中共對網路空間主權之概念與作為

王 清 安
（國防部陸軍通信電子資訊訓練中心總隊長）

黃 基 禎
（美國加州柏克萊大學東亞研究中心研究員）

摘 要

近年來網路攻擊事件已經對一個國家的政治、經濟與軍事造成一定的影響。其主要原因是國家行爲者，在國家境內無法針對跨國境資料流動實施管轄。各國相繼成立「網路安全法」，賦予政府可以監控資訊流動，以保障網路用户與企業資料安全，及強化國家境內關鍵基礎設施資安防護。因此，形塑網路空間主權，建構資料在地化（data localization）管理，已成爲解決網路空間衝突、分攤維護國際和平的可行性手段。

雖然建立資料在地化管理，可以保護個人、企業與國家安全。然而，本研究發現，中共形塑的網路空間主權，自 2016 年《網絡安全法》頒布後，政府部門依法對境內的網路用户、網路營運商實施管轄，其網路空間已建構出與世界網路隔離的內部網路。與此同時，中國政府整合軍、民網路產業合作，其所建構出的網路空間疆界，在政治上，已對現行網路空間秩序產生衝擊。經濟上，將增加全球網路營運商進入中國大陸市場的成本，致使貿易保護形成，不利於全球化經濟發展。此外，軍事上，在國安部門獲得外商進入中國大陸市場所繳出的商品原始碼後，將有利於掌握、監控他國網路資訊，爲戰時創造出不對稱作戰優勢。總體而言，中共所形塑的網路主權，絕非僅是強化國家境內的網路安全，而實現強國夢、強軍夢的具體表現。

關鍵詞：網路空間、網路空間主權、網路安全、網路疆域

* * *

DOI：10.30389/MCS.201903_62(1).0003

壹、前　言

沒有網路安全，就沒有國家安全。無政府狀態的網路空間秩序，將威脅到用戶數據安全、數位金融發展及國家整體運作。根據 2015 年，中共國家主席習近平主持《互聯網第二屆大會》開幕致詞時表示：「當前互聯網領域發展不平衡、秩序不合理等問題日益嚴重。國際社會應該在相互尊重、信任的基礎上，加強合作，以共同構建和平、安全的網路空間。」（朱國賢、霍小光、楊依軍 2015）隔年底，中共首度出版《國家網路空間安全戰略》更明確指出，網路空間同等於陸地、海洋、天空、太空等重要領域；其網路主權已成爲國家主權組成的重要部分（中國互聯網路信息中心 2017）。由中共宣告網路空間主權的行爲，凸顯出網路空間的利益與安全，將是中共的核心利益。換言之，也意味著中國政府將對跨國境的數據資料，採取更多的管制措施，以強化網路安全防護作爲。

自由、開放的網際網路，加速了數位經濟全球化、政治民主化的發展。同時，跨境數據資料卻也弱化國家主權。基此，中共爲強化境內的網路安全，透過形塑網路主權，已提升對跨國數據資料的管轄權。但此舉也將挑戰現行以美國所主導的網路空間秩序。根據 Paul R. Burgman（2016）表示，中共所呼籲各國彼此尊重的網路主權，其主要目的，就是希望建構網路空間的新秩序，以制衡美國在網路空間的霸權地位。但令人弔詭的是，2015 年底中、美雙方在美國首府華盛頓簽訂「打擊網路犯罪及相關事項指導原則」協議，針對網路反恐合作、執法培訓等達成共識（人民網 2015）。故在中共形塑網路主權後，其所建構出的網路空間疆界，將衝擊到美、中兩國安全與利益的發展。

總而言之，中共爲強化國家境內網路安全，透由實體疆界的國際政治（international politics）主權概念，在虛擬網路空間進行主權的宣告（claim），以期建構出網路空間疆界，支持其國際網路安全治理的話語權。然而，中共形塑的網路主權，對其網路安全如此重要。但根據我國期刊論文網站，截至 2017 年 5 月中旬止，僅數篇探討中共網路主權發展，且側重於網路媒體審查與管制，而忽略中共企圖要成爲網路強國的戰略目標。故本文首先，藉由探討網路主權所管轄之對象與範圍，以瞭解其網路空間主權對國家安全之影響。其次，分析中共發展網路主權背景及目的，以探究建構網路主權之戰略目標。第三，評估其建構網路空間疆界化（cyber territorialization）之管轄範圍，以檢視其形塑網路主權對區域安全之影響。最後，以美國蘋果電腦在中共遭審查個案，論證中共形塑網路主權之意涵。

貳、網路主權緣起與發展

由於網路空間是用於貿易、通訊和其他用途的國際共享資源的全球公共領域。但隨著網路攻擊範圍已危害到國家利益與安全。形塑數據在地化管理，將成爲預防網路安全衝突，和平發展網路秩序的重要手段。

一、網路主權緣起與定義

（一）網路主權之緣起

主權爲國際體制上，國際法所認定其所屬的法定領域，賦予國家行爲者之統治權，其目的爲保護國家境內人民、財產安全。根據 2010 年中共《中國互聯網狀況白皮書》首度指出，維護網路安全，是保障國家安全與維護社會公共利益的必然要求；在中共境內的網際網路屬於國家主權管轄範圍內，應受到尊重和維護（中華人民共和國務院新聞辦公室 2010）。隨後於 2011 年 9 月，中共聯合俄羅斯、塔吉克、烏茲別克等四國，向聯合國大會提交《資訊安全國際行爲準則》，重申網際網路有關的公共政策的決策權屬於各國的主權，各國都擁有權利並承擔責任（Shanghai Cooperation Organization 2011）。由中共宣示網路主權的行爲，凸顯出數據資訊自由的傳播，對中共內部安全已造成極大的威脅。

不可諱言，在虛擬、自由的網路空間中，賦予政府合法監控網路用戶的數據資料權利，勢必會影響到現行網路空間秩序。尤其在個人資料安全，更將衝擊到歐洲人權公約所規定的言論自由。但隨著雲端技術、物聯網及移動通信 5G 的發展，數據資料已成爲戰略資源。因此，建構數據在地化的管理，強化以國家行爲者在自由、開放的網路空間監管職責，已成爲各國維護網路安全重要手段。

（二）網路主權之定義

雖然，網路空間是由網路用戶，透由國家境內的關鍵網路基礎設施，及美國主導的網際網路國際規範等建構而來。但隨著網路安全日益重要，影響網路空間的建構不再僅受限於網路科技，還須考量國家的安全與利益。

1. 西方學者

隨著網路空間擴及到政治、經濟、軍事等領域，確保國家境內的網路系統安全正常運作，已是政府部門重要職責。根據 2012 年德國法蘭克福大學的 Wolff Heintschel von Heinegg 教授表示，國家有權對國家境內的網路基礎設施和網路活動進行控制，及行使管轄權。同時，須保護位於領土主權範圍內的網路、通訊等基

礎設施，不受其他國家的干涉，凡對國家境內的網路基礎設施產生不利影響，將被視爲侵犯國家主權（Heinegg 2012）。另外，Mike Chapple（2014, 62）指出：網路空間主權爲一個國家領土內的網路基礎設施，該國政府應有管轄的權利，也包含網際網路頻寬流量。另外，值得注意的是，由於網路空間主權的形塑，不利於數據資料自由流動，也意味著將挑戰美國所主導的網路空間秩序。根據曾任美軍網路作戰行動部門的 Scott D. Applegate（2016, 191-192）表示，網路空間主權的形塑，如果沒有美國所主導的國際協議承認其權利，其所定義的主權效用是有限的。同時，網路空間的自然地理學不符合邏輯地理學，以美國系統的邏輯邊界爲例，美國軍方擁有超過 3,500 個地點的 88 個國家全球邏輯域，單純依靠實體邊界，將無法建立網路空間邊界。不僅如此，2013 年美國國防部發布的《網路空間作戰聯合條令》（cyberspace Operations）更指出：網路空間包含實體網路（physical network）、邏輯網路（logical network）及網路行爲體（Cyber-persona）三個層次；其中每一層都可以進行網路空間作戰（United States Department of Defense 2013, I2-3）。因此，從西方學者與美國軍方所認定的網路空間主權，即爲國家境內的實體空間中網路、資訊等關鍵基礎設施與數據資料等爲其政府管轄的對象。換句話說，網路空間主權的建構，有利於網路科技弱勢的國家，但卻不利於擁有網路科技優勢的美國。這也說明美國政府爲何始終反對網路空間主權建構的主因。

事實上，規範網路空間屬於政府管轄權的對象，在國際組織上已得到基本共識。根據 2013 年 6 月 24 日，聯合國《從國際安全的角度來看資訊和電信領域發展政府專家組》決議內容第 20 條指出：國家對在其領土內對資訊、通訊技術基礎設施具有管轄權（United NationsGeneral Assembly 2013, 8）。另外，2015 年 6 月，聯合國大會新的政府專家組，就規範、規則或者國家在網路領域責任以及建立信任措施，並建設可在全球範圍實施的國際合作達成了實質性共識報告（A/70/174）指出：「在使用資訊通信技術時，各國必須遵守其他原則中的國際法、國家主權，以和平手段解決紛爭，並且不干預其他國家的內部事務。」（United Nations General Assembly 2015, 7-10）因此，在資訊、通訊技術等關鍵基礎設施被視爲國家主權範疇後，意味著對未來處理國際網路安全爭議問題，網路主權概念將扮演極爲重要的角色。

2. **中國大陸學者**

中國學界普遍認爲：沒有網路安全，就沒有國家安全；並認爲網路攻擊不僅可以癱瘓敵國指揮中樞、經濟發展，運用網路宣傳將可顛覆他國政權，瓦解敵國民族意識。根據中共網路安全專家的惠志斌（2012, 19）表示：網路主權係爲國家對

本國的網路新聞傳播進行管理的權利。從政治立場來看，網路主權是國家允許或禁止資訊在其網路空間內流通的最高權威，包括平等共用網路空間資訊和傳播資源的權利。另外，從法律觀點來看，網路主權爲國家在網路空間擁有的自主權和獨立權，具體包括：國家境內的資訊輸出、入的管理權，及數據傳播的控制權。曾任中國外交部條法司司長的黃惠康在《網路問題布達佩斯國際會議》亦公開提出：「網路空間主權是國家主權在網路空間的自然延伸，應受到尊重和維護。」；其網路主權原則，應依據該國網路發展的能力，並考慮該國民衆的意願，借鑑國際法的基礎上，制定適當的網路政策與法律，依法管理網際網路。（中華人民共和國外交部 2012）由中共形塑網路主權的範圍，其管轄的對象著重於網民言論內容及媒體傳播管轄。在政治意識型態始終被中共視爲國家安全的核心利益，網路用戶自然成爲被管轄的重點目標。

