美中關係的網路安全問題

林正義

（中央研究院歐美研究所研究員）

摘　要

自歐巴馬政府起，網路安全已成了美中兩國持續且棘手的衝突問題。中國的網路間諜活動，對美國的國家安全利益構成嚴重的挑戰。同樣地，美國亦對中國政府及「華為」進行網路入侵與電話監聽。蓋北京否認其政府參與對美國的網路入侵，但與美方達成網路安全合作五點共識。歐巴馬總統偏好建立雙邊對話機制以緩和美中緊張，而川普總統則選擇將網路安全與貿易談判掛勾的策略；另外，中國尋求聯合國系統主導下的網路安全國際規範，並曾與美國協商「信心建立措施」。但是，能否達成網路空間運作規範仍有待觀察。

關鍵詞：網路安全、網路間諜、網路主權、華為、美中關係

壹、前言

老布希(George H. W. Bush)、柯林頓(Bill Clinton)總統任內，美中關係發展在3T的議題上面臨諸多挑戰，分別是天安門（Tiananmen，人權）、臺灣(Taiwan)、貿易（Trade，最惠國待遇）。小布希(George W. Bush)總統任內（2001-2009年），美國與中國是「坦率(candid)、建設(constructive)、合作(cooperative)」3C關係。歐巴馬(Barack Obama)總統任內（2009-2017年），美中是「積極、建設與全面性關係」(positive, constructive and comprehensive relationship)，但新增網路安全

（cybersecurity，中國大陸稱為網絡安全）的嚴重分歧。2013 年美國國安局(National Security Agency)外雇人員史諾登(Edward Snowden)揭發美國對多個友邦、對手國（包括對中國）的監聽事件，美國媒體、企業也遭中國網路駭客入侵。2015 年美國政府指控中國駭客入侵竊取「聯邦人事管理局」(Office of Personnel Management, OPM)資料，而使網路安全成為中國國家主席習近平訪美最棘手的問題。川普(Donald Trump)政府的美中關係更進入網路科技的「圍堵戰」。

根據美國商務部的「國家標準與科技研究所」(National Institute of Standards and Technology)的定義，網路安全係指「保護或防護網路空間的使用免於網路攻擊」，涉及軟硬體與電子、有線通訊系統的實體安全；資訊儲存、監控能力；決策者與民眾對資訊的正確認知、分析與使用等。美中討論的網路安全，至少有四個層面，第一，透過網路進行的不法「網路犯罪」(cyber crime)行為；第二，駭侵取得企業機密、政府資訊與情報的「網路間諜」(cyber espionage)行為；第三，攻擊或防禦關鍵基礎設施、軍事目標的「網路戰」(cyber warfare)；第四，基於政治目的在網路空間進行毀壞行動、製造恐慌的「網路恐怖主義」(cyber terrorism)。[1]由於網路攻擊的隱密性、不易立即察覺，若與軍事作戰結合，可在國防安全發揮「不對稱作戰」(asymmetric warfare)的效果，而網路「假訊息」的散布更是惡意影響力發揮的途徑。2013-2015 年，美國「國家情報總監」(Director of National Intelligence)

1. 「資訊安全」比「網路安全」範圍廣，兩者有重疊的部分是「數位資訊」，但「資訊安全」尚有未存放網路的官方機密文件。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)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(cyber warfare)。請見 Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), pp. 16-17。「資訊作戰」(information operations)是軍事作戰的一種型式。「資訊戰」用語出現較早，「網路安全」則普遍被使用。

克萊普(James Clapper Jr.)將網路威脅視為對美國的首要戰略威脅，凌駕恐怖主義所造成的威脅。[2]川普總統顧問及貿易與製造業政策辦公室主任(Assistant to the President and Director of the Office of Trade and Manufacturing Policy)納瓦羅(Peter Navarro)指控中國必須停止對美國的七項「致命惡行」，其中二項與網路安全有關，分別是竊取美國智慧財產權、駭侵美國電腦。[3]本文聚焦在「網路間諜」安全議題的探討，針對軍事層面的「網路戰」或跨國層面的網路惡意影響力輸出，將在另文探討。本文首先探討歐巴馬、川普對中國網路威脅的評估，再論及中國如何因應，並以文獻分析法，歸納、分析網路安全為何是美中關係的重大新興議題。[4]

貳、歐巴馬因應中國網路安全威脅

歐巴馬政府調整小布希政府與中國舉行年度「戰略經濟對話」

2. U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, D.C.: U.S. Department of Defense, 2015), p. 9.
3. 其他五項包括：強迫技術轉讓；對美國市場進行傾銷；大力補貼中國國企；進口芬太泥(Fentanyl)；操縱貨幣。Zack Budryk, "Top aide: China must end 'Seven Deadly Sins' to stop trade war," *The Hill*, August 4, 2019, <https://thehill.com/homenews/sunday-talk-shows/456092-top-aide-names-seven-deadly-sins-china-must-end-to-stop-trade-war>。
4. 國內有關網路安全論文，請見林穎佑，〈美「中」網路安全競合情勢分析〉，《亞太評論》，第 2 卷第 1 期　，2016 年 2 月，頁 55-70；朱志平、梁德昭，〈習近平時期美中網路安全競逐〉，《遠景基金會季刊》，第 17 卷第 2 期，2016 年 4 月，頁 1-61；張凱銘，〈「避險」視角下的中國對美國的網路強國戰略研究〉，《問題與研究》，第 57 卷第 3 期，2018 年 9 月，頁 97-137；王清安、黃基禎，〈中共對網路空間主權之概念與作為〉，《中國大陸研究》，第 62 卷第 1 期，2019 年 3 月，頁 67-100；張凱銘，〈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〉，《遠景基金會季刊》，第 21 卷第 1 期，2020 年 1 月，頁 107-170。

(Strategic Economic Dialogue)，使之成為「戰略」與「經濟」雙軌的「戰略與經濟對話」(Strategic and Economic Dialogue)，分由國務卿、財政部長在對話擔任領銜的角色，一共舉行八輪。直至 2013 年 4 月，美國正視網路安全在美中關係的嚴重性，國務卿凱瑞(John Kerry)宣布在「戰略與經濟對話」之下的「戰略安全對話」(Strategic Security Dialogue)成立一個跨部會的「網路工作小組」(Cyber Working Group)，並在該年首度舉行對話。在此之前，中國駭客在對可口可樂（2009 年）、「谷歌」（Google，2010 年）、國防工業公司「洛克希德馬丁」（Lockheed Martin，2007-2009，2011 年）先後網路入侵竊密，美國 F-35 戰機引擎與雷達設計圖亦遭竊。[5] 然而，歐巴馬政府國安官員一直低調處理，沒有採取雙邊及多邊外交施壓、網路攻擊行動、經濟制裁或法律行動，以報復中國政府及軍方駭客，因而引起對中國強硬派的不滿。時任副國務卿史坦伯格(James Steinberg)提及日益增加的網路空間是兩國互不信任的來源（2009 年 9 月）；時任國防部長蓋茲(Robert Gates)注意到中國網路攻擊能力的提升；蓋茲繼任者潘內塔(Leon Panetta)訪問北京與習近平會面時（2012 年 9 月），亦沒有凸顯網路安全在美中關係的優先性。[6]

---

5. Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins Publishers, 2010), p. 234; David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (Victoria Australia: Scribe Publication, 2018), p. 100.

6. James Steinberg, "Administration's Vision of the U.S.-China Relationship," September 24, 2009, *American Institute in Taiwan*, <https://web-archive-2017.ait.org.tw/en/administrations-vision-of-the-us-china-relationship.html>; Robert M. Gates, *Duty: Memoirs of a Secretary at War* (New York: Alfred A. Knopf, 2014), pp. 391, 524-525, 527-529; Leon Panetta, *Worthy Fights: A Memoir of Leadership in War and Peace* (New York: Penguin, 2014), pp. 444-447.

一、歐巴馬在第二任期初公開指控中國網路入侵

歐巴馬政府一直到中國對《紐約時報》（*New York Times*，2013年）、「美國鋼鐵公司」（U.S. Steel Corporation，2014年）、「阿勒格尼技術公司」（Allegheny Technologies Incorporated, ATI，2014年）、「太陽能世界」（Solar World，2014年）、美國第二大醫療保險公司「安信」（Anthem，2015年）、「聯邦人事管理局」（2015年）進行一連串網路入侵後，才決定公開指控中國，要求北京必須制止國家資助(state-sponsored)的網路攻擊行為。[7]實際上，美國國安部門也對中國進行網路攻擊，但宣稱不入侵竊取私人企業，取得資料也不提供美國企業牟利之用，但中國駭客將取得的商業機密，成為中國企業談判參考，或軍方發展先進武器的藍圖。美國網路攻擊的目標，包括中國前國家主席胡錦濤、商務部、外交部、銀行和電訊科技業「華為技術有限公司」（以下簡稱「華為」）。尤其是，美國擔心中方利用華為在世界各地的設施從事間諜活動。[8]

中國對美國的網路攻擊不僅限於政府，也及於民間部門。《紐約時報》在調查報導中國總理溫家寶家族涉及不法商業交易之後，就持續受到中國駭客的網路攻擊。[9]2013年2月，歐巴馬總統發布第13636號行政命令，要求商務部長責成「國家標準與科技研究所」建立一套

7. Keith Bradsher, “Retaliatory Attacks, Online,” *New York Times*, May 21, 2014, p. B1; James R. Clapper, *Facts and Fears: Hard Truths from A Life in Intelligence* (New York: Random House, 2018), pp. 533-538.

8. 2009年初，美國國家安全局啟動針對華為的網路駭侵，滲入深圳總部，複製客戶資料、內部培訓檔案、電子郵件、產品的原始碼等。David E. Sanger & Nicole Perlroth, “U.S. Penetrated Chinese Servers It Saw as Spy Risk,” *New York Times*, March 23, 2014, p. A1。

9. Nicole Perlroth, “Hackers in China Attacked The Times for Last 4 Months,” *New York Times*, January 31, 2013, p. A1.

「網路安全架構」(Cybersecurity Framework) 嚴格保護美國關鍵基礎設施，並與私部門建立更好的資訊分享機制。[10]同月，美國資訊安全公司「麥迪安」(Mandiant)公布《高度持續性威脅 I：揭露中國網路間諜的一個單位》(*APT1：Exposing One of China's Cyber Espionage Units*)報告，指稱中國自 2006 年就有「一個講中文所組成的、資源充足的秘密組織，能夠直接連結上海電信基礎設施，多年以來，一直在 61398 部隊的門外，進行多年、公司規模電腦間諜活動，從事如同 61398 部隊為外界所知的任務」。[11]若 2010 年「谷歌事件」讓美國懷疑中國的戰略意圖，「麥迪安報告」則讓美國政府更加確認，而這也是「有史以來最直接點名中國的『網路間諜』問題的研究報告」。[12]2013 年 3 月，習近平與歐巴馬就網路安全問題通話交換意見，提到「中方堅決反對任何形式的駭客活動。中方願同美方以建設性方式就網路安全問題保持溝通」；歐巴馬亦簽署法案要求「美國太空總署」、司法部、商務部需有「聯邦調查局」審查許可，方能採購中國

10. The White House, "Executive Order--Improving Critical Infrastructure Cybersecurity," February 12, 2013, *The White House President Barack Obama*, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

11. Mandiant Corporation, "APT1: Exposing One of China's Cyber Espionage Units," February 2013, *FireEye*, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>; John P. Carlin & Garret M. Graff, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (New York: PublicAffairs, 2018), pp. 245-250; Scott Warren Harold, Martin C. Libicki, & Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica: Rand Corporation, 2016), pp. 45-50.

12. 李峥，〈中美網路安全互動：挑戰與機遇〉，《復旦學報》（上海），2016 年第 3 期，2016 年 6 月，頁 148。相關討論請見 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, pp. 101-104.

資訊公司產品。[13] 之後兩國立即成立跨部會「網路工作小組」。

2013 年 6 月，習近平與歐巴馬在加州安納柏格(Annenberg)莊園會面同意，雙方為減少誤判風險，需要針對網路安全建立規則與處理方式。在高峰會前兩天，美國爆發史諾登事件，揭露美國駐中國大使館設立監聽基地、監控中國大陸的電腦系統、竊取中國大型企業的商業機密等。[14] 中方質疑美方在駭客攻擊上採取「雙重標準」，不僅是「駭客之王」，也「削弱了美國政府對網絡空間治理的主導權和可信度」。[15] 另一方面，美國企圖引渡滯留在香港的史諾登，中國大陸未正面回應，雙方關係陷入緊張。七月，美中「網路工作小組」開始運作，隨後舉行第二次「網路工作小組」會議（12 月），除探討網路空間國際規範與原則外，同意兩國「電腦緊急因應小組」(Computer Emergency Response Team)的強化、協調與合作，並持續就網路議題對話。[16]

2014 年 5 月下旬，美國司法部以中國解放軍對美國網路竊密長達八年為名，起訴解放軍總參三部二局（61398 部隊）五名現役軍官。公布時間點是在時任解放軍總參謀長房峰輝甫結束訪美，北京因而決定

13.〈習近平同奧巴馬通電話 就網路安全等問題交換意見〉，《新華網》，2013 年 3 月 14 日，<http://www.cac.gov.cn/2013-03/15/c_133138873.htm>；Alina Selyukh & Doug Palmer, “U.S. Law to Restrict Government Purchases of Chinese IT Equipment,” *Reuters*, March 28, 2013, <https://www.reuters.com/article/us-usa-cybersecurity-espionage-idUSBRE92Q18O20130328>。

14. Dean Cheng, *Cyber Dragon: Inside China’s Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017), p.145.

15.汪曉風，〈斯諾登事件後美國網絡情報政策的調整〉，《現代國際關係》（北京），2018 年第 11 期，2018 年 11 月，頁 63。

16. U.S. Department of State, “U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track,” July 12, 2013, *U.S. Department of State*, <https://2009-2017.state.gov/r/pa/prs/ps/2013/07/211861.htm>.

