airiti

習近平時期美中網路安全競逐

朱志平
（淡江大學管理科學研究所博士候選人）

梁德昭
（淡江大學資訊管理學系副教授）

摘　要

在習近平於 2012 年底中共十八大接班成為中國領導人之前，美國與中國大陸在網路安全領域的齟齬便時有所聞，迄今亦為兩國關係焦點之一。在網路安全領域，美國可說傲視群倫，然隨著中國政經實力崛起之後，已不時傳出對美尋釁之舉。不論是政經領域的竊密、軍事領域的抗衡，甚至是國內立法的管制，中國可說無時不與美國競逐，除實現習近平所謂「網絡強國」之目標外，更有意挑戰美國之領導地位。因此，本文主要目的係從攻勢現實主義視角，結合政經、軍事及國內管制面向之案例，析論美中兩國於習近平時期在網路安全領域之競逐。

關鍵詞：網路安全、攻勢現實主義、新型大國關係、美中關係、網路犯罪

airiti

壹、前言

在習近平於 2012 年底中共十八大接任中共總書記之前，美國與中國大陸在網路安全領域的齟齬便時有所聞，也成為兩國關係的焦點之一。特別當習近平 2012 年 2 月以中國國家副主席身分訪美時，美國副總統拜登(Joe Biden)在午餐演講便點明網路安全是需要美中雙方緊密合作的議題之一。[1] 隨著習近平 2013 年 3 月出任國家主席後，歐巴馬於 2013 年 3 月 18 日藉著發電祝賀習近平就任中國國家主席之際，亦再次提及網路攻擊議題，並且強調網路攻擊對美國智慧財產權所造成之損失。[2]

然而，歐巴馬的論調似乎並未被習近平所接受，由習近平 2013 年 6 月 7 日在加州與歐巴馬進行莊園峰會時有關網路安全的談話，似可看出端倪。當歐習兩人被問到關於網路安全問題，歐巴馬表示，網路安全是世界各國的議題，並非美中之間獨有的議題，希望雙方能達成此一問題的解決之道；習近平則表示中國也是受害者，也希望積極解決此一問題，並指出媒體的報導使各方誤以為網路安全主要威脅來自中國，或者被認為這是兩國間最大問題。[3]

雖然美中雙方對網路安全看法分歧，但雙方仍試圖建構管道進行

---

1. The White House, “Remarks by Vice President Biden and Chinese Vice President Xi at the State Department Luncheon,” February 14, 2012, *The White House*, <https://www.whitehouse.gov/the-press-office/2012/02/14/remarks-vice-president-biden-and-chinese-vice-president-xi-state-departm>.
2. Nicole Perlroth, “Cyberattacks a Topic in Obama Call With New Chinese President,” *New York Times*, March 14, 2013, <http://bits.blogs.nytimes.com/2013/03/14/cyberattacks-prominent-in-obama-call-with-new-chinese-president/?_r=0>.
3. 〈談網路攻擊　習近平：中國也是受害者〉，《ETtoday 東森新聞雲》，2013 年 6 月 8 日，<http://www.ettoday.net/news/20130608/219833.htm>。

airiti

對話。時任中國外交部部長助理鄭澤光於 2013 年 7 月 5 日表示，美中網路安全工作組將於 7 月 8 日在美國舉行第一次會議，雙方將針對網路安全及工作組的建設深入交換意見。[4] 但好景不常，隨著美國於 2014 年 5 月起訴並通緝 5 名中國解放軍軍官，中國隨即中止兩國網路安全工作組活動以為報復，而此為美國首次以網路間諜罪名起訴外國政府官員，尤其針對中國軍官可說更為罕見。[5]

於此同時，中國亦明白揭櫫成為「網絡強國」之戰略目標。2013 年中共十八屆三中全會之後，成立「中共中央網絡安全和信息化領導小組」，並於 2014 年召開第一次會議。習近平在該次會議中便明白指出，中國大陸網民數量世界第一，[6] 中國已成為網路大國，沒有網路安全就沒有國家安全，沒有資訊化就沒有現代化，並且提出要建設中國為「網絡強國」之戰略目標。[7]

事實上，網路空間議題涉及「網路治理」問題，屬於「全球治理」的新興議題。當中國想成為網路強國，首當其衝的，莫過於是已在網路空間稱霸已久的美國，而美中兩國在網路空間安全領域之競逐

4. 中央社，〈中美網路小組　將舉行首次會議〉，《中時電子報》，2013 年 7 月 5 日，<http://www.chinatimes.com/realtimenews/20130705004146-260409>。
5. 〈柯瑞：中國駭客 製造寒蟬效應〉，《世界日報網》，2014 年 7 月 11 日，<http://www.worldjournal.com/266365/article-%E6%9F%AF%E7%91%9E%EF%BC%9A%E4%B8%AD%E5%9C%8B%E9%A7%AD%E5%AE%A2-%E8%A3%BD%E9%80%A0%E5%AF%92%E8%9F%AC%E6%95%88%E6%87%89/?npg=2>。
6. 中國大陸截至 2015 年 6 月，網民規模達 6.68 億，網路普及率為 48.8%。請見中國互聯網絡資訊中心，〈第 36 次中國互聯網絡發展狀況統計報告〉，2015 年 7 月 22 日，《中國互聯網絡資訊中心》，<https://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201507/t20150722_52624.htm>。
7. 〈習近平：把我國從網絡大國建設成為網絡強國〉，《新華網》，2014 年 2 月 27 日，<http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm>。

airiti

亦漸趨白熱。中國爭取制定世界網路規則的態度，亦反映在習近平2015年12月16日在第二屆世界網際網路大會開幕談話。習近平指出，

> 網絡安全是全球性挑戰，沒有哪個國家能夠置身事外、獨善其身，維護網絡安全是國際社會的共同責任。各國應該攜手努力，……
>
> 中國願同各國一道加強對話交流，有效管控分歧，推動制定各方普遍接受的網絡空間國際規則，制定網絡空間國際反恐公約，健全打擊網絡犯罪司法協助機制，共同維護網絡空間和平安全。
>
> 各國應該加強溝通交流，完善網絡空間對話協商機制，研究制定全球互聯網治理規則，使全球互聯網治理體系更加公正合理，更加平衡地反映大多數國家意願和利益。[8]

面對新興崛起的大國－中國，與既存大國－美國在網路安全之間的競逐，本文將從攻勢現實主義(Offensive Realism)角度加以剖析，探討中國崛起之作為與美國如何回應。本文首先將針對攻勢現實主義與網路安全進行分析，爬梳兩者之間的關聯，並作為探討習近平時期美中兩國於網路安全領域競逐之理論基礎；其次，作者將從政經領域探討中國在該領域之作為，例如透過網路竊取美國政府員工個資或商業機密資料等，以及美國之回應作為；第三，作者將從軍事領域探討中國網軍的建構與作為及美國之應對策略；第四，作者將從美中兩國國內管制層面分析中國相關法令對美影響及美國之有關措施。

綜前所述，本文主要目的係透過攻勢現實主義視角，結合政經、軍事及國內管制面向之案例，析論美中兩國於習近平時期在網路安全領域之競逐。

8.〈習近平在第二屆世界互聯網大會開幕式上的講話（全文）〉，《中國共產黨新聞網》，2015 年 12 月 16 日，<http://cpc.people.com.cn/BIG5/n1/2015/1216/c64094-27937316.html>。

airiti

貳、攻勢現實主義與網路安全

隨著科技發展日新月異，網路空間對全球化而言扮演相當重要的角色，國與國之間在貿易、交通、文化等範疇藉網路空間互動交流，形成安全與利益錯綜複雜之國際關係。[9]

從攻勢現實主義角度而言，該主義雖重視地緣因素，然重視地緣因素的原因係因受制於地理限制，網路因超越地緣因素，而國家為確保其生存之心態並不會有所改變，為確保其生存，更有利於國家追逐權力。政治學者米爾斯海默(John Mearsheimer)根據下列五大基本命題，最後認定大國間會追逐權力並爭奪霸權：

1. 國際體系處於無政府狀態。
2. 大國本身具備某些用於侵略擴張的軍事力量，能傷害甚至摧毀對手。
3. 國家永遠無法把握其他國家的意圖。
4. 生存是大國的首要目標。
5. 大國是理性行為者。[10]

若從這五大基本命題分析美中網路安全競逐，首先，國際體系處於無政府狀態，在網際網路空間亦復如此，尤其是史諾登(Edward Snowden)事件的爆發，[11] 對美中關係亦造成影響，特別是在網路安全

9. 梁德昭、朱志平、林凱薰，〈國家主權延伸至網路空間之討論〉，《前瞻科技與管理》，第 2 卷第 2 期，2012 年 11 月，頁 3-4。
10. John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton & Company, 2001), pp. 30-31.
11. 2013 年 6 月，時任美國國家安全局技術外包人員的史諾登透過媒體揭露美國國安局代號為「稜鏡」(PRISM)的監控計畫，報導請見 Barton Gellman & Laura Poitras, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program,” *The Washington Post*, June 7, 2013, <https://www.washingtonpost.com/investigations/us-intelligence-mining-data-

airiti

方面，除美中兩國之外，亦使各國開始思考網路空間的安全規範。在無政府狀態的情況下，身為網路大國的美國卻把網路空間作為國家利益博弈的新領域，對相關的治理規則未能與其他國家獲致共識，其算計亦成為影響網路安全規則制定的最大因素。特別是在其意識形態與國家利益雙重考量下，美國積極追求網路空間的技術與戰略長期優勢，並往往以自身需求為主，在強調網路資訊自由化的同時，卻也主導網路規則制定權；在高舉國家安全大纛的同時，卻也對網路安全採取雙重標準。[12]

其次，大國本身具備某些用於侵略擴張的軍事力量，能傷害甚至摧毀對手，以美國而言，美國在 2013 年針對總統動用網路武器權力進行秘密法律審查，結果顯示，若美國發現有可靠證據證明將遭到來自網路的重大網路攻擊，總統就可以下令先發制人。新政策還將對情報部門搜索遠在他地的電腦系統以尋找攻擊美國的跡象的相關工作作出規定。而且如果得到總統批准，即便兩國尚未宣戰，情報部門也可以通過植入毀滅性代碼來攻擊敵人。[13]

除此之外，美國亦積極組建網路部隊，美國網路司令部(Cyber Command)司令亞歷山大(Keith Alexander)2013 年 3 月表示，美國正在新增 40 支網路小隊，其中有 13 支的重點是進攻，其他 27 支的重點是培訓和監控。如果美國在網路空間遭受重大攻擊時，將可向其他國家發起進攻性的網路攻擊。[14]

---

from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>。

12. 賈秀東，〈網絡安全不容「霸王條款」〉，《人民日報》（海外版），2013 年 7 月 9 日，<http://paper.people.com.cn/rmrbhwb/html/2013-07/09/content_1265989.htm>。

13. David E. Sanger & Thom Shanker, “Broad Powers Seen for Obama in Cyberstrikes,” *New York Times*, February 3, 2013, <http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html>.

airiti

同樣地，中國亦設有網路部隊，最為西方熟知的莫過於「61398 部隊」。61398 部隊係中國網軍重要部隊之一，隸屬於原負責情報蒐集的解放軍總參謀部第三部第二局，其對美國企業、政府機關的攻擊行動平均持續一年，有一案例長達 4 年又 10 個月，對象包括軍方承包商、化學、礦業、衛星電信企業等各種重要產業；同時，據西方調查結果，該部隊最令人擔憂之處，在於其攻擊重點已不只竊取資訊，還包括掌握控制電力網等重要基礎設施的能力。同時，中國國營之中國電信公司亦以國防名義，提供該部隊專用的高速光纖網路。[15]

第三，國家永遠無法把握其他國家的意圖，雖然美國身為網路大國，然對美中兩國而言，雙方都自認為是受害者，美國認為其境內大量電腦遭到入侵，許多企業及政府機密易遭竊取，而中國則向來主張自己才是網路攻擊的受害者，此種認知亦使雙方關係陷入緊張。雖然在史諾登事件之後，沒有證據顯示美國曾利用網路武器攻擊中國的目標，但是中國的新聞媒體和軍方刊物，卻常常引述美國和以色列針對伊朗核計畫實施的複雜網路攻擊，藉此證明美方也在利用網路空間獲取戰略優勢。[16]

第四，生存是大國的首要目標，對美中兩國而言，隨著習近平的上臺，也讓歐巴馬政府找到提出改善網路安全的契機。歐巴馬藉著向

---

14. Mark Mazzetti & David E. Sanger, “Security Leader Says U.S. Would Retaliate Against Cyberattacks,” *New York Times*, March 12, 2013, <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html>.
15. Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units,” February 20, 2013, pp. 2-60, *Mandiant*, <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.
16. David E. Sanger & Mark Landler, “U.S. and China Agree to Hold Regular Talks on Hacking,” *New York Times*, June 1, 2013, <http://www.nytimes.com/2013/06/02/world/asia/us-and-china-to-hold-talks-on-hacking.html>.

airiti

習近平發電祝賀之際，在賀電內提到網路攻擊的議題，並提到網路攻擊對美國智慧財產權所造成的損失。甚至連與歐巴馬不同政黨的眾議院情報委員會(House Intelligence Committee)主席羅傑斯(Mike Rogers)在接受採訪時亦表示，「在與中國進行的任何一次談話中，美國都要準備三個議程：第一，網路安全；第二，網路安全；第三，網路安全。」[17] 可看出中國對美國發動網路攻擊之複雜程度，已嚴重威脅到美中關係。

第五，大國是理性行為者，事實上，美中雙方雖在網路安全認知分歧，雙方卻也願意透過溝通及對話來試圖降低雙邊緊張關係。正也因此，美中兩國於 2013 年 7 月 8 日在戰略安全對話架構下舉行了第一次網路工作組會議。中國外交部、國防部、公安部、工業和資訊化部、商務部、國務院新聞辦公室和美國國務院、國防部、國土安全部、司法部、財政部、商務部、聯邦調查局及總統國家安全事務委員會等部門官員參加。雙方就網路工作組機制建設、兩國網路關係、網路空間國際規則、雙邊對話合作措施，以及其他共同關心的問題進行坦誠並深入的交流。雙方表示，願本著相互尊重、平等對話的原則建設好這一機制，使之為雙方增信釋疑、管控分歧、拓展合作發揮積極作用。[18]

更進一步而言，美中網路安全問題，其根本原因在於雙方對網路空間認知差異：美國試圖確保在網路空間行動自由之餘，亦可繼續擁有對國際網路空間之控制權；中國則希望確認網路空間與國家主權之關係，換言之，中國亦希望在確定網路空間的主權歸屬時，相關公共

