關的是，降低網路脆弱性、防護關鍵基礎設施。[24] 2018年9月，美國《國防部網路戰略總結》(*Summary of Department of Defense Cyber Strategy 2018*)報告公布，取代歐巴馬政府的2015年《國防部網路戰略》，其中最重大的調整是，美國軍隊將「使用攻擊性網路能力與創新性概念，確保在全方域的衝突中網路空間作戰得以發揮」(employ offensive cyber capabilities and innovative concepts that allow for the use of cyberspace operations across the full spectrum of conflict)，亦可先制攻擊(Preempt)、擊敗或嚇阻針對美國關鍵基礎設施的惡意網路活動（如表3）。[25]

川普政府在2018年9月《美國國家網路戰略》(*National Cyber Strategy of the United States of America*)，宣稱此乃2003年之後13

表3　川普政府國防部公布的網路戰略報告

| | |
|---|---|
| 2018/4《網路指揮部願景》(Command Vision for U.S. Cyber Command) | 1.達成及維持優於對手的能力。創造網路空間優勢，以便增強在各領域的行動。<br>2.創造資訊優勢以支援作戰結果，以及達到戰略影響的成效。<br>3.運用網路空間以便增加靈活性及機動反應。<br>4.擴張、深化及善用夥伴關係。 |
| 2018/9《2018國防部網路戰略總結》(2018 Department of Defense Cyber Strategy Summary) | 1.建立具有毀滅性的聯合武力加快發展網路能力、增進創新與靈活性、利用自動化及數據分析，有效確認威脅及防護、採用成熟的民用網路技術能力。<br>2.網路空間的競爭及嚇阻：嚇阻惡意的網路行爲、持續對抗日常惡意網路活動、增強美國關鍵基礎設施的恢復能力。<br>3.加強盟友關係及吸引新的夥伴加入：與民間建立互信的夥伴關係、促進國際夥伴關係、加強網路空間的行爲規範。<br>4.改革國防部：將網路警覺性併入國防部機關文化、加強網路安全課責性、尋找價格合理與靈活耐用的軟硬體採購方案、運用白帽駭客集體找出網路弱點。<br>5.培育相關人力：維持一組隨時準備好的網路人員、增強國家網路人才、在國防部建立軟硬體專長的核心能力、建立網路頂尖人才的管理計畫。 |

資料來源：作者整理自美國國防部網站資料。

24 其他的支柱包括：風險判定(Risk Identification)；阻止網路空間犯罪行為；減輕後果影響；達成網路安全效果。國土安全部亦列出網路安全的指導原則：風險處理優先排序；代價與有效性的評估；創新與靈活性；聯邦與非聯邦機構的協調與合作；全球國際性合作共同創建開放、互通與安全可靠的網路；商務、國際安全、表達自由與創新同時擁有的平衡發展；國家隱私、民權、個人自由價值的確保。U.S. Department of Homeland Security, *Department of Homeland Security Cybersecurity Strategy* (Washington, DC: U.S. Department of Homeland Security, 2018), pp. 1-6, <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf>（檢索日期：2020年7月23日）

25 U.S. Department of Defense, *Summary-Department of Defense Cyber Strategy 2018* (Washington, DC: U.S. Department of Defense, 2018), p. 2.

年的第一本由白宮所公布的網路戰略報告，指出：「經由保護網路、系統、功能及數據確保國土防衛」，改善運輸、海事、太空網路安全；培養安全、數位經濟、強大國內創新，以促進美國經濟繁榮」；強化美國能力以確保和平與安全；與友邦盟國協調建立國際「網路嚇阻倡議」(Cyber Deterrence Initiative)，在必要時，懲罰那些惡意網路使用者；擴大美國海外影響力，拓展一個開放、互通性、可靠、安全的網路；建立國際網路能量夥伴關係，抵消全球競爭者（暗指中共）的影響力。[26] 依據國家安全顧問波頓(John Bolton)的說法，此一報告要在網路攻擊行動決策上，揚棄歐巴馬政府過度強調程序而非政策辯論，偏向網路防禦而極少採取攻擊的政策，但亦坦承「網路嚇阻」說比做容易，攻勢行動必須保密，多說也會將美軍能力曝光，致使對手有準備方案。[27]

2019年1月，「國家情報總監」公布《美國國家情報戰略》(*National Intelligence Strategy of the United States of America*)將「網路威脅情報」(cyber threat intelligence)列在反恐、反擴散、反情報與安全的重要性之前，指出美國情報社群需要提升對手可能使用網路行動的警覺，將可付之行動的「網路威脅情報」分送各部門以防護關鍵基礎設施；強化外交、軍事、經濟、金融、執法等措施，嚇阻、反制惡意網路行為者與活動。[28] 美國國防部於2019年7月公布2019～2023會計年度的《數位現代化戰略》(Digital Modernization Strategy)指出四項目標，分別為：創新以取得競爭優勢；效率與能力提升到最佳化；確保靈活韌性防衛態勢的網路安全；培養一支立即派上用場的數位戰士，而國防部資訊長(Chief Information Officer)的優先任務依序是網路安全、人工智慧、雲端、指管通訊($C^3$)。[29]

美國國防部在2019年6月《印太戰略報告：整備、夥伴關係與促進一個聯網區域》(*Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region*)指出，增強預防、嚇阻與因應網路攻擊的工具，美國與日本、澳洲透過定期訊息交換和評估，加強在網路和太空領域的合作，提高共同行動的能力，集資協助印太地區基礎設施的建構，以維持印太地區穩定。[30] 2020年5月，美國白宮公布的《美國對中華人民共和國的戰略途徑》(*United States*

26 The White House, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, 2018), p. I, 10, 25.

27 John Bolton, *The Room Where It Happened: A White House Memoir* (New York: Simon & Schuster, 2020), pp. 176-182.

28 U.S. Office of Director of National Intelligence, *National Intelligence Strategy of the United States of America* (Washington, DC: U.S. Office of Director of National Intelligence, 2019), p. 11.

29 U.S. Department of Defense, *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY 19-23* (Washington, DC: U.S. Department of Defense, 2019), p. 4.

30 U.S. Department of Defense, *Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region* (Washington, DC: U.S. Department of Defense, 2019), pp. 18-27, <https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF>（檢索日期：2020年7月23日）

*Strategic Approach to the People's Republic of China*)，特別針對中共惡意網路空間行為(Malicious Cyber Activities)，美國承諾與盟國、志趣相投的夥伴合作，要求北京遵守負責任的國家行為規範。美國國防部亦增加網路空間和太空能力的投資，支援進攻性和防禦性的網路空間作戰(Offensive and Defensive Cyberspace Operations)，以嚇阻與反制中共軍隊取得科技優勢的可能性。[31]

## 參、中共的網路戰略

中共「信息戰（資訊戰）之父」沈偉光在1987年於《解放軍報》刊登〈信息戰的崛起〉一文。沈偉光認為「信息戰」呈現形式有心理戰、情報戰、電子戰、電腦病毒戰、精確戰、隱形戰等。[32] 他認為「信息戰」在軍事領域有十大影響：爭奪制信息權；軍隊結構轉向信息型；戰爭威懾日增；不戰而屈人之兵；回（在）家打仗成為可能；人的因素第一；決勝取決於大腦思維戰；高技術戰爭更激烈；強化軍隊信息建設；軍事軟科學作用增加。[33] 中共專家進入21世紀後，加速對軍事信息安全的研究，提到軍事洩密、駭客攻擊、信息戰能力不足的三大問題，指出資訊安全具有「六性」特徵，亦即保密性、完整性、可用性、可控性、佔有性、責任性，並由物理安全、通信安全、輻射安全（電磁輻射引起的資訊擴散）、計算機（電腦）與網路安全等構成；它有七大環節（原理）：風險分析、保障策略、主動防護、深透檢測、安防認證、動態響應、災難恢復。[34]「網路安全」或「網路戰」的用語，逐漸凌駕「信息安全」或「信息戰」，能否打贏網路戰，成為中共軍隊能否打贏高技術戰爭的重要關鍵，尤其需要將美國、美軍當作重點研究對象。「網路戰」成為超限戰的一種，具有跨國性、隱蔽性、無規則性巨大破壞力，而這種「威脅對網路大國美國的危害，肯定比其他國家更甚」。[35]

