● 作者/Andrea Little Limbago ● 譯者/章昌文 ● 審者/劉宗翰

網路治國的多面向本質

One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft

取材/2015年第3季美國聯合部隊季刊(*Joint Force Quarterly*, 3rd Quarter 2015)

網路治國術的本質是多面向的。圖爲美國國家網路安全與通信整合中心。(Source: REUTERS/達志)

外界普遍認爲網路治國僅限於軍事領域等少數用途，其實這是一種過度簡化的想法。美國必須建立網路治國的架構，才能了解其涵蓋幅度，掌握其本質，以更適切發揮其潛能。

網際空間常被稱為第五領域，隱涵其未來角色是繼陸、海、空、太空之後的下個主戰場。不過，這種論述過度簡化了網際空間，低估其對這些領域中和橫貫其間的變革上之巨大影響。再者，僅將網路劃定為戰場和強制領域，則會對國家和非國家行為者利用網路治國實現其目標的各種途徑見樹不見林。將網際空間比擬成對國際體系具有阻擾效應的第五領域，雖然是保守說法，但截至目前為止，對行為者利用網路在地緣政治上有所斬獲的各種方式，則鮮少有人探討。從一端的Stuxnet到另一端政府贊助的臉書帳號，國家與非國家行為者可用的數位阻斷手段已大幅增加，現在甚至連權力遞嬗也常在網際空間先行公諸於世。例如，泰國近期在政變後，戒嚴法是透過推特(Twitter)和一新設的臉書帳號正式宣布，並被一些研究人員戲稱為是一次「加主題標籤的網路政變」(*#cybercoup*)。

為了更適切評估網路作為可達成國家安全目標領域──從反介入/區域拒止到治理、民主化和經濟成長──的戰略意涵，決策者需要一個縝密、多重的網路治國架構，用來驗證網路治國是否能當作軍事手段，甚或

在快速創新單元會議(Rapid Innovation Cell meeting)中，科瓦拉(Josh Kvavle)博士(右方)爲時任美海軍軍令部長的格林納(Jonathan Greenert)上將展示頭戴式谷歌眼鏡。(Source: US Navy/Peter D. Lawlor)

是一種更為全面的治國型態。早就該有這樣的一個架構，幫助說清楚持續影響國際政治體系的大量科技干擾。儘管軍事組成部分相當關鍵，但網路治國經常只透過此種強制的觀點來檢視，而實際上，其範圍要寬廣的多。即使軍事層面中的網路治國，也鮮少提及此一領域內可供行為者運用的各種手段，這使得從網路審查到網路諜報活動的每件事情全都混在一起，成了「網路攻擊」的泛稱，這些對照同樣嚴重妨礙執行者和理論家評估網路治國戰略影響能力。

拿網路研究和核武戰略研究的發展相互比較，奈伊(Joseph Nye)指出，「網路領域的戰略研究，在時序上相當於1960年，但在概念上等同於1950年。」[1] 簡言之，網際空間的分析與理論趕不上作戰環境的改變，導致理論與實踐的戰略意涵落空。此一理論上的停滯，應歸責於在分類上僅將

網際空間視為一個衝突領域，限縮了決策者了解網際空間有諸多方式可廣泛利用於治國。但網際空間的軍事化並非是此一現象的唯一罪魁禍首；另外有部分則要歸咎於科技圈和國家安全政策界間的隔閡，網際空間論述的科技屬性，成了條理清晰去理解網路治國的障礙。此外，科技變革的神速，也使決策者和為數更多之戰略研究學界很難與網路領域內的快速發展步調一致。

網路治國的範圍

乍看之下，建構一個用於分析和了解各種施行網路治國的理論架構或許看來迂腐。不過，欠缺這樣一個架構，將導致網路治國只不過是個攻擊手段的看法一直延續下去。希利(Jason Healey)在其所著《激戰領域》(*A Fierce Domain*)中指出，「網路」(*cyber*)一詞已日益軍事化。[2] 儘管最初是個中性詞彙，但目前提到網路，通常是暗指攻擊行為，而在探討網際空間具正向的科技影響時，則是使用「網際網路」(*Internet*)。其實，在過去15年間，將網際空間當作一獨特領域的探討已經劇減，如同圖1描繪的，在谷歌執行搜尋「網際空間」一詞傾向的快速檢視時，此種趨勢相當明顯，網路更常被當作像網路戰、網路犯罪和網路攻擊等各類攻擊活動的字首。