17. Nicole Perlroth, “Cyberattacks a Topic in Obama Call With New Chinese President.”

18. 支林飛，〈張業遂和伯恩斯共同主持第三次中美戰略安全對話〉，《中國政府網》，2013 年 7 月 10 日，<http://www.gov.cn/jrzg/2013-07/10/content_2443808.htm>。

airiti

政策問題的決策權屬於國家主權，但並未堅持主權應涵蓋網路空間一切事務。此外，對美中雙方而言，美國的網路安全利益主要聚焦在關鍵基礎設施的安全、網路空間自由及商業技術機密安全；中國的網路安全利益則關注社會政治穩定、資訊基礎設施及網路系統，以及網路資訊與數據安全，[19] 雙方所關切之安全利益亦有不同。

表 1　美中對網路空間認知及安全利益之比較

國別 項目	美國	中國
網路空間認知	確保在網路空間行動自由之餘，亦可繼續擁有對國際網路空間之控制權。	確認網路空間與國家主權之間關係；希望在確定網路空間的主權歸屬時，相關公共政策問題的決策權屬於國家主權。
主要網路安全利益	1. 關鍵基礎設施的安全 2. 網路空間的自由安全 3. 商業技術機密的安全	1. 社會政治穩定 2. 資訊基礎設施及網路系統的安全 3. 網路資訊與數據的安全

資料來源：作者自行整理。

在此情形下，隨著習近平上臺之後，由於中國政經綜合國力崛起，美中網路安全競逐亦漸趨白熱，而此亦可作為檢視攻勢現實主義之適當案例。畢竟崛起強權挑戰守成強權有許多方式，相較下，網路安全競逐係成本較低但影響甚鉅，成為最為可行之方式，特別是面對不同的安全利益考量。結合前述米爾斯海默所提之五大前提，大國可能基於對國家安全的恐懼(fear)，因而尋求自助(self-help)，而自助的方式便是追求自國的權力最大化(power maximization)。[20] 這種行為模式，在美中網路安全競逐中亦不時出現，作者亦將於後文中分別從政經、

19. 周琪、汪曉風，〈網絡安全與中美新型大國關係〉，《當代世界》（北京），2013 年第 11 期，2013 年 11 月，頁 30-32。

20. John J. Mearsheimer, *The Tragedy of Great Power Politics*, p. 32.

airiti

軍事及國內管制等面向之案例，結合攻勢現實主義論點進行觀察與驗證。

參、中國網軍竊取美國政經機密

隨著歐巴馬政府執政逐漸進入尾聲，網路安全議題值得注意之處在於其 2015 年 2 月所公布之《國家安全戰略》(*National Security Strategy*, NSS)，直接點名中國經由網路竊取商業機密獲利行為。該報告指出，美國「在網路安全方面將採取必要行動保護企業並捍衛網路，以對抗私人或中國政府透過網路竊取商業機密獲利。」[21] 此《國家安全戰略》報告，亦為歐巴馬第二任期與中國在網路安全議題互動定調，顯示美國已將中國網路竊密行為提升到國家安全戰略層面。

對歐巴馬而言，其第二任期正值中國新領導人上臺之際，面對美中之間漸趨白熱的網路安全議題，似乎是個改善的契機。畢竟，對美國而言，不論是美國國防部，或是谷歌(Google)、洛克希德馬丁(Lockheed Martin)等美國政府及企業網站過去均曾遭受網路攻擊，儘管美方多將攻擊來源瞄準中國，然中國向來對此一概否認。然而，早在習近平上臺之前，中國官方媒體「中央電視臺」2011 年 7 月便曾播出中國軍方遂行網路攻擊的畫面，而攻擊目標恰好就是美國網站。當時公布畫面顯示該攻擊系統出自於「中國人民解放軍電子工程學院」，電腦螢幕呈現兩個選項，分別為「全球資訊網阻斷服務攻擊」及「分散式阻斷服務攻擊」(DDoS)。之後是「選擇攻擊目標」、「輸入目標 IP 位址」等對話框，而畫面中選擇的攻擊目標 IP 位址，經查是美國阿拉巴馬大學(University of Alabama)註冊。此畫面一經播出，亦反駁中國一再聲稱從未基於政治目的進行網路攻擊。[22]

---

21. The White House, “National Security Strategy,” February 6, 2015, p. 24, *The White House*, <https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>.

airiti

歐巴馬在習近平出任中國國家主席之後，便曾藉發送賀電之際，向習近平強調網路攻擊對美國的影響。但中國一直否認自己應為美國公司遭駭客襲擊負責，並稱中國也是駭客襲擊的受害者。在與美國官員進行討論時，中國代表也經常拒絕討論經濟間諜問題；[23]甚至如中國外長楊潔篪便曾公開批評，認為國際間對中國政府實行駭客攻擊的指責是種抹黑行為。[24]

儘管美國情報官員曾私下表示已掌握中國政府參與網路攻擊的證據。但隨著美國稜鏡計畫因史諾登事件而曝光，更讓外界震驚美國透過網路大規模侵犯他國主權，尤其是美國一直表示遭受其他國家網路攻擊，儼然一副網路安全受害國的模樣。中國學者沈丁立對此亦曾表示，近年來美國對中國和香港遂行高達 6.1 萬項的網路攻擊計畫，可以想見，只要其中任何一項得逞，相關的政府、個人及企業的電子通信將大門洞開，國家機密和個人隱私也將蕩然無存，中國安全必然面臨嚴重威脅。[25]

中國對美國網路攻擊如此恐懼之原因，在於以思科(Cisco)為主的美國科技業「八大金剛」[26]已深入中國大陸各種不同領域。以思科為

22.管淑平，〈解放軍「駭」美／央視播出「證據」 中國賴不掉〉，《自由時報電子報》，2011 年 8 月 26 日，<http://news.ltn.com.tw/news/world/paper/519296>。

23. Nicole Perlroth, “Cyberattacks a Topic in Obama Call With New Chinese President.”

24. David Barboza, “In Wake of Cyberattacks, China Seeks New Rules,” *New York Times*, March 10, 2013, <http://www.nytimes.com/2013/03/11/world/asia/china-calls-for-global-hacking-rules.html?_r=0>.

25.沈丁立，〈美國賊喊捉賊貽害世界〉，《環球網》，2013年6月17日，<http://opinion.huanqiu.com/opinion_world/2013-06/4031340.html>。

26.美國科技業的「八大金剛」是指思科、IBM、谷歌、高通(Qualcomm)、英特爾(Intel)、蘋果(Apple)、甲骨文(Oracle)、微軟(Microsoft)。

airiti

例，更是在中國電信骨幹網路、四大銀行、海關、公安、武警、工商、教育等政府機構，以及鐵路、航空、港口、石油、傳媒等不同領域占有相當分額，亦可說是全面滲透到中國電信、金融、石油、化工等關係到國計民生的關鍵資訊基礎設施，使中國國家安全可說猶如門戶洞開；加上思科與美國政府及軍方關係密切，其如此長驅直入中國大陸，影響嚴重程度令人難以想像。[27]

從稜鏡計畫的曝光，可看出美國為確保在網路空間的主導地位，採取權力極大化的作為，其監控對象不只如中國這些對手國家，甚至還包括西方盟邦。正也因此，面對美國如此嚴重的網路安全威脅，中共於 2014 年成立「中共中央網絡安全和信息化領導小組」，並由習近平親自擔任組長，體現中國保障網路安全、維護國家利益及推動資訊化發展的決心。[28]如同習近平在召開「中共中央網絡安全和信息化領導小組」首次會議時所強調，網路安全和資訊化係攸關國家安全與國家發展之重大戰略問題，中國雖已成為網路大國，但沒有網路安全就沒有國家安全，沒有資訊化就沒有現代化。要建設中國為網路強國不僅要有自己的技術，其戰略部署更要與「兩個一百年」目標同步推進，並且要彙聚人才資源以建設政治強、業務精、作風好的強大隊伍。該領導小組更要發揮集中統一領導作用，制定實施國家網路安全和資訊化發展戰略、宏觀規畫和重大政策，不斷增強安全保障能力。[29]

雖然中國方面強調遭受來自美國的網路頻繁攻擊，並且也堅稱反對任何形式的駭客攻擊行動，[30]但習近平上臺之後，中國對美國政經領

27.秦安，〈對美國“八大金剛”不能不設防〉，《環球網》，2013 年 6 月 4 日，<http://opinion.huanqiu.com/opinion_world/2013-06/3997929.html>。

28.江蔚，〈中央網絡安全和信息化領導小組成立：從網絡大國邁向網絡強國〉，《新華網》，2014 年 2 月 27 日，<http://news.xinhuanet.com/2014-02/27/c_119538719.htm>。

29.〈習近平：把我國從網絡大國建設成為網絡強國〉。

30.David Barboza, “China’s President Will Lead a New Effort on Cybersecurity,”

airiti

域網路竊密行為仍時有所聞。根據美國聯邦調查局局長柯米(James Comey)表示，中國對美國大公司所發動的駭客攻擊非常猖獗，幾乎無處不在，對美國企業所造成的損失估計高達數十億美元。[31]

一、解放軍網路竊取美企業機密遭起訴

2014 年 5 月 19 日，美國時任司法部長霍德(Eric Holder)親自舉行記者會，對外界說明美國司法部以「網路間諜」罪名起訴 5 名中國軍官，出席者還包括負責國家安全、檢察、調查等工作的各部門官員。美國政府指控該 5 名 61398 部隊成員竊取美國的核電、鋼鐵、太陽能等科技機密，受害者都是著名企業，包括西屋(Westinghouse)電氣公司、美國鋁業公司(Alcoa World Alumina)、阿利根尼技術公司(Allegheny Technologies)、美國鋼鐵公司(U.S. Steel Corp.)、美國鋼鐵公司工會，以及創設於德國的太陽能世界公司(SolarWorld)等。此為美國首次以網路間諜罪名起訴外國政府官員，亦即首次以司法途徑控告外國政府以網路竊取美國商業機密。[32]值得注意之處，在於美國企業因為

New York Times, February 27, 2014, <http://www.nytimes.com/2014/02/28/world/asia/china-announces-new-cybersecurity-push.html>.

31. James Cook, "FBI Director: China Has Hacked Every Big US Company," *Business Insider*, October 6, 2014, <http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10>.

32. Office of Public Affairs, U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, *U.S. Department of Justice*, <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>；劉屏、朱建陵，〈涉竊 150 家公司機密　美政府告解放軍 5 軍官〉，《中時電子報》，2014 年 5 月 20 日，<http://www.chinatimes.com/newspapers/20140520000344-260102>。

airiti

商業機密遭竊問題損失嚴重，眾議員魯珀斯柏格(Dutch Ruppersberger)便曾表示，美國企業 2012 年總計損失逾 3,000 億美元，而其中大部分是中國駭客所致。[33]

面對美國指控，中國立刻提出美國對中國大陸網路攻擊數據加以反駁，並稱美國才是當今世界上最大的網路竊密者，也是中國網路的頭號攻擊國。中國國家互聯網信息辦公室（網信辦）發言人指出，根據中國國家互聯網應急中心資料顯示，2014 年 3 月 19 日至 5 月 18 日，2,077 個位於美國的木馬或僵屍網路控制伺服器，直接控制中國境內約 118 萬臺主機。135 臺位於美國的主機承載 563 個針對中國境內網站的釣魚頁面，造成網路欺詐侵害事件約 1.4 萬次；2,016 個位於美國的 IP 對中國境內 1,754 個網站植入後門，涉及後門攻擊事件約 5.7 萬次。[34]

同時，中國外交部發言人秦剛也針對美方起訴中國軍官一事表示，美方捏造事實，以網路竊密為由起訴 5 名中國軍官，嚴重違反國際關係基本準則，損害美中合作與互信。中方已在第一時間向美方提出抗議，敦促美方立即糾正錯誤、撤銷所謂起訴，中方並決定中止美中網路工作組活動。此外，秦剛亦與網信辦立場一致，強調中國政府和軍隊及其相關人員從不從事或參與網路竊取商業秘密活動，並稱中國是美方網路竊密和監聽、監控的嚴重受害者。[35]

然而，遭美方起訴的 5 名中國軍官並不在美國境內，中國亦不可能

---

33. Michael Martina, “Quarter of U.S. firms in China face data theft: business lobby,” *Reuters*, March 29, 2013, <http://www.reuters.com/article/us-china-us-hacking-idUSBRE92S02P20130329>.

34.〈國家互聯網信息辦公室公布美國攻擊中國網絡最新數據〉，《新華網》，2014 年 5 月 20 日，<http://news.xinhuanet.com/politics/2014-05/20/c_126520505.htm>。

35.中華人民共和國外交部，〈中方強力反擊美方「起訴」中方人員〉， 2014 年 5 月 20 日，《中華人民共和國外交部》，<http://www.fmprc.gov.cn/web/fyrbt_673021/dhdw_673027/t1157508.shtml>。

airiti

交出該等遭起訴軍官。美國學者韓森(Fergus Hanson)認為，美中雙方本來可以定期召開網路安全工作小組，並試圖建立網路運作準則，畢竟美國自 2013 年 5 月起已持續向中國施壓，望其減少支持網路商業間諜活動，國防部亦首次點名中國應為一系列網路攻擊行動負責。但隨著史諾登事件的發生無疾而終，而美國此次採取司法手段，可能使商業間諜議題再度受到重視，無疑是有助於美國重新對中國進行施壓。[36] 此外，美國學者史國力(Adam Segal)則認為，中國不僅將忽視美國司法部協助請求之外，亦將宣傳美國才是真正的駭客帝國。即便中國外交部宣布暫緩美中網路安全小組會議與美中戰略暨經濟對話有關網路議題，惟仍不致對美國企業展開報復。[37]

二、美國人事管理局遭網路駭客攻擊

面對中國在政經領域所進行的網路竊密行為，美國不只將網路安全議題拉高到國家安全戰略層次，更進一步地，美國亦採取司法手段作為回應。美國 2015 年版《國家安全戰略》便提到，美國將在美國及國際法律約束下捍衛自身權益以對抗網路攻擊，並使惡意網路攻擊者付出代價，包括透過針對非法網路行動所展開之起訴行為。[38]

美國加大對網路竊密攻擊行為之制裁力道言猶在耳之際，便爆發美國聯邦政府網路遭中國駭客入侵並竊取大量現職及離職人員資料。

美國人事管理局(Office of Personnel Management, OPM)於 2015 年 6 月 4 日表示，該局遭到網路攻擊，攻擊目標主要係聯邦雇員之個人

36. Fergus Hanson, “Moving Past Snowden,” *The Brookings Institution*, May 21, 2014, <http://www.brookings.edu/blogs/up-front/posts/2014/05/21-theft-us-intellectual-property-snowden-hanson>.