2012年中共十八大報告在「加速推進國防與軍隊現代化」一節提到「高度關注海洋、太空、網絡空間安全」。中共三位解放軍軍官在一篇論文中，分析網路戰具有下列特點：作戰的力量多元、空間廣闊、行動隱蔽、雙方不對稱、效果顯著，但敵人的網路戰也會破壞指揮資訊系統、滲透軍事資訊網路、侵入武器控制網路與癱瘓空防作戰系統。[36] 共軍少將、總參四部（電子反制與雷達）副部長郝葉力，提到網路戰是「信息時代的原子彈」，有5種基本作戰樣式：情報

31 The White House, *United States Strategic Approach to the People's Republic of China* (Washington, The White House, 2020), pp. 7-16, <https://www.whitehouse.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.20.20.pdf>（檢索日期：2020年7月23日）

32 沈偉光，《新戰爭論》（北京：人民出版社，1997年），頁121。

33 沈偉光，〈信息戰對人類社會的深刻影響及戰略對策〉，沈偉光主編，《中國信息戰》（北京：新華出版社，2005年），頁259。

34 張春江、倪健民主編，《國家信息安全報告》（北京：人民出版社，2001年），頁152-173；劉由芳、韓強主編，《軍事信息安全原理》（北京：國防大學出版社，2005年），頁14-18。

35 喬良、王湘穗，《超限戰與反超限戰》（武漢：長江文藝出版社，2016年），頁100。

36 田成信、張峰、江飛，〈網絡戰對作戰的影響及對策〉，《國防科技》，第35卷第5期，2014年10月，頁103-104。

戰、阻癱戰（控網和癱網）、防禦戰、心理戰與網電一體戰；美國人最怕的是「天網被破」、「本土被襲」、「航母被毀」、「網路被癱」。[37]

中共與美國在網路空間的軍事運用能力雖有距離，但在正式建立「戰略支援部隊」之前，即已探討網路軍事防禦性、攻擊性，以發揮「不對稱作戰」的效果。中共在2011年組建「用來訓練其他網絡部隊的網絡藍軍」，而在整體的軍兵種中，「海陸空天電網，網就是最後一個層級」。[38] 2014年2月，中央網路安全和信息化領導小組成立，習近平將網路安全與信息化並舉，並提升原有國務院組織層級。2014年6月，中共解放軍成立「網絡空間戰略情報研究中心」，旨在「匯集各方信息渠道和信息源，形成權威的網絡情報研究資源；牽頭軍內外相關動態情報力量，組建高效網絡空間動態跟蹤研究體系」，以擴大「軍隊在網絡空間研究領域的影響力」。[39] 2015年，中美兩國先後正式成軍「網路任務部隊」；12月，習近平宣布推動國防與軍隊改革，成立「戰略支援部隊」，由原先的總參三部（技術偵察）、四部（電子反制與雷達）及資訊部組建而成，兼具網路攻擊、防禦及偵察等功能，可遂行資訊戰，在複雜的電磁環境下，彌補解放軍能力的不足。[40] 中共亦加強網路空間作戰力量、關鍵設備自主化與國產化的水準，發揮網路空間意識形態安全的力量。[41] 中共發展網路攻擊行動，不僅威脅其他區域內國家的關鍵節點(Critical Nodes)，更提升對美國「反介入及區域拒止」(Anti-Access and Area Denial, A2/AD)的能力，使美軍在東海、臺海、南海的軍事干預面臨更大的風險。

由上海社會科學院公布的《中國網路空間安全發展報告(2015)》，指出網路空間與核子、航太領域並列為三大戰略空間，「網絡空間作戰已經取代陸戰場時代的坦克、海戰場的航空母艦、空戰場的戰鬥機，成為貫穿未來戰場的主要作戰行為。」[42] 以軍隊為主體構建國家網路空間安全力量是國際的通用做法，有助於網路空間態勢感知能力、網路空間防禦能力、網路空間反應能力、網路空間調查取證能力、網路空間進攻能力在國

37 郝葉力，〈大國網絡戰略博奕與中國網絡強國戰略〉，《國際關係研究》，2015年第3期，2015年，頁7-12。

38 新京報，〈國防白皮書披露軍兵種發展戰略　將加快網絡空間力量建設〉，《人民網》，2015年5月27日，<http://military.people.com.cn/BIG5/n/2015/0527/c1011-27061489.html>（檢索日期：2020年7月23日）

39 齊洋、王瑤，〈我軍網絡空間戰略情報研究中心揭牌成立〉，《解放軍報》，2014年6月26日，<http://news.mod.gov.cn/big5/pla/2014-06/26/content_4518762.htm>（檢索日期：2020年7月23日）

40 中華人民共和國國防部，〈國防部新聞發言人就深化國防和軍隊改革有關問題接受媒體專訪〉，《國防部網》，2016年1月1日，<http://www.mod.gov.cn/affair/2016-01/01/content_4635502.htm>（檢索日期：2020年7月23日）；U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2016* (Washington, DC: U.S. Department of Defense, 2016), pp. 2-3; U.S. Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (Washington, DC: U.S. Defense Intelligence Agency, 2019), pp. 45, 97-98.

41 嚴明，〈高度關注網絡空間安全〉，《南京政治學院學報》，第6期，2013年，頁111-113。

42 惠志斌、唐濤主編，《中國網路空間安全發展報告》（上海：社會科學文獻出版社，2015）。

家範圍內的有效整合」，以因應美國對中共進行全面圍堵與遏制。[43]

2015年5月，北京公布《中國的軍事戰略》白皮書，反映中共軍事戰略的「全面性」，除傳統軍事威脅，也關注非傳統軍事威脅，涉及海洋、太空、網路、核力量等四個重大安全領域。此一白皮書指出中共軍隊應「加快網路空間力量建設，提高網路空間態勢感知、網路防禦、支援國家網路空間鬥爭和參與國際合作的能力，遏控網路空間重大危機，保障國家網路與信息安全，維護國家安全和社會穩定」。[44] 這與2015年美國國防部所揭櫫的網路安全戰略近似。中共白皮書亦提到，不少國家都在發展網路空間軍事力量，「中國是黑客攻擊最大的受害國之一，網絡基礎設施安全面臨嚴峻威脅，網絡空間對軍事安全影響逐步上升」。

2016年12月，中共「國家互聯網信息辦公室」發布《國家網絡空間安全戰略》，其中涉及網路國防安全部分有：一、「謀求戰略主動權的競爭日趨激烈」，因為「個別國家強化網路威懾戰略，加劇網路空間軍備競賽」；二、若要和平，就需「信息技術濫用得到有效遏制，網絡空間軍備競賽等威脅國際和平的活動得到有效控制，網絡空間衝突得到有效防範」；三、若能確保「網絡安全風險得到有效控制，國家網絡安全保障體系健全完善，核心技術裝備安全可控，網絡和信息系統運行穩定可靠」，才能得到真正的安全。中共強調網路防禦的原則，如「不得使用或威脅使用武力的原則，防止信息技術被用於與維護國際安全與穩定相悖的目的，共同抵制網絡空間軍備競賽、防範網絡空間衝突。反對以國家安全為藉口，利用技術優勢控制他國網絡和信息系統、收集和竊取他國資料，更不能以犧牲別國安全謀求自身所謂絕對安全」。[45] 此一論調與中共為了要終結核武，就必須發展核武相似。在網路安全的道德訴求難以實現之下，必須要發展網路攻擊能力，方能降低美國的網路嚇阻與攻勢作為。這顯示中共以訴求網路防禦為名，也以發展攻勢能量為實。

中共主張國家機關控制的「網路空間主權」，相較於開放、自由的網路使用，更著重消極被動的內部控制。如上述《國家網絡空間安全戰略》報告，指出：一、「堅決反對通過網路顛覆我國國家政權、破壞我國國家主權的一切行為」；二、「防範、制止和依法懲治任何利用網路進行叛國、分裂國家、煽動叛亂、顛覆或者煽動顛覆人民民主專政政權的行為；防範、制止和依法懲治利用網路進行竊取、洩露國家秘密等危害國家安全的行為；防範、制止和依法懲治境外勢力利用網路進行滲透、破壞、顛覆、分裂活動」。中共一如其他各國重視關鍵基礎設施的防護，這些設施包括：公共通信、廣播電視傳輸等服務的基礎資訊網路；能源、金融、交通、教育、科研、水利、工業製造、醫療衛