經濟治國最初被視為是國家強制力的形式，但此種見解在趨勢上同樣有所改變，由於更自由的全球經濟取代了重商主義，戰略家也開始認為經濟治國具安撫作用，認定經濟手段有潛力促進和平與發展，這也有助於確保不將經濟治國視為只是權力政治中的強制手段。正如經濟治國通常意味著將經濟做為具說服力的一種政治工具，網路治國同樣會被認為是使用網路手段來達成政治目標。此外，不同於其他治國手段，網路手段並沒有被劃分到個別的範疇中，網路治國的影響遍及外交、資訊、軍事和經濟等各種實力的組成部分，這很可能是因為網際空間的獨特本質，和包括實體及溝通領域在內的多重層面。不過，在各種狀況中，網路治國都被用來做為在這些實力組成部分中達成政治目標的方式。和經濟治國在重商主義期間崛起的情況類似，在目前全球化和資訊科技充斥的時代，網路治國已躍居為無處不在的首選手段。

與普遍看法相左，運用網路治國是在施加硬實力(例如強制、懲罰)、軟實力(諸如勸說採取相同目標、吸引)，以及介於其間的一切作為，儘管絕非一份詳盡清單，但圖2描繪出最常用網路手段範圍的一個廣泛分

圖1 興趣趨勢 新聞提要

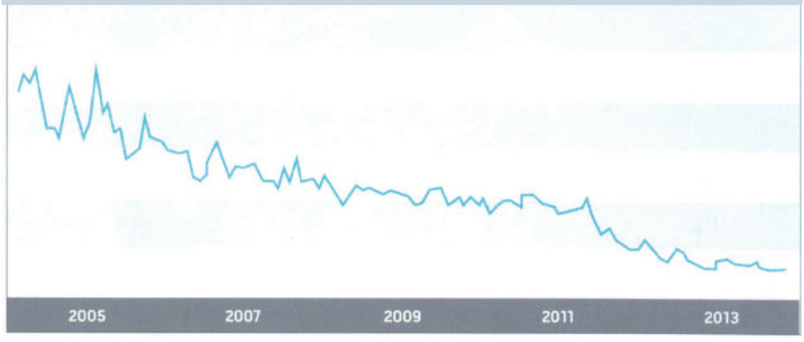
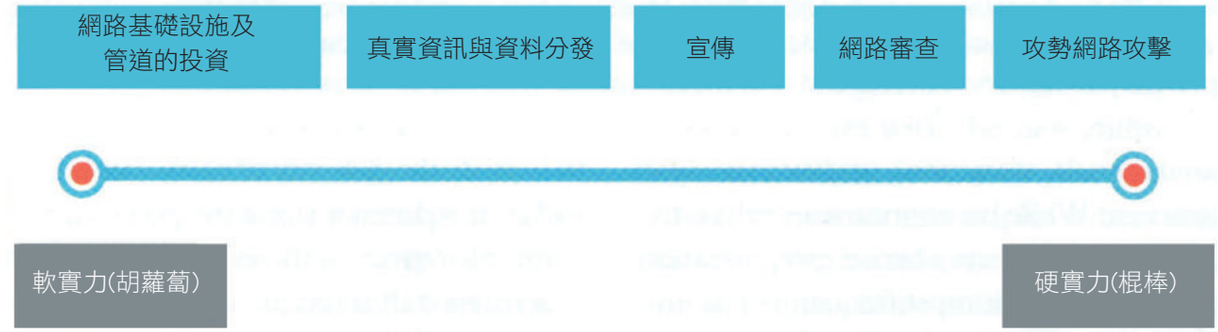


圖2 網路治國的範圍



類，從一端的網際網路自由和存取等正誘因，到另一端的攻勢網路攻擊，此架構描繪出在此範圍兩端的網際空間「實體」層面，和位居中間地帶的「溝通」層面。

本文其餘部分將提供目前在整個實力領域中運用網路治國的具體案例，並藉此建議理解與充分利用網路做為治國工具的一個戰略架構，如同下列案例所闡明的，國家和非國家行為者會以各種方式運用網路治國，俾實現諸般目標。和其他治國形式一樣，出於善意或惡意的企圖都可能使用網路治國之道，結合使用的手段，應用網路治國究竟算是胡蘿蔔或是棍棒，企圖成了一項附加的決定因素。因此，本文目的並非為了提供網路治國中每個可能手段的詳盡綜覽，而是在擴展對網際空間的認識，將此領域實力範圍內可用的多種手段都涵括其中。此外，如同案例所述，網路治國具有獨特的不對稱本質，不僅能使大國握有大權，也可成為較弱小行為者在國際舞臺上擁有不成比例的影響手段。