除此之外，中國大陸學界也主張要維護國家境內網路安全，除強化網路用戶、媒體傳播的管轄權外，還須防禦外在的網路駭客，利用國家境內的網路代理伺服器實施網路攻擊。根據中國工程院院士方濱興（2017）表示，防禦網路任何攻擊，中國政府有權對境內網路資訊實施管理。然而，限於目前國際網際網路「功能變數名稱與 IP 分配與管理」，由美國獨霸操控影響，致無法獲得網路主權平等對待。另外，網路基礎設施，應成爲網路主權的有形邊界，而由美國主導的網際網路的協議，則由各自國家依區域負責管理的「頂層網域（Top Level Domain）」及註冊其下的功能變數名稱，形成網路主權的無形邊界。（馬民虎、張敏 2015, 95）不僅如此，2016 年楊海濤教授亦表示：網路代理伺服器、路由器和終端設備，均屬於中共網路主權管轄對象，無論是否在中國大陸的物理邊界上，入侵網路邊界應被視爲侵犯主權。（Yang and Zhang 2016, 84）。由中共形塑出的網路主權資料得知，其管轄對象除包含國家境內的資訊、通訊等關鍵基礎設施與資訊用戶、媒體等外，還包括了國家境內由美國主導的網路協議。換句話說，凡連接進入中共所建構的網路空間中，均爲管轄的對象，也意味著隨著中共的移動通信及國防武力的增長，其網路代理伺服器、或網路用戶等，可以部署至全世界各個地方後，其網路空間的疆界也隨之擴大。

3. **我國學者**

網際網路加速全球化經濟發展，維護網路安全已成爲各國政府極力維護的目標。根據 2012 年，我國梁德昭等研究表示，因應日益嚴重的網路安全威脅，解決國際間網路衝突有效的方案，將是以國土延伸之概念，在網路空間中發展出國家主權新的意涵。同時，界定網路邊疆，其國家境內的資訊主機與骨幹線路所構成的

實體平台，與網路中的各個節點連接分散於各處的資訊系統，應爲政府所管轄。（梁德昭、朱志平、林凱 2012, 9-10）。另外，網路主權爲國家控制本國網路空間的權力，只要在國家領土內的網際網路相關硬體、內容、服務等，該國政府都有充分管轄權力（傅文成 2016, 35-36）。除此之外，網路空間的虛擬疆域（virtual territoriality）概念，是可以用網路代理伺服器（proxy servers）存取權限，勾勒出虛擬邊界（virtual borders）進行劃分，並對網路空間的治理權，與實體疆界的國家行爲者有密不可分的關係（Hwang 2017, 97）。故國家境內資訊、通訊等關鍵基礎設施建構的網路空間，即爲政府部門的管轄對象。同時，網路代理伺服器存取權限，也應該成爲政府的管轄對象。

綜合網路主權論述，其共同點爲在國家境內中的資訊、通訊科技等關鍵基礎設施，如實體鏈路，所建構的網路空間，應受國家政府所管轄。而不同點，在於中共與我中華民國學者認爲，網路主權還包括國家境內所的虛擬網路空間，無論是物理層、或是使用者、網路代理伺服器。因此，宣告網路主權，意味著網路、資訊等關鍵基礎設施，將被視爲陸權架構上的資產，政府有權對其網路空間行使國家主權，其管轄的對象爲透由網際網路進入該國家的網路空間，即應受到該國政府的管轄。而管轄的範圍，隨著網路科技能力發展，也將擴及全球。（以「國家行爲者」形塑網路主權之管轄的對象、範圍如表 1）

表 1　網路主權之管轄的對象、範圍對照表

區分 / 類別	對象	範圍
美國	國家境內的網路、通訊等關鍵基礎設施、網路活動及數據流量。	實體疆界：由國家境內的網路、通訊等關鍵基礎設施，所建構而出的網路空間。
中共	國家境內的網路、通訊等關鍵基礎設施、網路活動及數據流量。 新增：資料使用者、營運商、傳播媒體及網路代理伺服器。	實體疆界：物理空間：國家境內的網路、通訊等關鍵基礎設施 虛擬疆界：隨著中共的移動通信及國防武力的增長，其網路代理伺服器、或網路用戶，將可部署至全世界各個地方，其網路空間的疆界隨之擴大。
中華民國	國家境內的網路、通訊等關鍵基礎設施、網路活動及數據流量及網路代理伺服器。	實體疆界：由國家境內的網路、通訊等關鍵基礎設施，所建構而出的網路空間。 虛擬疆界：網路代理伺服器（proxy servers）存取權限，勾勒出虛擬邊界。

資料來源：根據西方學者、中共及我中華民國學者整理而成，資料引自 Heinegg（2012）；惠志斌（2012）；Yang and Zhang（2016）、梁德昭、朱志平、林凱薰（2012）；Hwang（2017）。

二、網路主權對國家安全之影響

隨者資訊、通訊等科技基礎設施涵蓋至國家工業基礎設施、企業金融、軍事等領域，維護網路安全，已成爲確保國家安全重要議題。

（一）網路安全、網路戰爭與國際法之問題

網路空間已成爲網路駭客，或有組織的網路部隊，威脅他國網路安全，獲得勝利的最佳戰場。建構集體安全概念，參考國際法與武裝衝突法，已嚇阻他國約束網路行爲者，維護網路空間秩序。根據 2013 年版《塔林手冊》（Tallinn Manual）第一章第二節「國家責任」指出：國家對於歸屬其網路行動負有國際法責任，經由該國境內網路基礎設施所發動的網路攻擊，可將該國視爲攻擊嫌疑國，遭受到網路攻擊的國家可以採取適當的反制措施。另外，在第二章第二節有關於「自衛權」表示，遭受網路攻擊的國家可以行使自衛權（Schmitt 2013）。另外，《塔林手冊》中的網路戰交戰規則，制約了位居劣勢的國家運用網路科技，發揮不對稱作戰的優勢，進而擾亂國際網路秩序的影響力（朱莉欣 2014,135）。不僅如此，《塔林手冊》的編纂，制定了網路空間國際治理的規則，提供網路戰法理反擊的依據（何駿、趙立軍、王鵬 2017, 9）。故在《塔林手冊》出版後，國家主權在網路空間的行爲準則得到一個國際規範的重要參考文件。

不可諱言，網路空間尚是個無政府狀態，在無法釐清網路攻擊行爲，《塔林手冊》將無法約束網路空間行爲，而實施網路反擊也將違反國際法。根據曾任美國國防情報局、北約《網路防衛卓越中心》（NATO Cooperative Cyber Defence Centre of Excellence，CCDCOE）網路安全講師的 Jeffrey Carr（2012, 33-34）表示，由於程式代碼無法區分用於和平或是惡意，所以無法用條約來約束其網路行爲。同時，網路空間具有去中間化的特質，如 2011 年北韓網路駭客，通過虛擬私人網路（Virtual Private Network，VPN：俗稱翻牆軟體），連接分布全球網域伺服器之部署英國伺服器，進而攻擊美國政府網站（Carr2012,33-34）。另外，美國學者 Catherine A. Theohary 更指出，《塔林手冊》第五條的規定：成員國遭網路攻擊時，同盟國可以提供軍事援助，將觸發聯合國憲章第 51 條規定的國家自衛權。另外《塔林手冊》第四條：該條文適用集體安全，以保護成員國安全和領土完整，但無法清楚定義網路攻擊者的動機及歸屬原則，如政治上的網路恐怖攻擊或是以財務上的網路竊取等，將使該條文無法適用。（Theohary and Rollins 2015, 4-5）故若無法明確定義網路攻擊是軍事行動，及網路攻擊者身處何地主權問題，與遭網路攻擊反擊使

用比例，其《塔林手冊》的合法性與實用性，將遭受到質疑。

（二）網路空間衝擊國家安全

自由、開放的網際網路，已威脅到國家整體安全。自 2015 年 12 月以來，烏克蘭的電力中斷是由於網路攻擊所造成，其關鍵基礎設施電力設施遭網路攻擊已不再是假設性問題。同時，該病毒造成電網停電或物理損壞電網設備，對美國電網的網絡攻擊可能導致總的經濟損失從 2430 億美元到 1 萬億美元（Douris 2017）。事實上，根據 2013 年 Thomas Rid（2013, 79）表示：由於網路攻擊的行爲都是非暴力的，既不傷害機器，也不傷害人；其影響範圍，除對工業控制系統造成物理危害外，最重要的將破壞消費者對公司和政府產品和服務的信心。另外值得注意的是，2018 年美國約翰霍普金斯大學高級國際研究學院（SAIS）的兼職教授 Seth G. Jones（2018）指出，未來戰爭將朝向政治戰爭發展；其軍事手段將運用、情報、公共廣播和心理戰等行動，以實現國家目標。如俄羅斯利用攻擊性網路計劃，隱蔽其行動。然後，再利用歐洲和跨大西洋的裂縫，破壞歐盟和北約的凝聚力。因此，網路攻擊武器市場化的發展，其威脅已不亞於實體空間的破壞，並對國家主權產生衝擊。換句話說，無法確保網路安全，將會對國家建設與發展造成損害，且會危及國家的主權與安全。因此，形塑網路主權的概念，將是以國家行爲者須去面對與聲索的新型主權。

三、網路主權未來發展

無法管轄數據資料的傳遞，就沒有網路安全。根據 2015 年美國網路政策倡議（Cyber Policy Initiative）組織的聯合主席 Tim Maurer（2015, 63-64）表示，隨著中國政府禁止使用 Windows 8 操作系統、澳大利亞政府禁止中國的華爲參與國家的建設寬帶網路，及美國國會 2013 年設立網路間諜審查程序限制政府中國 IT 設備的採購等，技術主權已成爲資料在地化的重要議題。另外，由於網路空間是由成千上萬台電腦、網路伺服器等組成，爲保護網路空間中的數據安全，政府部門須從戰略、法規和政策面制定相關作法，以確保網路安全（Setiawan, Syamsudin and Sasongko 2015）。不僅如此，隨著網際網路所帶來的安全問題，目前全球已有近 60 個國家發布網路安全戰略，在網路空間的軍事化進程中，已間接促成對網路主權概念的承認。同時，還有 50 多個國家頒布資訊安全保護法律，促成國家主權在網路空間地位的提升（崔文波 2017,8-9）。除此之外，爲確保虛擬化的雲端環境數據完整及安全，以往靠網路防火牆和網路漏洞掃描程序的外層防衛手段，已無法防

範應用程序級攻擊，政府、企業應運用雲端技術監控個人活動，掌握攻擊者身分，從而減輕潛在的損害（Astani 2016, 208-210）。另外值得注意的是，絕對的網路自由將爲網路安全帶隱患，爲提高網路空間的安全性，除須強化資訊和系統的安全性外，公民也必須放棄一些網路自由（Tasheva 2017）。因此，資料在地化的管理，已成爲全球確保網路安全的新趨勢，也意味著未來的網路空間，將不是自由、開放，取而代之的是監督與管理。