43 中國新聞網，〈報告：中國應以軍隊為主體整合國家網絡空間安全力量〉，《人民網》，2015年4月27日，<http://politics.people.com.cn/n/2015/0427/c70731-26910719.html>（檢索日期：2020年7月23日）

44 中華人民共和國國防部，《中國的軍事戰略》（北京：國務院新聞辦公室，2015），《國防部網》，<http://www.mod.gov.cn/regulatory/2015-05/26/content_4617812.htm>（檢索日期：2020年7月23日）

45 中國網信網，〈《國家網絡空間安全戰略》發布〉，《國防部網》，2016年12月27日，<http://www.mod.gov.cn/big5/regulatory/2016-12/27/content_4768313.htm>（檢索日期：2020年7月23日）

生、社會保障、公用事業等領域和國家機關的重要資訊系統，重要互聯網應用系統等。該報告指出：「採取一切必要措施保護關鍵資訊基礎設施及其重要資料不受攻擊破壞」；「堅持技術和管理並重、保護和震懾並舉，著眼識別、防護、檢測、預警、回應、處置等環節，建立實施關鍵信息基礎設施保護制度，從管理、技術、人才、資金等方面加大投入，依法綜合施策，切實加強關鍵資訊基礎設施安全防護」。國家關鍵資訊基礎設施防護是「政府、企業和全社會的共同責任」，更要「建立政府、行業與企業的網路安全資訊有序共用機制，充分發揮企業在保護關鍵資訊基礎設施的重要作用」。[46]

中共外交部2017年2月發布《網絡空間國際合作戰略》白皮書，再度提到加快網路建設、提高網路態勢感知及網路防禦能力，加強網路空間中的攻擊、監控、竊取等能力的迫切感。2019年7月，北京公布《新時代的中國國防》指出：網路安全是「中國面臨的嚴峻安全威脅」，需要「建設與中國國際地位相稱，與網絡強國相適應的網絡空間防護力量，築牢國家網絡邊防，及時發現和抵禦網絡入侵，保障信息網絡安全」。中共軍隊必須「加快網絡空間力量建設，大力發展網絡安全防禦手段」。其中，指出「戰略支援部隊」是「新型作戰力量」、「新質作戰能力的重要增長點」，包括：「戰場環境保障、信息通信保障、信息安全防護、新技術試驗等保障力量。按照體系融合、軍民融合的戰略要求，推進關鍵領域跨越發展」。[47]

## 肆、美國與中共對網路戰略的相互評估

美國國防部公布的年度中共軍力發展報告，對中共「網路作戰」(Cyber Operations)的解讀是，中方主張利用攻勢性作為，贏得「網路空間優勢」，嚇阻或降低對手（美國）以軍事行動攻擊中共的能力，認為網路攻擊是低廉的嚇阻，可向對手傳遞中方的能力與決心，在升高衝突時，可善加處理及運用。中共網路攻擊行動針對美軍、民間的關鍵節點，以低成本達到「反介入與區域拒止」的效果。「網路作戰」能力是，達成資訊優勢、有效反制強敵（美國）不可或缺的一環，但中共認為其網路人員訓練與創新不足有待提升。[48] 根據美國國防部的判斷，中共加速網路戰的發展，而且會在軍事衝突中，鎖定美國指管及後勤網路，在戰爭一開始就達到遲滯美國行動能力的目標。美國評估中共認為若能「完全擾亂」(Completely Disrupt)美國網路系統，就可癱瘓美國並取

46 同註44。有關中美網路空間戰略不同，請見蔡翠紅，〈中美網絡空間戰略比較：目標、手段與模式〉，《當代世界與社會主義》，2019年第1期，2019年，頁47-49。

47 中華人民共和國國防部，《新時代的中國國防白皮書》（北京：國務院新聞辦公室，2019年），請參見第三節。

48 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: U.S. Department of Defense, 2019), pp. 57, 64; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2018* (Washington, DC: U.S. Department of Defense, 2018), p.61; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2015* (Washington, DC: U.S. Department of Defense, 2015), p. 33.

得戰場的優勢。中共在網路防禦部分，可蒐集情報與攻防相關數據，侷限美軍行動，並與可直接、間接造成傷亡的「動能攻擊」(Kinetic Attacks)，結合成為「兵力倍增器」(Force Multiplier)。[49]

美國「網路作戰」的思維，極注意中共「戰略支援部隊」與「軍民融合發展委員會」的相關訊息。該部隊旨在鞏固網路與其他資訊相關要素時，整合發揮國家層級的偵察、攻擊、防禦協同作用。「戰略支援部隊」員額10萬人，包括七支軍事航天部隊、三支網路和信息戰部隊共10個單位，並以「強化技術偵察、電子對抗、網路攻防和心理戰等新型作戰支援能力」為目標。[50]「戰略支援部隊」強調太空與網路空間的重要性，因此，美國國防部指出該部隊「在以臺灣緊急的設定中，負責電子戰、網路行動，任務之一是在現代化的資訊戰中，掌握及維持戰場資訊控制」。[51]

美國國防部擔憂中共經由軍民融合，結合科學突破與軍事運用結合運用。川普政府認為中共「華為公司」正是利用民營企業的外衣，為中共軍隊採購外國技術，混淆國防與民間部門的界限。2020年5月，川普政府宣布吊銷與中國解放軍院校相關研究生的簽證。最主要顧慮是，中共長期以來透過「民掩護軍」，對美國與西方國家進行「異國採花，中國釀蜜」，學習與偷取西方科技，再回頭過來對西方國家造成科技能力凌駕的成果。中共利用人工智慧、先進機器人，運用於強化預測、製造及指管通電監測與偵察、無人載具、人機組合(Human-Machine Teaming)、群集科技(Swarming Technology)、殺傷性自動武器等領域。美國亦認為中共藉由半導體與先進演算，來增進網路行動、武器設計、縮短研發周期；利用量子科技來確保全球通訊、強化演算與解碼能力(Computing and Decryption Capabilities)、偵測隱形載台(Detection of Stealth Platforms)及強化潛艦航行；極音速及導能武器，來進行全球打擊、擊敗飛彈防禦系統及反衛星、反無人機能力；利用先進材料與可替代能源以改進軍事設備與武器系統。[52] 這使與共軍有密切關係的網路資通信科技公司，以「合法掩護非法」，經由各種民間管道取得美國科技，並壯大中共軍力。[53]

美國政府宣稱它與中共最大不同是，不會將竊取的資訊用於企業牟利。美國國防部一直追蹤中共對美國政府、國防部及在各地的電腦系統的入侵與竊取資訊，因為中共

49 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2019*, pp. 64-65.

50 歐錫富、黃宗鼎主編，《2018中共政軍發展評估報告》（臺北：國防安全研究院，2018年），頁45，106；林穎佑，〈中共戰略支援部隊的任務與規模〉，《展望與探索》，第15卷第10期，2017年10月，頁119。

51 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2019*, pp. 65, 88.

52 *Ibid*., p. 102.