37. Adam Segal, “Department of Justice Indicts Chinese Hackers: What Next?” *Council on Foreign Relations*, May 19, 2014, <http://blogs.cfr.org/asia/2014/05/19/department-of-justice-indicts-chinese-hackers-what-next/>.

38. The White House, “National Security Strategy.”

airiti

身分資訊(Personally Identifiable Information, PII)，影響對象涉及 210 萬現任雇員及 200 萬離退休人員與前雇員。雖然人事管理局並未明指中國，惟相關官員毫不懷疑是從中國所發起的網路攻擊，然尚未確定是否獲中共官方支持。[39]

但是，這卻是美國政府聯邦電腦系統自 2014 年以來第三起重大網路遭入侵事件，前兩起事件分別是 2014 年白宮及國務院電子郵件系統遭俄羅斯駭客入侵，以及人事管理局系統疑似遭中國駭客入侵竊取曾申請絕對機密安全權限之雇員資料。換言之，美國人事行政局電腦系統遭駭並非首次，且根據美方追蹤發現，該網路攻擊源自於中國。此亦凸顯美國起訴中國軍官並未對其形成威脅，從而促使其不再對外國目標實施駭客攻擊。更讓美方官員擔心之處，係美國將無法阻止來自中國的網路攻擊，因為中國方面無需為網路攻擊付出代價，反而終止美中之間許多網路安全相關之正式及非正式對話。[40]

更讓美方感到擔心之處，在於隨著更為深入調查後，情報官員發現中國駭客可能獲取了美國外交官等政府官員的中國親屬、朋友及頻繁連絡人的姓名，內容涉及美國外交官、白宮官員、從事核武器或核

39. United States Office of Personnel Management, "OPM to Notify Employees of Cybersecurity Incident," June 4, 2015, *United States Office of Personnel Management*, <https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/>; David E. Sanger & Julie Hirschfeld Davis, "Hacking Linked to China Exposes Millions of U.S. Workers," *New York Times*, June 4, 2015, <http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html?_r=0>.

40. Michael S. Schmidt, David E. Sanger, & Nicole Perlroth, "Chinese Hackers Pursue Key Data on U.S. Workers," *New York Times*, July 9, 2014, <http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0>; David E. Sanger & Julie Hirschfeld Davis, "Hacking Linked to China Exposes Millions of U.S. Workers."

airiti

情報工作的能源部官員、負責處理跨太平洋夥伴協定(Trans-Pacific Partnership, TPP)談判等敏感經濟議題的商務部或貿易相關的政府機構官員在世界各地的親朋好友的資訊，而這些資訊可能會被北京用來要脅和報復。[41]

除此之外，美方官員更承認中國駭客已獲得人事管理局電腦系統的管理員權限(administrator privileges)，並且已建構一個能讓大量資料傳回中國的電子管道。[42]透過大量的人員資料，中國可以將過去蒐集的資訊與人員進行比對，藉由刪去法與大數據分析(big data analytics)，獲得美國派駐在中國情報人員資料，進行反情報工作，同時亦可作為「魚叉式網路釣魚」(spear phishing)攻擊的工具，進一步擴大入侵美國政府網路系統範圍。[43]

對美國而言，中國駭客入侵美國人事管理局所造成的影響與損失難以估計，更導致時任局長阿庫利塔(Katherine Archuleta)引咎辭職，並可看出美國通緝中國網軍 61398 部隊 5 名軍官並未能嚇阻網路攻擊與竊密行為。即便時任美國司法部長霍德聲稱國家行為者透過網路進行商業間諜活動難逃美國法律制裁，中國對美國之駭客攻擊更是有增

41. David E. Sanger & Julie Hirschfeld Davis, "Hackers May Have Obtained Names of Chinese With Ties to U.S. Government," *New York Times*, June 10, 2015, <http://www.nytimes.com/2015/06/11/world/asia/hackers-may-have-obtained-names-of-chinese-with-ties-to-us-government.html>.

42. David E. Sanger, Nicole Perlroth, & Michael D. Shear, "Attack Gave Chinese Hackers Privileged Access to U.S. Systems," *New York Times*, June 20, 2015, <http://www.nytimes.com/2015/06/21/us/attack-gave-chinese-hackers-privileged-access-to-us-systems.html?_r=0>.

43. Mark Mazzetti & David E. Sanger, "U.S. Fears Data Stolen by Chinese Hacker Could Identify Spies," *New York Times*, July 24, 2015, <http://www.nytimes.com/2015/07/25/world/asia/us-fears-data-stolen-by-chinese-hacker-could-identify-spies.html>.

airiti

無減，並且持續攻擊美國政府及企業，美國國防部亦表示中國駭客每天試圖入侵其系統達上萬次。[44]

簡言之，從攻勢現實主義視角而言，史諾登事件的爆發，凸顯作為網路強國的美國仍試圖採取權力最大化的手段以維持其在世界的優勢；而中國竊取美國國安機密不僅著眼於間諜戰，同時亦展現其欲與美國競逐全球強權地位與影響力，透過網路竊密來達成權力極大化的目的，例如美國現代武器重要技術多由民間企業掌握，中國亦可藉網路滲透等間諜行動或商業交易以獲取軍民兩用科技，可大幅節省其研發經費，並縮短與美國實力之差距。[45]

肆、美中兩國在網路軍事領域的抗衡

美國學者奈伊(Joseph S. Nye, Jr.)表示，40 年前，美國國防部創造了網路，時至今日，許多人認為美國在網路領域的軍事運用仍占有領先地位。[46]對美中兩國而言，在軍事領域的網路安全競逐上，美國相較下自然可說具有相當優勢，然而此一優勢正在逐漸流失當中。根據美國蘭德公司(RAND)2015 年研究指出，中國大陸軍方從 2000 年代中期起，便一直積極參與大規模網路間諜活動，也因此成為備受媒體關注之議題。由於其攻擊最常見之目標係防禦措施較少之企業及非機密

44. Elias Groll, “The U.S. Hoped Indicting 5 Chinese Hackers Would Deter Beijing’s Cyberwarriors. It Hasn’t Worked,” *Foreign Policy*, September 2, 2015, <http://foreignpolicy.com/2015/09/02/the-u-s-hoped-indicting-5-chinese-hackers-would-deter-beijings-cyberwarriors-it-hasnt-worked/>.

45. Jacqueline Newmyer Deal, “How the U.S. Should Respond to the Latest Chinese Hack,” *National Review*, July 13, 2015, <http://www.nationalreview.com/article/421105/how-us-should-respond-latest-chinese-hack-jacqueline-newmyer-deal>.

46. Joseph S. Nye, Jr., “Cyber War and Peace,” *CNN*, April 10, 2012, <http://globalpublicsquare.blogs.cnn.com/2012/04/10/nye-cyber-war-and-peace/>.

airiti

性之政府系統，故對中國大陸在網路戰方面的能力，可能存在誇大之虞。然而，儘管如此，中國大陸的網路攻擊能力仍不斷增強，並判斷最近幾年與美國之差距已漸趨縮小。美國原本相對於中國大陸具有「巨大優勢」(Major advantage)，但到 2010 年則已經降至「具優勢」(Advantage)。[47]

一、中國網軍之組成與對美影響

相較於發明網際網路的美國，中國則於 1999 年 11 月 10 日首次於《解放軍報》提出網軍應成為繼陸、海、空三軍後之新軍種，並肩負捍衛網路主權及遂行網路作戰之任務；同時亦借鏡美國發展，將網軍分為「攻擊」、「防禦」及「安全維護」部門。攻擊部隊負責滲透、監控、摧毀敵方網路系統及竊取與竄改情資；防禦部隊則負責資安防護系統，抵禦外來網路攻擊；安全維護部隊則負責在遭受駭客入侵攻擊後，及時修補網路漏洞並追查攻擊來源。[48]中國的網軍組成，主要由解放軍及國家安全部負責攻擊、公安部負責防禦、工業和信息化部負責安全，其架構及活動如表 2 所示。

47. Eric Heginbotham, et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017* (Calif: RAND Corporation, 2015), p. 283.

48. 吳任傑，〈中共網軍發展研究〉，《陸軍後勤季刊》，102 年第 4 期，2013 年 11 月，頁 103。

airiti

表 2 中國網軍主要架構及其具體分工

型態	負責單位	具體分工
攻擊	解放軍、國家安全部	1. 解放軍：依各單位業管遂行網路情蒐及攻擊，並負責電子對抗及網路體系的防護。 2. 國家安全部：針對各國國際戰略、政經科技情報實施蒐集、研判及偵測科技器材研發，並提供網軍情蒐資訊。
防禦	公安部	負責國內網路預防、制止和偵查違法犯罪活動，監督管理公共資訊網路安全工作。
安全維護	工業和信息化部	負責管理通信業、指導推進資訊化建設、維護國家資訊安全等。

資料來源：作者整理自吳任傑，〈中共網軍發展研究〉，頁 104。

雖然中國的網軍可區分成此三類型態，但就軍事領域部分而言，基本上，中國網軍可說緊盯美國發展而採取相應作為，其最主要原因，莫過於美中軍事實力相差懸殊所致。早在波灣戰爭之後，面對美國高端戰力優勢無人能敵之際，中國可說極力效法美國之軍備及戰術，並設法提升軍力層次。例如在 2007-2008 年間，中國駭客入侵美國國防工業承包商洛克希德馬丁(Lockheed Martin)電腦網路，蒐集 F-35 戰機計畫之核心資料，並顯然利用所獲資料設計其殲-31 隱形戰機。[49]

除藉由網路竊取軍事科技機密外，中國在網軍建制上亦隨著美國而有所作為。2009 年 6 月 23 日，時任美國國防部長蓋茲(Robert M. Gates)下令成立「網路司令部」(Cyber Command)，遂行軍事網路行動，以因應網路科技所帶來的機會與挑戰。[50]中國也在美國網路司令部

49. Paul McLeary & David Francis, "Pentagon Says It Is Moving to Protect Its Cyber Flanks," *Foreign Policy*, April 9, 2015, <https://foreignpolicy.com/2015/04/09/pentagon-says-it-is-moving-to-protect-its-cyber-flanks/>.

50. Robert M. Gates, "Memorandum to Secretaries of the Military Departments, Subject: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," June

airiti

成軍後，於 2010 年 7 月 19 日成立「總參謀部信息保障基地」，時任解放軍總參謀長陳炳德與四位副總參謀長及四總部有關領導均出席成立大會。該基地的成立，係為貫徹落實時任中國國家主席胡錦濤重要戰略思想、推進共軍資訊化建設科學發展之重要步驟，亦為加強共軍資訊化建設集中統管的重大作為，向外表明共軍建制序列中已具有戰略資訊支援保障力量。外界認為這次共軍高調的對外宣布成立戰略性網路作戰部隊，從該基地設於北京並直屬總參謀部，成立大會是由總參謀長率全體副參謀長參加，可看出共軍之重視程度。該基地的設立，被視為因應美國建立網路司令部之原因，在於共軍過去沒有統一集中的管理系統，指揮隸屬於不同部隊的資訊技術中心，該基地亦將是指揮共軍各部門之網際網路戰略資訊中心。[51]

面對中國積極發展網路戰力，美國國家情報總監克萊佩(James R. Clapper)於 2011 年 3 月 10 日在參議院軍事委員會聽證會指出，中國日益增強的網路戰能力讓美國感到擔憂，其擁有龐大機構並投入大量資源蒐集美國情報；特別是在 2010 年 4 月 8 日，中國電信把大批美國和其他國家的網際網路通訊路徑強行經過中國，這種情況持續了 17 分鐘。受到影響的包括美國政府、參議院、海軍、陸軍、空軍、海軍陸戰隊、國防部，以及 500 強企業。[52]

翌年(2012)，當習近平甫以國家副主席結束訪美行程不久，美中因

23, 2009, pp. 1-3, *National Security Archive*, <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf>.

51. 陳國輝，〈共軍組建信息保障基地意涵〉，《展望與探索》，第 8 卷第 8 期，2010 年 8 月，頁 21-22。

52. James R. Clapper, "Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Committee on Armed Services," March 10, 2011, pp. 25-27, *Office of the Director of National Intelligence*, <https://www.dni.gov/files/documents/Newsroom/Testimonies/20110310_testimony_clapper.pdf>.

airiti

網路安全所引發之緊張關係並未因此稍歇。美國國會所屬之美中經濟暨安全審議委員會(U.S.-China Economic and Security Review Commission)於 2012 年 3 月的報告指出，中國商業公司正將尖端科研技術轉給中國軍方，且軍方與中國大型通信公司關係密切，受國家資助地對美國軍方、政府和私營企業使用的網路的入侵創造了條件。中國此舉將可能導致國家安全或公眾安全關鍵基礎設施所依賴的系統和網路嚴重失靈。該報告從軍事角度評估指出，中國在電腦網路運行中的能力已經先進到足夠對美國軍方在衝突中執行任務構成真正的危險。[53]

美國國家情報總監克萊佩 2013 年 3 月 12 日針對全球威脅評估發表看法，並將網路安全視為首要威脅。[54] 此亦使得歐巴馬對中國的網路威脅在習近平上臺後改變過去隱而不提的態度，並在接受訪問時首次明確表示中國駭客襲擊美國事件背後有政府的支持。歐巴馬並表示，美國對中國傳達的立場十分明確，美方期待中國切實遵守有關網路安全的國際協定與法律。[55] 時任國家安全顧問的唐尼倫(Tom Donilon)亦指

53.〈報告：中國網絡戰爭能力危及美國軍隊〉，《BBC 中文網》，2012 年 3 月 8 日，<http://www.bbc.com/zhongwen/trad/science/2012/03/120308_us_china_cyberwar.shtml>；美中經濟暨安全審議委員會報告全文請見 Bryan Krekel, Patton Adams, & George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," March 7, 2012, pp. 1-136, *U.S.-China Economic and Security Review Commission*, <http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf>。

54. James R. Clapper, "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," March 12, 2013, pp. 1-3, *Office of the Director of National Intelligence*, <http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf>.