暫停「網路工作小組」對話。2014 年 12 月，中國外交部長王毅與美國國務卿凱瑞通話討論「索尼」(Sony)公司遭受網路攻擊一事，宣稱北京「反對一切形式的網路攻擊和網路恐怖行為，反對任何國家或個人利用他國境內設施對第三國發動網路攻擊」。[17] 然而，更嚴重的網路安全挑戰在 2015 年爆發。

二、美國「聯邦人事管理局」事件促成美中網路五點共識

2015 年 6 月歐巴馬政府揭露「聯邦人事管理局」高達 2,150 萬筆現任和前任聯邦僱員、眷屬的個人訊息，遭中國大陸駭客竊取。2014 年 3 月，美國「聯邦人事管理局」曾發現中國大陸駭客進入其系統，但未取得資料，隨後安裝防入侵軟體，顯然無法有效阻止。[18] 美國政府指控這是中國軍方有組織的駭客行為。被竊取的美國個人資料包括：社會安全碼(SSN)、住所及教育背景、受雇背景、家人親屬商業往來銀行、健康紀錄、刑事與金融背景，甚至有指紋、調查訪談、使用者名字、密碼等。這意味中國擁有包括美國內閣官員、情報人員在內等敏感訊息，與聯邦政府有合作關係的承包商和分包商的資訊亦包含其內。[19] 中

17. 中華人民共和國外交部，〈王毅同美國國務卿克里通電話〉，《中國新聞網》，2014 年 12 月 22 日， <http://www.chinanews.com/gn/2014/12-22/6897113.shtml>。中國可能利用北韓為掩護攻擊「索尼」，請見 Dennis F. Poindexter, *The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests* (Jefferson: McFarland & Company, Inc., Publishers, 2018), p. 38。有關起訴解放軍軍官決策過程，請見 John P. Carlin & Garret M. Graff, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*, pp. 268-271。

18. Michael S. Schmidt, David E. Sanger, & Nicole Perlroth, "Chinese Hackers Pursue Key Data on U.S. Workers," *New York Times*, July 10, 2014, p. A1.

19. David E. Sanger, "Hackers Also Stole Fingerprints of 5.6 Million Workers, Personnel Agency Says," *New York Times*, September 24, 2015, p. A21.

國大陸掌握數百萬筆聯邦雇員資訊之後，可用作黑函威脅，或透過網路釣魚(phish)電子郵件，獲取美國企業或政府更多的敏感訊息。《華爾街日報》(*Wall Street Journal*)社論以「歐巴馬網路潰堤」為題，指出北京在取得資料之後，可以查閱美國駐中國大使館的名單，找出沒有列在名冊的情報人員或間諜，讓美國國內遭遇了 911 式的網路攻擊(A cyber 9/11 at home)。[20]

時任「聯邦人事管理局」主任艾丘麗塔(Katherine Archuleta)在事件之後去職，但她在美國參議院軍事委員會聽證會不願意指名中國。時任「國家情報總監」克萊普則公開指出中國是首要的嫌疑者(the leading suspect)。克萊普認為中國並沒有違反一般國家從事間諜情報蒐集活動的範疇，中國所做的是「網路間諜」活動而非「網路戰爭」。這意味美國也可對其他國家從事「網路間諜」活動。克萊普反對採取明確的網路報復行動，並舉時任財政部長蓋特納(Tim Geithner)意見為例，一旦中國以網路反擊，駭入美國華爾街金融體系，局面會是如何？這種意見阻止了其他部會首長鷹派的報復主張。[21]此一事件卻使克萊普決定提升「網路指揮部」(Cyber Command)的位階，不再隸屬「戰

20. "Obama's Cyber Meltdown," *Wall Street Journal*, June 24, 2015, p. A12, <https://www.wsj.com/articles/obamas-cyber-meltdown-1435097288>。對中國情報官員吸收與解析偷自美國網路情報能力之看法，請見 Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, Issue 3, Winter 2014/15, pp. 7-47；Andrea Gilli & Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security*, Vol. 43, Issue 3, Winter 2018/19, pp. 141-189。

21. James R. Clapper, *Facts and Fears: Hard Truths from A Life in Intelligence*, p. 535; Nigel Inkster, *China's Cyber Power* (New York: Routledge, 2016), pp. 68-69; Dennis F. Poindexter, *The Chinese Information War*: *Espionage, Cyberwar, Communications Control and Related Threats to United States Interests*, p. 14.

略指揮部」(Strategic Command)之下。[22]

歐巴馬政府在事件之後增強對中國的施壓。2015 年 9 月，習近平首次對美進行國是訪問。習訪美前，根據歐巴馬政府提供的名單，逮捕數名中國駭客；中美兩國亦針對第一份管制網路安全文件進行協商，考慮納入不攻擊對方關鍵基礎設施。[23]習近平在訪問華盛頓首府之前，在西雅圖與美國五個州（加州、華盛頓、俄勒岡、密西根、愛荷華州）的州長及資訊科技業領袖會晤，拜訪微軟(Microsoft)，並出席「美中互聯網工業論壇」(U.S.-China Internet Industry Forum)座談會，聽取美方相關業界對網路安全的疑慮。[24]習近平倡議中美「新型大國關係」之際，不得不有所妥協，除表明無意追求南海軍事化，也與歐巴馬達成網路安全五點共識：

1.對另一方就惡意網路活動，提供資訊及協助的請求，給予及時回應。

2.兩國政府均不從事，或者在知情情況下支持網路竊取智慧財產權，包括貿易秘密，以及其他機密商業資訊，以使其企業或商業行業在競爭中處於有利地位。

3.承諾共同努力找出和推動國際社會網路空間合適的國家行為準則。

4.維持打擊網路犯罪及相關事項高層聯合對話機制。

5.就網路安全意外事件加強執法溝通，互相提供及時的回應。[25]

---

22. James R. Clapper, *Facts and Fears: Hard Truths from A Life in Intelligence*, p. 541.

23. Andrew Blake, "China Arrests Hackers Following Request from U.S.—Report," *Washington Times*, October 12, 2015, <https://www.washingtontimes.com/news/2015/oct/12/china-arrests-hackers-following-request-from-us-re/>.

24. Jane Perlez & Nick Wingfield, "Chinese Leader Hears Tough Complaints of American Business," *New York Times*, September 24, 2015, p. A21.

25. The White House, "Fact Sheet: President Xi Jinping's State Visit to the

美中兩國以資料說明書(Fact Sheet)方式，而非以單獨的網路協議或備忘錄簽署五點共識，顯見有許多歧見未能解決，不攻擊對方的關鍵基礎設施，沒有納入共識，為兩國網路攻擊行動預留空間。不過，在此之前（2015 年 7 月），美中與其他國家在聯合國政府專家小組(Group of Government Experts)上，已有放棄攻擊關鍵基礎設施的建議，加上《武裝衝突法》(*Law of Armed Conflict*)限制此類行為，剩下的將是查證的問題。[26]美中同意不相互竊取貿易、企業機密，承諾加強執法打擊犯罪、探討建立國家網路行為準則，卻是一大突破。美中同意每年舉行兩次網路對話會議，處理網路安全相關問題，避免問題惡化。2015 年 12 月初，中美首度舉行「網路犯罪及相關事項高層聯合對話」(High-Level Joint Dialogue on Cybercrime and Related Issues)，由時任中國公安部長、中央政法委副書記郭聲琨，與時任美國司法部長林琪(Loretta E. Lynch)、時任美國國土安全部長詹遜(Jeh Johnson)共同主持，重心置於網路犯罪與相關議題，達成指導綱領，確認將設立熱線、網路兵推計畫，另針對網路安全個案、網路反恐合作、執法培訓等取得共識。[27]

2016 年 5 月，美中另設立「國際網路空間規範及相關問題資深專

United States," September 25, 2015, *The White House President Barack Obama*, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

26. Scott Warren Harold, Martin C. Libicki, & Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, p. 71.

27. U.S. Department of Justice Office of Public Affairs & U.S. Department of Homeland Security of Public Affairs, "First U.S.-China High-Level Joint Dialogue on Cybercrime And Related Issues Summary Of Outcomes," December 2, 2015, *U.S. Department of Homeland Security*, <https://www.dhs.gov/news/2015/12/02/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary>.

家會議」(Senior Experts Group on International Norms in Cyberspace and Related Issues)，分由美國國務院及中國外交部負責主談。六月，美中舉行第二次打擊「網路犯罪及相關事項高層聯合對話」，檢討網路兵推的成果（2016 年 4 月舉行），檢視熱線機制的範圍、目標與程序等。[28] 九月，歐巴馬與習近平利用 G-20 杭州會議場合舉行高峰會，兩人觸及網路安全合作議題，包括：網路犯罪調查、企業網路通信、關鍵基礎設施網路防護、網路兵推等。[29] 11 月，第二次「國際網路空間規範及相關問題資深專家會議」在北京舉行。12 月，美中兩國召開第三次「網路犯罪及相關事項高層聯合對話」，正式啟動熱線機制，討論進一步防範駭客入侵、網路詐欺與網路恐怖主義等問題。[30] 即使美中發表網路安全五點共識，並召開多項會議，但絕大多數的觀察者對中方能否確實履行不具有信心，懷疑中國持續對美國進行「網路間諜」活動。[31] 因此，部分專家認為美國政府應採取更進一步的制裁行動。

---

28. U.S. Department of Justice Office of Public Affairs, "Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue," June 14, 2016, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue>.

29. The White House, "U.S. Fact Sheet for President Obama's Bilateral Meeting with President Xi Jinping," September 3, 2016, *The White House President Barack Obama*, <https://obamawhitehouse.archives.gov/the-press-office/2016/09/03/us-fact-sheet-president-obamas-bilateral-meeting-president-xi-jinping>.

30. U.S. Department of Justice Office of Public Affairs, "Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," December 8, 2016, *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues>; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2016* (Washington, D.C.: U.S. Department of Defense, 2016), p. 37.

三、歐巴馬未強力制裁中國「網路間諜」案

歐巴馬總統雖曾在「聯邦人事管理局」事件之前（2015 年 4 月）簽署一項行政命令，當美國國家安全、外交政策、經濟健全或金融穩定遭受危急時，可對竊密的間諜個人、公司、政府進行制裁，使中國人士或企業無法接近美國市場，企業負責人無法進入美國。[32] 然而，歐巴馬政府並未完全禁止政府部門採購中國資訊科技產品，起訴中國解放軍軍官，卻未有強力制裁行動，也未採取攻擊性的網路報復，而是透過政府雙邊對話機制，使中國節制網路空間的行為，主要考慮是不願意破壞美中關係。[33] 歐巴馬與中國舉行八輪「戰略與經濟對話」談判、促成氣候變遷《巴黎協定》(*Paris Agreement*)的簽署，針對重大軍事演習通知、海空機艦近接相遇安全規則、「網路間諜」遏止等類似「信心建立措施」，這些決策均反映「新自由機制主義」(Neo-Liberal Institutionalism)的實踐。這也與歐巴馬領導風格有關，因他相信透過雙邊對話，可使北京改變「網路間諜」的行為，例如，習近平接受五點共識，也願意與美方進行一系列的對話。當然，歐巴馬政府認定「網路間諜」是一種情報行為，也抑制了對北京的強硬制裁的行動。

歐巴馬政府安全戰略從「轉向亞太」(Pivot toward Asia-Pacific)

---

31. "The Obama-Xi Cyber Mirage," *Wall Street Journal*, September 29, 2015, p. A10.

32. The White House, "Executive Order – 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'" April 1, 2015, *The White House President Barack Obama*, <https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.