53 Bill Gertz,“Pentagon: Major Chinese Companies Have Close Military Links,” *Washington Times*, June, 25, 2020, <https://www.washingtontimes.com/news/2020/jun/25/pentagon-major-chinese-companies-have-close-milita/>（檢索日期：2020年7月23日）

利用其網路能力，針對美國外交、經濟、學術和國防工業基地(Defense Industrial Base, DIB)部門，蒐集情報、敏感資訊以取得軍事優勢。這種「網路間諜」行為不僅使中共國防高科技產業受益，也驅使中共的軍事現代化。透過對美國領導階層觀點的瞭解，也可運用於外交事務與「一帶一路」的談判。因此網路竊取者不限於共軍，中共「國家安全部」亦竊取美國民航客機引擎等敏感科技。同時，共軍可在危機事件前後，先行掌握美國國防網路、軍事部署、後勤及相關軍事能力的狀況，增強因應美方軍事行動的能力。

中共與美國既是戰略競爭者，雙方均想在軍事衝突中具有嚇阻、延遲、破壞和降低對手能力的操作，雙方也都防範軍事優勢被侵蝕，關鍵基礎設施和經濟繁榮被破壞。[54] 北京注意到，美國與澳洲、日本分別在共同防禦或安保條約中，將網路戰納入集體防禦與安全想定的一環。北京特別注意美國在其官方文獻中，將中共、俄羅斯、北韓、伊朗網路威脅的排名逐年提前。例如，2015年6月《美國軍事戰略》(*National Military Strategy*)中共排名第四，2016年2月《國防態勢聲明》(*Defense Posture Statement*)排名第二，2018年10月《美國國防戰略》(*National Defense Strategy*)排名第一。[55] 中共期刊許多論述亦聚焦對中美網路安全關係的競爭與合作、網路空間戰略的比較、川普網路戰略的調整等。

中共由2013年「史諾登事件」(The Snowden Affair)看出美國的資訊霸權與雙重標準。川普政府上台之際，如中共在2017年《網絡空間國際合作戰略》，對中美的網路關係認為競爭中有合作，尤其是兩國針對網路安全議題有多次對話與協商。然而，兩國網路戰略競爭永遠大於合作。中共學者專家指出中美兩國對於網路自由、治理與主權問題有立場差異，相互指責對方為駭客攻擊的來源，而在網路軍備建設上相互提防。[56] 復旦大學教授蔡翠紅歸納美國網路空間戰略有五點：「控制網絡核心和主導運行規則」、「強化關鍵基礎設施網絡安全」、「保持網絡空間綜合實力優勢」、「促進政企緊密合作」、「在國際上打造聯盟和夥伴關係」，這些與中共強調網路主權、網路治理架構、自主網路技術發展、國家間合作與和平發展治理環境，有不同的重心。[57]

中共軍方對網路軍備控制，如何以國際力量制約美國也早有研究。北京以多邊機制對照美國單邊主導，在多邊機制中，結合非民主體制的國家，形成以中共為核心的集團（如「上海合作組織」）立場。西方國家主導的規範，不管是《塔林手冊》(*Tallinn Manuel*)或《網路空間信任與安全巴黎呼籲》(*Paris Call for Trust and Security in Cyberspace*)，中共抱持觀察、防範甚於參與、倡議或接

54 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2019*, pp. 65, 104.

55 Lyu Jinghua, "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Defense' to 'Defending Forward'," *Lawfare*, October 19, 2018, <https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward>（檢索日期：2020年8月20日）

56 奕文莉，〈中美在網絡空間的分歧與合作途徑〉，《現代國際關係》，2012年第7期，2012年，頁29-30。

57 蔡翠紅，〈中美網絡空間戰略比較：目標、手段與模式〉，頁44-47。

受的立場。北京不完全拒斥《塔林手冊》，甚至同意武漢大學國際法學者黃志雄參與2.0新版的討論過程。北京主張國家網路主權，禁止網路空間武力使用，而《塔林手冊》允許對已發生或即將發生的網路武裝攻擊，可行使武力自衛權（先發制人）及採取依比例的反制措施，對關鍵基礎措施攻擊時需有慎重的責任(Duty of Care)等規範，對中共網路安全有不利的影響。[58] 中共尤其擔心美國對中共關鍵基礎設施施以網路攻擊，必須提升網路攻防兼備的能量。中共專家瞭解《塔林手冊》是西方及美國專家主導下的產物，沒有法律拘束力，仍呼籲網路空間必須「去軍事化」或「網路裁軍」。雖不排除在「信息安全、網絡安全、重大基礎設施安全保護方面出現一些單邊、雙邊或多邊的承諾」，但中共與美國兩國均沒有參與由法國總統馬克宏(Emmanuel Macron)發動連署的《網路空間信任與安全巴黎呼籲》。[59]

2015年9月，習近平與歐巴馬達成推動國際網路行為準則的共識。2016年5月、11月，中共外交部軍備控制司司長王群與美國國務院「網路問題協調人辦公室」(Office of the Coordinator for Cyber Issues)負責人潘特(Christopher Painter)主談的「國際網路空間規範及相關問題資深專家會議」，前後召開兩次會議。[60] 中共與美國均期待達成網路安全合作框架，尤其避免網路攻擊關鍵基礎設施，但實際發展卻是在低層次的打擊「網路犯罪」，有些司法協助合作，未能上升到高層次的軍事規範。[61] 值得注意的是，美中兩國亦在2016年5月、12月召開針對外太空的安全對話。川普總統上台之後，中美展開關稅、經貿多輪的談判，習近平不再提建立「新型大國關係」，加上兩國均強化網路攻擊的戰略，短期內幾無可能達成「信心建立措施」。

2017年4月，川普與習近平在佛羅里達州「海湖莊園」(Mar-a-Lago)會晤，兩人同意設立四個部長層級的「全面對話機制」如「外交與安全對話」(Diplomatic and Security Dialogue)、「執法與網路安全對

58 崔文波，〈塔林手冊對我國網絡安全利益的影響〉，《江南社會學院學報》，第15卷第3期，2013年9月，頁24-25。請見規則第9條、15條的討論；Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), p. 36, 63.

59 吳翔、翟玉成，〈網絡軍控：倡議、問題與前景〉，《現代國際關係》，2011年第12期，2011年，頁20；黃志雄，〈國際法視角下的網絡戰及中國的對策〉，《現代法學》，第37卷第5期，2015年9月，頁156。Erica D. Borghard and Shawn W. Lonergan, "Confidence Building Measures for the Cyber Domain," *Strategic Studies Quarterly*, Vol. 12, Issue 3, Fall 2018, pp. 30-31.

60 Christopher Painter, "International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms," *Statement Before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*, May 25, 2016, <https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm>（檢索日期：2020年7月23日）

61 耿召，〈特朗普時期中美網絡安全合作分析〉，《美國問題研究》，2018年第2期，2018年，頁167；顏琳、陳俠，〈美國網絡安全邏輯與中國防禦性網絡安全戰略的建構〉，《湖南師範大學社會科學學報》，第4期，2014年，頁34-40；倪海寧，〈美軍網絡戰理論和實踐〉，《國際資料信息》，第7期，2008年，頁14-18。

話」(Law Enforcement and Cyber Security Dialogue)、「社會與文化對話」(Social and Cultural Dialogue)、「全面經濟對話」(Comprehensive Economic Dialogue)。其中，中美「外交與安全對話」在2017年6月、2018年11月召開兩次，雖承諾針對「網路與太空安全進行諮商，強化在核武與戰略議題深化溝通」，卻無進一步發展。美國與中共在2017年10月唯一召開的「執法與網路安全對話」會議，由美國國土安全部、司法部長與中方公安部長共同主持。相較於歐巴馬在一年之內（2015年12月；2016年6月；2016年12月）舉行三輪部長層級「打擊網路犯罪及相關事項高層聯合對話」(High-Level Joint Dialogue on Combating Cyber Crimes and Related Issues)，川普總統顯然無意延續此一對話機制。美國與中共在「執法與網路安全對話」會議，重申兩國在網路安全五點共識，願意及時分享網路犯罪、暴力恐怖活動等相關資訊，對刑事司法協助請求迅速回應。更難得的是，兩國「考慮未來在關鍵基礎設施網路安全努力(Considering Future Efforts on Cybersecurity of Critical Infrastructure)，並透過熱線機制，就緊急網路犯罪與重大網路安全事件等，及時在領導或工作階層進行溝通。」[62]

川普政府的自由開放「印太戰略」認定中共從事全球性的網路偷竊，鎖定智慧財產、機密企業與科技資訊等領域。[63] 川普政府在網路安全的議題上，加深對中共警戒，由雙邊對話解決，調整為單方政策作為，更在國會議員要求下，朝向對中共網路資通信大廠的制裁發展。2020年5月，美國商務部延續對「華為公司」的禁令。美國國務卿蓬佩奧(Mike Pompeo)痛斥「華為公司」是不值得信賴的供應商，是中共的工具，不僅偷竊美國科技，也協助伊朗逃避制裁。美國警告歐洲、東南亞國家讓「華為公司」參與電信基礎設施建造的危險性。8月，蓬佩奧更發動「乾淨網路」(Clean Network)計畫，圍堵「華為公司」；北京隨之提出「全球數據安全倡議」與美國互別苗頭。