55. "Transcript: President Obama's Exclusive Interview With George

airiti

出，越來越多美國企業對源自於中國大規模且具針對性的網路竊取商業秘密資訊及智慧財產權技術感到嚴重擔憂，並強調白宮正尋求北京能公開承認問題的迫切性、承諾打擊中國駭客，以及同意參加建立全球標準的對話。[56]

除此之外，美國國防部在 2013 年中國軍力報告當中，亦明確指責中國軍方對美國政府的電腦系統及國防承包商的攻擊日益增多，並表示在 2012 年，世界各地大量的電腦系統，包括美國政府名下的系統，持續成為侵入目標，其中一些可直接歸咎於中國政府和軍方。雖然中國的首要目標係為竊取工業技術，然許多侵入行為似乎旨在深入了解美國決策者之想法，而同樣的資訊蒐集亦可輕易用來建立對美國國防網路、後勤及可在危機時期動用的相關軍事能力的理解。[57]

甚至在習近平訪美前夕，美國媒體更披露中國駭客竊取美國至少 24 種先進武器的設計圖，包括先進的F-35 聯合戰鬥機(Joint Strike Fighter, JSF)、F-22 猛禽式(Raptor)戰鬥機、F/A-18 戰鬥機、魚鷹型(V-22 Osprey)傾斜旋翼飛機、黑鷹直升機、愛國者飛彈(PAC-3)、反制飛彈的

Stephanopoulos," *ABC News*, March 13, 2013, <http://abcnews.go.com/blogs/politics/2013/03/transcript-president-obamas-interview-with-george-stephanopoulos/>.

56. Mark Landler & David E. Sanger, "U.S. Demands China Block Cyberattacks and Agree to Rules," *New York Times*, March 11, 2013, <http://www.nytimes.com/2013/03/12/world/asia/us-demands-that-china-end-hacking-and-set-cyber-rules.html?rref=collection%2Ftimestopic%2FDonilon%2C%20Thomas%20E.&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=10&pgtype=collection&_r=0>.

57. Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," May 6, 2013, p. 36, *U.S. Department of Defense*, <http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf>.

airiti

「終端高空區域防禦系統」(Terminal High Altitude Area Defense, THAAD)、海軍神盾艦的彈道飛彈防禦系統(Aegis Ballistic Missile Defense System)，以及可在近海巡邏的濱海戰鬥艦(Littoral Combat Ships, LCS)等，對美國的國家安全構成重大威脅。[58]

然而，在習近平時期，真正引發外界關注的，莫過於 61398 部隊。根據美國智庫「2049 計畫研究所」(Project 2049 Institute)研究指出，該部隊隸屬於解放軍總參謀部第三部第二局，並以美國和加拿大為目標，關注有關政治、經濟和軍事情報。更令美方擔心的是，61398 部隊一系列攻擊行動，不僅是為竊取情報，其目的還包括獲取操縱美國關鍵基礎設施，包括電網和其他公用事業設施能力。[59]

根據 2049 計畫研究所對 61398 部隊之研究，可看出該部隊頗具相當規模，其組織架構如圖 1 所示。

58. Caitlin Dewey, "The U.S. weapons systems that experts say were hacked by the Chinese," *The Washington Post*, May 28, 2013, <https://www.washingtonpost.com/blogs/worldviews/wp/2013/05/28/the-u-s-weapons-systems-that-experts-say-were-hacked-by-the-chinese>.

59. David E. Sanger, David Barboza, & Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *New York Times*, February 18, 2013, <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=0>.

airiti

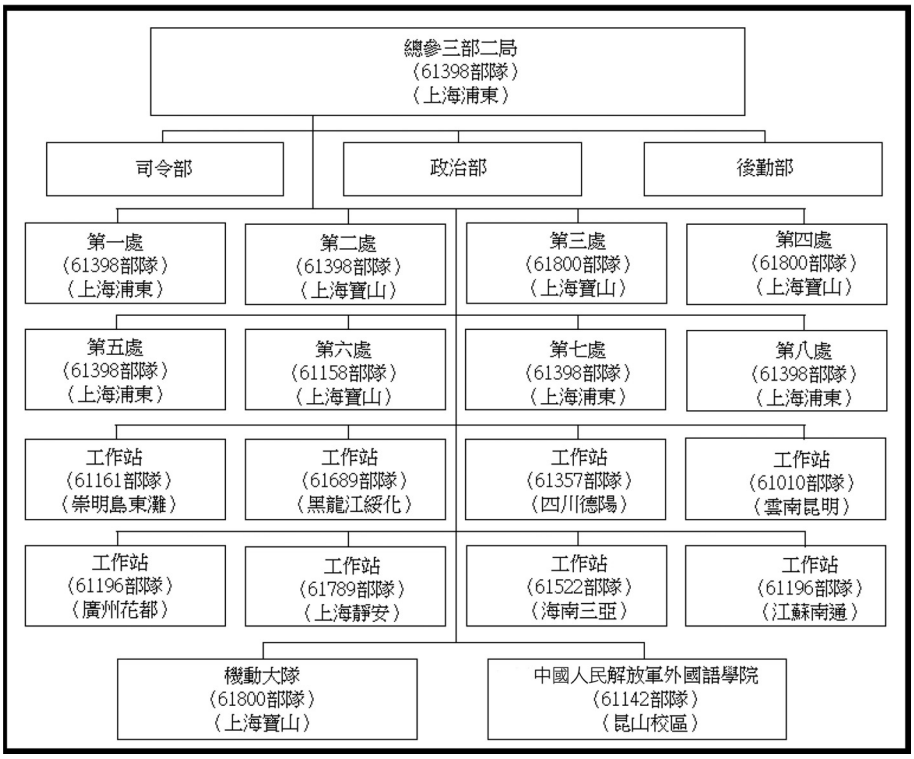

圖 1　解放軍總參第三部第二局 61398 部隊組織架構圖

資料來源：譯自 Mark A. Stokes, “The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398,” July 27, 2015, p. 5, figure 2, *2049 Project Institute*, <http://www.project2049.net/documents/Stokes_PLA_General_Staff_Department_Unit_61398.pdf>。

雖然 61398 部隊 5 名軍官曾於 2014 年 5 月遭到美國司法部以「網路間諜」罪名起訴，但就在其遭起訴後不久，美方亦發現另有幾百次針對美歐航太衛星技術公司及研究組織的網路攻擊行動源自總部位於上海的解放軍 61486 部隊。據美方人士表示，即便在美國起訴 61398 部

airiti

隊的成員後，61486 部隊並未表現出有所收斂的跡象。[60]

61486 部隊攻擊的目標包括美國的政府部門及防務承包商，以及航天和衛星產業研究機構的網路，有時也會與 61398 部隊成員分享資源並進行交流。值得注意之處，在於根據網路紀錄顯示，某次行動中，駭客在實施攻擊時還使用了與 61398 部隊成員一樣的 IP 地址，亦反映出 61398 部隊與 61486 部隊很可能進行合作。[61]

據 2049 計畫研究所指出，61486 部隊與 61398 部隊均屬於總參三部，不過前者隸屬於第十二局。[62] 如前所述，61486 部隊針對航天及衛星產業相關研究機構網路進行攻擊並竊取資訊，有助於其成立太空部隊；[63] 該部隊之作為，亦呼應中國將太空戰爭與網路戰爭的軍事力量結合，這兩者是中國軍方咸認可擊敗美國的兩大王牌。更值得關注之處，在於中國試圖同時動員軍人與平民發起數位「人民戰爭」的方

60. Michael S. Schmidt, David E. Sanger, & Nicole Perlroth, “Chinese Hackers Pursue Key Data on U.S. Workers.”

61. Nicole Perlroth, “2nd China Army Unit Implicated in Online Spying,” *New York Times*, June 9, 2014, <http://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html?_r=0>.

62. 根據 2049 計畫研究所研究指出，總參三部各局部隊代號分別為第一局（61786 部隊）、第二局（61398 部隊）、第三局（61785 部隊）、第四局（61419 部隊）、第五局（61565 部隊）、第六局（61726 部隊）、第七局（61580 部隊）、第八局（61046 部隊）、第九局（從缺）、第十局（61886 部隊）、第十一局（61672 部隊）及第十二局（61486 部隊），請見 Mark A. Stokes, Jenny Lin, & L. C. Russell Hsiao, “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure,” November 11, 2011, pp. 7-11, *2049 Project Institute*, <http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf>。

63. Zachary Keck, “China’s Military Creates New Space Force,” *The Diplomat*, September 10, 2014, <http://thediplomat.com/2014/09/chinas-military-creates-new-space-force/>.

airiti

式，來打贏這場網路戰爭。[64]

在數位「人民戰爭」的思維下，中國大陸的高等院校亦成為解放軍駭客的訓練基地，包括河北武漢大學、山東藍翔技校、上海交通大學、解放軍信息工程大學在內，均與 61398 部隊關係密切。武漢大學計算機學院「空天信息安全與可信計算教育部」重點實驗室，其經費主要由包括總參三部在內之軍事機構贊助，為中國大陸最新網路戰術研發中心，亦為中國主要的資訊安全與網路戰中心之一。山東藍翔高級技工學校，為中國大陸民辦職業院校中唯一向部隊輸送專業技術士官的學校。上海交通大學、河南鄭州解放軍信息工程大學則與網軍長期密切合作，研發新型網路戰術。[65]

面對中國在軍事領域積極發展網路能力抗衡美國，美國網路安全學者龔培德(David C. Gompert)與李比奇(Martin Libicki)表示，雖然美國全球軍力遠勝於中國，北京極可能利用網路戰先發制人，以避免軍事失敗和削弱美國軍事系統，同時亦可對雙方之間的衝突施加影響。目前，中國施用的網路戰呈現「升級」狀態，目標不僅針對國家、政府及商業基礎設施和網路，更大的可能是破壞對方的軍事系統運作，即毀損對方的軍事防禦及攻擊能力。[66]

---

64. Bill Gertz, “China’s Military Preparing for ‘People’s War’ in Cyberspace, Space,” *Washington Free Beacon*, July 30, 2013, <http://freebeacon.com/national-security/china-military-preparing-for-peoples-war-in-cyberspace-space/>.

65. 中央社，〈美媒點名陸 4 高校涉及駭客行為〉，《中時電子報》，2013 年 5 月 16 日，<http://www.chinatimes.com/realtimenews/20130516005087-260409>。

66. David C. Gompert & Martin Libicki, “Cyber Warfare and Sino-American Crisis Instability,” *Survival*, Vol. 56, No. 4, August-September 2014, pp. 7-22, *IISS*, <http://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc>.

airiti

美國政府亦積極評估中國的網路攻擊實力，2014 年 11 月 20 日，時任美國網路司令部司令羅傑斯(Michael Rogers)在眾議院情報委員會作證指出，中國有能力透過網路襲擊美國電網在內之重要基礎建設；美方調查顯示，一些國家、地區及個人可能會利用美國網路系統漏洞，對美國基礎設施發動攻擊，並認為此現象將成為未來趨勢。這是美國第一次由官方公開證實，中國網軍可能威脅美國的國防安全。[67] 此外，美國國防部情報局(Defense Intelligence Agency)局長史都華(Vincent Stewart)亦於 2015 年 2 月 3 日在眾議院軍事委員會作證指出，儘管美國對中國仍保有技術上的優勢，但中國持續藉由網路間諜活動從美軍承包商大量竊取機密，導致美國對中國的技術優勢受到威脅。[68] 美國情報總監克萊佩 2016 年的全球威脅評估亦表示中國依然持續對美國政府、企業進行網路間諜活動。[69]

二、美國網軍之發展與因應作為

有鑑於此，美國在歐巴馬上臺之後，可說加速推動網軍的發展，亦即藉由權力極大化的作為，繼續維持其在網路領域之領先優勢。從 2009 年開始，美國不僅設立網路司令部，並在各軍種亦成立網路司令

---

67. Jamie Crawford, “The U.S. government thinks China could take down the power grid,” *CNN*, November 21, 2014, <http://edition.cnn.com/2014/11/20/politics/nsa-china-power-grid/>.

68. Matthew Pennington, “Intel chief warns US tech threatened by China cybertheft,” *AP*, February 3, 2015, <http://bigstory.ap.org/article/9d713a5fd6ab45d6b962bd380023e1d6/intel-chief-warns-us-tech-threatened-china-cyber-theft>.

69. United States Intelligence Community, “Worldwide Threat Assessment of the US Intelligence Community,” February 9, 2016, *United States Senate Committee on Armed Service*, <http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf>.

airiti

部，充分運用網路優勢與軍事優勢相結合，進一步確保美國的國家安全與利益（請見表 3）。

2013 年，當習近平接任中國國家主席之後，美國亦積極組建網路部隊，時任網路司令部司令亞歷山大曾於 2013 年表示，美國正新增 40 支網路小隊，其中 13 支的重點是進攻，其他 27 支的重點是培訓和監控。[70]

表 3　歐巴馬任內美國網軍發展大事記

時間	事件	要點
2009 年 6 月 23 日	美軍設立網路司令部	美國國防部部長蓋茲下令成立網路司令部，作為美國網路戰最高指揮機構。
2009 年 8 月 19 日	美國空軍網路戰司令部成立	整合網路、空中及太空行動以支持軍事行動。
2010 年 1 月 29 日	美國海軍艦隊網路戰司令部成立	整合海防作戰司令部、海軍網路戰司令部、海軍資訊作戰司令部等單位。
2010 年 10 月 1 日	美國陸軍網路司令部成立	負責主管陸軍網路任務、行動及功能。
2012 年 3 月 24 日	美軍向各戰區派駐網路戰分隊	美軍網路司令部於所有六個地區戰鬥司令部成立網路戰小組。
2013 年 1 月 29 日	網路司令部擴編	員額預計擴增五倍，並成立國家任務部隊、網路保護部隊及作戰任務部隊等。
2013 年 3 月 15 日	宣布新增 40 支網路戰部隊	網路司令部司令亞歷山大於國會表示將增設 40 支網路戰部隊。
2014 年 3 月 4 日	美國將設立 133 支網路部隊	2014 年《四年期國防總檢》(*Quadrennial Defense Review*, QDR)提出美國將設立 133 支網路部隊的戰略目標。
2015 年 4 月 15 日	美國將於 2018 年以前設立 133 支網路隊伍	2015 年美國國防部網路戰略報告提出美國將設立 133 支網路部隊，並於 2018 年完成。

70. Mark Mazzetti & David E, Sanger, “Security Leader Says U.S. Would Retaliate Against Cyberattacks.”

airiti

2016 年 4 月 5 日	美國已成立 123 支網路作戰部隊	網路司令部司令羅傑斯於參議院軍事委員會聽證會表示，美軍迄今已建成 123 支網路作戰部隊，總人數 4,990 人。由三大部分組成，27 支執行進攻任務的作戰部隊，68 支是保護國防部內部網路的網路保護部隊，13 支是國家任務部隊，主要保護美國國內電網、核電站等重要基礎設施。另外還有支援隊伍 25 支，其中，27 支隊伍具備全面作戰能力，68 支隊伍具備初步作戰能力。