參、中共宣告網路主權背景與目的

網路空間已擴及至政治、經濟及軍事等領域中，誰奪取網路空間的制高點，誰就擁有網路空間的主導權。

一、中共宣告網路主權之背景

（一）政治環境

隨著網路科技的進步，網際網路已消弭政府掌握資訊傳播的優勢地位。同時，跨國境的數據資料，使得國家主權的疆界變得模糊。根據 2013 年 8 月 19 日中共國家主席習近平主持「全國宣傳思想工作會議」時表示：網際網路已成爲輿論鬥爭的主戰場；網路空間搞不好，將會成爲心頭之患（中國數字時代 2013）。另外，2014 年 9 月 27 日香港暴發「佔中」事件，駭客組織對香港律政司、警務處和香港電台、無線電視等媒體共 31 個網站，實施阻斷式網路服務攻擊或網頁篡改。同時，煽動民眾與政府作對，中共當局應納入警惕（洪京一 2015, 14-15）。因此，網際網路成爲民眾直接參與政治平台後，其網路空間權力的個體化，將影響到國家、社會與個人的權力結構。換句話說，自由的網路空間，已威脅中共執政的正當性，也意味著無法管轄網路空間言論，將無法確保國家內部安全。

（二）經濟環境

沒有自主的網路科技，就無法確保數據資料安全。根據 2014 年曹如中指出，自 20 世紀 90 年代以來，中共在政治、經濟、軍事等領域遭西方各國滲透。尤其 2013 年史諾登「稜鏡計劃」（PRISM）和 2014 年微軟 XP 停擺事件，凸顯出中共網路安全受制於人的困境（曹如中、曾瑜、郭華 2014, 15-16）。此外，2014 年用以數據資料交換的網路代理伺服器，在中共境內至少有 3 萬台伺服器存有程式密鑰

安全漏洞（Heartbleed bug）①；其影響對象爲微信、淘寶等社交網站等。同時，在中共境內仍有 30% 網路廠商，未能針對心血安全漏洞程式，強化網路安全防護措施（裴毅東 2014）。不僅如此，隨著雲端資料庫、大數據、物聯網等網路科技的整合，網路雲端存儲資料已成爲網路駭客極易攻擊的對象，爲中共網路安全管理體系帶來巨大的挑戰（洪京一 2015, 17-18）。故在面臨網路科技落後，且民間企業與民衆對網路安全防護觀念淡薄，自由、開放的網路空間，已威脅到中共推動數位經濟發展。

（三）軍事環境

誰奪取網路空間的制高點，誰就取得戰場上的主動權。2013 年，中共境內政府網站遭篡改數量爲 2340 個，相較於 2012 年增長 34.9%，且在境內被植入後門程序的政府網站爲 2425 個；其重要機敏資訊外洩，已威脅到中共整體國家安全（洪京一 2015, 109）。另外，根據 2014 年中共互聯網新聞研究中心所出版的《美國是如何監視中國的—美國全球監聽行動紀錄》更指出，中共遭美國國安局網路監控；其對象包含中共境內的清華大學的主幹網路、電訊公司 Pacnet 在香港總部的網路機房，甚至連個人使用的騰訊聯天軟體和中國移動的即時通訊工具，都在美國國安局 NSA 的監控範圍（互聯網新聞研究中心編著 2014, 15-19）。除此之外，自 2013 年美國史諾登揭露美國國安部門監控中國大陸網路行爲後，中共網路空間採取更爲緊縮政策，以確保國家境內的網路數據資料安全。同時，並加強網路科技發展能力，逐步提高軍事能力，如利用網路攻擊中斷美國常規部隊指揮與管制（Austin 2015, 168）。由中共遭美國入侵的網路行爲，凸顯出網路科技落後，將無法確保境內網路安全。換言之，形塑網路主權，合法賦予中國政府具有管轄國家境內的數據權利，對維護網路安全，至關重要。

總而言之，宣告網路空間主權對中共的必要性，首先於自由、開放網路空間所驅使的政治民主化，已對中國共產黨的威權統治產生衝擊；其次，網路科技落後，且中國大陸網路用戶對網路安全防護觀念淡薄，不利於國家推動數位經濟發展。最後，由中共遭網路安全威脅的程度，凸顯出其網路空間防護的薄弱，其網路空間的權力真空，已威脅到中共的國防武力的發展。換句話說，中共所呼籲各國彼此尊重各自的網路主權，其實就在解決中共境內的網路輿論內政問題，各國應相互不干

註① 美國谷歌安全部門及芬蘭網路安全公司科諾康，發現原用以保護網路伺服器中的程式密鑰中存有心血的安全漏洞（Heartbleed bug）；該漏洞影響會使電子支付、電子郵件等網站的用戶敏感數據面臨遭竊取的風險。同時，還威脅到網路伺服器、路由器和無線電分享器等網路設備。

涉。同時，強化政府部門對虛擬經濟的管轄權，將是中共維護經濟發展的重要手段。此外，形塑網路空間主權，也意味著向世界宣告中國國防武力的立場，是禁止運用網路駭客行爲，破壞他國網路安全，以防止他國藉機挑釁，引發網路衝突。

二、中共宣告網路主權之目的

承上所述，網路安全已威脅到中共維護國家主權、安全及利益。爲實現中國夢、強軍夢，須建構安全網路空間秩序。

（一）增加政治影響力

主權意味著以國家行爲者，在其境內具有最高的統治權。根據 2016 年底，《國家網路空間安全戰略》指出，網路空間已成爲國家主權的新疆域，確保在自由、開放的網路空間中維護國家主權、安全與發展利益，實現網路強國的戰略目標。同時，參與國際網路空間規則制定，形塑負責任的大國形象（中國互聯網路信息中心 2017）。另外，在網路空間中，中國政府所追求的是一個和諧的理想秩序。同時，更強調遵守秩序的重要性，及個人中立與社會穩定（林幼嵐 2016, 57）。同年，由北約「網路防衛中心」所出版的一份報告《中國和網路：態度、戰略、組織》（China and Cyber: Attitude, Strategies, Organisations）表示，在中國政治文化中，維護社會秩序比網路空間維護個人隱私更爲重要，舉凡在中共境內的國內、外網路用戶，應受其本國國家所管制（Raud 2016, 8-9）。因此，形塑網路主權，其政治目的，透由建構網路空間的新秩序，形塑中共的國際形像，將有利於提升國際政治的影響力。

（二）提升數位經濟競爭力

隨著數位經濟的整合，網路主權的建構，有利於網路科技自主化的發展，提升市場占有率。根據 2015 年 10 月 29 日《中國共產黨第十八屆中央委員會第五次全體會議公報》指出，爲實現網路強國戰略目標，須推動「互聯網 +」行動計畫（中華人民共和國工業和資訊化部 2015）。隔年《中華人民共和國國民經濟和社會發展第十三個五年規劃綱要》第六篇拓展網路經濟空間更指出：『加快建立網路空間應用的基礎共性標準，和關鍵技術標準研製推廣，將增強國際標準制定中的話語權。』（新華網 2016）。根據 2016 年魏亮、魏薇研究證實，中共扶植的網路科技公司，如華爲、阿里巴巴、騰訊等，其市場占有率已較以往增加。同時，已對國際市場造成影響力（魏亮、魏薇等 2016, 19）。事實上，曾任《史蒂文斯理工學院》

Jennifer L. Bayuk 教授表示：中共的網路安全政策，允許該政府對網路空間進行隔離、監控，其主要目的之一，就是爲維護其經濟發展利益（Bayuk et al.2012,7-8）。因此，建構網路主權，其經濟目的，將有助扶植其國內網路科技產業的競爭力，推動數位經濟整合。

（三）強化不對稱作戰優勢

誰擁有網路空間的制高點，誰就擁有主導戰場的主動權。根據 2013 年中共國務院所發表《中國武裝力量的多樣化運用》指出，要打贏資訊化條件下的局部戰爭；其中，就必須搶占網路空間的制高點（中華人民共和國國務院新聞辦公室 2013）。2015 年《中國的軍事戰略》更指出：加快網路空間力量建設，提高網路偵察、防禦、支援，以確保國家安全和社會發展（中華人民共和國國務院新聞辦公室 2015）。另外，中國政府的網路戰略目標，除避免虛擬天安門事件發生外。同時，還爲打贏數位化的全球化戰爭做好準備（林幼嵐 2016, 62-63）。此外，中共解放軍的網路部隊，編制於前中共解放軍前總參謀部第三和第四部門網路作戰部門，即說明中國政府企圖依靠網路戰力，以建構出不對稱作戰優勢，實現地區霸權地位（Domingo 2016）。故在國際上有關網路戰尚未清楚定義前，形塑網路主權，其軍事目的有利於中共監控數據流動，提升網路防禦能力，及形塑網路部隊反擊的正當性。

總之，中共形塑網路主權的目的，政治上，對內透過網路審查，以維護內部政治意態管理；對外，建構網路空間新秩序，提升政治層面的影響力。經濟上，扶植國內網路科技產業站穩市場，強化國際競爭力。軍事上，透由《網絡安全法》，要求進入中共國內、外網路營運商，須在中共境內設置數據中心，並繳出程式原始碼，消弭因使用他國研發作業系統，遭植入電腦病毒風險，並增加網路戰威懾能力。簡言之，中共宣告網路主權，其目的在於建構一個能符合中共爲核心利益的網路空間，並以支持推動「一帶一路」的數位經濟整合，實施中國夢、強軍夢的戰略目標。

肆、評估中共建構網路空間疆界化之範圍

在自由、開放的網路空間中，要建構網路空間疆界化（territorialization）；其考量因素，內部在於行政部門編組職能及網路科技實力；外部須考量到美國主導的現行網路空間管理秩序。