從川普政府的角度，「印太戰略」面臨最大的挑戰來自中共，除了傳統的陸、海、空、太空空間優勢爭奪之外，網路空間早已成為安全較勁的新領域。尤其是網上數據經由物聯網大量成長，加上5G通信使得新關鍵基礎設施，如自動駕駛車輛與智慧電網，可極致發揮。川普除「科技圍堵」中共之外，也承諾保護印太地區國家的資料跨境流動，網路安全免於受到威脅，促使數位經濟得以成長，建立「數位鏈結及網路安全夥伴」(Digital Connectivity and Cybersecurity Partnership)，擴大美國科技出口，經由技術援助支持通訊基礎設施發展，協助夥伴國家建立網路安全能量，以因應共同的威脅。[64]

62 “First U.S.-China Law Enforcement and Cybersecurity Dialogue Summary of Outcomes,” *U.S. Department of Justice*, October 6, 2017, <https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue>（檢索日期：2020年7月23日）

63 U.S. Department of Defense, *Indo-Pacific Strategy Report* (Washington, DC: U.S. Department of Defense, 2019), p. 8.

64 “Secretary Pompeo's Remarks at the Indo-Pacific Business Forum,” *American Institute in Taiwan*, July 30, 2018, <https://www.ait.org.tw/secretary-pompeos-remarks-at-the-indo-pacific-business-forum/>（檢索日期：2020年7月23日）

中共認為川普政府的網路安全戰略有諸多調整，不利於中美關係未來發展。中共學者普遍認為：在網路安全領域相互認知不斷惡化，在整體關係雪上加霜；網路安全成為兩國國家安全對抗的「新前線」；川普以利益導向，出現「泛網路安全化」、「國內政治化」，使兩國無法在科技、經貿領域正常合作等。他們也注意到川普政府增加對網路基礎設施、新技術的投資，強化海上運輸網路安全的國際規範，而且藉助「網路威懾加強防禦」。[65] 美國與中共在網路安全威脅，是合作取得協議，或是維持對立甚至對抗，將因不同的美國總統與美中關係發展而異，反映出網路國防安全的複雜性。

## 伍、對臺灣可能的影響

美國與中共的網路戰略不必然是臺灣增強網路安全能力的唯一因素。臺灣是中共網路持續攻擊的對象，除了「網路間諜」竊取機密資料之外，也承受中共藉由網路載台對臺灣進行的「假訊息」、心理戰，更可能在中共使用武力之下，政府無法正常持續運作。在美國歐巴馬總統上任之前，我國行政院有「國家資通安全會報」，推動資通安全基礎建設工作，國家安全會議亦將資訊安全列為國家九大安全威脅之一。歐巴馬上台後，行政院進而提出《國家資通訊安全發展方案》、出版《2010資通安全政策白皮書》、《關鍵資訊基礎建設保護政策指引》（2011年）。

在美中兩國相繼成立「網路任務部隊」、「戰略支援部隊」之後，中華民國國軍亦成立「資通電軍指揮部」應有參考或借鏡美中兩國的軌跡。美中在網路安全脆弱點之一在人才培育、專業技術不足的環節，臺灣亦不例外。中華民國國防部軍事院校、專業部隊對網路戰，相較於民間大學學者有較早的研究。國防理工學院資訊工程系從2016年開始「網路安全碩士在職專班」的招生；2018年成立的國防安全研究院設有「網路作戰與資訊安全」研究所。後者有培養智庫文職人員參與實務運作的經驗，除研判中共網路戰動態之外，亦可與美國網路安全智庫對話的平台。

### 一、臺灣增強對網路因素在國防安全的想定

美國專家長期關注解放軍的軍力成長及其對臺灣所造成的威脅，而網路攻擊成為對臺灣使用武力的選項之一，不管是單獨的網路攻擊或與電子戰、心理戰軍事行動併用，形成「混合威脅」(Hybrid Threat)或「反介入與區域拒止」的一種想定。[66] 這種可能性在習近平在軍事改革成立「戰略支援部隊」之後大為增加。2018年之前，美國國防部雖提到中國「資訊封鎖」(Information Blockade)或「資訊掌控」(Information Dominance)的進展，但幾無評論過該部隊在臺灣軍事想定的角色。

2018年與2019年美國國防部公布的《中

65 張騰軍，〈特朗普政府網路安全政策調整點分析〉，《國際觀察》，2018年第3期，2018年，頁68-72；耿召，〈特朗普政府《國家網絡戰略》：實效與理念並舉〉，《和平與發展》，2019年第1期，2019年，頁127-129；魯傳穎，〈中美關係中的網絡安全困境及其影響〉，《現代國際關係》，2019年第12期，2019年，頁18-20。

66 Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Denver, Colorado: Praeger, 2017), pp. 95-105.

華人民共和國軍事與安全發展》(*Military and Security Developments Involving the People's Republic of China*)指出，中共「戰略支援部隊」的成立，可能改進對臺灣遂行與協調「資訊作戰」，特別是與網路、電子作戰、反太空的能力，提供太空偵察給中央軍事委員會及東部戰區，改進解放軍指揮幹部對臺灣作戰序列與對設施的戰場覺知(Situational Awareness)；解放軍仍在尋找改革聯合指揮程序，在戰區層次上加大整合「資訊作戰」與「情監偵」(ISR)能力，但結構性改革已解決上述戰略能力整合的重大障礙。[67]

由中華民國國防部每兩年公布的《國防報告書》、每四年公布的《四年期國防總檢討》，可看出政府對中共網路威脅的重視。[68] 2009年的《四年期國防總檢討》，指出中共「已先後自中國大陸本土及境外地點，對我進行網路駭客、情蒐、無線網路入侵及病毒攻擊等試驗，戰時可能以癱瘓我政經軍資訊網路為目標，使我喪失正常運作能力」。[69] 2015年《國防報告書》提到「近來中共網軍透過社交工程、遠端滲透、病毒（惡意程式碼）感染、竊取或監控等方式，入侵我國政府機關與民間企業的情況極為嚴重，企圖影響國軍指管資訊系統運作及遲滯應變能力。未來共軍可能透過網路對特定目標進行攻擊，癱瘓我國關鍵基礎設施系統之運作，對我軍事作戰能力及國家安全產生極大威脅」。[70] 2017年《國防報告書》指出中共網軍「現階段已具備對我電磁參數及監偵與指管系統遂行偵蒐、阻斷與干擾等電子軟、硬殺能力」。[71] 2019年《國防報告書》指出共軍「已具備第二島鏈以西，海、空動態預警能力」，發展「網電一體戰」，可「對我政經重要機關實施網路資訊攻擊，伺機散播不實消息，冀達癱瘓我重要目標及擾亂民心之目的」。[72] 以上這些評估必然成為臺灣與美國共同檢視與尋求對策的焦點。

2013年，中華民國國防部在因應網路戰威脅，宣示提升「聯合資訊戰能力」，提出五點目標：「提升早期預警及聯合資訊安全防護能力」；「持續強化各項資安防護網能量」；「導入最新通資安全技術於軍事用途」；「執行資訊專業人員培育及訓練流路」；「持續發展綜合性資訊戰力，以確保國軍資電優勢」。[73] 2015年5月，民進黨智庫

67 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2016* (Washington, DC: U.S. Department of Defense, 2016), p. 86; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2018* (Washington, DC: U.S. Department of Defense, 2018), p. 96.