網路基礎設施及管道的投資

國家在網路基礎設施上的投資——儘管透過實體基礎建設，也會提升連接性——促成科技取向的解決之道，可廣泛用於困擾已開發和開發中世界的經濟、政治和社會議題。許多政府——甚至有些非國家行為者——推動網路基礎建設，透過經常與網際網路管道一致的正外部性(positive externalities)，使人們擁有權力。因此，政府在實體基礎設施擴充及網際網路管道上的投資，對達成政治目標絕對至關重要。政府藉資訊科技基礎建設——包括硬體及其法律層面——做為傳輸吸引與說服內容的機制，許多政治和經濟的正外部性都和有更多網際網路的使用權有關，尤其是在開發中世界更是如此。更多網際網路的使用權可增加民間的競爭力，提高教育機會，並激發經濟效率。例如，科技參與——唯有經由現有的網路基

礎設施才會有可能──能提供用來聯繫身陷險境者的途徑，藉由提供更多資訊、教育和經濟機會，以及娛樂的管道，連接性可變成防止激進化的一個重要工具。倚賴行動轉帳和網路銀行作為其經濟核心組成部分的人，可能的經濟效益尤其普遍。

隨著網際網路管道在全球持續擴展，網路治國此種軟實力模式影響目前地緣政治環境的可能性也許會繼續增加──尤其是國家為了獲得現代通訊系統而大幅改善過時科技的情況下。例如，世界銀行在2012年《發展中的資訊與通信》(*Information and Communication for Development*)報告中發現，行動寬頻對經濟成長的影響更甚於固定寬頻。[3] 在許多開發中國家，行動金融平臺可讓援助組織和國內族群規避經濟封鎖及提供協助，並與全球經濟整合。

在過去數年間，肯亞由於全力擴展其網際網路管道，因而在為數眾多的國家中獲得讚揚。根據世界銀行世界發展指標，肯亞的網際網路使用率，過去五年增長了400%。[4] 此事極為重要，尤其是在2007年的爭議性選舉之後，肯亞受到動亂加劇的威脅，當時僅有不到10%的人可連線到網際網路。此種管道的擴展所影響的不只是經濟，透過有機會使用線上教育工具和查詢日常市場價格(這是農業領域的關鍵知識)等資訊，也鼓舞了人力資本的發展。如同肯亞情況所示，投資擴展網際網路，對政府提供有效使用軟實力環境條件的能力至關重要。儘管不一定是新的建置，但政府挹注資源於開設與擴充網際網路架構與科技取向經濟的現象，近期受到相當密切的關注。例如，1970年代，印度在邦加羅爾(Bangalore)附近空出一塊區域，要建造一座電子城，不過，法律和經濟體制無法跟上，在1990年代經濟自由化活絡前，資訊科技轉運中心都未能真正興起。

逐步建構一套網路架構，不單是達成國家內部目標的一個手段，也和國家競逐區域影響力一樣，興起成為權力政治的一個組成部分。例如，光纖網路和手機信號塔可用來協助在國家間建立聯盟，並擴張大國的影響範圍。某些多國合作也愈來愈常使用此種戰術，以達成自身的目標，谷歌打算在非洲建立光纖網路的聯網計畫(Project Link)，就是一個很好的例證。相反的，歐洲/比利時為了避開美國的監視作為，設法建置了一條海底電纜，凸顯權力政治在網際空間中的角色。最後，建置網路基礎設施，有可能成為維和任務和衝突干預中的一種手段。在衝突過後，由於科技變成工具，因此在修復網路基礎設施上，可能變成和提供安全、飲水和電力等關鍵服務同等重要，各方的援助行動和財政支援，可藉此協調並有系統地分配，同時亦可做為衝突後重建政治、經濟和社會機構的牢固基礎。

真實資訊與資料分發

儘管大眾的探討絕大部分集中在網際網路的審查，但許多國家和非國家行為者也善於利用網際空間，做為散布真實資訊給人們的途徑，提供更大透明度，表明渠等意圖。在伊朗，魯哈尼(Hassan Rouhani)總統就開設一個較開放的網際網路平