一、遂行網路空間安全之部門編組

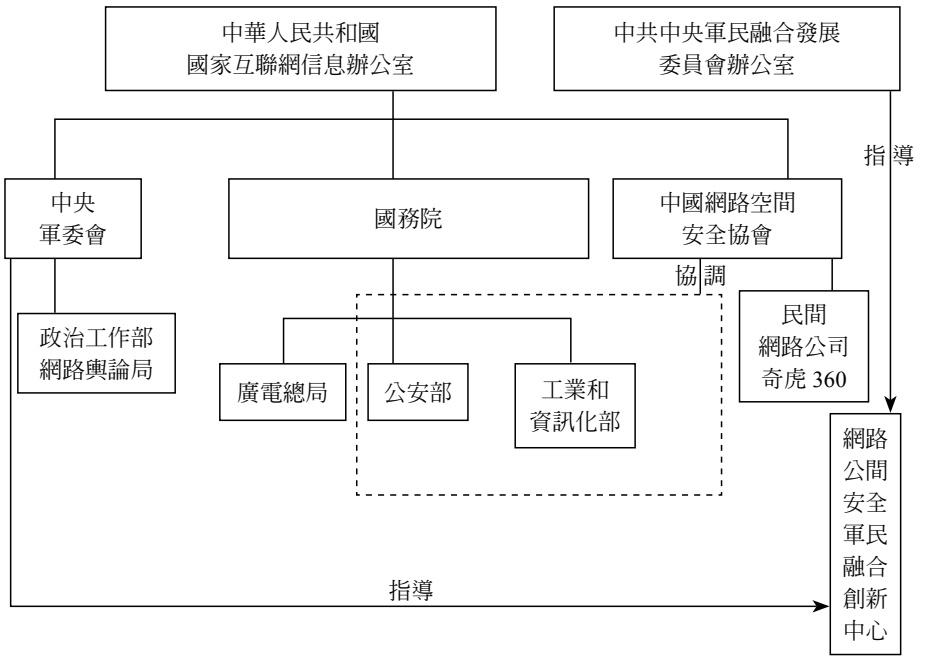
要強化網路安全防禦，在組織上就須建立在統一領導、各司其職的部門。隨著網路空間影響層面擴大，要確保數據資料的安全，須將分散於網路偵察、追蹤、處理、應變等部門實施整合。2014 年 2 月 27 日中共成立「中央網絡安全和資訊化領導小組」，並由國家主席習近平擔任小組長。該部門負責統籌協調各個領域的網路安全和資訊化重大問題（新華網 2014）。另外，中華人民共和國國家互聯網信辦公室，統籌下轄的工業和資訊化部（協調司）、公安部（網路安全保衛局）。（惠志斌、譚慶玲 2016）。此外，2017 年美國蘋果電腦公司所出售的 iBooks 商店，遭中共的國家新聞出版廣播電影電視總局要求關閉（Mozur and Perlez 2016）。不僅如此，中共解放軍爲強化內部網路安全，於 2017 年 11 月 19 日，由中央軍委「政治工作部」下轄之網路輿論局，成立「中國軍網舉報平臺」；其任務爲審查篡改軍事新聞標題、發布有害軍中資訊和低俗資訊、洩露軍事秘密、攻擊黨對軍隊絕對領導、暴露軍人身分等內容（李景璿、陳泰偉 2017）。

不僅如此，隨著中共網路人口數量的增加，爲強化動員社會力量，參與維護網路安全。2016 年 3 月 26 日中共成立首個「中國網路空間安全協會」；其組織包括民政部、工信部、公安部相關負責人及中國互聯網協會、奇虎 360、安天科技等單位（中國互聯網路信息中心 2017）。另外，2017 年 12 月底，中共中央「軍民融合發展委員會辦公室」和解放軍相關部門共同指導，民間網路公司奇虎 360 成立「網路空間安全軍民融合創新中心」。該中心的成立，爲落實網路強軍戰略之目標（張新、楊利程 2017）。因此，維護中共的網路空間安全部門，由「中央網絡安全和資訊化領導小組」統籌領導，中共解放軍及國務院下轄的工業和資訊化部（協調司）、公安部（網路安全保衛局）及國家新聞出版廣播電影電視總局，與民間「中國網路空間安全協會」。換句話說，中共的網路主權政策，在中國國家互聯網信辦公室統合，已成爲中共各部門的核心工作。其網路空間的疆界，也在各部門執行中建構出來（中共建構網路空間疆界編組圖，如圖 1）。

二、網路空間疆界之管轄能力

由於網路空間是網路用戶，透由國家境內的資訊關鍵基礎設施，及網路協議所建構而成。故要評估網路空間疆界建構的範圍，其對象是否能在政府管轄內。

圖 1 中共建構網路空間疆界編組圖



資料來源：根據中共官方「互聯網網路信息辦公室」、解放軍報及學者整理而成，資料引自惠志彬（2013）；中華人民共和國國家互聯網網路信息辦公室（2016）；張新、楊利程（2017）；李景璿、陳泰偉（2017）。

（一）網路用戶之管轄權

無法管轄數據資料的流動，即無法確保國家網路安全。根據 2016 年《中華人民共程國網絡安全法》第一條指出，『爲了保障網絡安全，維護網絡空間主權和國家安全、社會公共利益，保護公民、法人和其他組織的合法權益，促進經濟社會信息化健康發展，制定本法。』（中國人大網 2016）。隔年 1 月，中華人民共和國工業和資訊化部頒布的《工業和資訊化部關於清理規範互聯網網路接入服務市場的通知》，要求中國移動、中國聯通、中國電信等國營電信公司，嚴禁個人用戶申請 VPN 使用；而中共境內的企業須註冊相關服務，才可以租用專線連結到國際網路（中央社通訊社 2017）。不僅如此，2017 年 8 月 25 日中國網信辦公室頒布《互聯網跟帖評論服務管理規定》，要求在中共境內所有網路用戶，須按照「後臺實名、前臺自願」原則實施申請帳號。同時，網路營運商不得未經認證眞實身分提供

網路服務（中華人民共和國國家網信辦公室 2017）。由網路用戶與營運商受到更嚴密的審查行爲，意味著網路疆界將被勾勒出來。

然而，回顧歷史，中共爲強化內部網路安全，早已設立一套監控系統。中共自行研發的「中國國家防火牆」、或稱「防火長城」（Great Firewall，GFW），可以透由系統自動過濾不利於政府的言論。同時，還可以阻斷連結某些 IP，如臉書（Facebook）、影音共享網站（YouTube）與推特（Twitter）（過子庸 2011, 100）。此外，中國政府還曾以網路安全爲由，威迫外商網路公司交出可讓政府監控網民的原始碼，例如微軟。（呂晶華、成高帥譯 2011, 43-44）。不僅如此，2017 年 5 月，俄羅斯禁用與中國共產黨關係密切的騰訊公司研發的網路社群軟體—微信（WeChat）（高紫檀 2017）。同年 11 月底，印度亦要求駐紮在印「中」部隊，其智慧型手機中安裝微信（WeChat）、微博（weibo）等應用軟體刪除；其原因爲中共所研發之軟體，極可能已安裝間諜軟體或其他惡意程式（Pubby 2017）。

因此，中共爲強化境內用戶的數據資料流動，早已建置一套政府對人民的數據資料的監控權。但在 2016《網絡安全法》頒布後，將提供中國政府對境內的用戶進行查核及封鎖個人上網自由更多的管轄權。同時，該法還要求，無論國內、外等網路科技公司，凡進入中共市場，須主動程式原始碼及建設數據中心。換句話說，中共所形塑的網路主權，其管轄的對象已擴及到國家疆界之外，也意味著中共情報機構，可運用網路公司所提供的程式原始碼，監控凡使用中國民間研發網路設備的使用人，而無論其用戶是否在其國家境內。

（二）國家境內關鍵網路安全防護

要防範網路攻擊，就須確保國家境內的資訊、通訊等關鍵基礎設施，免遭網路攻擊行爲破壞。中共的網路空間結構區分爲核心層和大區層。核心層由北京、上海、廣州、瀋陽、南京、武漢、成都、西安等 8 個城市的核心節點組成，其功能爲連接國際網際網路，作爲大區層間的網路交換。他們之間爲不完全網狀結構，其中北京、上海、廣州核心層節點各設有國際出口網路代理伺服器，負責與國際網路連接。大區層爲中國政府境內 31 個省會城市依照核心層，構成 8 個大區網路，大區層網路提供大區內的資訊交換及中國內部網路 chinanet 的通路（惠志斌、譚慶玲 2016, 14）。此外，爲避免網路空間遭他國監控，規劃於 2030 年前，針對北京至上海核心層間的骨幹鏈路，部署總長共計 2000 公里的量子保密通信骨幹網路（洪京一 2015, 68-69）。另外，量子保密通信骨幹網路「京滬幹線」（712 公里），已於 2016 年 11 月 21 日從合肥至上海段開通，爲長江三角地區的金融、政務等行業

提供安全通信服務（徐海濤 2016）。因此，透過部署內、外分明的網路代理伺服器（國際出口：北京、上海、廣州），及量子保密通信骨幹網路等，中共的網路空間疆界，已比照陸權架構形塑出來。

除此之外，2015 年中國首款自主研發的防火牆（HT706-2000 型千兆），已由中國航天科工二院 706 所研發成功，並由軍方資訊安全測評完成認證；該裝備將部署於企業內部網路和公共網路間，提供隔離與訪問控制，已確保中共內部網路安全（中國國防科技信息中心 2015）。另外，根據 2016《網絡安全法》指出，政府應主動採取手段，監察來自國內、外的網路安全威脅，以保護國家境內的關鍵資訊、通訊設施，維護網路空間安全和秩序（中國人大網 2016）。除此之外，根據 2018 年蘭德公司的報告指出：中共網路空間的資訊操作系統，已成爲一個內部局部網路，與世界網際網路隔離；其能力預估已可防止網路空間邊界遭突破，包括防病毒攻擊能力，反駭客攻擊能力，及網路緊急處理恢復（Jeffrey Engstrom 2018, 115-116）。因此，在《網絡安全法》及網路科技提升，已使中共境內形成與全球網路形成區隔的內部網路。

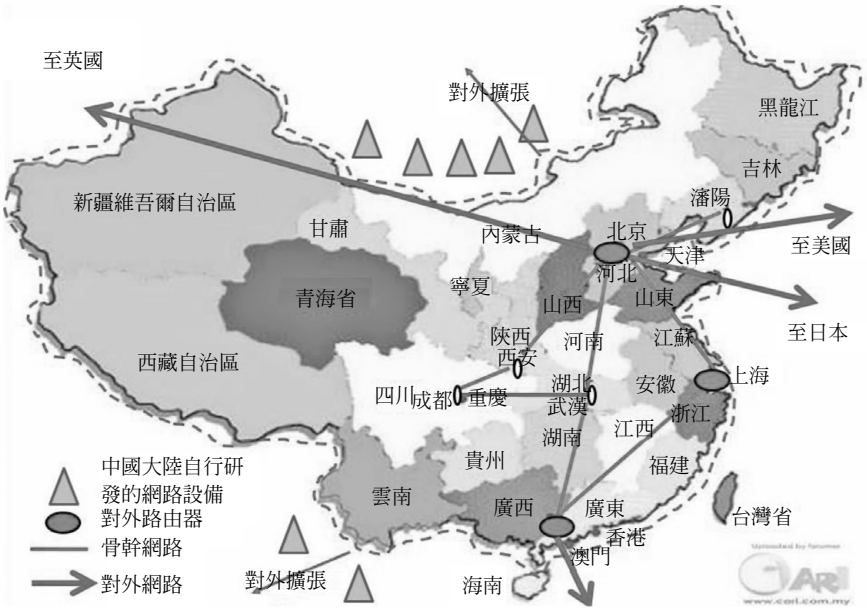
（三）網路協議

無邊疆的網路空間，誰擁有主導網路協議制定、技術優勢的國家，誰就奪佔網路空間制高。根據 2017 年 11 月 26 日，中共中央辦公廳、國務院辦公廳所頒布的《推進互聯網協議第六版（IPv6）規模部署行動計畫》指出，在中共省部級以上政府和中央企業網網站系統，及中共國家境內用戶量排名前 50 位的商業網站及應用系統，於 2018 年底全面更換爲中共所制定的 IPv6 協議，並於 2025 年底前，全國完成 IPv6 的普面更換（中華人民共和國工業和資訊化部 2017）。故由中共積極發展出的 IPv6 的網路協議，將使中共境內能連接上網的每一個資訊設備都有 IP 位置，也意味著中共境內有別於世界網路協議，將使中國政府可以更加掌握、追縱數據資料。