68 2000年《國防報告書》即有專章處理國防資訊管理，提到加速「國防資訊基礎建設」(Defense Information Infrastructure)，並籌建國軍資訊作戰能量。《中華民國89年國防報告書》（臺北：國防部，2000年），頁173-174。

69 中華民國98年《四年期國防總檢討》編纂委員會，《中華民國98年四年期國防總檢討》（臺北：國防部，2009年），頁25。

70 國防部「國防報告書」編纂委員會，《中華民國104年國防報告書》（臺北：國防部，2015年），頁60。

71 國防部「國防報告書」編纂委員會，《中華民國106年國防報告書》（臺北：國防部，2017年），頁44。

72 國防部「國防報告書」編纂委員會，《中華民國108年國防報告書》（臺北：國防部，2019年），頁40。

指出中共對臺灣的國防相關設施網路攻擊，屬於高風險但現有戰力明顯不足的威脅，國軍應列為大幅改善的第一順位，並主張「整合現有國軍資訊、通訊與電子相關之單位與能量，成立獨立的第四軍種」。蔡英文政府上台後，2017年以原有的「資電作戰指揮部」為基礎，整編成立國防部參謀本部「資通電軍指揮部」，使其在平時執行網路空間安全維護，戰時可協防國家關鍵資訊基礎設施。[74]

根據資通電軍指揮官馬英漢的報告，臺灣遭受的網路攻擊有80%來自中共，以2017年為例，國防部每一個月遭受61,208次網攻，2018年1～10月，每個月升高到75,368次。[75] 2018年5月，立法院三讀通過《資通安全管理法》，網路系統是關鍵基礎設施，網路狀態更「影響資通機能運作，構成資通安全政策之威脅」，需確保機密性、完整性及可用性（第三條）。2019年《國防報告書》主張「網路作戰」目標為「確保安全的國防網路環境」、「強化精確的網路情研能量」、「建立可恃的網路攻防戰力」，策略上特別指出「發展新式網路攻防戰具」、「研擬多元網路作戰計畫」。[76] 這顯示網路國防安全不僅是防禦，也需具備攻擊的能量。然而，臺灣如同美國網路戰略一樣遇到人才預算不足，更缺乏明確的授權與交戰規則。

除國防部之外，國家安全會議及行政院國家資通安全會報亦負責指導網路安全事務，「建構聯合資安防護機制，並結合各項演訓時機，將『國家關鍵資訊基礎設施防護(CIIP)』納入演練科目，強化國家整體資安防護能量」。[77] 蔡英文政府在2018年9月公布首部的「國家資通安全戰略報告」指出，政府必須有「超前部署、預置兵力」的國家級資安戰略，其落實與執行透過國家安全會議「國家資通安全辦公室」、行政院「資通安全處」及「國家通訊傳播委員會」，組成國家資安防護鐵三角，分別從國安、資安及通安等層面，保護國家與社會安全，建構國家整體資通安全防護網，與友邦進行國際聯防及情資分享。其中，通訊網路堪稱八大關鍵資訊基礎設施（政府、高科技園區、能源、水資源、通訊、交通、銀行與金融、緊急救援與醫院）之一，也是政府「持續營運」(Continuity of Operations)的神經骨幹。[78] 臺灣公私部門在網路情報的分享，亦是需要努力克服的挑戰。臺海兩岸在2011年簽署「核電安全合作協議」，針對事故有通報的責任，隱含中共承諾不攻擊臺灣的核電設施，但不見得擴及其他關鍵基礎設施。中共對臺灣使用各種「銳實力」(Sharp Power)手段，如遊

73 中華民國102年《四年期國防總檢討》編纂委員會，《中華民國102年四年期國防總檢討》（臺北：國防部，2013年），頁39-40。

74 新境界文教基金會國防政策諮詢小組，《2025年臺灣軍事防衛能量》（臺北：新境界文教基金會國防政策諮詢小組，2015年），頁10、16；國防部「國防報告書」編纂委員會，《中華民國106年國防報告書》，頁76。

75 Ma Ying-han, "Military Cyber Threats and Responses," *Defense Security Brief*, Vol. 7, Issue 2 December, 2018, p. 6.

76 國防部「國防報告書」編纂委員會，《中華民國108年國防報告書》，頁69。

77 國防部「國防報告書」編纂委員會，《中華民國104年國防報告書》，頁107-108。

78 國家安全會議國家資通安全辦公室，《國家資通安全戰略報告》（臺北：國家安全會議，2018年），頁6、23-33。

說收買、滲透顛覆等，並經由網路與通信載台傳播不實訊息，更使臺灣面臨另一個面向的「網路安全」問題。

二、強化臺美網路安全的合作

有關美國與臺灣的網路安全合作，為外界所知者較少。臺灣與美國雖無外交關係，但透過雙方代表處在2007年簽署《資通訊科技論壇的參考範圍》(Information and Communication Technology Forum Terms of Reference)協議，兩國國防部針對網路中心戰(network centric warfare)及其科技發展等相關議題，可進行定期討論。臺美在2011年簽訂《強化預防及打擊重大犯罪協議》(Agreement on Enhancing Cooperation in Preventing and Combating Serious Crime)，對「網路犯罪」問題防範可加強合作。這兩項協議反映臺美在網路安全的合作起步較早。

中共對美國長期對臺灣出售「信息技術含量高的高技術裝備」，擔憂對其「爭奪信息優勢的臺海戰爭」會有不利的影響。[79] 美國國會成立的「美中安全與經濟審議委員會」(U.S.-China Economic and Security Review Commission, USCC)在2014年與2015年的年度報告，提到臺灣受到中共網路威脅及國際孤立的困境，建議行政部門邀請臺灣以觀察員身分，參加美國自2006年起的兩年一度「網路風暴」(Cyber Storm)演習，或者將臺灣納入美國主導的11國「國際觀察與警告網絡」(International Watch and Warning Network)，但歐巴馬政府未予以採納，美國從未邀請臺灣軍方參加「環太平洋」(Rim of the Pacific)、「紅旗」(Red Flag)空對空戰鬥訓練或「網路風暴」等演習。[80] 由此可見，未來美臺網路安全的合作，或可使臺灣在美國「印太戰略」找到適當的角色。

川普總統上台後，每年在簽署的「國防授權法」(National Defense Authorization Act)強化與臺灣的合作。例如2019年提到協助臺灣建構不對稱戰力，如「指揮、管制、通訊及情報」($C^3I$)、2020年提到「指揮、管制、通訊、電腦、情報、監視、偵察」($C^4ISR$)及其他匿蹤、智能化、精準武器。2019年11月，臺灣自2013年起舉辦「網路攻擊與防衛演習」(Cyber Offensive and Defensive Exercise, CODE)，係美國首度與臺灣合辦，另有10國參與演習或擔任觀察員，以如何防禦因應攻擊金融系統為重點。[81] 美國派遣專家觀察每年「漢光演習」，「網路作戰」在各種軍事想定中的角色更是焦點。美國亦協助臺灣加入美國「國家網路安全與通訊整合中心」(National Cybersecurity and Communications Integration Center)或「國際網路安全卓越中心」(InterNational Cyber Security Center of Excellence, INCS-COE)，使臺灣有更多國際參與的機會。[82]

美國與臺灣透過「全球合作與訓練

79 馮毅，〈關於我軍信息與網絡安全的幾點思考〉，沈偉光主編，《中國信息戰》（北京：新華出版社，2005年），頁102、109、113-115。

80 U.S. Congress, *2015 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: U.S. Government Printing Office, 2015), p. 516; U.S. Congress, 2018 Report to Congress of the U.S.-China Economic and Security Review Commission (Washington, DC: U.S. Government Printing Office, 2018), p. 368.