資料來源：作者整理自徐俊勇、崔在華、元芳，〈美國網絡空間軍事力量發展情況分析〉，《中國信息安全》（北京），2014 年第 1 期，2014 年 1 月，頁 42-43；〈美建逾百支網軍主攻中俄〉，《大公網》，2016 年 4 月 7 日，<http://news.takungpao.com.hk/world/exclusive/2016-04/3302887.html>；United States Army Cyber Command and Second Army, "Establishment of U.S. Army Cyber Command," April 15, 2015, *United States Army Cyber Command and Second Army*, <http://www.arcyber.army.mil/Organization/ARCYBERHistory>；C. Robert Kehler, "Twenty-Fourth Air Force Activation," *24th Air Force*, August 19, 2009, <http://www.24af.af.mil/news/story.asp?id= 123163965>；United States Navy, "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," *United States Navy*, January 29, 2010, <http://www.navy.mil/submit/display.asp?story_id=50954>；United States Department of Defense, "Quadrennial Defense Review 2014," March 4, 2014, p. 41, *United States Department of Defense*, <http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf>；United States Department of Defense, "The Department of Defense Cyber Strategy," *United States Department of Defense*, April 15, 2015, <http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy>。

2014 年 3 月 4 日，美國國防部公布 2014 年《四年期國防總檢》，提出美國將設立 133 支網路部隊的戰略目標，包括 13 支「國家任務部隊」(National Mission Teams, NMTs)、8 支「國家支援部隊」(National Support Teams, NSTs)、27 支「作戰任務部隊」(Combat Mission Teams, CMTs)、17 支「作戰支援部隊」(Combat Support Teams, CSTs)、18 支「國家網路防禦部隊」(National Cyber Protection Teams, CPTs)、24 支「國家網路防禦維護部隊」(Service CPTs)，以及 26 支「作戰指揮與國防部資訊網路防禦部隊」(Combatant Command and DOD Information Network CPTs)。[71]

這 133 支網路部隊於美國國防部 2015 年 4 月 25 日所提出之《國

airiti

防部網路戰略》(*The Department of Defense Cyber Strategy*)則區分為四大類，分別為 13 支「國家任務部隊」(National Mission Teams, NMTs)、68 支「網路防禦部隊」(Cyber Protection Teams, CPTs)、27 支「作戰任務部隊」(Combat Mission Teams, CMTs)，以及 25 支「支援部隊」(Support Teams, STs)，並預計在 2018 年組建完成。[72]

即便美國在成立網軍之際，亦希望與中國開誠布公討論網路安全。2014 年 4 月，時任美國國防部長黑格(Chuck Hagel)便前往北京與中國軍方高層針對網路安全議題進行討論，其中提及美國國防部保護美國網路不受攻擊及利用其網路技術來對付中國等對手的新戰略。最主要的，黑格擔心美中兩國間網路攻擊和反擊迅速升級的可能性越來越大，特別當歐巴馬向習近平提出美國遭受大量來自中國的網路攻擊後，美國遭到攻擊不減反增，大多數仍是針對矽谷、軍事承包商及能源企業竊取技術及智慧財產權，而黑格認為當中許多攻擊都與解放軍網路戰部隊有關。黑格此行向中方強調，美軍將盡量做到透明，同時也希望中國做到同樣的公開、透明和克制；同時，黑格並表示，美國不希望將網路空間軍事化，並提及對其他國家最低限度使用網路武器之戰略，試圖向中國在內的國家保證，美國不會常規性地針對其使用網路武器。[73]

2015 年 2 月 11 日，歐巴馬邀請習近平九月赴美進行國事訪問，歐巴馬亦趁機呼籲，要求北京當局採取迅速行動，拉近雙方在網路間的分歧。[74]在習近平赴美進行國事訪問前，美中雙方官員正針對首個網路

71. United States Department of Defense, “Quadrennial Defense Review 2014.”

72. United States Department of Defense, “The Department of Defense Cyber Strategy.”

73. David E. Sanger, “U.S. Tries Candor to Assure China on Cyberattacks,” *New York Times*, April 6, 2014, <http://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html?_r=0>.

74. 程靜，〈美中 9 月峰會　網絡安全或成焦點〉，《大紀元》，2015 年 2 月 12

airiti

武器控制協定進行談判，雙方共同承諾，在和平時期不首先使用網路武器破壞另一方的關鍵基礎設施。此類協定可以制約針對發電站、銀行系統、手機網路及醫院的攻擊，但目前中國被指在美國實施的大部分攻擊行為，都不在該協議的制約範圍內。[75] 無獨有偶地，就在習近平即將會晤歐巴馬之際，美國人事管理局卻又公布 560 萬筆聯邦雇員的指紋資訊遭中國竊取。指紋遭竊或使中國能藉此確定情報人員、國防人員和政府承包商身分。[76]

歐巴馬 2015 年 9 月 25 日在白宮會晤習近平後，在聯合記者會上表示，兩國政府已達成協議，雙方將不從事網路間諜活動以竊取對方的商業情報。雙方將針對網路犯罪建立高層對話機制，若任何一方被指從事網路攻擊行動，兩國政府高層官員將予以審查，雙方亦同意將建立熱線以討論相關問題。未來，美國國土安全部部長及司法部部長將代表美方，共同主持此對話機制。該協議還包括若一方違反約定將遭受之制裁。歐巴馬表示，為嚇阻和懲治網路攻擊的犯罪行為，雙方將利用必要的工具。例如，去年美國對中國從事網路商業間諜活動的 5 名軍事官員作出了刑事起訴。歐巴馬說，兩國政府在制止網路間諜與入侵方面的工作還有許多要做，未來美國將繼續與中方和其它國家共同開展合作，從而保護各國在網路活動中應遵循的國際準測。他說，美國也將繼續使用必要的工具，保護美國公司及公民的合法利益。[77]

日，<http://www.epochtimes.com/b5/15/2/12/n4364927.htm>。

75. David E. Sanger, “U.S. and China Seek Arms Deal for Cyberspace,” *New York Times*, September 19, 2015, <http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html>.

76. David E. Sanger, “Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says,” *New York Times*, September 23, 2015, <http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html>.

77. The White House, “Remarks by President Obama and President Xi of the

airiti

但是，該協議似乎主要涉及應對商業間諜之作法，而未針對中國以往所採之傳統間諜活動，如中國之前通過網路入侵美國人事管理局電腦系統並竊取逾 2,200 萬前任及現任美國聯邦雇員的個人資訊。[78]

綜前所述，美國向來在網路領域的軍事用途上穩執牛耳，即便中國近年積極追趕，雙方實力仍有一定差距，反應在實質作為上亦有所不同（請見表 4）。

表 4　美中兩國在網路安全之軍事領域比較

項目＼國別	美國	中國
軍事指揮機制	美軍網路司令部目前隸屬於美國國防部下轄之戰略司令部。網路司令部司令由中將擔任，作戰命令則是由總統通過國防部長下達至戰略司令部。	中國網軍原以總參謀部下轄之技術偵查部（總參三部）為主，另外包括各大軍區、國防科研機關及各級軍事院校等。然隨著中國自 2015 年底推動軍事改革後，總參網路攻防部隊已改劃入戰略支援部隊，受中共中央軍事委員會指揮。
機構相互關係	美國網路司令部下轄陸海空軍及海軍陸戰隊網路司令部，預計至 2018 年設立 133 支網路部隊，並朝向升格成為聯合網路作戰司令部發展，目前則是各軍兵種建立自己的網路安全隊伍。	根據中國推動軍改之「軍委管總、戰區主戰、軍種主建」原則，戰略支援部隊屬於獨立軍種部隊，按照軍種主建的原則，僅負責相關部隊的軍政管理工作，不具備作戰指揮功能。戰略支援部隊主要由軍委直接指揮，部分部隊在配屬戰區作戰時由戰區指揮部指揮。國防科研機關負責相關準則研擬，各級軍事院校則負責解放軍科技人才培育工作。

資料來源：作者自行整理。

對美國而言，美國在歐巴馬政府任內加緊網軍建設，係針對包含

People's Republic of China in Joint Press Conference," September 25, 2015, *The White House*, <https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>.

78. 柳芳，〈美中首腦達共識　不從事網絡商業間諜活動〉，《大紀元》，2015 年 9 月 26 日，<http://www.epochtimes.com/b5/15/9/26/n4536290.htm>。

airiti

中國在內的其他國家，除避免遭受網路攻擊之外，亦可保障自身網路安全，更希望藉此與盟邦合作以加強關係，進一步阻止威脅，確保國際安全與穩定。由此可看出美國仍舊採行權力極大化之作為，確保國家利益免遭嚴重的網路攻擊。尤有甚者，在必要時，美國亦會發動網路攻擊以捍衛其國家利益，如美國首度宣布對造成全球威脅的伊斯蘭國(Islamic State, IS)發動網路攻擊。[79] 相較下，中國則因為實力遠遜於美國，於是在加強網軍建設之際，更進一步藉網軍力量支持其軍力發展與增進其國家安全。中國藉由網軍竊取相關先進武器機密及航太科技技術，不僅可省去高昂的開發成本，並有助於提升本土國防工業，更能與總體建軍目標相結合，此亦使中國難以在軍事領域放棄網路竊密舉動。即便美中針對網路軍控達成共識，然該協議並未針對中國藉由網路所遂行之傳統間諜活動進行規範，將使美中雙方未來在網路領域之軍事用途上恐再次面臨衝突。

伍、美中雙方各自強化國內網路管制

對美中兩國而言，在強化各自國內網路管制上，雙方均有所作為，但其目標則有所不同。對中國而言，從 2010 年中東茉莉花革命所引發的民主浪潮，到史諾登事件所揭露的全球網路監控，更讓其試圖加強國內網路管制，以降低來自西方國家在虛擬網路世界所造成的威脅。然而，如美國學者史國力指出，美國對中國至少有三種網路攻擊類型可以考慮，分別是從事駭客活動，披露令中國領導層尷尬的資訊；讓中國網民進入被封鎖的、中國以外的網站；削弱或解除中國境內對資訊的控制。[80] 特別是面對中國為打壓境內不同意見所設置的網路

79. David E. Sanger, “U.S. Cyberattacks Target ISIS in a New Line of Combat,” *New York Times*, April 24, 2016, <http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0>.

80. Adam Segal, “Revealed: Why China and America are Set to Clash in

airiti

審查及控制系統「長城防火牆」(Great Firewall, GFW)，美國情報單位亦希望藉由突破長城防火牆的封鎖，讓中國領導人知道，若其不適度限制對美國的網路攻擊，則其最重視的事情，亦即對國內政治具有絕對的話語權一事，可能將會受到威脅。[81]

一、中國藉技術與立法加強網路安全審查與言論管控

自習近平上臺以後，對言論之控制似更勝以往，特別是當美中兩國在網際網路領域競逐漸趨白熱之際，習近平亦加強對網路的關注。習近平在 2013 年中共十八屆三中全會後強調，網路和資訊安全牽涉國家安全和社會穩定，是中國面臨新的綜合性挑戰；如何加強網路法制建設和輿論引導，確保網路資訊傳播秩序和國家安全、社會穩定，業已成為中國所面臨的突出問題。[82] 2014 年，習近平更強調沒有網路安全就沒有國家安全，[83] 特別是每一個國家在資訊領域的主權權益都不應受到侵犯，網路技術再發達也不能侵犯他國的資訊主權，而各國都有權維護自己的資訊安全，更不能犧牲別國安全謀求自身所謂絕對安全。[84]

在此前提下，中國大陸一方面擴大對外國科技公司實施網路安全

Cyberspace," *National Interest*, August 3, 2015, <http://www.nationalinterest.org/blog/the-buzz/revealed-why-china-america-are-set-clash-cyberspace-13479>.

81. David E. Sanger, "U.S. Decides to Retaliate Against China's Hacking," *New York Times*, July 31, 2015, <http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html>.

82. 習近平，〈關於《中共中央關於全面深化改革若干重大問題的決定》的說明〉，《新華網》，2013 年 11 月 15 日，<http://news.xinhuanet.com/politics/2013-11/15/c_118164294.htm>。

83. 〈習近平：把我國從網絡大國建設成為網絡強國〉。

84. 〈習近平巴西談互聯網治理〉，《新華網》，2014 年 7 月 17 日，<http://politics.people.com.cn/BIG5/n/2014/0717/c1024-25296103.html>。

airiti

審查，另方面亦加強對國內網路言論的控制。

首先，就擴大實施網路安全審查而言，網信辦於 2014 年表示，將針對進入中國市場的重要資訊技術產品及其提供者進行網路安全審查，審查的重點在於該產品的安全性和可控性，旨在防止產品提供者利用提供產品的方便，非法控制、干擾、中斷使用者系統，非法蒐集、存儲、處理和利用使用者有關資訊，對不符合安全要求的產品和服務，將不得在中國境內使用。網信辦意有所指地提及史諾登事件，再次強調沒有網路安全就沒有國家安全，並提到中國的網路安全審查並非首創，美國早有先例；早在 2012 年，美國就以國家安全為由對中國企業進行安全審查。[85] 在此同時，中國亦拿美國網路設備廠商思科作為目標大肆批評，認為思科的路由器產品幾乎參與中國所有基礎資訊網路和重要資訊系統的重大專案建設，卻存在嚴重的「預置式後門」，甚至和美國政、軍兩界打得火熱，利用其在中國網路資訊市場的技術產品優勢，扮演了不光彩的角色，成為美國推行網際網路強權的重要技術倚仗。[86]

除網路設備商思科之外，中國也將目標對準微軟的作業系統，中國中央國家機關政府採購中心亦發布〈關於進行資訊類協定供貨強制節能產品補充招標的通知〉，要求中央機關採購所有電腦類產品不允許安裝 Windows 8 作業系統，因為該系統具有高不可控度，運行該系統的電腦存在著被監控的風險。[87]

85.〈國家網信辦：我國將出臺網路安全審查制度〉，《中國網信網》，2014 年 5 月 22 日，<http://www.cac.gov.cn/2014-05/22/c_126534290.htm>。

86.武竹，〈美國思科路由器預置“後門”意欲何為〉，《中青在線》，2014 年 5 月 26 日，<http://article.cyol.com/news/content/2014-05/26/content_10138288.htm>。

87.〈中央國家機關政府採購電腦對 Win8 說“不”〉，《中青在線》，2014 年 5 月 22 日，<http://zqb.cyol.com/html/2014-05/22/nw.D110000zgqnb_20140522_1-12.htm>。

airiti

其次，針對加強對國內網路言論的控制而言，除既有之網路審查系統外，中國大陸亦開始採取專家稱為「大砲」(Great Cannon)之網路攻擊策略，導入大量流量癱瘓目標網站，加強網路管制與審查。2015年3月底，協助用戶規避網路審查之Greatfire.org網站遭受網路攻擊，咸認係中國所為。中國挾市場龐大之經濟優勢，脅迫他方遵守規則，全球網路治理及全球網路安全面臨嚴峻挑戰。[88]

值得注意地是，外界亦質疑中國大陸境內知名科技公司協助政府對網路進行管制，其中，以中國大陸三大科技公司騰訊、阿里巴巴與百度最為外界所懷疑，如騰訊曾遭外界質疑審查其微信用戶之言論；百度則遭指控在日本及越南用戶電腦上植入間諜軟體，以及限制巴西用戶搜尋敏感關鍵字。同時，儘管百度聲稱不知情，「大砲」系統係運用百度網站流量作為攻擊工具。雖然上述指控尚未經系統化查證，且此三者係公開上市公司，不同於華為或中興通訊，並未明顯接受中共資助或扶持。儘管如此，若欲於中國大陸市場營運，勢須避免違背官方意願，即便西方科技公司如微軟、蘋果、領英(LinkedIn)等，皆曾被指運用其產品協助中共管制網路，微軟甚至被控管制中國境外用戶之搜尋結果，中國企業自然更難以倖免。[89]

以領英為例，為了進入中國廣袤的市場，不僅願意遵守中國的言論規則外，並將其中文網站7%股份，讓渡給兩家頗具背景的中國風險投資公司。同時，領英使用軟體演算法和人工審閱相組合的方式，對中國境內的中英文網站就中國當局認為具有政治敏感性的內容進行審

88. Rogier Creemers, “Disarming the Great Cannon,” *Foreign Policy*, April 10, 2015, <https://foreignpolicy.com/2015/04/10/great-cannon-china-internet-cyber-attack-baidu>.