33. Bill Gertz, *iWar: War and Peace in the Information Age* (New York: Threshold Editions, 2017), p. 127.

更名為「亞洲再平衡」(Asia rebalancing)，但實質內容卻無重大不同。「亞洲再平衡」的政策內容為：第一，強化美國在區域的安全同盟體系與防衛部署；第二，深化與崛起大國（中國、印度）之間的夥伴關係；第三，加強參與東協、東亞高峰會的活動，在東協總部派駐一位美國大使；第四，與中國建立穩定與建設性關係，表明無意圍堵中國；第五，促進區域的經濟建構(economic architecture)，如推動建立「跨太平洋夥伴關係」(Trans-Pacific Partnership)。歐巴馬總統對中國的政策，顯示「自由主義」合作的傾向，無論是美中建立新型大國夥伴關係，以尋求戰略穩定，所凸顯的「互賴自由主義」(Interdependence Liberalism)，或強調兩國透過「戰略與經濟對話」機制解決網路爭議的「新自由機制主義」，再輔以從低階的打擊網路犯罪，到安全敏感議題如網路禁止攻擊關鍵基礎設施的「功能自由主義」(Functional Liberalism)，均可看出與單邊主義及「攻勢現實主義」有重大的歧異。

依歐巴馬第一任期負責亞太事務的助理國務卿坎博(Kurt Campbell)的說法，美中關係發展出「管理競爭、促進合作」兩套工作計畫，雙方主要歧見依序為：中國軍事現代化改變亞洲戰略平衡；中國在東海與南海的海洋主張；中國日益獨斷的網路空間作為；中國補貼企業與操縱匯率；中國人權問題與臺灣議題。[34] 網路安全在「亞洲再平衡」戰略的優先性不高。歐巴馬政府即使面對中國駭客的入侵，在 2014 年 11 月「亞太經合會」(Asia-Pacific Economic Cooperation, APEC)北京高峰會，宣布給予中國國民以旅客和商務人士最長可達 10 年的多次入境簽證、中國學生獲得有效期為五年的簽證。中方同意將更多、更新的美國資訊科技產品（如全球定位系統 GPS、醫療設備、電玩產品）納入關稅減免的範圍。美中更達成受人矚目的降低碳排放量協議，歐巴馬成功促使習近平承諾中國在 2030 年之前，限制碳的排放量，並將非

34. Kurt M. Campbell, *The Pivot: The Future of American Statecraft in Asia* (New York: Hachette Book Group, 2016), pp. 237-245.

石化能源的使用比重，提升至20%。[35]美中兩國軍隊在反制海盜、海上搜索救難、人道救援等有多面向合作，歐習兩人亦在 APEC 年會確認美中達成的〈重大軍事行動相互通報信心建立措施機制〉(On Notification of Major Military Activities Confidence-Building Measures Mechanism)、〈公海海域海空軍事安全行為準則〉(Rules of Behavior for Safety of Air and Maritime Encounters)兩項諒解備忘錄。

2015 年美國「聯邦人事管理局」事件後，習近平與歐巴馬立即達成的網路安全五點共識，讓中方免於美國的制裁。美國除了經濟制裁之外，可採取外交施壓、嚴格執法、結合軍方與情報單位駭客反擊的力量等，讓北京了解網路攻擊會嚴重影響美中雙邊的關係。美國亦提升政府部門與企業的網路安全防護，與其他友邦加強網路防護資訊的合作，提升與中國的網路對話至部長層級。歐巴馬總統在任期最後一年成立「強化國家網路安全委員會」(Commission on Enhancing National Cybersecurity)，調查報告建議「聯邦人事管理局」在 2020 年前，協助政府新增 200 位文人網路專家計畫，但沒有指名批判中國。[36]川普政府 2017 年上臺之後，美中只舉行一次部長層級的「執法與網路安全對話」（請見表 1），網路安全也進入一個更為複雜的新面向。

35. "The U.S. and China Reach a Landmark Climate Deal," *Washington Post*, November 12, 2014, <https://www.washingtonpost.com/opinions/the-us-and-china-reach-a-landmark-climate-deal/2014/11/12/a1f49f4c-6aa5-11e4-a31c-77759fc1eacc_story.html>.

36. U.S. Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (Washington, D.C.: U.S. Commission on Enhancing National Cybersecurity, 2016), p. 57.

表 1 2009 年以來美中舉行的網路安全會談

時 間	會談名稱	主要參與者	備 註
2013 年 6 月	美中元首在加州安納柏格莊園(Annenberg Estate)的非正式會晤	歐巴馬、習近平	同意針對網路安全建立規則與處理方式，以建立互信、減少誤判風險等。
2013 年 7 月	在華府同時舉行第五輪美中「戰略與經濟對話」與第一次「網路工作小組」會議	美國國務卿凱瑞、中國國務委員楊潔篪，以及美中政府相關部門專家	2013 年 4 月美國在「戰略與經濟對話」下的「戰略安全對話」成立「網路工作小組」。
2013 年 12 月	第二次「網路工作小組」會議	美國國務院、中國外交部，以及美中政府相關部門專家	美中討論網路安全問題，但 2014 年美國司法部起訴解放軍駭客後，北京決定中斷此一小組。
2015 年 9 月	在華府舉行「美中元首高峰會」	歐巴馬、習近平	達成五點網路安全共識，同意每年舉行兩次網路對話會議，處理網路安全相關問題。
2015 年 12 月	在華府舉行第一次美中「打擊網路犯罪及相關事項高層對話」	美國司法部長林琪(Loretta Lynch)、美國國土安全部長詹遜(Jeh Johnson)、中國公安部長郭聲琨	達成打擊網路犯罪及相關事項指導綱領，確認設立熱線，在網路安全個案、網路反恐、執法培訓等取得共識。
2016 年 5 月	第一次「國際網路空間規範及相關問題資深專家會議」	美國國務院、中國外交部，以及美中政府相關部門專家	討論網路安全領域的國際法及雙邊「信心建立措施」等議題。
2016 年 6 月	第八輪「戰略與經濟對話」及第二次打擊「網路犯罪及相關事項高層聯合對話」	美國國務卿凱瑞、中國國務委員楊潔篪；美國司法部長林琪、美國國土安全部長詹遜、中國公安部長郭聲琨	檢視熱線機制的範圍、目標與程序，檢討兵推成效。
2016 年 9 月	在杭州G20 會議的「美中元首高峰會」	歐巴馬、習近平	探討網路犯罪調查、關鍵基礎設施網路防護、網路兵推等網路安全合作。
2016 年 11 月	在北京舉行第二次「國際網路空間及相關問題規範資深專家會議」	美國國務院、中國外交部，以及美中政府相關部門專家	討論網路安全領域的國際法及雙邊「信心建立措施」等議題。
2016 年 12 月	第三次打擊「網路犯罪及相關事項高層聯合對話」	美國司法部長林琪、美國國土安全部長詹遜、中國公安部長郭聲琨	正式啟動熱線、打擊網路詐欺、網路恐怖主義。
2017 年 4 月	美中元首在佛羅里達州「海湖莊園」會晤	川普、習近平	同意設立「執法與網路安全對話」。

2017 年 10 月	「執法與網路安全對話」	美國時任司法部長塞辛斯(Jefferson B. Sessions III)、代理國土安全部長杜克(Elaine Duke)、中國公安部長郭聲琨	重申歐、習達成的五點共識，在資訊分享、打擊網路犯罪方面合作，考慮在關鍵基礎設施防護上，建立熱線機制。
2017 年 11 月	在北京舉行「美中元首高峰會」	川普、習近平	重申落實歐、習達成的五點共識。

資料來源：作者自行整理。

參、川普因應中國網路安全的威脅

2017 年 4 月，川普與習近平在於佛羅里達州「海湖莊園」會晤，同意美中設立四個對話機制：「外交與安全對話」(Diplomatic and Security Dialogue)、「執法與網路安全對話」(Law Enforcement and Cyber Security Dialogue)、「社會與文化議題對話」(Social and Cultural Issues Dialogue)、「全面經濟對話」(Comprehensive Economic Dialogue)。五月，川普簽署〈強化聯邦政府系統組織與關鍵基礎設施網路安全〉(Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)行政命令，要求國務卿限期提出「網路安全國際合作的交往戰略」(An Engagement Strategy for International Cooperation in Cybersecurity)。[37]10 月，美中兩國首度召開「執法與網路安全對話」會議，美方由時任司法部長塞辛斯(Jefferson B. Sessions III)、代理國土安全部長杜克(Elaine Duke)與中國公安部長郭聲琨共同主持，重申歐巴馬與習近平在 2015 年網路安全的五點共識，兩國表示在打擊網路犯罪方面的合作，考慮未來在關鍵基礎設施網路安全的防護(con-

37. 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/>.

sidering future efforts on cybersecurity of critical infrastructure)，透過熱線機制，就緊急網路犯罪和與重大網路安全事件等，及時在領導或工作階層進行溝通。[38]11 月，川普總統訪問北京，與習近平舉行高峰會，強調在網路竊取智慧財產、恐怖主義份子利用網路犯罪、網路槍枝買賣、兒童色情等問題上，相互給予執法的協助。[39]然而，隨著川普對中國的戰略出現重大的調整，網路犯罪議題變得相對次要。

川普政府的美中關係除經貿談判之外，不熱中與中國進行外交、軍事、網路安全等議題的協商，在「讓美國再次偉大」口號下，意味美國霸權的維持。這類似「修昔底德陷阱」(Thucydides Trap)、霸權「興衰現實主義」(Rise and Fall Realism)或「權力移轉理論」(Power Transition Theory)的分析。[40]既有霸權與崛起強權針對國際關係規則的制訂、現狀的維持、領導地位的爭奪，可能有「預防性戰爭」或「挑戰者戰爭」。川普為使美國霸權地位不受中國的挑戰，在美中經貿協定前後，擴大網路科技安全的競爭範疇，將主要戰線集中對中國華為的科技圍堵。然而，川普政府退出多個國際組織，卻可能讓挑戰的中國增加取代美國領導地位的機會。中國透過「國際電信聯盟」(International Telecommunication Union, ITU)、「上海合作組織」、聯合國等推動「網路主權論」，削弱美國的「網路霸權」及其倡導的

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

39. The White House, "Remarks by President Trump and President Xi of China in Joint Press Statement," November 9, 2017, *The White House*, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-xi-china-joint-press-statement-beijing-china/>.

40. 有關「興衰現實主義」六篇論文的討論，請見 Colin Elman & Michael A. Jensen, eds., *Realism Reader* (London: Routledge, 2014), pp. 205-242。

「網路自由論」即為一例。

一、川普提高對中國網路科技威脅的認知

2017 年 12 月，川普的第一份《美國國家安全戰略》(*National Security Strategy of the United States of America*)報告，將中國、俄羅斯定位為「修正主義強權」(revisionist powers)、「戰略競爭者」(strategic competitors)。此一報告指控中國利用「網路增強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；俄羅斯則被歸咎使用資訊、攻擊性網路行動，結合秘密情報行動、假帳號與社群媒體等輸出其影響力。[41] 2018年，美國「國家情報總監」的「國家反情報與安全中心」(National Counterintelligence and Security Center)公布的《網路空間的外國經濟間諜》(*Foreign Economic Espionage in Cyberspace*)報告，將中國列在俄羅斯、伊朗之前，儼然成為最大的威脅來源，指出中國透過下列途徑對美國進行經濟間諜活動，如：利用科技與商業人士非傳統的情報蒐集者、中美合資計畫、研究夥伴、學術性合作、科技投資、併購、幌子公司(front companies)、人才招募、情報人員活動、法律與規範等。中國鎖定的美國企業以能源、生物科技、國防科技、環境保護、高端製造、資通訊科技為主。[42]

川普政府網路安全政策最大特色是，將網路科技安全與美中貿易逆差掛勾在一起，達到「一石多鳥」的目的，例如：阻止中國網路竊取智慧財產權、降低美中貿易逆差、減少中國網路監視科技危害人

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

42. U.S. National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace, 2018," 2018, p. 6, *U.S. National Counterintelligence and Security Center*, <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>.

權、因應中國網路科技可能領先的威脅，延緩中國取代美國霸權。2016 年 12 月，歐巴馬政府阻止德國政府允許中國「福建宏芯」(Fujian Grand Chip)投資基金收購德國半導體製造廠「愛思強」(Aixtron)。川普政府「美國外資審查委員會」(Committee on Foreign Investment in the United States, CFIUS)基於國家安全考慮，對中國高科技公司併購歐美國家晶片廠與企業，採取更嚴格的立場。例如，2017 年 9 月，禁止中資背景「峽谷橋股權」(Canyon Bridge Capital)併購美國晶片廠「萊迪思半導體公司」(Lattice Semiconductor Corp)；2018 年 1 月，阻止馬雲的阿里巴巴旗下「螞蟻金服」(Ant International)收購金融轉帳服務公司「速匯金」(MoneyGram International)；2018 年 4 月，終止中國「海航集團」(HNA Group)併購美國「天橋基金」(Skybridge Capital)的計畫。北京的回應是，相關國家對中國企業海外收購「正常的商業行為」，應給予公平的待遇，避免對投資者信心產生影響。

2018 年 2 月，時任中國國務委員楊潔篪提到計畫在年內召開中美四個對話機制會議。[43]北京顯然未預見川普對美中高層對話機制已做出改變。11 月，美中雖舉行第二輪「外交與安全對話」會議，但原訂 2018 年召開的第二輪「社會與文化議題對話」、「執法與網路安全對話」會議從此未再召開。相較於歐巴馬在一年之內舉行三輪部長層級的網路安全對話會議，川普總統顯然無意延續此一對話機制。川普政府的自由開放「印太戰略」(Indo-Pacific Strategy)雖不排斥中國，但國防部認定中國從事全球性的網路偷竊，並鎖定美國智慧財產、機密企業與科技資訊。[44]國務卿蓬佩奧(Michael Pompeo)針對中國「一帶一

43. "China, U.S. should make good use of four dialogue pillars: Chinese state councilor," *Xinhua*, February 9, 2018, <http://www.xinhuanet.com/english/2018-02/09/c_136961876.htm>.