81 Kathrin Hille, "US and Taiwan Host Security Exercise to Boost Cyber Defence," *Financial Times*, November 4, 2019, <https://www.ft.com/content/7d6c78cc-fec8-11e9-b7bc-f3fa4e77dd47>（檢索日期：2020年7月23日）

架構」(Global Cooperation and Training Framework)，已經常舉行跨國專家會議，增加臺灣與多方在網路安全對話，亦是未來可能更加強化的方向。2019年7月，美國眾議員雷克理夫（John Ratcliffe；共和黨，德州）針對「2020會計年度國防授權法案」(H.R. 2500)提出一項修正案並獲得通過，要求成立美臺工作小組研擬預防性計畫，協調因應來自中共網路攻擊的威脅，強化美臺網路夥伴(Cyber Partnership)等安全議題。[83] 雷克理夫被川普總統提名為「國家情報總監」，並於2020年6月就任，由此可見美臺針對中共網路威脅，當有增進合作的空間。

基於川普政府對「華為公司」及其相關企業的禁令，臺灣亦無法置身度外。2019年4月行政院公布「各機關對危害國家資通安全產品限制使用原則」，擴大要求中央與地方公部門及相關各公營機構，不得採購及使用危害國家資通安全的廠商產品，衝擊到提供相關產品給「華為公司」的臺灣廠商。2020年5月，在川普政府持續對「華為公司」予以出口禁令，台積電立即宣布在美國亞利桑那州投資興建一座5奈米晶圓廠，並停止接受來自「華為公司」的新訂單。美國國務卿蓬佩奧認為此一決定有助強化美臺關係，降低美國對中共的經濟依賴。[84] 蓬佩奧倡議的國際「乾淨網路」計畫，涵蓋乾淨的電信運營商、商店、應用軟體、雲端、電纜、通道，納入30多個國家，同意使用受信任的供應商打造5G網路，臺灣的「中華電信」、「遠傳」、「臺灣大哥大」、「亞太電信」、「臺灣之星」全被列入。美國與臺灣亦公布「5G安全共同宣言」，保護通訊網路不受操縱，隱私與個人自由獲得保障。

## 陸、結　　論

歐巴馬、川普政府與習近平主政的中共，均將網路戰略提升到國家戰略層級，反映網路空間安全議題的重要性。歐巴馬政府由白宮主導網路戰略，搭配國防部設立「網路指揮部」並與「國家安全局」密切結合，指揮官與局長同為一人，清楚界定網路戰略的重要性與指揮體系。習近平除設立「國家安全委員會」指導網路安全議題，共軍亦於2015年底新設「戰略支援部隊」，統籌網路事務。臺灣則於2017年成立「資通電軍指揮部」。這些任務部隊說明國防體系在網路戰略發展的關鍵地位。

在美國與中共的網路安全關係上，歐巴馬總統採取接觸與對話，著重防範中共對美國的「網路間諜」活動。歐巴馬與中共達成網路安全五項共識、密集舉行打擊網路犯罪的定期會議，顯示自由主義合作的思考。川普總統傾向採取單邊主義行動，美中四項「全面對話機制」，在2018年底後未再舉行對話。川普總統雖承諾遵行美中網路安全五項共識，但實際發展卻有不同。川普專注與中共進行關稅與貿易談判，因對中共「華

82 郭恆孝，〈臺美舉行大規模網路攻防演練之分析〉，《國防安全週報》，2019年11月22日，頁30-31。INCS-COE有日本、英國、美國大學等成員。

83 U.S. House of Representatives, "House Passes Rep. Ratcliffe's U.S.-Taiwan Cyber Partnership Amendment," *U.S. House of Representatives*, July 12, 2019, <https://ratcliffe.house.gov/news/documentsingle.aspx?DocumentID=1405>（檢索日期：2020年7月23日）

84 Ana Swanson, "New U.S. Rule Inflicts More Pain on Huawei," *New York Times*, May 16, 2020, p. B4.

為公司」採取敵視立場、實施制裁，斷其供應鏈，削弱中共網路資通信科技的崛起，而這是沒有繼續進行對話的原因。美國與中共在網路戰略存在競爭關係，中共快速發展網路攻防能量、擴展網路資通信科技市場，縮短兩國網路能力差距，使美國感受到競爭壓力。從長遠觀點來看，不能排除類似歐巴馬時代兩國網路合作的可能性。

美中臺的「網路任務部隊」，都未放置於陸海空三軍之內，顯示網路部隊的特殊性。美中高度重視網路安全，因與兩國的太空、核武、衛星武器有密切的關連。美國與中共高度依賴網路所進行的高科技戰爭，讓網路空間成為衝突時執行對稱作戰的載台。美中針對網路安全的高層對話始於歐巴馬政府，但侷限於網路偷竊情報行為，或針對網路犯罪進行執法的合作。即使美中兩國政府避免涉入「網路間諜」行為，但既然是情報蒐集，就難以阻止透過網路竊取政治與軍事情報，甚至結合軍事工具的使用。

臺灣網路安全夾處在美中之間，政府一方面強化政府網路安全的機制，另一方面強化與美國等國的網路安全對話。臺灣在安全領域一向受到國際孤立的限制，無法公開與他國進行安全的合作，但因為網路、情報的隱密性，相對的限制較少。尤其臺灣是中共網路攻擊的跳板，臺灣提供的具體個案與經驗，比其他相關國家更具參考價值。美中臺的「網路任務部隊」除保護自身國防外，更需維護關鍵基礎設施，如水電、金融與通訊體系等。美臺都遭受中國大陸的網路入侵，進行相關交流與合作是自然的趨勢。馬英九執政時期兩岸關係雖然緩和，但中共對臺灣的網路入侵或情報蒐集，並沒有因此而停止。臺灣在因應中共的網路駭客，與美國相比較，顯得更為低調，但不意味國家網路資通信安全的防護因此受到忽略。面對美中網路戰略發展，臺灣的網路安全政策當有調整及借鏡之處。

（收件：109年7月24日，接受：109年10月29日）

# 參考文獻


## 中文部分

### 專書

沈偉光，1997。《新戰爭論》。北京：人民出版社。

沈偉光主編，2005。《中國信息戰》。北京：新華出版社。

張春江、倪健民主編，2001。《國家信息安全報告》。北京：人民出版社。

喬良、王湘穗，2016。《超限戰與反超限戰》。武漢：長江文藝出版社。

惠志斌、唐濤主編，2015。《中國網路空間安全發展報告》。上海：社會科學文獻出版社。

劉由芳、韓強主編，2005。《軍事信息安全原理》。北京：國防大學出版社。

歐錫富、黃宗鼎主編，2018。《2018中共政軍發展評估報告》。臺北：國防安全研究院。

### 期刊論文

田成信、張峰、江飛，2014。〈網絡戰對作戰的影響及對策〉，《國防科技》，第35卷第5期，頁103-105。

吳俊德、賴達文，2018。〈2011-2018年美國網路戰略沿革〉，《國防安全週報》，第16期，頁20-25。

林穎佑，2017。〈中共戰略支援部隊的任務與規模〉，《展望與探索》，第15卷，第10期，頁102-128。

奕文莉，2012。〈中美在網絡空間的分歧與合作途徑〉，《現代國際關係》，第7期，頁28-33。

倪海寧，2008。〈美軍網絡戰理論和實踐〉，《國際資料信息》，第7期，頁14-18。

耿召，2018。〈特朗普時期中美網絡安全合作分析〉，《美國問題研究》，第2期，頁151-175。

耿召，2019。〈特朗普政府《國家網絡戰略》：實效與理念並舉〉，《和平與發展》，第1期，頁116-130。

郝葉力，2015。〈大國網絡戰略博奕與中國網絡強國戰略〉，《國際關係研究》，2015年第3期，頁7-12。

崔文波，2013。〈塔林手冊對我國網絡安全利益的影響〉，《江南社會學院學報》，第15卷第3期，頁22-26。

張騰軍，2018。〈特朗普政府網路安全政策調整點分析〉，《國際觀察》，第3期，頁64-79。

郭恆孝，2019/11/22。〈臺美舉行大規模網路攻防演練之分析〉，《國防安全週報》，第74期，頁27-30。

蔡翠紅，2019。〈中美網絡空間戰略比較：目標、手段與模式〉，《當代世界與社會主義》，2019年第1期，頁42-49。

魯傳穎，2019。〈中美關係中的網絡安全困境及其影響〉，《現代國際關係》，第12期，頁16-22。

顏琳、陳俠，2014。〈美國網絡安全邏輯與中國防禦性網絡安全戰略的建構〉，《湖南師範大學社會科學學報》，第4期，頁34-40。

嚴明，2013。〈高度關注網絡空間安全〉，《南京政治學院學報》，第6期，頁111-

113。

**官方文件**

中華人民共和國國防部，2019。《新時代的中國國防白皮書》。北京：國務院新聞辦公室。

中華民國98年《四年期國防總檢討》編纂委員會，2009。《中華民國98年四年期國防總檢討》。臺北：國防部。

中華民國102年《四年期國防總檢討》編纂委員會，2013。《中華民國102年四年期國防總檢討》。臺北：國防部。

新境界文教基金會國防政策諮詢小組，2015。《2025年臺灣軍事防衛能量》。臺北：新境界文教基金會國防政策諮詢小組。

國防部「國防報告書」編纂委員會，2000。《中華民國89年國防報告書》。臺北：國防部。

國防部「國防報告書」編纂委員會，2015。《中華民國104年國防報告書》。臺北：國防部。

國防部「國防報告書」編纂委員會，2017。《中華民國106年國防報告書》。臺北：國防部。

國防部「國防報告書」編纂委員會，2019。《中華民國108年國防報告書》。臺北：國防部。

國家安全會議國家資通安全辦公室，2018。《國家資通安全戰略報告》。臺北：國家安全會議。

**網際網路**

中華人民共和國國防部，2015/5/26。〈中國的軍事戰略〉，《中華人民共和國國防部》，<http://www.mod.gov.cn/regulatory/2015-05/26/content_4617812.htm>。