總體來說，中共形塑網路主權的概念，在其政策及網路科技的支持下，中共的網路空間疆界已被勾勒出來。尤其自 2016 年《網路安全法》頒布後，已使中國政府可以對國家境內的網路營運商，要求繳出商品之原始碼，並配合自行研發的防火長城，將對網路用戶實施更嚴密的監控。同時，在國家主導通信保密量子技術的骨幹鏈路及網路協議 IPv6，將可建構出防範敵國對中共網路空間攻擊的屏障。換言之，中共形塑的網路主權，其網路空間疆界的基準點，將區分爲實體疆界的國家境內的資訊、通訊等關鍵基礎。另外，虛擬邊疆，隨國防武力與他國使用中共民間網

路科技所研發的系統，也隨之擴大（中共形塑網路主權之網路空間疆界示意圖，如圖 2）

圖 2　中共形塑網路主權之網路空間疆界示意圖



資料來源：作者自行整理。

三、中共建構網路空間之挑戰

中共宣告網路主權將挑戰到美國推廣民主、自由普世價值的網路戰略目標。

（一）自由、民主是美國影響世界的軟實力

民主和平論始終爲美國維持國際體系最好的論述。運用網路社群媒體傳播，獲取國內民眾支持，提升國際輿論的影響力，已成以國家行爲者運用網路影響他國的發展趨勢。2010 年 1 月，曾任美國國務卿的希拉蕊（Hillary Clinton）公開表示，美國將盡全力捍衛網際網路的自由。同時，鼓勵各國對全球公共網域的尊重，各國政府不應阻礙人民使用網路、訪問網站的自由（Thierer 2010）。另外值得一提，2018 年 1 月 6 日美國副國務卿 Steve Goldstein 就公開表示，針對伊朗爲阻止反政

府活動，切斷國內網路通訊、及封鎖廣泛使用的 Instagram 等社交媒體網站，美國不會袖手旁觀（Fears 2018）。此外，中共倡議網路主權，最大的困難和挑戰，來自於單邊主義和強權政治及國際網路空間的霸權主義（王春暉 2016, 14）。故中共宣告網路主權，企圖建構出與世界隔離的網路空間，已衝擊到美國運用民主、自由形塑國際和平。換句話說，中共要形塑網路主權，第一個挑戰，將是維護大國國際聲譽，以避免陷入西方國家所認爲的「中國威脅論」。

（二）侵犯美國網路空間的商業利益

隨著全球化經濟發展，自由、開放的網路空間，將帶全球便利的經貿發展；反之，單方面的形塑出的網路疆界，將不利於經貿交流。2013 年，Kris E. Barcomb（2013）表示，美國應強化網路空間在作業系統、搜尋引擎、通信裝備基礎設施、雲端運算、治理論壇、密碼體系及網際網路路由協定等七大戰略要點建設，以維護美國政府、企業及個人的網路安全。同時，透由七個網路空間的戰略要點的優勢，以促進美國私營企業在網路空間的增長及強化美國在網路空間的影響力。另外值得注意的是，中共有系統的補助其網路、電信產業和私營設備供應商發展；其目的爲提升經濟發展與政治影響力，如 2009 年的 Facebook、Twitter 被禁止進入中共市場爲例，時間點比新浪微博推出的時間稍早一點（林幼嵐 2016, 60）。因此，強佔網路空間優勢，已成爲中、美兩國必爭的戰略目標。然而，中共所形塑出網路主權，已造成國外營運商進入中共市場的成本，此舉已衝擊美國私營企業利益。故第二個挑戰，將是中共網路科技競爭力不及美國，且美國基於自身利益，勢必將會有所反擊，如 2018 年美國限制中共民營通信公司，如華爲，此舉將不利於中共網路商品行銷至世界各國。

（三）衝擊到美國國防戰略目標與安全

由於網際網路的創建，始於美國國防部爲強化指揮、管制鏈路演變而來。故奪佔網路空間的制高點，始終是美國國家利益最優先選擇的戰略目標。根據 2011 年，美國白宮首度出版的《網路空間國際戰略》指出，美國將繼續保持網路空間因開放性與自由行動性，所帶給全球的益處。同時，反對任何國家試圖將網路空間變成一個分離的國家內部網路（The White House 2011）。不僅如此，據 2017 年，Susan Shirk（2017）研究建議，美國在網路空間政策上應繼續與亞洲盟友保持密切關係。同時，對中共採取強硬姿態，以捍衛美國網路空間自身利益。因此，中共自行所建構出的網路空間疆界，就軍事層面，已阻礙美國爲確保自身安全與利益，可監控全球的戰略企圖。故第三個挑戰，爲中共的網路空間防禦體系，在網路科技無

法超越美國，與網路部隊無法捍衛疆界，美國網路部隊可依照戰略企圖自由行動。

另外值得注意的是，要捍衛網路空間安全與利益，仍須要有國防武力的網路部隊。要確保政府部門與商業間網路空間不受侵害，政府部門應建構出網路部隊，使其資訊能在於實體網路中形成隔離（Andress and winterfeld 2014, 35-36）。此外，根據 2015 年美國國會報告指出，雖然《塔林手冊》已規範出網路戰交戰規則，適用於國際法與武裝衝突法的事項。但在網路科技無法辨識網路攻擊者的身分，及可能來自個人的宗教狂熱或經濟的動機，或是以國家行爲者所策定的網路攻擊爲軍事行爲前提下，《塔林手冊》僅能提供規範網路戰的交戰規則，而無法約束國際上網路行爲（Theohary and Rollins 2015, 5）。因此，中共網路科技及網路部隊實力不及美國，所建構的網路空間國防長城，將無法達成網路嚇阻戰略。

整體來說，美、中兩國在網路主權的共同點，均以維護國家自身安全與利益爲出發點。但不同之處，在於美國所主張的網路自由論，是透由自由、開放的全球網路空間，將其民主、自由價值推廣於全球，進而影響國際體系。同時，在網路科技優勢支持，爲其民間網路科技企業帶來更多利益。此外，美國國安部門，利用網路科技優勢，進而監控全球重要情資，以確保國家利益與安全。然而，在中共所建構的網路空間疆界，雖然網路科技無法與美國抗衡，但在國家主導網路政策，及軍、民科技共同發展，且擁有龐大的網路人口約爲 7.31 億（全球網路人口數最大），已使中共網路空間隔離於世界網際網路之中（中共與美國建構網路主權分析表，如表 2）。

表 2　中共與美國建構網路主權分析表

區分 / 項目	中共	美國政府
政策立場	網路主權論	網路空間自由論
目的	打破網路空間現行秩序。 維護中國政府網路空間利益與安全，以建構屬於中國政府可以管理的網路空間。	維持網路空間現行秩序。 維護美國網路空間利益與安全，以建構屬於美國可主導的網路空間。
對象	不論是網路空間之物理層，如關鍵基礎設施、網路協定，或是企業的資料庫，及個人數據資料（社群媒體個人網路言論），均爲管轄對象。（針對網路內容傳播實施審查、刪除）	網路空間物理層爲管轄範圍。而個人的數據資料，須經由法院同意後，始可監控（但不實施內容審查）。 另外，以嚇阻網路反恐主義，可監控全球用戶資料。

區分 / 項目	中共	美國政府
作法	宣告網路主權。 呼籲各國彼此間能相互尊重網路空間文化；透由國際合作方式，將國家主權延伸至網路空間。	呼籲網路空間自由論。主導國際合作，隨著美國兵力投射的擴張，將國家主權延伸網路空間。
技術	發展網路科技自主。	網路科技出口於全球。
網路協定	中共於 2025 年於國家境內完成 IPv6 推廣協議。	由美國掌握分配網路資源。

資料來源：作者自行調製。

伍、個案探討—以美國蘋果爲例

2016 年底中國政府頒布《網絡安全法》後，蘋果電腦依法繳出商品之原始碼，並於其境內設置數據中心，以利中國政府部門監控數據流動。基此，透由蘋果電腦在中共發展個案，以實證網路主權之意涵。

一、個案說明

隨著網路社群媒體對國家政權穩定產生衝擊，維護政治意識形態的安全，已由網路延伸至個人使用的通信手機。2016 年 2 月 23 日，美國蘋果公司首度被迫將商品共享源代碼之原始碼，交給中共網路監管機構實施檢查（Benner and Mozur 2016）。同年，4 月下旬，美國蘋果的 iBooks 商店和 iTunes 電影服務，在中共上市僅半年後便被關停（Sewell 2016）。隔年 4 月中共北京的美國蘋果公司，遭中共的國家互聯網信息辦公室、公安局以及一個文化法規執法隊約談，隨即下架了《紐約時報》開發的新聞應用（Carlos 2017）。不僅如此，同年 7 月，蘋果公司在中國貴州省，投資 10 億美元設置首個海外的數據中心。蘋果公司亦表示：在中共增設數據中心，不僅讓蘋果電腦符合《網絡安全法》，也可提高蘋果電腦產品服務速度和可靠性（Mozur and Benner 2015）。由美國蘋果電腦依《網絡安全法》，被迫繳出商品程式之原始碼及設置數據中心，意味著中共網路主權，已如同國家主權在網路空間得以延伸，數據在地化已在中共境內被落實管理。

二、分析

（一）管轄權

網路空間的管轄權，爲政府對其國家境內的數據資訊有權合法的管理。2017 年 7 月，蘋果公司投資 10 億美元，在貴州省建設 iCloud 數據中心（Ghosh 2017）。即符合中共 2016 年底《網安法》第三十七條：關鍵資訊基礎設施的運營者在中華人民共和國境內運營中收集和產生的個人資訊和重要資料應當在境內存儲（中國人大網 2016）。另外值得注意的是，原蘋果智慧型手機在中國象徵財富和時尚，但隨中國年輕的中產階層消費者越來越願意嘗試華爲、小米等手機；其主要原因爲 2014 年末蘋果公司推出的 6S 與之前款式無太大差異，且華爲旗艦機型搭載的相機，據中共市場評估比蘋果公司研發更好（Mozurand Benner 2015）。因此，蘋果電腦面臨著中共市場競爭壓力及《網絡安全法》規定，但爲了穩固中共的市場，蘋果電腦不顧違反人權隱私，選擇繳出商品之原始碼，供中共官方監控數據資料。換句話說，中共所形塑的網路主權，其數據管轄權將從消極管理的模式，朝向積極管理的模式，網路空間疆界已被形塑出來。