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

路」的政策，主張在印太地區建立「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。[45]川普政府在網路安全的議題上，加強對中國的警戒，由歐巴馬時期的雙邊對話解決，調整為單方政策作為，更在國會議員的要求下，啟動對中國網路資訊科技大廠的制裁。

2018 年 1-2 月，美國眾議員康納威（Mike Conaway，共和黨，德州）與錢妮（Liz Cheney，共和黨，懷俄明州）、參議員盧比歐（Marco Rubio，共和黨，佛羅里達州）和卡登（Tom Cotton，共和黨，阿肯色州）提出《防護美國政府通訊法案》(*Defending U.S. Government Communications Act*)禁止美國政府機關採購華為、「中興通訊」(Zhongxing Telecommunication Equipment, ZTE)、「大唐」(Datang Telecomm Technology)等中國產品與服務，並禁止將其設備做為美國電信設施的核心技術。[46]一月，川普政府施壓兩家美國電信運營商美國電報電話公司(AT&T)和威瑞森公司(Verizon)，放棄與中國華為合作在美國銷售手機。四月，川普政府以中興通訊違反美國政府對伊朗與北韓制裁，將內有高通(Qualcomm)晶片的手機輸出到該等國家，而決定七年內禁止美國科技廠商出售產品給中興通訊。5 月 8 日川普致電習近

45. Michael Pompeo, "Secretary Pompeo's Remarks at the Indo-Pacific Business Forum," July 30, 2018, *American Institute in Taiwan*, <https://www.ait.org.tw/secretary-pompeos-remarks-at-the-indo-pacific-business-forum/>.

46. Mike Conaway, "Conaway, Cotton, Rubio, Cheney, and Ruppersberger Raise Concerns about Google's Partnership with Huawei," June 20, 2018, *Mike Conaway 11th District of Texas*, <https://conaway.house.gov/news/documentsingle.aspx?DocumentID=398400>; Dennis F. Poindexter, *The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests*, pp. 29-30; David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, p. 264.

平，除北韓議題外，習近平提到美方若能在中興通訊予以寬容，將欠川普一個人情；隨後雙方達成妥協，罰款中興通訊 10 億美金，時任國家安全顧問波頓(John Bolton)稱這對該公司「不僅是緩刑，更是生命的新契機」。[47]

2018 年 9 月，白宮公布《美國國家網路戰略》(*National Cyber Strategy of the United States of America*)，強調保護網路、系統、功能及數據，以確保國土防衛；培養安全繁榮的數位經濟、壯大國內創新，以促進美國經濟繁榮；強化美國確保和平與安全的能力；與盟友協調強化嚇阻的途徑，必要時懲罰那些惡意使用網路工具者；擴大美國海外影響力，確保一個開放、互通性、可靠、安全的網路。[48]波頓宣稱這改變了歐巴馬在網路安全所採取的被動、防禦態勢，因其帶來更多挑釁、衝突與傷害。對美國而言，網路安全不僅是國防部、國內的網路防護，也包括對外的網路作戰攻擊能力、協助盟邦與友邦的網路能力建構。美國的「網路戰」例子是，在 2010 年與以色列秘密地對伊朗核設施植入「震網」(Stuxnet)電腦蠕蟲；2018 年對敘利亞的飛彈攻擊，搭配網路攻擊敘利亞管制中心，使其誤報飛彈攻擊預定到達時間，但波頓承認「網路嚇阻說得比做得容易」。[49]

二、展開對華為的制裁與圍堵行動

2019 年 1 月，參議員卡登、眾議員蓋拉格（Mike Gallagher，共

47. John Bolton, *The Room Where It Happened: A White House Memoir* (New York: Simon & Schuster, 2020), pp. 293-295.

48. The White House, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, 2018), p. 3；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》（北京），2019 年第 1 期，2019 年 3 月，頁 122-123。

49. John Bolton, *The Room Where It Happened: A White House Memoir*, pp. 176, 181.

和黨，威斯康辛州）於參眾兩院提出《電信拒絕令執行法》(*Telecommunications Denial Order Enforcement Act*)，規定美國晶片及零組件不得出售給違反美國制裁法規、出口管制禁令的華為與「中興通訊」。[50]川普政府經由智慧財產權的保護，縮減對中國貿易逆差，除可將網路科技安全納入貿易談判解決，也可藉其違法蒐集美國資訊秘密、迫害中國少數民族人權、違背聯合國對伊朗制裁為由，對中國展開網路安全科技制裁。

川普政府正視中國在敏感科技能力對美國霸權的挑戰。2019 年 5 月，川普援引《國家緊急經濟權力法》(*International Emergency Economic Powers Act*)、《國家緊急法》(*National Emergencies Act*)，以國家安全為由發布〈保護資訊科技與服務供應鏈行政命令〉(Executive Order on Securing the Information and Communications Technology and Services Supply Chain)，基於「外國對手」(foreign adversaries)增加利用資通訊科技與服務的脆弱性，「進行對美國與人民惡意的經濟與企業間諜等網路行動」，「構成美國國家安全、外交政策、經濟的一項異常與特別威脅」，宣布基於「國家緊急」狀態，禁止美國企業採購對國家安全帶來威脅的外國電信廠設備。[51]行政命令雖未點名任何國家或企業，但有五處提及「外國對手」，顯然是針對華為、中興通訊在內的中國電信大廠。美國商務部基於華為從事「有違美國國家

50. Mike Gallagher, "Gallagher, Cotton, Van Hollen & Gallego Introduce Bill to Impose Denial Orders on Chinese Telecomm Companies That Violate US Sanctions," January 16, 2019, *Congressman Mike Gallagher Representing the 8th District of Wisconsin*, <https://gallagher.house.gov/media/press-releases/gallagher-cotton-van-hollen-gallego-introduce-bill-impose-denial-orders-chinese>.

51. The White House, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019, *The White House*, <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>.

安全與外交政策利益」，將其與 70 家附屬事業列入出口管制「實體清單」(entity list)，必須有商務部「工業及安全局」(Bureau of Industry and Security)簽發出口執照方可放行。[52] 此舉使華為難以出售部分產品，其新手機將無法搭載谷歌應用程式，美國電腦晶片公司也將切斷對華為第五代行動通訊(5G)無線網路的供應鏈。[53]

2019 年 6 月，川普政府進一步將中國超級電腦製造商如「曙光」(Sugon)、「天津海光」(Tianjin Haiguang Advanced Technology Investment Co., Ltd)、「成都海光集成電路」(Chengdu Haiguang Integrated Circuit)、「成都海光微電子技術」(Chengdu Haiguang Microelectronics Technology)，以及「無錫江南計算技術研究所」(Wuxi Jiangnan Institute of Computing Technology)等，列為「實體清單」，阻止中方取得美國高性能運算、軍事應用等科技項目。10 月，川普政府基於中國新疆維吾爾自治區迫害人權因素，除制裁該自治區內 20 個單位外，並將中國八家生產監視、人臉辨認、聲音辨識、人工智慧、奈米等科技公司，以助長違反少數民族人權為由，列為美國科技產品管制的「實體清單」。[54] 川普政府以中國當局迫害人權為由，對中國資通訊科技公司的制裁，達到阻止中國科技凌駕美國的趨勢。中國的量

52. U.S. Embassy and Consulates in China, "Department of Commerce Announces the Addition of Huawei to the Entity List," May 2019, *U.S. Embassy and Consulates in China*, <https://china.usembassy-china.org.cn/department-of-commerce-announces-the-addition-of-huawei-to-the-entity-list/>.

53. David E. Sanger, "Huawei Ban Gains Trump a Wall at Last," *New York Times*, May 28, 2019, pp. A1, A11。美國商務部隨後決定對華為的出口黑名單提供少量的暫時性豁免，讓其部分供應商和客戶，在 90 天內免受嚴苛的貿易懲罰。

54. Ana Swanson & Paul Mozur, "Chinese Entities Blacklisted As U.S. Cites Rights Abuses," *New York Times*, October 8, 2019, p. B4。這些中國高科技公司，包括大華科技 (Dahua Technology)、海康威視(Hikvision)、科大

子計算、3D 製造、引導人工智慧的演算法等，亦成為美國擴大打擊與遏止中國的項目。

華為在 5G 技術領先，國際市場價格具有優勢，加上與中國黨政軍密切關係，在 2008-2018 年期間獲得中國政府各項補貼至少 750 億美金，但因曾長期竊聽「非洲聯盟」(African Union)網路設施，而成為川普眼中的「邪惡科技公司」代名詞。[55] 華為亦涉嫌竊取美國無線網路運營商 T-Mobile US 測試智慧型手機的機器人技術。2018 年 12 月，在美國的要求下，加拿大以違反伊朗貿易制裁禁令為由，逮捕華為財務長孟晚舟。美國國會議員除了擔心中國華為的先進資訊科技之外，亦指出北京頒布的《國家情報法》第七條規定，中國資訊科技公司必須「依法支持、協助和配合國家情報工作，保守所知悉的國家情報工作秘密」。2018 年 11 月「美中經濟暨安全檢討委員會」(U.S.-China Economic and Security Review Commission)報告，要求白宮「管理及預算局」(Office of Management and Budget)確保政府機構能解決源自中國，包括潛在的網路、操作、實體、資訊及數據安全問題；要求美國「國家電信暨資訊管理局」(National Telecommunications and Information Administration)和「聯邦傳播委員會」(Federal Communications Commission)確保 5G 技術在美國迅速、安全佈建；要求商務部重新評估美國對中國軍民兩用技術的出口管制政策。[56]

美國參議員卡登和參議員華納（Mark Warner，民主黨，維吉尼亞

訊飛(IFLYTEK)、曠視(Megvii Technology)、商湯(Sense Time)、美亞柏科(Meiya Pico Information Co. Ltd)、依圖科技(Yitu Technologies)、乙麟科技有限公司(Yilin Science and Technology Co. Ltd)。

55. Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019, <https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736?mod=searchresults&page=1&pos=20>.

56. Kate O'Keeffe, "U.S. Panel Warns China Tech Prowess Threatens U.S.

州）指稱華為具嚴重的網絡安全風險，在情報分享網絡內之「五眼聯盟」（Five Eyes，澳洲、加拿大、紐西蘭、英國和美國）國家不應使用該公司智慧型手機和設備。他們更於 2019 年 7 月提出《防衛美國 5G 未來法案》(*Defending America's 5G Future Act*)監督川普政府嚴守對華為的科技管制。川普政府不僅在單邊、雙邊層次圍堵華為，更遊說美國盟邦共同因應中國 5G 威脅，不要允許華為參與該國 5G 網路構建，否則將縮減彼此的情報共享。[57]

2019 年 2 月，美國副總統彭斯(Mike Pence)在「慕尼黑安全會議」(Munich Security Conference)點名華為，呼籲所有美國安全夥伴必須保持警覺，拒絕任何可能破壞西方國家通訊科技或國家安全系統完整性的企業。[58] 10 月，彭斯在「威爾遜中心」(Wilson Center)演講提到，美國聯邦調查局在調查 1,000 件竊取美國智慧財產權的案例有一半是來自中國；為保護美國智慧財產權、美國人民隱私、國家安全，將採取強烈措施因應華為、中興的違法行為，並呼籲美國與盟邦（如日本）確保亞洲 5G 的建構，不要讓北京有控制關鍵基礎設施與資料的機會。[59]

川普政府試圖說服全球盟友在其網路中禁用華為的 5G 設備，使各國政府和企業被迫在西方路線和中國模式之間做出選擇。北京裝設超

Security," *Wall Street Journal*, November 14, 2018. < https://www.wsj.com/articles/u-s-panel-warns-china-tech-prowess-threatens-u-s-security-1542171601>.

57. David Brunnstrom, "Pompeo Tells Germany: Use Huawei and Lose Access to Our Data," *Reuters*, May 31, 2019, <https://www.reuters.com/article/us-usa-germany/pompeo-to-germany-use-huawei-and-lose-access-to-our-data-idUSKCN1T10HH>.

58. David E. Sanger, Julian E. Barnes, Raymond Zhong, & Marc Santora, "U.S. Scrambles to Outrun China in New Arms Race," *New York Times*, January 27, 2019, p. A1.

59. Wilson Center, "Remarks by Vice President Pence at the Frederic V. Malek Memorial Lecture," October 24, 2019, *The White House*, <https://www.

級防火牆的成功經驗，鼓勵許多專制政府試圖封鎖國內網際網路，加強了社會與政治控制，而中國也成為「數位威權主義」(digital authoritarianism)的代表。西方國家網路運作的最高原則是自由主義及寬鬆的規範，原是國際默認的標準，但一些開發中國家正朝中國的網路發展模式發展。美國「自由之家」(Freedom House)估計至少有 38 個國家的網路及手機通訊基礎設施，是由中國科技公司負責建構，並選擇中國網路平臺如阿里巴巴、騰訊與百度，受到北京當局的嚴密監控、審查與干預，而中國自 2015 年起在 65 個網路自由調查的國家之中紀錄最差。[60]2019 年 10 月，美國參議院少數黨領袖舒默（Chuck Schumer，民主黨，紐約州）、參議員卡登針對類似臉書的中國應用程式「抖音」(TikTok)，要求美國情報機關調查是否其涉及影音分享平臺蒐集資訊及審查美國用戶所見內容，進而成為中國對外輸出假訊息、惡意影響力的渠道。[61] 2020 年 9 月，川普基於此一理由對抖音與微信採取禁令或限制。

歐巴馬政府奠定美中兩國網路安全對話的基礎。川普總統上臺雖重申歐巴馬與習近平所達成的五點共識，卻只舉行一輪部長層級「執法與網路安全對話」，網路安全機制未再發揮作用。兩國的資訊科技競逐，伴隨貿易戰而日益升溫。川普總統發動對中國的關稅戰，限制中國資通訊科技業對美國的投資。中國也悄悄恢復對美國的「網路間

whitehouse.gov/briefings-statements/remarks-vice-president-pence-frederic-v-malek-memorial-lecture/>.