89. Sarah Logan, “Beijing’s Great Cannon exposes vulnerable Chinese tech firms,” *Lowy Institute for International Policy*, May 4, 2015, <http://www.lowyinterpreter.org/post/2015/05/04/Beijings-Great-Cannon-exposes-vulnerable-Chinese-tech-firms.aspx>.

airiti

查。如果發布的內容被封禁，使用者會收到電子郵件發送的通知，告知其貼文內含「在中國遭到禁止的內容」，「將不會被領英在中國的會員看到」。[90]

除透過技術層面管控網路言論之外，中國亦透過立法手段對網路言論進行控制。中國在 2015 年通過《國家安全法》，第 25 條便規定

> 國家建設網絡與信息安全保障體系，提升網絡與信息安全保護能力，加強網絡和信息技術的創新研究和開發應用，實現網絡和信息核心技術、關鍵基礎設施和重要領域信息系統及數據的安全可控；加強網絡管理，防範、制止和依法懲治網絡攻擊、網絡入侵、網絡竊密、散布違法有害信息等網絡違法犯罪行為，維護國家網絡空間主權、安全和發展利益。[91]

明確呼應習近平所說，沒有網路安全就沒有國家安全。

同時，中國亦於 2015 年提出《網路安全法》（草案），其主要內容聚焦於維護網路主權和戰略規則、保障網路產品和服務安全、保障網路運行安全、保障網路數據安全、保障網路資訊安全、監測預警與應急處置，以及網路安全監管體系。[92] 從中國對「網路空間主權」的強

---

90. Paul Mozur & Vindu Goel, "To Reach China, LinkedIn Plays by Local Rules," *New York Times*, October 5, 2014, <http://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html?_r=0>.

91.《中華人民共和國國家安全法》係 2015 年 7 月 1 日為第 12 屆全國人民代表大會常務委員會第 15 次會議通過，該法共分為七章、84 條。全文請見〈中華人民共和國國家安全法〉，《人大新聞網》，2015 年 7 月 10 日，<http://npc.people.com.cn/BIG5/n/2015/0710/c14576-27285049.html>。

92.《中華人民共和國網路安全法》（草案） 係 2015 年 6 月經過第 12 屆全國人民代表大會常務委員會第 15 次會議審議，該草案共分為七章，68 條。草案及說明全文請見〈網路安全法（草案）〉，《中國人大網》，2015 年 7 月 6 日，<http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm>。

airiti

調，不僅凸顯出其欲確保對境內網路的絕對控制權力之外，亦具對外積極宣示之意涵。在對內管控部分，《草案》第 43 條對於來源於境外的違禁資訊「應當通知有關機構採取技術措施和其他必要措施阻斷資訊傳播」，以及第 50 條出於維護國家安全和社會公共秩序、處置重大突發社會安全事件的需要「可以在部分地區對網路通信採取限制等臨時措施」，這些中國視為合理必要的管控舉措可能引發美方對於打壓網路言論自由的擔心和指責。相較下，中國在對外宣示部分並未作出過於強硬之表示。最主要地，莫過於網路空間仍然是處於無政府狀態之全球公共領域(Global Commons)，在面對具有優勢的美國，《草案》第 5 條提出將「積極開展網路空間治理、網路技術研發和標準制定、打擊網路違法犯罪等方面的國際交流與合作，推動構建和平、安全、開放、合作的網路空間」的主張，藉以提升中國在網路空間全球治理領域中之能見度與話語權。[93]

二、美國藉國安名義限制中國企業作為與反制中國竊密

相對於中國而言，美國擔心中國可藉其價格低廉的資訊科技產品攻占美國市場，並可趁機竊取機密，便主要針對硬體方面進行管制。如前美國國防部資深安全政策分析師馬洛夫(F. Michael Maloof)於 2012 年便指出，中國透過華為及中興兩家電訊供應商製造後門，使其為世界各地電訊商安裝不同電訊設備同時亦提供後門設計，好讓中國政府能監控並獲得各種不同的資訊，包含上網及通話資料等，並有機會修改甚至破壞原有內容。同時針對所獲得之加密數據，中國政府亦想盡辦法試圖加以解碼。[94]

---

93. 檀有志，〈中國網絡安全法草案的外揚與內抑〉，《FT 中文網》，2015 年 8 月 4 日，<http://www.ftchinese.com/story/001063323?full=y>。

94. F. Michael Maloof, “China: ‘Pervasive access’ to 80% of telecoms,” *WND*, July 1, 2012, <http://www.wnd.com/2012/07/chinese-have-pervasive-access-

airiti

以華為公司為例，面對外界有關網路間諜的指控，被廣泛認為有中共軍方背景的華為公司高層稱，所有的政府都在通過網路間諜行為獲取情報。然而，華為內部運作如同情報機構，其商貿活動、人員調配都要聽命於中共，並為解放軍的一支精銳網路戰部隊提供服務，類似於前蘇聯國家安全委員會(Комите́т госуда́рственной безопа́сности, KGB)式的情報部門；根據美國中央情報局(Central Intelligence Agency, CIA)、公開情報中心(Open Source Center, OSC)2011 年 10 月報告指出，華為在過去三年從中國政府拿到近 2.5 億美金的資助，為中國提供情報服務。[95]

面對此一威脅，美國眾議院情報委員會 2012 年亦發表調查報告，認定華為與中興對美國國家安全造成威脅，強調中國有能力、有機會，以及有動機運用通訊公司以達到不可告人的目的。該報告除建議美國公司不要與華為及中興有商業往來外，亦建議美國政府採購應避免購買帶有華為及中興公司產品的設備，以避免給間諜行為打開後門。[96] 針對國會的建議，歐巴馬亦於 2013 年簽署法案，禁止包括司法部、商務部、航空航天局及聯邦調查局在內的聯邦政府機構，採購中國所有、運營或提供補貼的企業製造、加工或組裝的資訊技術產品。[97]

如前所述，美國為確保其在網路領域之優勢，早在中國之前便以資訊安全為由進行國家安全審查，並對中國相關貿易採取限制措施，主要手段包括：[98]

---

to-80-of-worlds-telecoms/>.

95. Open Source Center, “Huawei Annual Report Details Directors, Supervisory Board for First Time,” October 5, 2011, pp. 1-12, *Federation of American Scientists*, <http://fas.org/irp/dni/osc/huawei.pdf>.

96.〈美國認定華為中興威脅其國家安全〉，《BBC 中文網》，2012 年 10 月 8 日，<http://www.bbc.com/zhongwen/trad/chinese_news/2012/10/121008_us_china_huaweizte>。

97.秦安，〈對美國“八大金剛”不能不設防〉。

airiti

第一，透過美國外國投資委員會（Committee on Foreign Investment in the United States，以下簡稱 CFIUS）對中國資訊科技產業赴美投資進行國家安全審查，如 2005 年聯想併購案便提出相當嚴格的限制條件，讓聯想被迫簽訂國家安全協議；2008 年，華為與貝恩資本(Bain Capital)試圖聯合併購 3com 公司，最終遭到 CFIUS 否決；2011 年，華為對三葉系統(3 Leaf system)的收購案，亦在CFIUS阻撓下被迫停止。

第二，美國政府或國會對政府部門、重點企業採購中國資訊科技產品進行直接干涉，如聯想在美國投資之後，美國國務院受議員施壓，調整對聯想電腦的採購計畫；2010 年 8 月，華為與美國電信商史普林特(Sprint)價值 60 億美元的電信合約亦在美國政界警告下夭折。

第三，美國眾議院情報委員會 2012 年對中興、華為進行特別調查並發表調查報告，其結果令中興、華為徹底退出美國市場。

第四，2013 年，美國國會通過《2013 財政年度綜合繼續撥款法》，限制美國 4 個政府部門（司法部、商務部、航空航天局及聯邦調查局）購買中國企業生產之資訊技術設備。

然而，面對中國所提出的擴大實施網路安全審查，由美國商會(United States Chamber of Commerce)領頭的 17 個貿易團體敦促美國政府對中國的審查政策表示抗議，呼籲美國政府應立即採取行動，與中國官員磋商，從而扭轉這些將對資通訊技術(Information and Communication Technology, ICT)產業造成影響且令人不安的中國政府新政策。[99] 對此，美國官員亦大肆抨擊中國政策，並將其定性為反競爭的貿易壁壘，同時亦質疑中國的「網路主權」概念，重申美國捍衛網路自由，

98. 左曉棟，〈近年中美網絡安全貿易糾紛回顧及其對網路安全審查制度的啟示〉，《中國信息安全》（北京），2014 年第 8 期，2014 年 8 月，頁 70。

99. Paul Mozur, “Trade Groups Urge U.S. to Push Against Chinese Regulations,” *New York Times*, February 5, 2015, <http://bits.blogs.nytimes.com/2015/02/05/trade-groups-urge-u-s-to-push-against-chinese-regulations/?_r=0>.

airiti

以及支持促進國際商貿的國家網路空間行為規範。[100]

除官員抨擊中國政策之外，美國也擴大加強對網路攻擊的因應作為。美國總統歐巴馬於 2015 年 4 月 1 日簽署行政命令，授權美國政府針對發起網路攻擊的個人、組織及嫌疑人作出制裁，包括凍結個人資產。該制裁計畫目標主要針對海外的網路駭客。主要涉及嚴重威脅美國國家安全及經濟穩定的網攻犯罪、對美國重要基礎設施造成危害、擾亂或破壞美國政府電腦系統，以及盜取美國公司商業機密或美國公民的個人資訊並以此牟利等行為。[101]

同時，前述美國於 2014 年透過司法部門起訴 5 名解放軍網攻竊密行為，亦凸顯出歐巴馬時期在因應中國網路攻擊上的重大轉變。事實上，美國針對網路攻擊與網路竊密的行為，可說設有相關法律作為因應，包括《對外情報監視法》(*Foreign Intelligence Surveillance Act*)、《電子通信隱私法》(*Electronic Communications Privacy Act*)、《經濟間諜法》(*Economic Espionage Act*)、《電腦詐欺及濫用法案》(*Computer Fraud and Abuse Act*)、《愛國者法案》(*Patriot Act*)及相關通信安全系統監控法規等。[102] 換言之，過去美國主要係透過相關法律及審查手段規範與限制中國設備輸入美國，但從起訴解放軍網路竊密行為後，反映出未來美國將以健全的反網路竊密法律體系為依據，對中國相關行為提出司法控訴，不僅透過法律手段讓網路竊密行為者付出

---

100. J. Michael Daniel, Robert Holleyman, & Alex Niejelow, "China's Undermining an Open Internet," *Politico*, February 4, 2015, <http://www.politico.com/magazine/story/2015/02/china-cybersecurity-114875>.

101. The White House, "Executive Order 13694 of April 1, 2015: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015, pp. 18077-18079 *U.S. GPO*, <https://www.gpo.gov/fdsys/pkg/FR-2015-04-02/pdf/2015-07788.pdf>.