（二）平等權

網路科技的發展，已成爲影響該國商業競爭的主要因素。由網路科技長久以來爲美國所操控，網路科技的不平等，已讓中共網路空間受到威脅。同時，中共逼使蘋果電腦，要進入該國市場須與地方政府、企業合作，此舉意味著中國宣告網路主權即爲保護其經濟利益（Limbgao 2016）。此外，《網絡安全法》其主要目的之一爲阻礙外國公司在中共境內的競爭力（Zhao 2016）。事實上，中共「互聯網 +」行動計畫，爲推動網路技術發展，實施創新驅動和網路強國的戰略意義，並在全球綜合國力的競爭力立於不敗之地（郎平 2016, 62）。因此，中共形塑網路主權，即爲打破長久以來，網路科技市場受限美國大企業的限制。同時，扶植國內網路科技競爭力。換言之，中共形塑網路主權，將實現其商業發展平等權。

（三）捍衛權

無法捍衛網路主權，即無法確保國家安全；無法監控他國對本國網路空間的監控權，也將無法維護其網路安全與利益。中共爲保障中共用戶人之數據安全，要求蘋果電腦在中共境內銷售產品，須繳出商品之原始碼；其原因爲智慧型手機能夠跟蹤用戶位置並記錄用戶時間，提供美國情報機構監控用戶數據內容（Lee 2014）。另外，中國政府爲避免美國間諜機構利用美國製造的軟體代碼，監視海外目標，已

要求在購買產品之前，如思科和微軟，接受嚴格的安全檢查（Rawlinson 2015）。因此，在外國網路科技廠商，進入中共市場須繳出商品之原始碼，已間接證明中共形塑的網路主權，可以捍衛其網路空間安全與利益。

總而言之，蘋果電腦自中共 2016《網路安全法》頒布後，陸續遭中國政府各部門審查，並下架相關 App，如蘋果新聞網站，意味著中國政府對網路用戶及營運商，得到更多的管轄權。其次，蘋果電腦被迫繳出商品之原始碼，及在中共境內設立首個海外數據中心，將增加進入中共市場成本，使中共國內廠商獲得平等權。最後，獲得商品之原始碼後，將有助於中國公安部門、解放軍掌握網路攻擊源位置，捍衛網路安全與利益。簡言之，中共建構的網路疆界，已使網路空間從個人—政府，擴及到個人—企業—政府，並使虛擬網路空間形塑出網路國防長城，屏蔽網路攻擊行爲（美國蘋果電腦遭中共《網絡安全法》行爲分析表，如表 3）。

表 3　美國蘋果電腦遭中共《網絡安全法》行為分析表

對照 區分	中共《網安法》條例	蘋果電腦的 處置行爲
管轄權	《網安法》第四十一條：網路運營者須依法律等規範，保存個人資訊；及第四十二條：網路運營者應當採取技術措施，收集個人資訊安全，並向有關主管部門報告。另外，第六十四條，凡未依上述規定執行：主管部門可根據情節沒收違法所得，並處違法所得一倍以上十倍以下罰款。	刪除 App 相關應用程式
平等權	《網安法》第三十七條：凡在中華人民共和國境內的資訊、通訊等營運商，須將用戶資料存儲於境內。另外，第六十六條，凡未依規定執行者，沒收違法所得，並處五萬元以上五十萬元以下罰款，並責令關閉網站、吊銷營業執照。	投資 10 億美元於中共貴州成立數據中心
捍衛權	《網安法》第十條：網路營運商，必須保障網路安全、資料的完整性；第二十一條：網路運營商應設立數據中心，採取監測、記錄網路運行狀態，並不得少於六個月；第二十二條：網路產品存有安全缺陷、漏洞等風險時，應立即採取補救措施，並按照規定及時告知用戶，及向有關部門報告。	繳出程式密鑰供政府部門監控

資料來源：作者自行調製。

陸、結論

網路空間是繼陸、海、空、太空的第五個空間。隨著網路安全對全球數位經濟、國家主權、安全發展威脅日益增加，建構數據在地化已成爲世界各國家，確保網路空間安全與利益的重要手段。在世界各國數據在地化的法案陸續通過後，網路主權已成是以國家行爲者必須去面對與聲索的新型主權。簡言之，在未來國際體系中，網路主權所扮演的角色將是越來越重要。在這股趨勢發展下，我國《資通安全管理法》正在立法審議階段，相關形塑網路主權的概念所涉及管轄的對象、範圍，是否將抵觸到人權隱私、智慧財產權等議題，均將成爲我國研討的基準點。

雖然，數據在地化已成爲各國確保網路安全的重要手段，但對威權體制的中共而言，網路主權所形成網路空間疆界化（cyber territorialization），恐將對區域安全產生影響。回顧 2011 年至 2016 年，中共所宣告的網路主權，從確保社會安全演變，至建構網路空間新秩序，其共同點在於加強對內部政治形態的審查。不同之處，在於隨著行動支付、數位經濟的發展，建構網路主權將有助於扶植國內網路科技，間接強化網路安全防護能力。同時，更有助於國防武力之網路部隊監控數據流動，進而捍衛網路空間與利益。然而，其所產生的後果，政治上，將成爲打壓國內政治異議的政治工具。經濟上，形成經貿競爭不公平，衝擊到自由經貿發展。軍事上，透由掌握商品之原始碼後，有助於網路部隊監控他國資訊，進而支持中國軍事武力的軟、硬殺手段，有利於網路戰略嚇阻。整體而言，中共宣告網路主權，即實現其中國夢、強軍夢，對區域安全將產生影響。

除此之外，中共所形塑出的網路空間疆界，已衝擊到美國所主導自由、民主的網路空間，傳播民主、自由價值影響國際體系。同時，也將增加民間企業進入中共市場的成本，與美國的國防戰略利益。基此，美國爲維護國家利益，勢必將採取反制措施，如 2018 年中國華爲通信公司，無法進入美國市場。因此，中共是否會因美國的施壓而改變網路政策，或是配合外交、經濟等手段，以強化其網路空間的影響力，便值得後續觀察。

* * *

（收件：106 年 3 月 27 日，接受：107 年 10 月 5 日）

Exploring PRC's Concept of Cyber Sovereignty

Ching-An Wang
General Commander
Army Communication Electronics Information Training Center, R.O.C.

Ji-Jen Hwang
Research Fellow
Institute of East Asian Studies
University of California, Berkeley U.S.A.

Abstract

Given the number of cyber-attacks in recent years, it has been confirmed that cyber-attacks can cause a huge impact on a state's political, economic, and military aspects due to the fact that the state actors cannot exercise jurisdiction over cross-border data flows within the territories. A so-called Cyber-Security Law was therefore established by states to empower their governments to monitor the flow of data in order to safeguard the security of users and enterprises in the cyberspace, as well as to strengthen the information security protection of national critical infrastructures in the state. Therefore, the shaping of cyber sovereignty and the construction of data in localized management have become extremely important tools for preventing cyber conflicts and maintaining international peace.

Technically, generating data can be managed locally so that personal, business, and national security can be protected. However, this study finds that, in terms of China's cyber sovereignty, since the "Cyber-Security Law" was promulgated in 2016, by law, the CCP has legitimacy to implement jurisdictions in internet users and telecom operators, and also shape cyber sovereignty into

an isolated network from the world's networks. At the same time, the Chinese government has integrated its military and civilian networking industry to create a so-called cyber territoriality. Politically, it has had an impact on the current order in cyberspace. Economically, it may increase the cost of global network operators entering the Chinese mainland market, resulting in the formation of trade protection, which is not conducive to global economic development. In addition, when the national security department has obtained the source codes of foreign merchants entering the China's market, the department may use this information to facilitate the controlling and monitoring of information in other countries' networks and to create asymmetric operational advantages in the wartime. In conclusion, the strategic implication of China's cyber sovereignty is not only to strengthen the national cyber security, but also to realize the dream of great power and the dream of a powerful military.

Keywords: Cyberspace, Cyber Sovereignty, Cyber Security, Cyber Territoriality

參考文獻

人民網，2015，〈中美舉行首次打擊網絡犯罪及相關事項高級別聯合對話〉，http://military.people.com.cn/BIG5/n/2015/1203/c1011-27885053.html，查閱時間：2018/3/14。People. 2015. “Zhongmei juxing shouci daji wanglu fanzui ji xiangguan shixiang gaoji bie lianhe duihua” [China and the United States hold the first high-level joint dialogue on cybercrime and related issues]. (Accessed on March 14, 2017).

中國人大網，2016，〈中華人民共和國網路安全法〉，http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm，查閱時間：2018/3/14。The National People’s Congress of the People’s Republic of China. 2016. “Zhonghua renmin gongheguo wanglu anquanfa ” [China Cyber Security Law]. (Accessed on March 14, 2017).

中國互聯網路信息中心，2017，〈中國互聯網路發展狀況統計報告〉，http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201701/P020170123364672657408.pdf，查閱時間：2018/3/14。China Internet Network Information Center.2017.“ Zhongguo hulian wanglu fazhan zhuangkuang tongji baogao” [China Internet Network Development Statistics Report]. (Accessed on March 14, 2017).

中國國防科技信息中心，2015，〈中國芯防火牆國內率先通過認證〉，《現代軍事》，（460）：109。2015. “Ziyouzhuyi he zuqun rentong: souxun Taiwan minzuzhuyi de yishixingtai jichu” [Liberalism and Ethnic Identity: Searching the Ideological Foundation of Taiwanese Nationalism]. *Modern Military*, (460): 109.

中國數字時代，2013，〈網傳習近平8•19講話全文：言論方面要敢抓敢管敢於亮劍〉，http://chinadigitaltimes.net/chinese/2013/11/%E7%BD%91%E4%BC%A0%E4%B9%A0%E8%BF%91%E5%B9%B38%E2%80%A219%E8%AE%B2%E8%AF%9D%E5%85%A8%E6%96%87%EF%BC%9A%E8%A8%80%E8%AE%BA%E6%96%B9%E9%9D%A2%E8%A6%81%E6%95%A2%E6%8A%93%E6%95%A2%E7%AE%A1%E6%95%A2/，查閱時間：2018/3/14。China Digital Times.2013.“Wangchuan Xijinping 8•19 jianghua quanwen: yanlun fangmian yao ganzhua ganguan ganyu liang jian” [Full text of President Xi Jinping's 8•19 Speech: Speech Should Dare to Censorship that Dare to shine the Wword]. (Accessed on March 14, 2017).