60. Adrian Shahbaz, "Fake News, Data Collection, and the Challenge to Democracy," *Freedom on the Net 2018*, Noverber 3, 2020, Accessed, *Freedom House*, <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>.

61. Li Yuan, "China's TikTok Blazes New Ground. That Could Doom It," *New York Times*, November 5, 2019, <https://www.nytimes.com/2019/11/05/business/tiktok-china-bytedance.html>.

諜」活動。2019 年 2 月，美國網路安全公司「群擊」(Crowdstrike)指出，中國放棄與前總統歐巴馬停止網路駭侵企業的共識，例如 2018 年對美國通訊部門的駭客攻擊次數比以前更甚。[62] 在新冠肺炎疫情爆發之後，2020 年 5 月川普政府發現，中國駭客入侵美國疫苗與藥物研發機構的惡意行為。[63]

肆、北京低調因應美中網路安全問題

一、加速提升網路能力縮小中美差距

在歐巴馬政府升高對中國「網路間諜」指控之際，2013 年 11 月 12 日，中共十八屆三中全會決定設立國家安全委員會。之後中共總書記習近平在「中央國家安全委員會」第一次委員會議提出 11 種總體安全觀，依序為：政治安全、國土安全、軍事安全、經濟安全、文化安全、社會安全、科技安全、信息（資訊）安全、生態安全、資源安全、核安全。其中，「信息安全」排在第八位。[64] 中國官方認為網路帶來訊息新渠道、生產新空間、經濟新引擎、文化新載體、治理新平臺、交流新紐帶、主權新領域，但網路也可能危害政治安全、侵蝕文

62. Alyza Sebenius, “China Has Abandoned a Cybersecurity Truce With the U.S., Report Says,” *Bloomberg*, February 19, 2019, <https://www.bloomberg.com/news/articles/2019-02-19/china-abandons-cybersecurity-truce-with-u-s-report-says>; Adam Segal, “A New Old Threat Countering the Return of Chinese Industrial Cyber Espionage,” December 6, 2018, *Council for Foreign Relations*, <https://www.cfr.org/report/threat-chinese-espionage>.

63. David E. Sanger & Nicole Perlroth, “U.S. to Accuse China of Trying to Steal Data,” *New York Times*, May 11, 2020, p. A7.

64.〈習近平：堅持總體國家安全觀 走中國特色國家安全道路〉，《新華網》，2014 年 4 月 15 日，<http://www.xinhuanet.com/politics/2014-04/15/c_1110253910.htm>。

化安全、破壞社會安全。[65] 習近平在機構改革上，為突出網路安全的重要性，將原有「國家信息化領導小組」及其下「網絡安全協調小組」，合併為「中央網絡安全和信息化領導小組」。2014 年 2 月，習近平主持該小組第一次會議時指出，沒有網路安全就沒有國家安全，沒有信息化就沒有現代化。[66]

從習近平的角度，「網絡安全對國家安全牽一髮而動全身」，但網路安全只是國家安全的一環，因為有許多資訊、情報、文件、作戰構想等，不存在於網路空間。網路安全卻是國力的倍增器，也使傳統的國家安全增添新的面貌與挑戰。網路攻擊的源頭難以追蹤或咎責，而受攻擊者難以察覺，也使得網路在國家安全的角色愈來愈重要。根據美國國防部定義，「不對稱作戰」指的是迴避或破壞對手優勢，並抓住其弱點，採取截然不同於對手慣用作戰模式的方法。以己之強，擊敵之弱，使用非正規、難預測或創新方法的攻擊或防衛，達到損小、利多的不成比例的效果。非正統的游擊戰、恐怖主義攻擊、「網路作戰」均屬之。在武器選擇上，機動、匿蹤、精準、智能化、低成本、敵難反制等亦屬之。

2016 年 4 月，習近平在網路安全和資訊化工作座談會，指出「互聯網核心技術是我們最大的『命門』，核心技術受制於人是我們最大

65. 中國國家互聯網信息辦公室，〈國家網絡空間安全戰略〉，2016 年 12 月 27 日，《國家互聯網信息辦公室》，<http://www.cac.gov.cn/2016-12/27/c_1120195926.htm>；中國國家信息中心，《中國網絡媒體社會價值白皮書》，2020 年 4 月 13 日，頁 17，《國家信息中心》，<http://www.sic.gov.cn/News/79/10458.htm>。

66. 〈中央網絡安全和信息化領導小組第一次會議召開 習近平發表重要講話〉，《新華網》，2014 年 2 月 27 日，<http://www.cac.gov.cn/2014-02/27/c_133148354.htm>。2018 年 3 月，因應十九大後機構改革，原有領導小組更名為「中央網絡安全和信息化委員會」，並見 Nigel Inkster, *China's Cyber Power*, p. 41。

的隱患。……我們要掌握我國互聯網發展主動權，保障互聯網安全、國家安全，就必須突破核心技術這個難題，爭取在某些領域、某些方面實現『彎道超車』」。習近平強調「網絡安全威脅和風險日益突出，－特別是國家關鍵資訊基礎設施面臨較大風險隱患，網絡安全防控能力薄弱，難以有效應對國家級、有組織的高強度網路攻擊」。習近平進一步提出：一、要建立的正確的網路安全觀；二、加速建立金融、能源、電力、通信、交通等關鍵資訊基礎設施的安全保障體系；三、建立全天候全方位感知網路安全態勢；四、加強網路安全防禦與威嚇能力，特別是「大國網絡安全博弈，不單是技術博弈，還是理念博弈、話語權博弈」。[67] 習近平顯然是針對「網路最先進」、「網路霸權」的美國為目標。若要達到此目標，中國除「研發並應用自主可控的網絡信息技術產品」、「加強建設網絡空間軍事力量」之外，更要建立「國家網絡安全戰略」，以及通過網路安全各項立法。[68]

2016 年 11 月中國人大常委會通過《網絡安全法》。12 月，中國國家互聯網信息辦公室發布《國家網絡空間安全戰略》。《網絡安全法》宣示「保障網絡安全，維護網絡空間主權和國家安全、社會公共利益」，多項條文涉及「關鍵資訊基礎設施」與美國及其企業。例如，強調「採取措施，監測、防禦、處置來源於中華人民共和國境內外的網路安全風險和威脅，保護關鍵資訊基礎設施免受攻擊、侵入、干擾和破壞」（第五條）；任何在中國大陸「收集和產生的個人資訊和重要數據應當在境內存儲」（第 37 條）；「境外的機構、組織、個人從事攻擊、侵入、干擾、破壞等危害中華人民共和國的關鍵資訊基礎設施的活動，造成嚴重後果的，依法追究法律責任」（第 75 條）。

67.〈習近平在網信工作座談會上的講話全文發表〉，《新華網》，2016 年 4 月 25 日，<http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm>。

68.程玉，〈中美雙邊關係中網絡安全問題的成因、摩擦與對策〉，《黨政幹部學刊》（瀋陽），2014 年第 7 期，2014 年 7 月，頁 34-35。

《國家網絡空間安全戰略》亦指出戰略任務之一是，「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、響應、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」。

中國網路安全不僅限於國內網路使用管理、關鍵基礎設施的防護層面，也必須為更大的外交戰略「一帶一路」服務，藉由網路基礎設施的建造與聯通，達到政策溝通、貿易暢通與產業合作的目標。中國在 2017 年 3 月公布的《網絡空間國際合作戰略》提到緊密結合「一帶一路」政策，「支持中國的互聯網企業聯合製造、金融、信息通信等領域企業先走出去，按照公平原則參與國際競爭，共同開拓國際市場，構建跨境產業鏈體系」。更重要地是，中國必須「推動與周邊及其他國家信息基礎設施互聯互通和『一帶一路』建設，讓更多國家和人民共享互聯網帶來的發展機遇」。這意味中國在網路安全負有擴大外交影響力的責任，提供其他國家一種不同於美國網路基礎設施與經濟發展的選擇。當川普政府對中國「一帶一路」有所疑慮，中國的宣示顯然為華為帶來麻煩與阻礙。

2018 年 4 月，習近平指出網路安全是「軍民融合的重點領域和前沿領域，也是軍民融合最具活力和潛力的領域」。[69] 習近平身兼「中央軍民融合發展委員會」主任，更加深美國國務院的疑慮，認為中國軍民融合發展戰略危及全球的安全。[70] 解放軍與電訊業者、科技公司如華為，以及至少 46 家大學保持密切合作關係，超過 1,000 萬名的網路民

69. 張曉松、朱基釵，〈習近平：自主創新推進網路強國建設〉，《新華網》，2018 年 4 月 21 日，<http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm>。

70. Christopher Ashley Ford, “The PRC’s ‘Military-Civil Fusion’ Strategy Is a Global Security Threat,” March 16, 2020, *U.S. Department of State*, <https://www.state.gov/the-prcs-military-civil-fusion-strategy-is-a-global-security-threat/>.

兵，扮演解放軍的後方安全力量。[71]2019 年 7 月，北京公布《新時代的中國國防》白皮書指出：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」。[72]中國對網路空間所帶來的資訊開放必須防範，個人網路自由必須管制，國家安全列於首位，更需要建立網路空間的國際規則，而不是接受美國的領導。這也是中國與美國在虛擬戰場上互爭國際領導權的一環。簡言之，中國針對網路安全既要有「制網權（控制）」，也要有「治網權（治理）」。[73]

二、開展有別於美國的網路國際規則制訂

中國即使力爭國際網路空間的治理權，縮小中美網路技術資源與能力差距，但承認網路空間治理仍受制於美國。例如，美國及其盟友（荷蘭、瑞典、日本）掌握全球 13 臺根網域名稱服務器(root name server)，並主導「網際網路名稱與數字位址分配機構」(Internet Corporation for Assigned Names and Numbers, ICANN)分配網域名稱系統(domain name system)與 IP 地址服務。北京主張「把 ICANN 的職責移交給國際電信聯盟」，中美兩國可以加強在ICANN和「國際電信聯盟」機構下的雙邊對話，促進「兩國網絡安全合作，以及制定相互認可的網絡空間規則」。[74]中國與美國在「硬實力」（技術、軟硬件）、「軟實力」（標準、網絡文化、推特、臉書）的網路空間霸權存有結

71. Nigel Inkster, *China's Cyber Power*, p. 104.

72. 中華人民共和國國防部，〈《新時代的中國國防》白皮書全文〉，2019 年 7 月 24 日，《中華人民共和國國務院新聞辦公室》，<http://www.mod.gov.cn/big5/regulatory/2019-07/24/content_4846424.htm>。

73. 王軍，〈多維視野下的網絡戰：緣起、演進與應對〉，《世界經濟與政治》（北京），2012 年第 7 期，2012 年 7 月，頁 80-98。

74. 耿召，〈特朗普時期中美網絡安全合作分析〉，《美國問題研究》（上

構差距，又受到美國對中國採取「妖魔化」的指控，因此「不得不面對實力和資源有限，必須兼顧國內國外兩個大局，合理分配國內外資源」，方能提升「中國在國際上的話語權和影響力」。[75]因此，中國倡議由國際組織帶頭建立規範，節制美國的網路影響力，進而縮小中美兩國在網路空間能力的差距。

中國強調網路與資訊化主權，內部以國家政府機關為網路空間的主體，強調網路內容的管理，外部主張聯合國發揮領導作用。北京相信適用於發展中國家的是中國的「網路主權論」，而非美國的「網路自由論」。《國家網絡空間安全戰略》提到「推動制定各方普遍接受的網路空間國際規則、網路空間國際反恐公約，健全打擊網路犯罪司法協助機制」。中國、俄羅斯結合其他「上海合作組織」成員，先後在 2011、2015 年向聯合國大會提出〈資訊安全國際行為準則〉(International Code of Conduct for Information Security)，有意削弱美國在網絡空間國際治理的領導地位，並藉由網路主權規避國際人權法的適用。2014 年 11 月，中國在浙江烏鎮舉辦首屆「世界互聯網大會」(World Internet Conference)，並於同一地點陸續舉行年度會議。由一個控制網路自由使用的國家來主辦「世界互聯網大會」有其諷刺性，卻說明北京積極創造網路主權及網路空間國際治理的論述權。美國未派政府高層官員與會，也對美國廠商的「積極參與頗有微詞」。[76]

習近平與歐巴馬達成網路安全五點共識之後三個月，2015 年 12 月初，中方承認中國駭客入侵美國「聯邦人事管理局」，但堅持是駭客自主的犯罪行為，而非官方支助的網路攻擊。[77]12 月中旬，習近平在第

海），2018 年第 2 期，2018 年 2 月，頁 173-174。

75. 李艷，〈網絡空間國際治理中的國家主體與中美網絡關係〉，《現代國際關係》（北京），2018 年 11 期，2018 年 11 月，頁 46。

76. 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》（北京），2019 年第 12 期，2019 年 12 月，頁 18。谷歌執行長皮查伊(Sundar Pichai)、蘋果執行長庫克(Timothy Cook)在 2017 年曾出席。

二屆「世界互聯網大會」，提出「尊重網路主權、維護和平安全、促進開放合作、構建良好秩序」四個原則與五點主張。習近平指出「應該尊重各國自主選擇網路發展道路、網路管理模式、互聯網公共政策和平等參與國際網路空間治理的權利，不搞網路霸權，不干涉他國內政，不從事、縱容或支持危害他國國家安全的網路活動」。五點主張包括：一、加快全球網路基礎設施建設，促進互聯互通；二、打造網上文化交流共享平臺，促進交流互鑑；三、推動網路經濟創新發展，促進共同繁榮；四、保障網路安全，促進有序發展；五、構建網路治理體系，促進公平正義。[78]習近平暗指美國是「網路霸權」，而中國必須有成為「網路強國」的戰略，「尊重網路主權是反對網路霸權的必然要求」，也是「推進全球互聯網治理體系變革的關鍵」。[79]因此，中國也向聯合國安全理事會，提出擴大「國際電信聯盟」角色，取代ICANN的建議。[80] 2015 年 1 月，中國大陸出身的趙厚麟擔任「國際電信聯盟」的秘書長（任期四年），並於 2019 年連任，顯示北京企圖領導國際網路安全的國際規範制訂。

上海社會科學院公布的《中國網路空間安全發展報告(2017)》指出，川普主政之下，美國「將網路空間主要戰略對手從中國轉向俄羅

77. Michael Forsythe & David E. Sanger, “China Says Hacking of U.S. Workers’ Data Was Common Crime, Not State Act,” *New York Times*, December 3, 2015, p. A8.