102. 朱莉欣、武蘭，〈探秘美國網絡空間安全的法律之盾〉，《中國信息安全》（北京），2013 年第 3 期，2013 年 3 月，頁 77-78。

airiti

代價，亦有可能作為後續進一步行動之法律依據。[103]

雖然歐巴馬與習近平曾於 2015 年 9 月達成有關政府不支持網路商業間諜活動的協議，但面對前述美中諸多網路衝突，該協議能否緩和兩國緊張關係仍待觀察。畢竟協議之擬定或將面臨多重挑戰：其一，西方政府亦行監控、追殺洩密人士之實，相關協議恐難以在國內推行。其二，雙方缺乏互信。其三，民間網路巨擘及個別使用者亦具極大影響力，議題複雜程度超出國對國之範疇。其四，「安全」與「侵犯」難以定義與達成共識，若各國各行其道，執法將面臨困難。[104] 然根據美國國會「美中經濟暨安全評估委員會」(US-China Economic and Security Review Commission, USCC)於 2015 年 11 月 17 日發表年度報告說，美國在對抗來自中國由國家支持的網路攻擊上仍然缺乏準備，同時國際法沒有跟上網路戰的發展，而美國國會應當對美國法律在這方面的適用性作出評估。[105]

簡言之，由於美中兩國政治體制不同，呈現在國內網路安全的控制力道不同，加上兩國所面臨社會媒體的監督力量不同，反映在強化國內網路管制方面，亦可看出雙方聚焦重點及因應作為亦有所不同。從攻勢現實主義角度視之，均係出於恐懼對方而採取強化自身安全的自保行為：對於一黨專政的中國而言，不同於西方的「輿論監督權力」，習近平上臺後更著重於網路言論控制，並擔心美國的網路技術能突破其封鎖，輸入西方意識形態，危害其對網路空間言論的絕對掌

103. 閻曉麗，〈對美國起訴中國軍人網路竊密的法律思考〉，《中國信息安全》（北京），2014 年第 6 期，2014 年 6 月，頁 89-90。

104. Rogier Creemers, “Disarming the Great Cannon.”

105. U.S.-China Economic and Security Review Commission, “2015 Report to Congress of the U.S.-China Economic and Security Review Commission,” p. 13, *U.S.-China Economic and Security Review Commission*, November 17, 2015, <http://origin.www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF>.

airiti

控，特別是在史諾登事件後，更擴大到對相關網路設備進行審查，並同時透過國內立法手段，藉由法律來進一步控制網路言論，甚至連在網路上發表不同意見亦可能被視為是網路犯罪行為。相較下，美國則是擔心中國藉由價格較為低廉之資訊科技產品攻占美國市場，並可透過後門的設置而竊取機密，故過去多以國家安全的理由進行審查，進而規範或限制中國企業及設備進入美國。然隨著中國網軍竊密行為猖獗，使美國亦轉變焦點，改利用司法手段對網路竊密行為者提起告訴，並作為後續進一步報復行為之根據。然而，網際空間仍是國際公共領域，相關國際法及國內法的適用性仍在發展，對美中兩國而言，雙方亦須深入討論網路安全之互動並採取措施，以限制誤解對方意圖之作為；[106] 美中兩國雖達成不支持網路商業間諜行為協議，惟其成效仍有待觀察。[107]

陸、結論

美中在網路安全領域的齟齬在習近平上臺之前便時有所聞，最具代表地莫過於 2010 年谷歌退出中國大陸事件，除此之外，不論是網路審查、駭客竊密與攻擊，均成為美中交鋒之議題所在。習近平上臺後，美國希望藉著中國新領導人上臺之際，找出解決網路安全領域衝突之道，即便美中之間最後達成不支持網路商業間諜活動協議，然本文認為該協議對緩解美中於網路安全領域較勁程度相當有限。

從攻勢現實主義的視角，恰能貼切地解釋美中在網路安全領域迄今摩擦不斷的現況（請見表 5）。從攻勢現實主義的五大基本命題出

106. Jon R. Lindsay, “The Impact of China on Cybersecurity: Fiction and Friction,” *International Security*, Vol. 39, No. 3, Winter 2014-15, p. 47.

107. Tami Abdollah, “US official: Charges possible if Chinese hackers keep it up,” *Business Insider*, November 10, 2015, <http://www.businessinsider.com/ap-us-official-charges-possible-if-chinese-hackers-keep-it-up-2015-11>.

airiti

發，網路空間可說比現實國際體系更處於無政府狀態，現有國際法規範在處理網路安全議題上亦有不足之處，使各國的國家安全直接受到影響。同時，各國亦具備在網路領域擴張勢力之力量，能夠傷害甚至摧毀對手，即便如被外界視為神秘又落後的北韓，亦能發動網路攻擊，更遑論美中兩大強國。況且，國家永遠無法把握其他國家的意圖，美中雙方都自認為是網路安全的受害者，在網路對外作為更加以維護自身利益與生存為首要考量，而此亦呼應生存是大國的首要目標。惟即便美中在網路安全領域摩擦不斷，雙方仍能理性自制，試圖藉對話來降低緊張關係，避免陷入難以收拾的局面。

表 5　從美中兩國在網路安全領域互動驗證攻勢現實主義五大命題

攻勢現實主義論點	美中互動情形
國際體系處於無政府狀態	網路空間較現實國際體系更處於無政府狀態，現有國際法規範在處理網路安全議題上亦有不足之處，使美中兩國安全直接受到影響。
大國本身具備某些用於侵略擴張的軍事力量，能傷害甚至摧毀對手	美中兩國亦具備在網路領域擴張勢力之力量，能夠傷害甚至摧毀對手。
國家永遠無法把握其他國家的意圖	美中雙方都自認為是網路安全的受害者。
生存是大國的首要目標	美中在網路對外作為更加以維護自身利益與生存為首要考量。
大國是理性行為者	美中即便在網路安全領域摩擦不斷，雙方仍能理性自制，試圖藉對話來降低緊張關係，避免陷入難以收拾的局面。

資料來源：作者自行整理。

雖然美中達成協議，然其對緩解美中於網路安全領域較勁程度有限之原因，主要在於大國間為了求生存，基於對國家安全的恐懼，因而採取自助，而自助的方式便是追求自國的權力最大化；換言之，在雙方追求權力最大化的過程中，美中網路摩擦情形仍將持續，亦使協議難以獲致預期成效。

本文就政經、軍事及國內管制三大面向之案例，對美中在網路安

airiti

全領域競逐進行分析，可得知美中兩國皆基於恐懼而採取自助，進而以權力極大化的手段消除恐懼：就政經領域而言，史諾登事件的爆發，凸顯美國對於其他強權崛起可能挑戰自身地位的恐懼，而實行稜鏡計畫，試圖以權力極大化的手段來維持其在世界的優勢於不墜，中國則出於自身與美國之國力與科技差距，試圖透過網路竊密縮短差距並進一步與美國競逐全球強權地位與影響力；就軍事領域而言，中國網軍成立較美國晚，規模亦不如美國，軍事研發技術更瞠乎其後，使中國網軍不僅加強對美國軍事系統攻擊之外，更積極於竊取相關軍事科技以提升其軍隊實力，而美國網軍的擴編及網路空間戰略，所針對者不僅止於中國，更希望藉此強化與盟邦合作，進一步確保國家利益免於遭受網路攻擊影響。尤有甚者，如前所述，美國在必要時亦會發動網路攻擊以捍衛其國家利益，如其首度宣布對 IS 發動網路攻擊。

在強化國內管制面向上，中國恐懼美國透過網路技術與意識形態，使其境內出現如中東茉莉花革命情形，於是一方面擴大對外國科技公司實施網路安全審查，減少外國滲透顛覆之可能，另方面加強對國內網路言論的控制，避免出現煽動串聯之局面；美國則擔心中國挾其價格低廉之資通訊產品擴大美國市占率之際，亦從中於設備裡設置後門以竊取機密，便以國家安全為由進行審查，並對中國相關貿易採限制措施，以維護其在網路領域之優勢，特別是美國採取司法手段起訴中國軍官網攻竊密行為，亦為美國因應中國網攻之重大轉變。綜言之，美中在國內管制面均採取法律手段，然中國係以對內為主，進一步達成社會維穩目標；美國則以對外為主，作為後續進一步行動之法律依據，換言之，雖然有人批評美國起訴中國軍官無濟於事，然美國只是以此作為後續行動的基礎，俾於未來對中國能師出有名。

對美中兩國而言，雙方須深入討論網路安全之互動並採取防範措施以限制誤解對方意圖之作為。雖然攻勢現實主義有助於解讀美中於網路安全領域競逐之情況，但由於美中欠缺安全感的情形未變，雙方對網路空間治理及主權之認知差異，在欠缺相關法律規範及難以確定

airiti

網路實際行為者之下，美中在網路安全領域發生摩擦之情境短期內仍將持續，而美中所達成不支持網路商業間諜活動協議將是雙方合作解決衝突的起點。

（收件：2016 年 1 月 3 日，修正：2016 年 5 月 11 日，採用：2016 年 5 月 17 日）

airiti

參考文獻

中文部分

期刊論文

左曉棟，2014/8。〈近年中美網絡安全貿易糾紛回顧及其對網路安全審查制度的啟示〉，《中國信息安全》（北京），2014 年第 8 期，頁 69-72。

朱莉欣、武蘭，2013/3。〈探秘美國網絡空間安全的法律之盾〉，《中國信息安全》（北京），2013 年第 3 期，頁 76-80。

吳任傑，2013/11。〈中共網軍發展研究〉，《陸軍後勤季刊》，102 年第 4 期，頁 101-116。

周琪、汪曉風，2013/11。〈網絡安全與中美新型大國關係〉，《當代世界》（北京），2013 年第 11 期，頁 30-34。

徐俊勇、崔在華、元芳，2014/1。〈美國網絡空間軍事力量發展情況分析〉，《中國信息安全》（北京），2014 年第 1 期，頁 41-44。

梁德昭、朱志平、林凱薰，2012/11。〈國家主權延伸至網路空間之討論〉，《前瞻科技與管理》，第 2 卷第 2 期，頁 1-14。

陳國輝，2010/8。〈共軍組建信息保障基地意涵〉，《展望與探索》，第 8 卷第 8 期，頁 21-25。

閻曉麗，2014/6。〈對美國起訴中國軍人網路竊密的法律思考〉，《中國信息安全》（北京），2014 年第 6 期，頁 89-91。

網際網路

2012/3/8。〈報告：中國網絡戰爭能力危及美國軍隊〉，《BBC 中文網》，<http://www.bbc.com/zhongwen/trad/science/2012/03/120308_us_china_cyberwar.shtml>。

airiti

2012/10/8。〈美國認定華為中興威脅其國家安全〉，《BBC 中文網》，<http://www.bbc.com/zhongwen/trad/chinese_news/2012/10/121008_us_china_huaweizte>。

2013/6/8。〈談網路攻擊　習近平：中國也是受害者〉，《ETtoday 東森新聞雲》，<http://www.ettoday.net/news/20130608/219833.htm>。

2014/2/27。〈習近平：把我國從網絡大國建設成為網絡強國〉，《新華網》，<http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm>。

2014/5/20。〈國家互聯網信息辦公室公布美國攻擊中國網絡最新數據〉，《新華網》，<http://news.xinhuanet.com/politics/2014-05/20/c_126520505.htm>。

2014/5/22。〈中央國家機關政府採購電腦對 Win8 說“不”〉，《中青在線》，<http://zqb.cyol.com/html/2014-05/22/nw.D110000zgqnb_20140522_1-12.htm>。

2014/5/22。〈國家網信辦：我國將出臺網路安全審查制度〉，《中國網信網》，<http://www.cac.gov.cn/2014-05/22/c_126534290.htm>。

2014/7/11。〈柯瑞：中國駭客 製造寒蟬效應〉，《世界日報網》，<http://www.worldjournal.com/266365/article-%E6%9F%AF%E7%91%9E%EF%BC%9A%E4%B8%AD%E5%9C%8B%E9%A7%AD%E5%AE%A2-%E8%A3%BD%E9%80%A0%E5%AF%92%E8%9F%AC%E6%95%88%E6%87%89/?npg=2>。

2014/7/17。〈習近平巴西談互聯網治理〉，《新華網》，<http://politics.people.com.cn/BIG5/n/2014/0717/c1024-25296103.html>。

2015/7/6。〈網路安全法(草案)〉，《中國人大網》，<http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm>。

2015/7/10。〈中華人民共和國國家安全法〉，《人大新聞網》，<http://npc.people.com.cn/BIG5/n/2015/0710/c14576-27285049.html>。

2015/12/16。〈習近平在第二屆世界互聯網大會開幕式上的講話（全

airiti

文）〉，《中國共產黨新聞網》，<http://cpc.people.com.cn/BIG5/n1/2015/1216/c64094-27937316.html>。

2016/4/7。〈美建逾百支網軍主攻中俄〉，《大公網》，<http://news.takungpao.com.hk/world/exclusive/2016-04/3302887.html>。

中央社，2013/5/16。〈美媒點名陸 4 高校涉及駭客行為〉，《中時電子報》，<http://www.chinatimes.com/realtimenews/20130516005087-260409>。

中央社，2013/7/5。〈中美網路小組 將舉行首次會議〉，《中時電子報》，<http://www.chinatimes.com/realtimenews/20130705004146-260409>。

中國互聯網絡資訊中心，2015/7/22。〈第 36 次中國互聯網絡發展狀況統計報告〉，《中國互聯網絡資訊中心》，<https://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201507/t20150722_52624.htm>。

中華人民共和國外交部，2014/5/20。〈中方強力反擊美方「起訴」中方人員〉，《中華人民共和國外交部》，<http://www.fmprc.gov.cn/web/fyrbt_673021/dhdw_673027/t1157508.shtml>。

支林飛，2013/7/10。〈張業遂和伯恩斯共同主持第三次中美戰略安全對話〉，《中國政府網》，<http://www.gov.cn/jrzg/2013-07/10/content_2443808.htm>。

江蔚，2014/2/27。〈中央網絡安全和信息化領導小組成立：從網絡大國邁向網絡強國〉，《新華網》，<http://news.xinhuanet.com/2014-02/27/c_119538719.htm>。

沈丁立，2013/6/17。〈美國賊喊捉賊貽害世界〉，《環球網》，<http://opinion.huanqiu.com/opinion_world/2013-06/4031340.html>。

武竹，2014/5/26。〈美國思科路由器預置“後門”意欲何為〉，《中青在線》，<http://article.cyol.com/news/content/2014-05/26/content_10138288.htm>。

柳芳，2015/9/26。〈美中首腦達共識 不從事網絡商業間諜活動〉，

airiti

《大紀元》，<http://www.epochtimes.com/b5/15/9/26/n4536290.htm>。

秦安，2013/6/4。〈對美國“八大金剛”不能不設防〉，《環球網》，<http://opinion.huanqiu.com/opinion_world/2013-06/3997929.html>。

習近平，2013/11/15。〈關於《中共中央關於全面深化改革若干重大問題的決定》的說明〉，《新華網》，<http://news.xinhuanet.com/politics/2013-11/15/c_118164294.htm>。

程靜，2015/2/12。〈美中 9 月峰會　網絡安全或成焦點〉，《大紀元》，<http://www.epochtimes.com/b5/15/2/12/n4364927.htm>。

賈秀東，2013/7/9。〈網絡安全不容「霸王條款」〉，《人民日報》（海外版），<http://paper.people.com.cn/rmrbhwb/html/2013-07/09/content_1265989.htm>。

管淑平，2011/8/26。〈解放軍「駭」美／央視播出「證據」中國賴不掉〉，《自由時報電子報》，<http://news.ltn.com.tw/news/world/paper/519296>。

劉屏、朱建陵，2014/5/20。〈涉竊 150 家公司機密　美政府告解放軍 5 軍官〉，《中時電子報》，<http://www.chinatimes.com/newspapers/20140520000344-260102>。

檀有志，2015/8/4。〈中國網絡安全法草案的外揚與內抑〉，《FT 中文網》，<http://www.ftchinese.com/story/001063323?full=y>。

英文部分

專書

Heginbotham, Eric, et al., 2015. *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996 – 2017*. Calif: RAND Corporation.

Mearsheimer, John J., 2001. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company.

airiti

期刊論文

Lindsay, Jon R., 2014-15/Winter. "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, No. 3, pp. 7-47.