中華人民共和國工業和資訊化部，2015，〈中國共產黨第十八屆中央委員會第五次全體會議公報〉，http://www.miit.gov.cn/n1146290/n1146392/c4391094/content.html，查閱時間：2018/3/14。Ministry of Industry and Information Technology of the People's Republic of China. 2015. “Zhongguo gongchandang di shiba jie zhong yang weiyuanhui

di wu ci quanti huiyi gongbao" [Communique of the Fifth Plenary Meeting of the 18th Central Committee of the Chinese Communist Party]. (Accessed on March 14, 2017).

中華人民共和國工業和資訊化部，2017，〈工業和資訊化部關於清理規範互聯網網路接入服務市場的通知〉，http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html:查閱時間：2018/3/14。Ministry of Industry and Information Technology of the People's Republic of China. 2017. "Gongye he zixunhuabu guanyu qingli guifan hulianwang wanglu jieru fuwu shichang de tongzzhi" [Circular of the Ministry of Industry and Information Technology on Clearing up and Regulating the Internet Access Service Market]. (Accessed on March 14, 2017)

中華人民共和國外交部，2012，〈外交部條法司司長黃惠康在網路問題布達佩斯國際會議上的發言〉，http://www.mfa.gov.cn/chn//gxh/zlb/ldzyjh/t977343.htm，查閱時間：2018/3/14。Ministry of Foreign Affairs of the People's Republic of China. 2012. "Waijiaobu tiaofasi sizhang Huanghuikang zai wanglu wenti budapeisi guoji huiyi shang de fayan" [Statement at Budapest Conference on Cyber Issues]. (Accessed on March 14, 2017)

中華人民共和國國家網信辦公室，2017，〈互聯網跟帖評論服務管理規定〉，http://www.cac.gov.cn/2017-08/25/c_1121541842.htm，查閱時間：2018/10/14。Cyberspace Administration of China.2017. "Hulianwang gentie pinglun fuwu guanli guiding" [Management Regulations of Internet Post Comment Service in China]. (Accessed on October 14, 2017).

中華人民共和國國務院新聞辦公室，2010，〈中國互聯網狀況〉，http://www.scio.gov.cn/zfbps/ndhf/2010/Document/662572/662572.htm，查閱時間，2018/2/14。The State Council Information Office of the People's Republic of China. 2010. "Zhongguo hulianwang zhuangkuang" [China's White Paper on Internet Status]. (Accessed on February 14, 2018).

中華人民共和國國務院新聞辦公室，2013，〈中國武裝力量的多樣化運用〉，http://www.scio.gov.cn/zfbps/ndhf/2013/Document/1312844/13128449.htm，查閱時間，2018/3/14。The State Council Information Office of the People's Republic of China. 2013. "Zhongguo wuzhuang liliang de duoyanghua yun yong" [The Diversified Employment of China's Armed Forces]. (Accessed on March 14, 2017).

中華人民共和國國務院新聞辦公室，2015，〈中國的軍事戰略白皮書〉http://www.scio.gov.cn/zfbps/ndhf/2015/Document/1435161/1435161.htm，查閱時間：2018/3/14。The

State Council Information Office of the People's Republic of China. 2015. "Zhongguo de junshi zhanlue baipishu" [China's Military Strategy]. (Accessed on March 14, 2017).

互聯網新聞研究中心編著，2014，《美國是如何監視中國的：美國全球監聽行動紀錄》，北京：人民出版社。China Internet News Research Center. 2014. *Meiguo shi ruhe jianshi zhongguo de*: *meiguo quanqiu jianting xingdong jilu* [*How the United States Surveillance China*: *United States Global Surveillance Operation Record*].Beijing: People's Publishing House.

方濱興，2017，〈一個自主開放的互聯網根域名解析體系〉，《信息安全學報》，2（4）：57-69。Feng, Bin-xing. 2017. "Yige zizhu kaifang de hulianwang gen yuming jiexi tixi" [An Autonomous Open Root Resolution Architecturefor Domain Name System in the Internet]. *Journal of Cyber Security*, 2 (4): 57-69.

王春暉，2016，〈互聯網治理四項原則基於國際法理應成全球準則：「領網權」是國家主權在網路空間的繼承與延伸〉，《南京郵電大學學報》，36（1）：8-15。Wang, Chun-hui. 2016. "Hulianwang zhili sixiang yuanze jiyu guoji fali yingcheng quanqiu zhunze:'lingwangquan' shi guojia zhuquan zai wanglu kongjian de jicheng yu yanshen" [Four Principles on Internet Governance Reflecting a Global Norm Based on International Law]. *Journal of Nanjing University of Posts and Telecommunications*, 36 (1): 8-15.

朱國賢、霍小光、楊依軍，2015，〈習近平出席第二屆世界互聯網大會開幕式並發表主旨演講強調加強溝通，擴大共識，深化合作，共同構建網路空間命運共同體：劉雲山主持開幕式並致辭〉，《解放軍報》，12月17日。Zhu, Guo-xian, Xiao-guang Huo, and Yi-jun Yang. "Xijinping chuxi dierjie shijie hulianwang dahui kaimushi bing fabiao zhuzhi yanjiang qiangdiao jiaqiang qoutong,kuoda gongshi，shenhua hezuo, gongtong goujian wanglu kongjian mingyun gongtongti: liuyunshan zhuchi kaimushi bing zhici" [Xi Jinping Attended the Opening Ceremony of the Second World Internet Conference and delivered a keynote speech. He emphasized the Need to Strengthen Communication, Expand Consensus, Deepen Cooperation, and Jointly Build a Cyber Space Community of Fate: Liu Yunshan Presided Over the Opening Ceremony and Delivered a Speech]. *Liberation Army Daily* (December 17).

朱莉欣，2014，〈「塔林網路戰國際法手冊」的網路主權觀評價〉，《河北法學》，32（10）：130-135。Zhu, Li-xin. 2014. "'Talin wangluzhanguojifa shouce' de wanglu zhuquanguan pingjia" [Cyber Sovereignty Concept of Tallinn Manual on the International Law Applicable to Cyber War Review]. *Hebei Law Science*, 32 (10): 130-135.

何駿、趙立軍、王鵬，2017，〈從「塔林手冊」視角看網路主權〉，《裝備學院學

報》，28（1）：6-10。He, Jun, Li-jun Zhao, and Peng Wang. 2017. “Cong ‘talin shouce’shijiao kan wanglu zhuquan” [Study on Cyberspace Sovereignty From the Perspective of the Tallinn Manual]. *Journal of Equipment Academy*, 28 (1): 6-10.

呂晶華、成高帥譯，Clarke, Richard A., and Robert K. Knake，2011，《網路戰：國家安全的新威脅及應對之策》，北京：軍事科學出版社。Lu, Jing-hua, and Gao-shuai Cheng, trans. Clarke, Richard A., and Robert K. Knake. 2011.W*angluzhan: guojia anquande xin weixie ji yingdui zhice* [*Cyber War: the Next Threat to National Security and What to Do about It*]. Beijing: Military Science Press.

李景璿、陳泰偉，2017，〈網路涉軍舉報平臺正式上線運行〉，《解放軍報》，11月19日。Li, Jin-gyi, and Tai-wei Chen. 2017.“Wanglu shejun jubao pingtai zhengshi shangxian yunxing” [Internet-related PLA’s Reporting Platform Officially Launched]. *Liberation Army Daily* (November 19).

林幼嵐譯，Frédéric Martel，2016，《全球網路戰爭：全球化vs在地化》，新北市：稻田出版有限公司。Lin, You-lan, trans.Frédéric Martel. 2016. *Quanqiu wanglu zhanzheng: quanqiuhua vs zaidihua* [*SMART. Enquête sur les internets*]. New Taipei City: Dao Tian.

洪京一主編，2015，《世界網路安全發展報告》，香港：和平圖書有限公司。Hong, Jing-yi. 2015.*Shijie wanglu anquan fazhan baogao* [*World Cyber Security Development Report*]. Hong Kong: Peace Books Limited.

郎平，2016，〈中國網路強國戰略與G20框架下的互聯網經濟治理〉，《世界知識》，1672：62-63。Lang, Ping. 2016. “Zhongguo wanglu qiangguo zhanlue yu G20 kuangjia xia de hulianwang jingji zhili” [Internet Economy Governance under G20 Framework]. *World knowledge*, 1672: 62-63.

徐海濤，2016，〈量子通信「京滬幹線」合肥至上海段開通〉，http://news.sciencenet.cn/htmlnews/2016/11/361537.shtm?id=361537，查閱時間：2018/3/14。ScienceNet. 2016.“Liangzi tongxin ‘jinghu ganxian’ hefei zhi shanghai duan kaitong” [Quantum Communication “Beijing-Shanghai Main Line” Hefei to Shanghai Section Opened]. (Accessed on March 14, 2017).

馬民虎、張敏，2015，〈資訊安全與網路社會法律治理：空間、戰略、權利、能力—第五屆中國資訊安全法律大會會議綜述〉，《西安交通大學學報》，35（2）：92-97。Ma, Min-hu, Min Zhang. 2015. “Zixun anquan yu wanglu shehui falu zhili: kongjian, zhanlue, quanli, nengli- diwujie zhongguo zixun anquan falu dahui huiyi zongshu” [Information Security and Legal Governance of Network Society: Space, Strategy, Rights and Capabilities- Review of the Fifth China Information Security Conference]. *Journal of*

Xi'an Jiaotong University, 35 (2): 92-97.

高紫檀，2017，〈俄羅斯宣布禁用中國通訊軟件微信〉，大紀元。http://www.epochtimes.com/gb/17/5/5/n9110292.htm，查閱時間：2017/5/6。Epoch Times. 2017.“Eluosi xuanbujinyong zhongguo tongxun ruanjian weixin” [Russia Announces Ban on Chinese Communication Software WeChat]. (Accessed on May 6, 2017).

崔文波，2017，〈芻議網絡空間主權〉，《江南社會學院學報》，19（1）：7-13。Cui, Wen-bo. 2017. “Chuyi wangluo kongjian zhuquan” [Discussion on Cyberspace Sovereignty]. *Journal of Jiangnan Social University*, 19 (1): 7-13.

張新、楊利程，2017。〈我國「網路空間安全軍民融合創新中心」成立〉，http://www.81.cn/gnxw/2017-12/27/content_7886012.htm，查閱時間：2018/3/14。Zhang, Xin, and Li-cheng Yang, ” Woguo ‘Wanglu kongjian anquan junmin ronghe chuangxin zhongxin’chengli” [China Unveils Its First Civil-military Cybersecurity Innovation Center]. (Accessed on March 14, 2017).

曹如中、曾瑜、郭華，2014，〈基於網路資訊安全的國家競爭情報體系構建研究〉，《情報雜誌》，33（8）：15-18。Cao, Ru-zhong, Yu Zeng, and Hua Guo. 2014. “Jiyuwangle zixun anquan de guojia jingzheng qingbao tixi goujian yanjiu” [Research on Establishment of National Competitive Intelligence System Based on Network Information Security]. *Information Magazine*, 33 (8): 15-18.