78. 中華人民共和國外交部，〈習近平：推進全球互聯網治理體系變革應堅持四原則〉，2015 年 12 月 16 日，《中華人民共和國外交部》，<http://www.fmprc.gov.cn/web/zyxw/t1324807.shtml>。

79. 〈堅持尊重網路主權原則　推動構建網絡空間命運共同體〉，《求是》，2016 年 2 月 29 日 ，<http://www.xinhuanet.com//politics/2016-02/29/c_128761848_2.htm>。

80. Dean Cheng, *Cyber Dragon: Inside China’s Information Warfare and Cyber Operations*, p. 62.

斯，為中美網路空間雙邊關係發展提供了窗口期。……進一步提升中美對話層級，穩步擴大網路空間的合作範圍」。[81]這種樂觀的看法與後來事實發展有出入，因為美國真正的網路科技空間對手是中國而非俄羅斯，尤其是環繞對於5G科技的模式、領導與規則制訂的角力。更重要地是，川普政府網路安全、經濟安全與國家安全「三合一」戰略，經由單邊主義修改美國《2018年出口管制法》(*Export Control Reform Act of 2018*)、《外國投資風險審查現代法》(*Foreign Investment Risk Review Modernization Act of 2018*)與啟動《國際突發事件經濟權力法》，箝制中國在高新資訊科技的壯大。依據中方專家的看法，川普政府所建立的美中「執法與網路安全對話」重心，不是在高位階的網路安全問題，兩國網路官員團隊「都沒能在國內建立起有效的統籌協調機制」，而使得兩國網路安全關係呈現「大局穩定但摩擦不斷的局面」。[82]這也是過度樂觀的評論，因為中國的網路資通訊業龍頭面臨最重大的危機。

三、對美國打擊華為保持低調

中國在網路安全能力提升上，主張「軍民結合、寓軍於民」的政策雖可理解，卻遭到川普政府的猜疑，2020年5月宣布吊銷與中國解放軍院校相關研究生的簽證。[83]從川普政府的角度，華為正是利用民營企業的外衣，為中國解放軍購買外國技術，而混淆和消除國防與民間部門的界限，令美國及其歐洲盟友必須更加提防。華為被迫聲明它是

81. 中國石油大學（華東）信息化建設處，〈中國網絡空間安全發展報告(2017)精讀〉，2017年11月10日，《中國石油大學》，<http://nic.upc.edu.cn/2018/0119/c7453a131181/pagem.htm>。

82. 魯傳穎，〈網絡空間大國博弈趨勢和中美對話機制演變〉，《信息安全與通信保密》（成都），2018年第2期，2018年2月，頁18-19。

83. Edward Wong & Julian E. Barnes, "Many Chinese Graduate Students and Researchers to Lose U.S. Visas," *New York Times*, May 29, 2020, p. A17.

私人企業為其員工所擁有，中國政府不干預其企業或產品安全，願對其顧客及其他政府簽署「不進行間諜」及「無後門」協議。[84]華為創辦人任正非在川普總統的杯葛與制裁下，一句「殺出一條血路」，被解讀華為要與美國正面周旋。[85]

2019 年 5 月，川普政府禁止美國企業出口晶片及採購華為電信設備。華為的回應是，這會讓美國使用次級品與更昂貴的設備，最終傷害到美國公司與消費者利益。6 月 18 日，在川、習通電中，習近平警告川普若不妥慎處理此事，將傷及兩國關係；6 月 28-29 日在G20 大阪會議，習近平再度提到在兩國貿易談判解決此一議題。川普雖一度想再寬鬆制裁，但遭核心幕僚反對，以免重蹈中興通訊先硬後軟的覆轍。[86]2020 年 5 月，美國商務部延續此一禁令。美國國務卿蓬佩奧痛斥華為是不值得信賴的供應商，是中國共產黨的工具並受惠於其命令，不僅偷竊美國科技，也協助伊朗逃避制裁。美方也採取更大的限制，只要使用到美國晶片製造設備與軟體的國內外公司，除非取得美國商務部許可，否則不能為華為及其子公司生產或設計晶片。[87]中國外交部認為這是美國「科技霸凌主義」，中國商務部提到這將損害中國企業利益，損害美國企業利益，也損害其他國家企業的利益，並將傷害全

84. Huawei, “Huawei’s Position Paper on Cyber Security,” November 2019, *Huawei*, <https://www.huawei.com/en/facts/voices-of-huawei/huawei-releases-its-position-paper-on-cyber-security>.

85. Dan Strumpf, “Huawei Founder Ren Zhengfei Takes Off the Gloves in Fight Against U.S.,” *Wall Street Journal*, June 6, 2020, <https://www.wsj.com/articles/huawei-founder-ren-zhengfei-takes-off-the-gloves-in-fight-against-u-s-11591416028?mod=searchresults&page=1&pos=2>.

86. John Bolton, *The Room Where It Happened: A White House Memoir*, pp. 308-309.

87. Michael R. Pompeo, “The United States Protects National Security and the Integrity of 5G Network,” May 15, 2020, *U.S. Department of State*,

球產業和供應鏈。

北京宣稱絕不會坐視不理美方的作法，將依照《國家安全法》（2015 年 7 月施行）與《網路安全審查辦法》（2020 年 6 月施行）等法律法規，對高通、思科(Cisco)、蘋果等美國企業，予以調查或限制，甚至暫停採購波音公司飛機等。[88] 實際上，北京卻相對低調，遲遲未採制裁措施，以免落實中國黨政軍是華為的真正老闆的指控。《國家安全法》提到「對影響或者可能影響國家安全的外商投資、特定物項和關鍵技術、網路資訊技術產品和服務」，可「進行國家安全審查，有效預防和化解國家安全風險」（第 59 條）。《網路安全審查辦法》亦有相同的規定（第一、二條）。在中美兩地均有投資的臺灣台積電，2020 年 5 月宣布到美國亞利桑那州投資 120 億美金生產五奈米晶片廠。台積電夾處在中美科技戰之間，美國利用台積電以對華為斷鏈來施壓中國，說明臺灣資通訊科技業面臨必須選邊的壓力。[89]

中國因應川普對華為的封殺，建立多條打開活路的途徑。北京為反制川普的「乾淨網路」(Clean Network)計畫號召排除中國電信公司、應用程式、雲端供應商和海底電纜的統一戰線，特別提出「全球數據安全倡議」，呼籲各國「應為所有企業提供開放、公正、非歧視的營商環境」。[90] 然而，北京亦威脅其他國家（如印度）若阻止華為業務，將對該國在中國經營的企業將予以反制，或威脅懲罰「匯豐銀行」

<https://www.state.gov/the-united-states-protects-national-security-and-the-integrity-of-5g-networks/>.

88.〈消息人士：美若對華為卡脖子，中方反擊清單上將有這些美方公司〉，《環球時報》，2020 年 5 月 15 日，<https://world.huanqiu.com/article/3yFXkzABKfP>。

89. Ana Swanson, Paul Mozur, & Raymond Zhong, "A Tech Fight, U.S. vs. China, Pulls In Taiwan," *New York Times*, May 20, 2020, p. B1.

90. Michael R. Pompeo, "Announcing the Expansion of the Clean Network to Safeguard America's Assets," August 5, 2020, *U.S. Department of State*,

（提供孟晚舟向伊朗匯款決定的資訊）；英國若不讓華為參與 5G 電訊建設，中國將取消在英國建造核電廠的計畫。[91] 華為亦推動供應商從美國移出至海外生產，並轉向歐洲國家，尋找參與 5G 網路基礎建設的機會。此一途徑反映北京官方與華為均認知到川普政府「關閉對中國高科技公司和兩國高科技產品的市場合作」，因此，「中國應當持續加深與歐洲的夥伴關係」及結合更多可以爭取的國家，共同反制美國霸權主義。[92]

四、與美國建立網路安全行為準則的可能性

中國網路資訊實力的提升，堅持「網路主權論」，對照美國堅持「網路自由論」，致使網路議題成為兩國戰略互疑的來源，但不意味兩國沒有合作的可能性。即使兩國發生「網路作戰」進而破壞對方的關鍵基礎設施，造成重大無辜傷亡的想定不一定實現，北京仍關切管控雙方的分歧，防止兩國分歧升高，避免出現敵對的軍事危機。中國大陸有多篇論文討論網路戰對國際法的挑戰、中美網路軍備控制的可能性，隱含中美兩國對於網路管理規則制訂的話語權競爭與合作。[93] 在 2015 年中美達成網路五點共識之後，中方樂觀認為網路空間可以成為

<https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/>；王毅，〈堅守多邊主義 宣導公平正義 攜手合作共贏—在全球數位治理研討會上的主旨講話〉， 2020 年 9 月 8 日，《中華人民共和國外交部》，<https://www.fmprc.gov.cn/web/wjbz_673089/zyjh_673099/t1812948.shtml>。

91. Bill Gertz, “Pompeo on Chinese Coercion,” *Washington Times*, June 10, 2020, <https://www.washingtontimes.com/news/2020/jun/10/mike-pompeo-accuses-china-of-bullying-hsbc/>.

92. 朱鋒，〈貿易戰、科技戰與中美關係的「範式變化」〉，《亞太安全與海洋研究》（北京），2019 年第 4 期，2019 年 8 月，頁 14。

93. 吳翔、翟玉成，〈網絡軍控：倡議、問題與前景〉，《現代國際關係》（北

中美關係合作的新面向。

北京基於網路空間的弱勢地位，主張中美需要有網路安全的「信心建立措施」(confidence-building measures, CBMs)，形塑對美國網路作為的規範，也可為習近平「新型大國關係」建立一個亮點。中國的看法並非一廂情願，美國部分專家也提出網路安全合作建議。中美針對網路安全對話就是「信心建立措施」一環，直到 2015 年習近平與歐巴馬達成網路安全五點共識之前，至少有兩個「二軌」對話論壇，聚焦於網路社會責任、治理、安全的溝通與對話，甚至探討網路安全「信心建立措施」協議內容。然而，中美網路安全對話的前景，受制於雙邊總體關係或對方的作為，雙方也常利用取消會議，來反應不滿。

2007-2015 年，中國互聯網協會與美國微軟公司每年召開「美中互聯網工業論壇」，匯集兩國網路科技公司執行長聚會，並邀請兩國政府官員如中國國務院新聞辦公室、中國國家互聯網資訊辦公室代表，或美國經濟發展、能源暨環境事務國務次卿(Under Secretary for Economic Growth, Energy, and the Environment)，開幕致詞或主題演講。2015 年，習近平訪美時更親自出席此一論壇。另外，中國現代國際關係研究院(China Institutes of Contemporary International Relations, CICIR)與美國戰略與國際研究院(Center for Strategic and International Studies, CSIS)在 2009-2015 年召開九次會議，從網路安全角度探討對兩國關係的影響，討論網路準則透明化、軍文職專家互訪、威脅資訊交換、決策過程及網路推演等。[94]

歐巴馬任內前副國務卿史坦伯格與布魯金斯研究所(Brookings In-

京），2011 年第 12 期，2011 年 12 月，頁 16-20；程群，〈網絡軍備控制的困境與出路〉，《現代國際關係》（北京），2012 年第 2 期，2012 年 2 月，頁 15-21。

94. The Center for Strategic and International Studies and the China Institute

stitute)研究員歐漢龍(Michael E. O'Hanlon)，提議美中兩國可先採取單方面的作為，如強化關鍵基礎設施的網路防護或降低脆弱度，避免陷入網路軍備競賽或淪為被報復的目標，而最終引發危機；雙方可以從網路竊取等共同威脅開始合作，進而建立有關網路偷竊的聯合調查及執法機制，北京可以加入《網路犯罪公約》(*Cyber Crime Convention*)，或透過聯合國途徑達成的網路條約，禁止使用網路攻擊關鍵基礎措施等民間目標。[95]中美專家也主張不應攻擊對方危機因應部門，以增加兩國信任、減少猜疑。[96]

習近平與歐巴馬達成的共識與國家網路行為準則的思考有關。2016 年 5 月與 11 月，時任中國外交部軍備控制司司長王群與時任美國國務院「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」召開兩次會議。[97]北京期待簽訂中美網路安全合作框架，建立「不衝突、不對抗、相互尊重、合作共贏」的原則，

---

of Contemporary International Relations, "Bilateral Discussions on Cooperation in Cybersecurity" June 2012, *CSIS*, <https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity/track-1>; Scott Warren Harold, Martin C. Libicki, & Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, pp. 49-51.