中華人民共和國國防部，2016/1/1。〈國防部新聞發言人就深化國防和軍隊改革有關問題接受媒體專訪〉，《中華人民共和國國防部》，<http://www.mod.gov.cn/affair/2016-01/01/content_4635502.htm>。

中國新聞網，2015/4/27。〈報告：中國應以軍隊為主體整合國家網絡空間安全力量〉，《人民網》，2015年4月27日，<http://politics.people.com.cn/n/2015/0427/c70731-26910719.html>。

中國網信網，2016/12/27。〈《國家網絡空間安全戰略》發布〉，《中華人民共和國國防部》，<http://www.mod.gov.cn/big5/regulatory/2016-12/27/content_4768313.htm>。

新京報，2015/5/27。〈國防白皮書披露軍兵種發展戰略　將加快網絡空間力量建設〉，《人民網》，<http://military.people.com.cn/BIG5/n/2015/0527/c1011-27061489.html>。

齊洋、王瑤，2014/6/26。〈我軍網絡空間戰略情報研究中心揭牌成立〉，《解放軍報》，<http://news.mod.gov.cn/big5/pla/2014-06/26/content_4518762.htm>。

外文部分

**專書**

Bolton, John, 2020. *The Room Where It Happened: A White House Memoir*. New York: Simon & Schuster.

Cheng, Dean, 2017. *Cyber Dragon: Inside*

*China's Information Warfare and Cyber Operations*. Denver. Colorado: Praeger.

Clarke, Richard A. and Knake, Robert K., 2010. *Cyber War: The Next threat to National Security and What to Do About It*. New York: HaperCollins Publishers.

Gates, Robert M., 2014. *Duty: Memoirs of a Secretary at War*. New York: Alfred A. Knopf.

Libicki, Martin C., 2007. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge: Cambridge University Press.

Sanger, David E., 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Broadway Books.

Schmitt, Michael N., ed., 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

**期刊論文**

Borghard, Erica D. & Lonergan, Shawn W., 2018. "Confidence Building Measures for the Cyber Domain," *Strategic Studies Quarterly*, Vol. 12, Issue 3, pp. 10-49.

Ma, Ying-han, 2018/12. "Military Cyber Threats and Responses," *Defense Security Brief*, Vol. 7, Issue 2, pp. 1-16.

**官方文件**

Joint Chiefs of Staff, 2014. "Information Operations," in Joint Chiefs of Staff, ed., *Joint Publication 3-13*. Washington, DC: Joint Chiefs of Staff. pp. II 5-13.

The White House, 2017. *National Security Strategy of the United States of America*. Washington, DC: The White House.

The White House, 2018. *National Cyber Strategy of the United States of America*. Washington, DC: The White House.

U.S.-China Economic and Security Review Commission, 2015/11. *2015 Report to Congress of the U.S.-China Economic and Security Review Commission*. Washington, DC: U.S. Government Printing Office.

U.S.-China Economic and Security Review Commission, 2018/11. *2018 Report to Congress of the U.S.-China Economic and Security Review Commission*. Washington, DC: U.S. Government Printing Office.

U.S. Department of Defense, 2015/4. *The DOD Cyber Strategy*. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense, 2015. *Military and Security Developments Involving the People's Republic of China 2015*. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense, 2016. *Military and Security Developments Involving the People's Republic of China 2016*. Washington, DC: U.S. Department of Defense.

U.S. Department of Justice, 2017/10/6. "First U.S.-China Law Enforcement and Cybersecurity Dialogue Summary of Outcomes," *U.S. Department of Defense*. <https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue>.

U.S. Department of Defense, 2018. *Military and Security Developments Involving the People's Republic of China 2018*. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense, 2018/9. *Summary-Department of Defense Cyber Strategy 2018*. Washington, DC: U.S. Department of Defense.

U.S. Department of Defense, 2019/6/1. *Indo-Pacific Strategy Report*. Washington, DC: U.S. Department of Defense.

U.S. Defense Intelligence Agency, 2019. *China Military Power: Modernizing a Force to Fight and Win*. Washington, DC: U.S. Department Intelligence Agency.

U.S. Department of Defense, 2019. *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY 19-23*. Washington, DC: U.S. Department of Defense.

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

U.S. Office of the Undersecretary of Defense for Acquisition Technology, and Logistics, 2017/2. *Defense Science Board (DSB) Task Force on Cyber Deterrence*. Washington, DC: U.S. Department of Defense.

U.S. Office of Director of National Intelligence, 2019. *National Intelligence Strategy of the United States of America*. Washington, DC: U.S. Office of Director of National Intelligence.

**報紙**

Swanson, Ana, 2020/5/16. "New U.S. Rule Inflicts More Pain on Huawei," *New York Times*, p. B4.

**網際網路**

Ashton Carter, 2015/4/23. "Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity," *Secretary of Defense Speech, U.S. Department of Defense*, <https://archive.defense.gov/speeches/speech.aspx?SpeechID=1935>.

Executive Office of the President of the United States, 2013/2. *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*. Washington, DC: Executive Office of the President of the United States, <https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf>.

Gertz, Bill, 2020/6/25. "Pentagon: Major Chinese Companies Have Close Military Links," *Washington Times*, <https://www.washingtontimes.com/news/2020/jun/25/pentagon-major-chinese-companies-have-close-milita/>.

Hille, Kathrin, 2019/11/4. "US and Taiwan Host Security Exercise to Boost Cyber Defence," *Financial Times*. <https://www.ft.com/content/7d6c78cc-fec8-11e9-b7bc-f3fa4e77dd47>.

Lyu, Jinghua, 2018/10/19. "A Chinese Perspective on the Pentagon's Cyber Strategy:

From 'Active, Defense' to 'Defending Forward'," *Lawfare*, <https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward>.

Painter, Christopher, 2016/5/25. "International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms," *Statement Before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*. Washington, DC: U.S. Department of State, <https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm>.

The White House, 2003/2. *The National Strategy to Secure Cyberspace*. Washington, DC: The White House, <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.>.

The White House, 2010/5. *National Security Strategy*. Washington, DC: The White House, <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>.

The White House, 2011/5. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: The White House, <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

The White House, 2015/9/25. "Fact Sheet: President Xi Jinping's State Visit to the United States," *The White House*, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.>.

The White House, 2020/5. *United States Strategic Approach to the People's Republic of China*. Washington, DC: The White House, <https://www.whitehouse.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.20.20.pdf>.

U.S. Congress, 2017/3/2. *Cyber Strategy and Policy*. Hearing, Committee on Armed Services U.S. Senate, 115th Congress, First Session, <https://www.armed-services. senate. gov/imo/media/doc/Alexander_03-02-17.pdf.>.

U.S. Department of Defense, 2011/7. *Department of Defense Strategy for Operating Cyberspace*. Washington, DC: U.S. Department of Defense. <http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.

U.S. Cyber Command, 2018/4. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>.

U.S. Department of Homeland Security, 2018. *Department of Homeland Security Cybersecurity Strategy*. Washington, DC: U.S. Department of Homeland Security. <https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-

Strategy_1.pdf>.

U.S. Department of Defense, 2019/6/1. *Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region*. Washington, DC: U.S. Department of Defense. <https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF>.

U.S. House of Representatives, 2019/7/12. "House Passes Rep. Ratcliffe's U.S.-Taiwan Cyber Partnership Amendment," *U.S. House of Representatives*, <https://ratcliffe.house.gov/news/documentsingle.aspx?DocumentID=1405>.