梁德昭、朱志平、林凱薰，2012，〈國家主權延伸至網路空間之討論〉，《前瞻科技與管理》，2（2）：1-14。Liang, De-zhao, Zhi-ping Zhu, and Kai-xuan Lin. 2012. “Guojia zhuquan yanshen zhi wanglu kongjian zhi taolun” [On Extending State Sovereignty over Cyber Space]. *Journal of Advanced Technology and Management*, 2 (2): 1-14.

傅文成，2016，〈大陸網路主權論述之情勢評析〉，《展望與探索》，14（5）：35-36。Fu, Wen-chen. 2016. “Dalu wanglu zhuquan lunshu zhi qingshi pingxi” [An Analysis of Mainland China’s Discussions on Cyber Sovereignty]. *Prospects and Exploration*, 14 (5): 35-36.

惠志斌，2012，〈新安全觀下中國網路資訊安全戰略的理論構建〉，《國際觀察》，2：19-24。Xin anquanguan xia zhongguo wangle zixun anquan zhanlue de lilun goujian” [Theoretical Construction of China's Network Information Security Strategy under the New Security Concept].*International Observation*, 2: 19-24.

惠志斌、譚慶玲，2016，《中國網路空間安全發展報告（2016）》，北京：社會科學文獻出版社。Hui, Zhi-bin, and Qing-ling Tan. 2016. *Zhongguo wanglu kongjian anquan*

fazhan baogao. [*Annual Report on Development of Cyberspace Security in China (2016)*]. Beijing: Social Sciences Academic Press.

新華網，2016，〈中華人民共和國國民經濟和社會發展第十三個五年規劃綱要〉，http://news.xinhuanet.com/politics/2016lh/2016-3/17/c_1118366322_8.htm，查閱時間：2018/3/14。Xinhuanet. 2016. "Zhonghua renmin gongheguo guomin jingji he shehui fazhan di shisan ge wu nian guihua gangyao" [The 13th Five-Year PLAN For Economic and Social Development of the People's Republic of China]. (Accessed on March 14, 2017).

過子庸，2011，〈美國研發「電郵饋入」（FOE）軟體穿越中共網路審查之探討〉，《前瞻科技與管理》，1（1）：99-113。Kuo, Tzu-Yung. 2011. "Meiguo Yanfa 'dianyou kuiru' (FOE) ruanti chuanyue zhonggong wanglu shencha zhi tantao" [A Study on the Invention of FOE by the US to Bypass CCP's Internet Censorship]. *Journal of Advanced Technology and Management*, 1 (1): 99-113.

裴毅東，2014，〈從心血安全漏洞談起：對中國網路安全露洞應對機制的建薄議〉，《現代軍事》，35-37。Qi, Yi-dong. 2014. "Cong xinxie anquan loudong tanqi: dui zhongguo wanglu anquan loudong yingdui jizhi de jianboyi" [Liberalism and Ethnic Identity: Searching the Ideological Foundation of Taiwanese Nationalism]. *Modern Military*, 35-37.

魏亮、魏薇等編著，2016，《網路空間安全》北京：電子工業出版社。Wei, Liang, and Wei Wei. 2003. *Wanglu kongjian anquan*. [*Cyberspace Security*]. Beijing: Electronic Industry Press.

Andress, Jason, and Steve Winterfeld. 2014. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. London: Elsevier.

Applegate, Scott D. 2016. "The Principle of Maneuver in Cyber Operations." Paper presented at 2012 *The 4th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE.

Austin, Greag. 2015. *Cyber Policy in China*. Cambridge: Polity.

Astani, Marzie. 2016. "Trendsand Preventive Strategiesfor Mitigating Cybersecurity Breaches in Organizations." *Issues in Information Systems*, 17(II): 208-214.

Barcomb, Kris E.. 2013. "From Sea Power to Cyber Power: Learning From the Past to Craft a Strategy for the Future." *Joint Force Quarterly*, 2nd quarter: 80-83.

Bayuk, Jennifer L., Jason Healey, Paul Rohmeyer, Marcus H Sachs., and Joseph Weiss. 2012. *Cyber Security Policy Guidebook*. Canada: Wiley.

Benner, Katie, and Paul Mozur. 2016. “Apple Sees Value in Its Stand to Protect Security.” https://www.nytimes.com/2016/02/21/technology/apple-sees-value-in-privacy-vow.html?_ga=2.260951117.1128833346.1497316750-1159746865.1483843645 (March 14, 2017).

Burgman, Paul R. 2016. “Securing Cyberspace: China Leading the Way in Cyber Sovereignty.” https://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-in-cyber-sovereignty/ (March 14, 2017).

Carlos, Tejada. 2017. “Apple Faces Inquiry in China Over App Store Content.” https://www.nytimes.com/2017/04/19/business/media/china-apple-app-store.html?_ga=2.261988685.1128833346.1497316750-1159746865.1483843645 (March 14, 2017).

Carr, Jeffrey. 2012. *Inside Cyber Warfare: Mapping the Cyber Underworld 2nd Edition*. USA: O'Reilly Media.

Chapple, Mike. 2014. *Cyberwarfare: Information Operations in a Connected World*. Burlington: Jones & Bartlett Learning.

Domingo, Francis C. 2016. “ Conquering a New Domain:Explaining Great Power Competition in Cyberspace.” *Comparative Strategy*, 35(2): 165.

Douris, Constance. 2017. “Danger! Virus Discovered That Targets America's Electrical Grid.”http://nationalinterest.org/blog/the-buzz/danger-virus-discovered-targets-americas-electrical-grid-21242?page=2 (March 14, 2017).

Engstrom, Jeffrey. 2018. *Systems Confrontation and System Destruction Warfare*: *How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*. California: RAND Corporation.

Fears,Danika. 2018. “White House urges Iran to stop blocking social media.”https://nypost.com/2018/01/02/white-house-urges-iran-to-stop-blocking-social-media/ (March 14, 2018).

Ghosh, Dipayan. 2017. “Apple’s Dangerous Market Grab in China.”https://www.nytimes.com/2017/07/18/opinion/apple-china-regulation.html / (July 18, 2017).

Heinegg, Wolff Heintschel. 2012. “Legal Implications of Territorial Sovereignty in Cyberspace.” Paper presented at 2012 *The 4th International Conference on Cyber Conflict*, Tallinn: NATO CCD COE.

Hwang, Ji-Jen. 2017 “China’s Cyber Strategy: A Taiwanese Perspective.” *Korean Journal of Defense Analysis*, 29 (1): 95-111.

Jones, Seth G. 2018.“The Return of Political Warfare.”https://www.csis.org/analysis/return-political-warfare (March 14, 2017).

Lee, Jason. 2014. “Apple iPhone a Danger to China National Security: State Media.” http://www.bbc.com/news/technology-27712908 (March 14, 2017).

Limbgao, Andrea. 2016. “The Global Push for Cyber Sovereignty Is the Beginning of Cyber Fascism.” http://thehill.com/blogs/congress-blog/technology/310382-the-global-push-for-cyber-sovereignty-is-the-beginning-of (March 14, 2017).

Maurer, Tim. 2015. *National CSIRTs and Their Role in Computer Security Incident Response*. Washington D.C.: GPPI.

Mozur, Paul and Jane Perlez. 2016. “Apple Services Shut Down in China in Startling About-Face.” https://www.nytimes.com/2016/04/22/technology/apple-no-longer-immune-to-chinas-scrutiny-of-us-tech-firms.html?_ga=2.229024220.1128833346.1497316750-1159746865.1483843645 (March 14, 2017).

Mozur,Paul, andKatie Benner.2015. “Apple Is Said to Deactivate Its News App in China.”https://www.nytimes.com/2015/10/12/technology/apple-is-said-to-deactivate-its-news-app-in-china.html (March 14, 2017).

Pubby, Manu. 2017. “Indian troops on China border told to format smartphones, delete 42 apps.”https://theprint.in/2017/11/28/troops-told-to-format-smartphones-delete-42-apps-after-chinese-spyware-threat (March 14, 2017).

Raud, Mikk. 2016. “China and Cyber: Attitude, Strategies, Organisation.” Paper presented at the *Annual Meeting of CCD COE*,Tallinn.

Rawlinson, Kevin. 2015. “US tech firms ask China to postpone intrusive rules.” http://www.bbc.com/news/technology-31039227 (March 14, 2017).

Rid, Thomas. 2013. *Cyber War will not Take Place*. Cambridge: Oxford University Press.

Schmitt, Michael N. 2013. “Tallinn Manual on the International Law Applicable to Cyber Warfare.” https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (March 14, 2017).

Setiawan,A. B., A. Syamsudin, and A. Sasongko. 2015. “Implementation of Secure Smart Grid as Critical Information Infrastructure in Indonesia: A Case Study in Smart Grid Electricity.” Paper presented at the 2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Jakarta.

Sewell, Bruce. 2016. “Deciphering the Debate Over Encryption: Industry andLaw Enforcement Perspectives.” https://docs.house.gov/meetings/IF/IF02/20160419/104812/HHRG-114-IF02-Wstate-SewellB-20160419.pdf/ (March 14, 2018).

Shanghai Cooperation Organization, Code of Conduct for Information Security. 2011. "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)" https://www.ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf (March 14, 2017).

Shirk, Susan. 2017. "Trump and China Getting to Yes With Beijing." *Foreign Affairs*, 96 (2): 20-27.

The White House. 2011. "International Strategy for Cyberspace."https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (March 14, 2017).

Theohary, Catherine A., and John W Rollins.2015. *Cyberwarfare and Cyberterrorism*: *In Brief*. Washington D.C.: Congressional Research Service.

Tasheva, Iva. 2017. "European cybersecurity policy: Trends and prospects." *Policy Brief*. Brussels: Eurpean Policy Centre.

Thierer, Adam. 2010. "Hillary Clinton's Historic Speech on Global Internet Freedom." https://techliberation.com/2010/01/21/hillary-clintons-historic-speech-on-global-internet-freedom/ (March 14, 2017).

United Nations General Assembly. 2013. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in theContext of International Security." https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf (March 14, 2017).

United Nations General Assembly. 2015. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." A/70/172 http://undocs.org/A/70/172. (March 14, 2017)

United States Department of Defense. 2013. "Joint Publication 3-12 (R) Cyberspace Operations." http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf (March 14, 2017)

Yang, Haitao, and Jian Zhang. 2016. "Network Boundary and Protection." Paper presented at 2016 *The International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Beijing, China.

Zhao, Frank, and Jesse Heatley. 2016. "China's Master Plan for IT Dominance." https://thediplomat.com/2016/08/chinas-master-plan-for-it-dominance/ (March 14, 2017).