95. James Steinberg & Michael E. O'Hanlon, *Strategic Reassurance and Resolve: U.S.-China Relations in the Twenty-First Century* (Princeton: Princeton University Press, 2014), pp. 173-180; Erica D. Borghard & Shawn W. Lonergan, "Confidence Building Measures for the Cyber Domain," *Strategic Studies Quarterly*, Vol. 12, Issue 3, Fall 2018, p. 30.

96. 唐嵐、史國力，〈減少和管理中美在網絡空間的衝突〉，《現代國際關係》（北京），2016 年第 10 期，2016 年 10 月，頁 52。

97. Christopher Painter, "International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms," May 25, 2016, *U.S. Department of State*, <https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm>.

並以避免網路攻擊關鍵基礎設施為訴求，但發展與結果不如預期。川普總統上臺之後，此一雙邊網路行為規範的對話，隨著中美展開關稅、經貿戰而不再舉行，習近平也不再提中美要建立「新型大國關係」。網路空間優勢地位的爭奪，成為中美大國競爭的重要面向。在川普政府時期，中美建構網路空間行為規則有其困難度，但美中兩國在網路安全威脅，是否可能合作取得協議，或是維持對立甚至對抗，隨著不同議題與不同的美中國家領導人而定。這也可了解網路安全威脅對美中關係涉及面向的複雜性，到了川普政府美中五點網路安全共識，雖「名存」但實質運作上全被擱置（請見表 2）。

表 2　美中網路安全議題

議　題	共識、精神與各說各話
維持網路安全高層對話	2015 年五點共識的規定
網路空間自由論與網路空間主權論	各有堅持
網路犯罪執法合作 （槍枝買賣、人口販運、金融盜領、病毒勒索等）	2015 年五點共識的精神
禁止網路竊取對方企業智慧財產權的「網路間諜」活動	2015 年五點共識的規定
「華為公司」列為兩國經貿談判一環	各有堅持
禁止入侵對方政府網站取得人事等機密資料的「網路間諜」活動	2015 年五點共識的精神
禁止癱瘓對方重大基礎設施	2015 年五點共識的精神
禁止攻擊對方軍事目標	2015 年五點共識的精神
網路安全意外加強執法溝通	2015 年五點共識的規定
惡意網路活動通報與提供協助	2015 年五點共識的規定
散播假訊息、誤導新聞、干預選舉、混淆人心、詆毀政府公信力	各有堅持

資料來源：作者自行整理。

伍、結論

在歐巴馬政府時期，美中網路安全政策發展上升到國家戰略層級。美中針對網路安全的高層對話開啟於歐巴馬政府，但局限於「網路間諜」竊取情報為主，重視經濟層面，而非政治軍事領域。即使美

中達成共識，避免涉入網路經濟間諜行為，但「網路間諜」既被視為情報蒐集的一項途徑，就意味無法阻止雙方繼續透過網路，竊取政治或軍事情報。歐巴馬政府對「網路間諜」予以容忍，不能輕言報復，避免受到反報復。這種沒有採取網路攻勢的反擊、報復，可能是美中「網路間諜」活動增多的原因。

川普政府雖宣示與中國有四個高層對話管道，但只專注經貿談判，部長級「執法與網路安全對話」只舉行一次，並停止歐巴馬任內所建立的資深官員網路對話管道。川普總統雖重申遵守歐巴馬與習近平的網路安全五點共識，但重心轉向對中國的關稅經貿戰，宣示採取網路攻勢作為，而不僅是網路防禦。川普針對華為及其相關企業所進行的「對內管制（實體清單）」，表面上是防範中國滲透網路空間，實質上對中國展開國際統一戰線，以「五眼聯盟」對中國的科技圍堵，美中儼然進入以科技戰為核心的新冷戰。川普政府縮減了對中國的貿易赤字，但更大的衝擊在於 5G 網路、人工智慧領域，來自中國的挑戰。川普政府以華為涉及竊取營業機密、違反對特定國家（伊朗）交易、迫害中國新疆人權等理由，以美國國內法律箝制中國的網路科技經由「一帶一路」向外輸出。這與歐巴馬政府訴求美中雙邊協商，促成中方改變「網路間諜」的作法相比較，顯然是更高遠的層次，也帶來美中新的不確定因素。

「網路主權論」與「網路自由論」、「網路間諜」行為與破壞關鍵基礎設施等議題的辯論，成為美中互不信任的來源。美中關係的人權問題可能受到忽略，臺灣議題也可能因兩岸關係緩和而重要性降低，但網路安全卻是無硝煙的新型戰爭，牽涉到美中的國際領導、影響力、網路科技地位的大國競爭。美中在全球網路空間的發展與治理上，同樣處於角力的階段，各自提供不同的模式發展。中國主張利用聯合國體制來制定國際規則，堅持網路治理機制的「共治」原則，直接挑戰美國的「網路霸權」，而使得兩國在網路空間尋求制定國家行為的規則，變得困難重重。美中因應網路安全的威脅，或可在爭議較

小的「網路犯罪」議題取得更多共識，但進一步要在「網路間諜」、「網路戰」有重大合作，將因不同的國家領導人而異，反映網路安全與美中關係發展的複雜性。

隨著美中綜合國力差距縮小，意識形態差異的既有霸權與新興強權競爭，正經由網路與科技的國力倍增器，透過取得個資、決策過程、談判底線、科技情報、企業智慧財產權等，使兩國關係進入全球性的角力。中國對於網路安全的重視，相對集中在防禦、治理層次的探討，對外攻擊或竊取層面的探討隱而不見，也不公開承認。美國與中國高度依賴網路所進行的「網路戰」，讓網路空間可能成為衝突時「不對稱作戰」的載臺。在平時，網路是中國政府機關、民間駭客對美國情報竊取的途徑。歐巴馬政府不願公開討論中國的「網路間諜」，或對中國強硬的制裁，但建立了廣泛的對話機制，以「新自由機制主義」來思考此一問題。川普政府另擇途徑，不惜使用網路攻擊與攻勢，圍堵華為，來降低中國對美國及其盟邦的威脅，削弱「一帶一路」下「數字絲綢之路」的發展。習近平為證明華為不是黨政軍的一環，難以大力反擊川普的制裁，更棘手的問題是，如何突破美國對中國網路資通訊業的「科技圍堵」。

※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》(105-2410-H-001-018-MY2)部分研究成果。

（收件：2020 年 6 月 24 日；修正：2020 年 10 月 20 日；採用：2020 年 10 月 27 日）

參考文獻

中文部分

期刊論文

王 軍，2012/7。〈多維視野下的網絡戰：緣起、演進與應對〉，《世界經濟與政治》（北京），2012 年第 7 期，頁 80-98。

王清安、黃基禎，2019/3。〈中共對網路空間主權之概念與作為〉，《中國大陸研究》，第 62 卷第 1 期，頁 67-100。

林穎佑，2016/2。〈美「中」網路安全競合情勢分析〉，《亞太評論》，第 2 卷第 1 期 ，頁 55-70。

朱志平、梁德昭，2016/4。〈習近平時期美中網路安全競逐〉，《遠景基金會季刊》，第 17 卷第 2 期，頁 1-61。

朱 鋒，2019/8。〈貿易戰、科技戰與中美關係的「範式變化」〉，《亞太安全與海洋研究》（北京），2019 年第 4 期，頁 1-14。

吳 翔、翟玉成，2011/12。〈網絡軍控：倡議、問題與前景〉，《現代國際關係》（北京），2011 年第 12 期，頁 16-20。

李 崢，2016/6。〈中美網路安全互動：挑戰與機遇〉，《復旦學報》（上海），2016 年第 3 期，頁 147-156。

李 艷，2018/11。〈網絡空間國際治理中的國家主體與中美網絡關係〉，《現代國際關係》（北京），2018 年第 11 期，頁 41-48。

汪曉風，2018/11。〈斯諾登事件後美國網絡情報政策的調整〉，《現代國際關係》（北京），2018 年第 11 期，頁 56-63。

唐 嵐、史國力，2016/10。〈減少和管理中美在網絡空間的衝突〉，《現代國際關係》（北京），2016 年第 10 期，頁 51-52。

耿 召，2018/2。〈特朗普時期中美網絡安全合作分析〉，《美國問題研究》（上海），2018 年第 2 期，頁 151-175。

耿 召，2019/3。〈特朗普政府「國家網絡戰略」實效與理念並舉〉，

《和平與發展》（北京），2019 年第 1 期，頁 116-130。
張凱銘，2018/9。〈「避險」視角下的中國對美國的網路強國戰略研究〉，《問題與研究》，第 57 卷第 3 期，頁 97-137。
張凱銘，2020/1。〈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〉，《遠景基金會季刊》，第 21 卷第 1 期，頁 107-170。
程　玉，2014/7。〈中美雙邊關係中網絡安全問題的成因、摩擦與對策〉，《黨政幹部學刊》（瀋陽），2014 年第 7 期，頁 31-35。
程　群，2012/2。〈網絡軍備控制的困境與出路〉，《現代國際關係》（北京），2012 年第 2 期，頁 15-21。
魯傳穎，2018/2。〈網絡空間大國博弈趨勢和中美對話機制演變〉，《信息安全與通信保密》（成都），2018 年第 2 期，頁 17-19。
魯傳穎，2019/12。〈中美關係中的網絡安全困境及其影響〉，《現代國際關係》（北京），2019 年第 12 期，頁 16-22。

網際網路

2013/3/14。〈習近平同奧巴馬通電話 就網路安全等問題交換意見〉，《新華網》，<http://www.cac.gov.cn/2013-03/15/c_133138873.htm>。
2014/2/27。〈中央網絡安全和信息化領導小組第一次會議召開 習近平發表重要講話〉，《新華網》，<http://www.cac.gov.cn/2014-02/27/c_133148354.htm>。
2014/4/15。〈習近平：堅持總體國家安全觀　走中國特色國家安全道路〉，《新華網》，<http://www.xinhuanet.com/politics/2014-04/15/c_1110253910.htm>。
2016/2/29。〈堅持尊重網路主權原則　推動構建網絡空間命運共同體〉，《求是》，<http://www.xinhuanet.com//politics/2016-02/29/c_128761848_2.htm>。

2016/4/25。〈習近平在網信工作座談會上的講話全文發表〉，《新華網》，<http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm>。

2020/5/15。〈消息人士：美若對華為卡脖子，中方反擊清單上將有這些美方公司〉，《環球時報》，<https://world.huanqiu.com/article/3yFXkzABKfP>。

王　毅，2020/9/8。〈堅守多邊主義 宣導公平正義 攜手合作共贏—在全球數位治理研討會上的主旨講話〉，《中華人民共和國外交部》，<https://www.fmprc.gov.cn/web/wjbz_673089/zyjh_673099/t1812948.shtml>。

中華人民共和國外交部，2014/12/22。〈王毅同美國國務卿克里通電話〉，《中國新聞網》，<http://www.chinanews.com/gn/2014/12-22/6897113.shtml>。

中華人民共和國外交部，2015/12/16。〈習近平：推進全球互聯網治理體系變革應堅持四原則〉，《中華人民共和國外交部》，<http://www.fmprc.gov.cn/web/zyxw/t1324807.shtml>。

中華人民共和國國防部，2019/7/24。〈《新時代的中國國防》白皮書全文〉，《中華人民共和國國務院新聞辦公室》，<http://www.mod.gov.cn/big5/regulatory/2019-07/24/content_4846424.htm>。

中國石油大學（華東）信息化建設處，2017/11/10。〈中國網絡空間安全發展報告(2017)精讀〉，《中國石油大學》，<http://nic.upc.edu.cn/2018/ 0119/c7453a131181/pagem.htm>。

中國國家信息中心，2020/4/23。《中國網絡媒體社會價值白皮書》，《國家信息中心》，<http://www.sic.gov.cn/News/79/10458.htm>。

中國國家互聯網信息辦公室，2016/12/27。〈國家網絡空間安全戰略〉，《國家互聯網信息辦公室》，<http://www.cac.gov.cn/2016-12/27/c_1120195926.htm>。

張曉松、朱基釵，2018/4/21。〈習近平：自主創新推進網路強國建

設〉，《新華網》，<http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm>。

英文部分

專書

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

Campbell, Kurt M., 2016. *The Pivot: The Future of American Statecraft in Asia*. New York: Hachette Book Group.

Carlin, John P. & Garret M. Graff, 2018. *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. New York: PublicAffairs.

Cheng, Dean, 2017. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*. Santa Barbara: Praeger.

Clapper, James R., 2018. *Facts and Fears: Hard Truths from A Life in Intelligence*. New York: Random House.