網際網路

2013/3/13. "Transcript: President Obama's Exclusive Interview With George Stephanopoulos," *ABC News*, <http://abcnews.go.com/blogs/politics/2013/03/transcript-president-obamas-interview-with-george-stephanopoulos/>.

Abdollah, Tami, 2015/11/10. "US official: Charges possible if Chinese hackers keep it up," *Business Insider*, <http://www.businessinsider.com/ap-us-official-charges-possible-if-chinese-hackers-keep-it-up-2015-11>.

Barboza, David, 2013/3/10. "In Wake of Cyberattacks, China Seeks New Rules," *New York Times*, <http://www.nytimes.com/2013/03/11/world/asia/china-calls-for-global-hacking-rules.html?_r=0>.

Barboza, David, 2014/2/27. "China's President Will Lead a New Effort on Cybersecurity," *New York Times*, <http://www.nytimes.com/2014/02/28/world/asia/china-announces-new-cybersecurity-push.html>.

Clapper, James R., 2011/3/10. "Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Committee on Armed Services," pp. 1-33, *Office of the Director of National Intelligence*, <https://www.dni.gov/files/documents/Newsroom/Testimonies/20110310_testimony_clapper.pdf>.

Clapper, James R., 2013/3/12. "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," pp. 1-30, *Office of the Director of National Intelligence*, <http://www.dni.gov/

airiti

files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf>.

Cook, James, 2014/10/6. "FBI Director: China Has Hacked Every Big US Company," *Business Insider*, <http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10>.

Crawford, Jamie, 2014/11/21. "The U.S. government thinks China could take down the power grid," *CNN*, <http://edition.cnn.com/2014/11/20/politics/nsa-china-power-grid/>.

Creemers, Rogier, 2015/4/10. "Disarming the Great Cannon," *Foreign Policy*, <https://foreignpolicy.com/2015/04/10/great-cannon-china-internet-cyber-attack-baidu>.

Daniel, J. Michael, Robert Holleyman, & Alex Niejelow, 2015/2/4. "China's Undermining an Open Internet," *Politico*, <http://www.politico.com/magazine/story/2015/02/china-cybersecurity-114875>.

Deal, Jacqueline Newmyer, 2015/7/13. "How the U.S. Should Respond to the Latest Chinese Hack," *National Review*, <http://www.nationalreview.com/article/421105/how-us-should-respond-latest-chinese-hack-jacqueline-newmyer-deal>.

Dewey, Caitlin, 2013/5/28. "The U.S. weapons systems that experts say were hacked by the Chinese," *The Washington Post*, <https://www.washingtonpost.com/blogs/worldviews/wp/2013/05/28/the-u-s-weapons-systems-that-experts-say-were-hacked-by-the-chinese>.

Gates, Robert M., 2009/6/23. "Memorandum to Secretaries of the Military Departments, Subject: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," *National Security Archive*, <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf>.

Gellman, Barton & Laura Poitras, 2013/6/7. "U.S., British intelligence

airiti

mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, <https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.

Gertz, Bill, 2013/7/30. "China's Military Preparing for 'People's War' in Cyberspace, Space," *Washington Free Beacon*, <http://freebeacon.com/national-security/china-military-preparing-for-peoples-war-in-cyberspace-space/>.

Gompert, David C.& Martin Libicki, 2014/8-9. "Cyber Warfare and Sino-American Crisis Instability," *Survival*, Vol. 56, No. 4, pp. 7-22, *IISS*, <http://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc>.

Groll, Elias, 2015/9/2. "The U.S. Hoped Indicting 5 Chinese Hackers Would Deter Beijing's Cyberwarriors. It Hasn't Worked," *Foreign Policy*, <http://foreignpolicy.com/2015/09/02/the-u-s-hoped-indicting-5-chinese-hackers-would-deter-beijings-cyberwarriors-it-hasnt-worked/>.

Hanson, Fergus, 2014/5/21. "Moving Past Snowden," *The Brookings Institution*, <http://www.brookings.edu/blogs/up-front/posts/2014/05/21-theft-us-intellectual-property-snowden-hanson>.

Keck, Zachary, 2014/9/10. "China's Military Creates New Space Force," *The Diplomat*, <http://thediplomat.com/2014/09/chinas-military-creates-new-space-force/>.

Kehler, C. Robert, 2009/8/19. "Twenty-Fourth Air Force Activation," *24th Air Force*, <http://www.24af.af.mil/news/story.asp? id=123163965>.

Krekel, Bryan, Patton Adams, & George Bakos, 2012/3/7. "Occupying

airiti

the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," pp. 1-136, *U.S.-China Economic and Security Review Commission*, <http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf>.

Landler, Mark & David E. Sanger, 2013/3/11. "U.S. Demands China Block Cyberattacks and Agree to Rules," *New York Times*, <http://www.nytimes.com/2013/03/12/world/asia/us-demands-that-china-end-hacking-and-set-cyber-rules.html?rref=collection%2Ftimestopic%2FDonilon%2C%20Thomas%20E.&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=10&pgtype=collection&_r=0>.

Logan, Sarah, 2015/5/4. "Beijing's Great Cannon exposes vulnerable Chinese tech firms," *Lowy Institute for International Policy*, <http://www.lowyinterpreter.org/post/2015/05/04/Beijings-Great-Cannon-exposes-vulnerable-Chinese-tech-firms.aspx>.

Maloof, F. Michael, 2012/7/1. "China: "Pervasive access' to 80% of telecoms," *WND*, <http://www.wnd.com/2012/07/chinese-have-pervasive-access-to-80-of-worlds-telecoms/>.

Mandiant, 2013/2/20. "APT1: Exposing One of China's Cyber Espionage Units," pp. 1-74, *Mandiant*, <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>.

Martina, Michael, 2013/3/29. "Quarter of U.S. firms in China face data theft: business lobby," *Reuters*, <http://www.reuters.com/article/us-china-us-hacking-idUSBRE92S02P20130329>.

Mazzetti, Mark & David E. Sanger, 2013/3/12. "Security Leader Says U.S. Would Retaliate Against Cyberattacks," *New York Times*, <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-

airiti

that-cyberattacks-pose-threat-to-us.html>.

Mazzetti, Mark & David E. Sanger, 2015/7/24. "U.S. Fears Data Stolen by Chinese Hacker Could Identify Spies," *New York Times*, <http://www.nytimes.com/2015/07/25/world/asia/us-fears-data-stolen-by-chinese-hacker-could-identify-spies.html>.

McLeary, Paul & David Francis, 2015/4/9. "Pentagon Says It Is Moving to Protect Its Cyber Flanks," *Foreign Policy*, <https://foreignpolicy.com/2015/04/09/pentagon-says-it-is-moving-to-protect-its-cyber-flanks/>.

Mozur, Paul, 2015/2/5. "Trade Groups Urge U.S. to Push Against Chinese Regulations," *New York Times*, <http://bits.blogs.nytimes.com/2015/02/05/trade-groups-urge-u-s-to-push-against-chinese-regulations/?_r=0>.

Mozur, Paul & Vindu Goel, 2014/10/5. "To Reach China, LinkedIn Plays by Local Rules," *New York Times*, <http://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html?_r=0>.

Nye, Joseph S., Jr., 2012/4/10. "Cyber War and Peace," *CNN* <http://globalpublicsquare.blogs.cnn.com/2012/04/10/nye-cyber-war-and-peace/>.

Office of Public Affairs, U.S. Department of Justice, 2014/5/19. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," *U.S. Department of Justice*, <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

Office of the Secretary of Defense, 2013/5/6. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," pp. 1-83, *U.S. Department of Defense*, <http://

airiti

archive.defense.gov/pubs/2013_China_Report_FINAL.pdf>.

Open Source Center, 2011/10/5. "Huawei Annual Report Details Directors, Supervisory Board for First Time," pp. 1-12, *Federation of American Scientists*, <http://fas.org/irp/dni/osc/huawei.pdf>.

Pennington, Matthew, 2015/2/3. "Intel chief warns US tech threatened by China cybertheft," *AP*, <http://bigstory.ap.org/article/9d713a5fd6ab45d6b962bd380023e1d6/intel-chief-warns-us-tech-threatened-china-cyber-theft>.

Perlroth, Nicole, 2013/3/14. "Cyberattacks a Topic in Obama Call With New Chinese President," *New York Times*, <http://bits.blogs.nytimes.com/2013/03/14/cyberattacks-prominent-in-obama-call-with-new-chinese-president/?_r=0>.

Perlroth, Nicole, 2014/6/9. "2nd China Army Unit Implicated in Online Spying," *New York Times*, <http://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html?_r=0>.

Sanger, David E., 2014/4/6. "U.S. Tries Candor to Assure China on Cyberattacks," *New York Times*, <http://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html?_r=0>.

Sanger, David E., 2015/7/31. "U.S. Decides to Retaliate Against China's Hacking," *New York Times*, <http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html>.

Sanger, David E., 2015/9/19. "U.S. and China Seek Arms Deal for Cyberspace," *New York Times*, <http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html>.

Sanger, David E., 2015/9/23. "Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says," *New York Times*, <http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html>.

airiti

Sanger, David E., 2016/4/24. "U.S. Cyberattacks Target ISIS in a New Line of Combat," *New York Times*, <http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0>.

Sanger, David E. & Julie Hirschfeld Davis, 2015/6/4. "Hacking Linked to China Exposes Millions of U.S. Workers," *New York Times*, <http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html?_r=0>.

Sanger, David E. & Julie Hirschfeld Davis, 2015/6/10. "Hackers May Have Obtained Names of Chinese With Ties to U.S. Government," *New York Times*, <http://www.nytimes.com/2015/06/11/world/asia/hackers-may-have-obtained-names-of-chinese-with-ties-to-us-government.html>.

Sanger, David E. & Mark Landler, 2013/6/1. "U.S. and China Agree to Hold Regular Talks on Hacking," *New York Times*, <http://www.nytimes.com/2013/06/02/world/asia/us-and-china-to-hold-talks-on-hacking.html>.

Sanger, David E. & Thom Shanker, 2013/2/3. "Broad Powers Seen for Obama in Cyberstrikes," *New York Times*, <http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html>.

Sanger, David E., David Barboza, & Nicole Perlroth, 2013/2/18. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *New York Times*, <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=0>.

Sanger, David E., Nicole Perlroth, & Michael D. Shear, 2015/6/20. "Attack Gave Chinese Hackers Privileged Access to U.S. Systems," *New York Times*, <http://www.nytimes.com/2015/06/21/us/attack-gave-chin-

airiti

ese-hackers-privileged-access-to-us-systems.html?_r=0>.

Schmidt, Michael S., David E. Sanger, & Nicole Perlroth, 2014/7/9. "Chinese Hackers Pursue Key Data on U.S. Workers," *New York Times*, <http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0>.

Segal, Adam, 2014/5/19. "Department of Justice Indicts Chinese Hackers: What Next?" *Council on Foreign Relations*, <http://blogs.cfr.org/asia/2014/05/19/department-of-justice-indicts-chinese-hackers-what-next/>.

Segal, Adam, 2015/8/3. "Revealed: Why China and America are Set to Clash in Cyberspace," *National Interest*, <http://www.nationalinterest.org/blog/the-buzz/revealed-why-china-america-are-set-clash-cyberspace-13479>.

Stokes, Mark A., 2015/7/27. "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398," pp. 1-24, *2049 Project Institute*, <http://www.project2049.net/documents/Stokes_PLA_General_Staff_Department_Unit_61398.pdf>.

Stokes, Mark A., Jenny Lin, & L. C. Russell Hsiao, 2011/11/11. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," pp. 1-32, *2049 Project Institute*, <http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf>.

United States Army Cyber Command and Second Army, 2015/4/15. "Establishment of U.S. Army Cyber Command," *United States Army Cyber Command and Second Army*, <http://www.arcyber.army.mil/Organization/ARCYBERHistory>.

U.S.-China Economic and Security Review Commission, 2015/11/17.

airiti

"2015 Report to Congress of the U.S.-China Economic and Security Review Commission," pp. 1-619, *U.S.-China Economic and Security Review Commission*, <http://origin.www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF>.

United States Department of Defense, 2014/3/4. "Quadrennial Defense Review 2014," pp. 1-64, *United States Department of Defense*, <http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf>.

United States Department of Defense, 2015/4/15. "The Department of Defense Cyber Strategy," *United States Department of Defense*, <http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy>.

United States Intelligence Community, 2016/2/9. "Worldwide Threat Assessment of the US Intelligence Community," pp. 1-29, *United States Senate Committee on Armed Service*, <http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf>.

United States Navy, 2010/1/29. "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," *United States Navy*, <http://www.navy.mil/submit/display.asp?story_id=50954>.

United States Office of Personnel Management, 2015/6/4. "OPM to Notify Employees of Cybersecurity Incident," *United States Office of Personnel Management*, <https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/>.

The White House, 2012/2/14. "Remarks by Vice President Biden and Chinese Vice President Xi at the State Department Luncheon," *The White House*, <https://www.whitehouse.gov/the-press-office/2012/02/14/remarks-vice-president-biden-and-chinese-vice-president-xi-state-departm>.

The White House, 2015/2/6. "National Security Strategy," pp. 1-29, *The*

airiti

White House, <https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>.

The White House, 2015/4/1. "Executive Order 13694 of April 1, 2015: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," pp. 18077-18079, *U.S. GPO*, <https://www.gpo.gov/fdsys/pkg/FR-2015-04-02/pdf/2015-07788.pdf>.

The White House, 2015/9/25. "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," *The White House*, <https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>.

airiti

U.S.-China Rival over Security in the Xi Jinping Era

Chih-ping Chu

(Ph.D. Candidate, Graduate Institute of Management Sciences, Tamkang University)

Te-chao Liang

(Associate Professor, Department of Information Management, Tamkang University)

Abstract

Since Xi Jinping became the leader of the People's Republic of China (PRC) at the 18th National Congress of the Chinese Communist Party (CCP) in 2012, cyber security has been the focus of U.S.-China relations. The U.S. currently holds an obvious advantage in the cyber security field, however, the PRC has been tempted to compete with the U.S. when it comes to cybercrime in the area of economic and political security, military disputes and control over domestic legislation. The PRC aims not only to realize President Xi's pledge to become a strong cyber power, but also to challenge the leading status of the U.S.. The main purpose of this article is to assess the competitive relationship between the U.S. and the PRC under Xi's leadership in respect to cyber security via offensive realism. The paper presents case studies on politics, economics, the military and internal control.

airiti

Keywords: Cyber Security, Offensive Realism, New Type of Major Power Relations, U.S.-China Relations, Cybercrime