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

Elman, Colin & Michael A. Jensen, eds., 2014. *Realism Reader*. London: Routledge.

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

Gertz, Bill, 2017. *iWar: War and Peace in the Information Age*. New York: Threshold Editions.

Harold, Scott Warren, Martin C. Libicki, & Astrid Stuth Cevallos, 2016. *Getting to Yes with China in Cyberspace*. Santa Monica: Rand Corporation.

Inkster, Nigel, 2016. *China's Cyber Power*. New York: Routledge.

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

Panetta, Leon, 2014. *Worthy Fights: A Memoir of Leadership in War and Peace*. New York: Penguin.

Poindexter, Dennis F., 2018. *The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests*. Jefferson: McFarland & Company, Inc., Publishers.

Sanger, David E., 2018, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Victoria Australia: Scribe Publication.

Steinberg, James & Michael E. O'Hanlon, 2014. *Strategic Reassurance and Resolve: U.S - China Relations in the Twenty-First Century*. Princeton: Princeton University Press.

期刊論文

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

Lindsay, Jon R., 2014-15/Winter. "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, Issue 3, pp. 7-47.

Gilli, Andrea & Mauro Gilli, 2018-19/Winter. "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security*, Vol. 43, Issue 3, pp. 141-189.

官方文件

U.S. Commission on Enhancing National Cybersecurity, 2016. *Report on Securing and Growing the Digital Economy*. Washington, D.C.: U.S.

Commission on Enhancing National Cybersecurity.

U.S. Department of Defense, 2015. *The Department of Defense Cyber Strategy*. Washington, D.C.: U.S. Department of Defense.

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

U.S. Department of Defense, 2019. *Indo-Pacific Strategy Report*. Washington, D.C.: U.S. Department of Defense.

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

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

報紙

2015/9/29. "The Obama-Xi Cyber Mirage," *Wall Street Journal*, p. A10.

Bradsher, Keith, 2014/5/21. "Retaliatory Attacks, Online," *New York Times*, p. B1.

Forsythe, Michael & David E. Sanger, 2015/12/3. "China Says Hacking of U.S. Workers' Data Was Common Crime, Not State Act," *New York Times*, p. A8.

Perlez, Jane & Nick Wingfield, 2015/9/24. "Chinese Leader Hears Tough Complaints of American Business," *New York Times*, p. A21.

Perlroth, Nicole, 2013/1/31. "Hackers in China Attacked The Times for Last 4 Months," *New York Times*, p. A1.

Sanger, David E., 2015/9/24. "Hackers Also Stole Fingerprints of 5.6 Million Workers, Personnel Agency Says," *New York Times*, p. A21.

Sanger, David E., 2019/5/28. "Huawei Ban Gains Trump a Wall at Last," *New York Times*, pp. A1, A11.

Sanger, David E., Julian E. Barnes, Raymond Zhong, & Marc Santora, 2019/1/27. “U.S. Scrambles to Outrun China in New Arms Race,” *New York Times*, p. A1.

Sanger, David E. & Nicole Perlroth, 2014/3/23. “U.S. Penetrated Chinese Servers It Saw as Spy Risk,” *New York Times*, p. A1.

Sanger, David E. & Nicole Perlroth, 2020/5/11. “U.S. to Accuse China of Trying to Steal Data,” *New York Times*, p. A7.

Schmidt, Michael S., David E. Sanger, & Nicole Perlroth, 2014/7/10. “Chinese Hackers Pursue Key Data on U.S. Workers,” *New York Times*, p. A1.

Swanson, Ana & Paul Mozur, 2019/10/8. “Chinese Entities Blacklisted As U.S. Cites Rights Abuses,” *New York Times*, p. B4.

Swanson, Ana, Paul Mozur, & Raymond Zhong, 2020/5/20. “A Tech Fight, U.S. vs. China, Pulls In Taiwan,” *New York Times*, p. B1.

Wong, Edward & Julian E. Barnes, 2020/5/29. “Many Chinese Graduate Students and Researchers to Lose U.S. Visas,” *New York Times*, p. A17.

網際網路

2014/11/12. “The U.S. and China Reach a Landmark Climate Deal,” *Washington Post*, <https://www.washingtonpost.com/opinions/the-us-and-china-reach-a-landmark-climate-deal/2014/11/12/a1f49f4c-6aa5-11e4-a31c-77759fc1eacc_story.html>.

2015/6/24. “Obama’s Cyber Meltdown,” *Wall Street Journal*, p. A12, <https://www.wsj.com/articles/obamas-cyber-meltdown-1435097288>.

2018/2/9. “China, U.S. should make good use of four dialogue pillars: Chinese state councilor,” *Xinhua*, <http://www.xinhuanet.com/english/2018-02/09/c_136961876.htm>.

Blake, Andrew, 2015/10/12. “China Arrests Hackers Following Request

from U.S.—Report," *Washington Times*, <https://www.washingtontimes.com/news/2015/oct/12/china-arrests-hackers-following-request-from-us-re/>.

Brunnstrom, David, 2019/5/31. "Pompeo Tells Germany: Use Huawei and Lose Access to Our Data," *Reuters*, <https://www.reuters.com/article/us-usa-germany/pompeo-to-germany-use-huawei-and-lose-access-to-our-data-idUSKCN1T10HH>.

Budryk, Zack, 2019/8/4. "Top aide: China must end 'Seven Deadly Sins' to stop trade war," *The Hill*, <https://thehill.com/homenews/sunday-talk-shows/456092-top-aide-names-seven-deadly-sins-china-must-end-to-stop-trade-war>.

The Center for Strategic and International Studies and the China Institute of Contemporary International Relations, 2012/6. "Bilateral Discussions on Cooperation in Cybersecurity," *CSIS*, <https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity/track-1>.

Conaway, Mike, 2018/6/20. "Conaway, Cotton, Rubio, Cheney, and Ruppersberger Raise Concerns about Google's Partnership with Huawei," *Mike Conaway 11th District of Texas*, <https://conaway.house.gov/news/documentsingle.aspx?DocumentID=398400>.

Ford, Christopher Ashley, 2020/3/16. "The PRC's 'Military-Civil Fusion' Strategy Is a Global Security Threat," *U.S. Department of State*, <https://www.state.gov/the-prcs-military-civil-fusion-strategy-is-a-global-security-threat/>.

Gallagher, Mike, 2019/1/16. "Gallagher, Cotton, Van Hollen & Gallego Introduce Bill to Impose Denial Orders on Chinese Telecomm Companies That Violate US Sanctions," *Congressman Mike Gallagher Representing the 8th District of Wisconsin*, <https://gallagher.house.

gov/media/press-releases/gallagher-cotton-van-hollen-gallego-introduce-bill-impose-denial-orders-chinese>.

Gertz, Bill, 2020/6/10. “Pompeo on Chinese Coercion,” *Washington Times*, <https://www.washingtontimes.com/news/2020/jun/10/mike-pompeo-accuses-china-of-bullying-hsbc/>.

Huawei, 2019/11. “Huawei’s Position Paper on Cyber Security,” *Huawei*, <https://www.huawei.com/en/facts/voices-of-huawei/huawei-releases-its-position-paper-on-cyber-security>.

Li, Yuan, 2019/11/5. “China’s TikTok Blazes New Ground. That Could Doom It,” *New York Times*, <https://www.nytimes.com/2019/11/05/business/tiktok-china-bytedance.html>.

Mandiant Corporation, 2013/2. “APT1: Exposing One of China’s Cyber Espionage Units,” *FireEye*, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

O’Keeffe, Kate, 2018/11/14, “U.S. Panel Warns China Tech Prowess Threatens U.S. Security,” *Wall Street Journal*, <https://www.wsj.com/articles/u-s-panel-warns-china-tech-prowess-threatens-u-s-security-1542171601>.

Painter, Christopher, 2016/5/25. “International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms,” *U.S. Department of State*, <https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm>.

Pompeo, Michael R., 2018/7/30. “Secretary Pompeo’s Remarks at the Indo-Pacific Business Forum,” *American Institute in Taiwan*, <https://www.ait.org.tw/secretary-pompeos-remarks-at-the-indo-pacific-business-forum/>.

Pompeo, Michael R., 2020/5/15. “The United States Protects National Security and the Integrity of 5G Network,” *U.S. Department of State*,

<https://www.state.gov/the-united-states-protects-national-security-and-the-integrity-of-5g-networks/>.

Pompeo, Michael R., 2020/8/5. "Announcing the Expansion of the Clean Network to Safeguard America's Assets," *U.S. Department of State*, <https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/>.

Sebenius, Alyza, 2019/2/19. "China Has Abandoned a Cybersecurity Truce with the U.S., Report Says," *Bloomberg*, <https://www.bloomberg.com/news/articles/2019-02-19/china-abandons-cybersecurity-truce-with-u-s-report-says>.

Segal, Adam, 2018/12/6. "A New Old Threat Countering the Return of Chinese Industrial Cyber Espionage," *Council for Foreign Relations*, <https://www.cfr.org/report/threat-chinese-espionage>.

Selyukh, Alina & Doug Palmer, 2013/3/28. "U.S. Law to Restrict Government Purchases of Chinese IT Equipment," *Reuters*, <https://www.reuters.com/article/us-usa-cybersecurity-espionage-idUSBRE92Q18O20130328>.

Shahbaz, Adrian, 2020/11/3 (accessed). "Fake News, Data Collection, and the Challenge to Democracy," *Freedom House*, <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism>.

Steinberg, James, 2009/9/24. "Administration's Vision of the U.S.-China Relationship," *American Institute in Taiwan*, <https://web-archive-2017.ait.org.tw/en/administrations-vision-of-the-us-china-relationship.html>.

Strumpf, Dan, 2020/6/6. "Huawei Founder Ren Zhengfei Takes Off the Gloves in Fight Against U.S.," *Wall Street Journal*, <https://www.wsj.com/articles/huawei-founder-ren-zhengfei-takes-off-the-gloves-in-fight-against-u-s-11591416028?mod=searchresults&page=1&pos=2>.

U.S. Department of Justice Office of Public Affairs, 2016/6/14. "Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue>.

U.S. Department of Justice Office of Public Affairs, 2016/12/8. "Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," *U.S. Department of Justice*, <https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues>.

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

U.S. Department of Justice Office of Public Affairs & U.S. Department of Homeland Security of Public Affairs, 2015/12/2. "First U.S.-China High-Level Joint Dialogue on Cybercrime And Related Issues Summary Of Outcomes," *U.S. Department of Homeland Security*, <https://www.dhs.gov/news/2015/12/02/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary>.

U.S. Department of State, 2013/7/12. "U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track," *U.S. Department of State*, <https://2009-2017.state.gov/r/pa/prs/ps/2013/07/ 211861.htm>.

U.S. Embassy and Consulates in China, 2019/5. "Department of Commerce Announces the Addition of Huawei to the Entity List," *U.S. Embassy and Consulates in China*, <https://china.usembassy-china.org.cn/department-of-commerce-announces-the-addition-of-huawei-to-the-entity-list/>.

U.S. National Counterintelligence and Security Center, 2018. "Foreign

Economic Espionage in Cyberspace 2018," *U.S. National Counterintelligence and Security Center*, <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>.

The White House, 2013/2/12. "Executive Order -- Improving Critical Infrastructure Cybersecurity," *The White House President Barack Obama*, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

The White House, 2015/4/1. "Executive Order – 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'" *The White House President Barack Obama*, <https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>.

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

The White House, 2016/9/3. "U.S. Fact Sheet for President Obama's Bilateral Meeting with President Xi Jinping," *The White House President Barack Obama*, <https://obamawhitehouse.archives.gov/the-press-office/2016/09/03/us-fact-sheet-president-obamas-bilateral-meeting-president-xi-jinping>.

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, 2017/11/9. "Remarks by President Trump and President

Xi of China in Joint Press Statement," *The White House*, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-xi-china-joint-press-statement-beijing-china/>.

The White House, 2019/5/15. "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," *The White House*, <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>.

Wilson Center, 2019/10/24. "Remarks by Vice President Pence at the Frederic V. Malek Memorial Lecture," *The White House*, <https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-frederic-v-malek-memorial-lecture/>.

Yap, Chuin-Wei, 2019/12/25. "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, <https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736?mod=searchresults&page=1&pos=20>.

The Cybersecurity Problem in U.S.-China Relations

Cheng-yi Lin

(Research Fellow, Institute of European and American Studies, Academia Sinica)

Abstract

From the Obama Administration onward, cybersecurity has represented a lingering and thorny conflict between the U.S. and China. Chinese cyber-espionage activities pose a serious challenge to the U.S. national security interests. By the same token, American intelligence has conducted extensive internet and phone surveillance on the Chinese government and Huawei. The Chinese government denies its involvement in cyberspace intrusions but agreed to a five-point consensus on cybersecurity cooperation with the United States. President Obama preferred building a bilateral cybersecurity dialogue mechanism to defuse the tension with China. President Donald Trump has chosen an approach of linking cybersecurity issues with the trade negotiations. China seeks international norms of cybersecurity under the United Nations system and sought confidence-building measures on cybersecurity with the United States. Whether China and the U.S. can reach certain norms regarding operations in cyberspace remains to be seen.

Keywords: Cybersecurity, Cyber Espionage, Cyber Sovereignty, Huawei, U.S.-China Relations