2015年3月，俄亥俄州國民兵電腦網路防護小組組員在2015年網路護盾(Cyber Shield 2015)演習期間，於印第安納州阿特貝瑞營區(Camp Atterbury)執行作業。(Source: Ohio National Guard/George Davis)

臺，儘管他的確施行強制的網路手段(隨後將會討論到這點)，但魯哈尼同時使用其推特帳號來傳遞更正面的透明訊息。不久前，他用推特向伊朗數學家及菲爾茲獎(Fields Medal)得主米爾札哈尼(Maryam Mirzakhani)道賀，並附上一張她沒戴面紗的照片——顯然有意凸顯開明的作風，並防止伊朗進一步的「人才外流」。這並非魯哈尼的單一事件，先前他亦曾在2013年9月紐約聯合國大會之後，將其與歐巴馬(Barack Obama)總統的電話內容在推特上發送。泰國政府在推特上宣布戒嚴令，同樣也可視為藉公開向更多民眾散布重要資訊，以提升透明度的一種途徑，推特仍是泰國民眾可藉以和軍方領導的新政府的一種互動機制。

政府也運用網路手段為其行動辯護，或間接表明那些若直接表達在政治上將屬不明智的意圖。例如，巴西總統羅賽芙(Dilma Rousseff)用她的推特帳號為巴西對世界盃的準備辯護，日本首相安

倍晉三(Shinzo Abe)看來也是用其推特帳號，向日本民眾表達其外交政策意圖，在推特上關注安倍的人雖屈指可數，但印度總理莫迪(Narendra Modi)卻是其中之一，是否顯示兩國間關係在未來會更趨緊密尚言之過早，但要告知民眾其領導者企圖或所關注的事，社群媒體是一簡單且巧妙的方式。

最後，行動科技對已開發和開發中世界的社區治安維護計畫提供了技術基礎，盧安達(Rwanda)實施的群眾外包(crowd-sourcing)方案，妥善利用行動平臺來強化法治，從而讓社區民眾有能力如同公民記者般傳送有關劫掠和暴力事件的消息。以真實與即時描述事件為目標的資訊群眾外包，並不限於國家行為者，但確實是更常被非國家行為者──像是非政府組織還有一般民眾──運用的一種戰術，在像委內瑞拉(Venezuela)的抗議、中國大陸溫州的火車事故、西非爆發的伊波拉危機等各式各樣的事件中，這是顯而易見的。誠然，分辨到底是放上真實資訊或是宣傳的網路行為，企圖扮演了重要的角色。政府虛假資訊的宣傳已變得日益普遍。

米爾札哈尼係2014年菲爾茲獎得主──在國際數學家大會(International Congress of Mathematicians)80年歷史中的首位女性獲獎者──鑑於「她在黎曼曲面(Riemann surfaces)及其模數空間下的動力學及幾何學的傑出貢獻」。(Source: courtesy of Maryam Mirzakhani)

網路治國的範圍涉及了地緣政治，憑藉的是軟硬實力的交互使用。

宣傳

網路治國的範圍涉及了地緣政治，憑藉的不僅是正面說服和吸引手段。網路治國也被政府和非國家行為者用於更具懲罰性的企圖與散播錯誤資訊。普丁(Vladimir Putin)的侵略行為就是利用網際空間做為其宣傳機器的例子，他曾用假的臉書帳號和其他知名的社群媒體管道，從正面角度來描述克里米亞的合併，甚至進而竄改烏克蘭極端分子所犯下的罪行和殘暴行為，他也用網路灌輸有關馬來西亞航空班機(Malaysian Flight 17)的論述，提出許多不可思議的情境，範圍從否認其遭到擊落，乃至宣稱自己才是遭鎖定的目標。與昔日領導人使用的傳統治國手段類似，他倚賴網路手段提升「團結在國旗周

在聯合奮進14號演習(Combined Endeavor 14)──世界最大規模的指揮、管制、通信與資訊系統演習──期間，一名斯洛維尼亞士兵評估任務小組對網路攻擊的回應。

(Source: USMC Forces Europe/Derrick K. Irions)

遭」(rally-round-the-flag)的效應，並獲得國內對俄國自身政策的支持。如同歷史上的案例，普丁運用的網路治國手段不只一種，而是將網路宣傳和增強審查，以及更多政府對網際網路的掌控整合在一起。中共對線上宣傳採取的做法則略有不同，政府雇用了線上評論人員，經常指的是五毛黨(50-cent party，譯註：意指每貼一則正面訊息就可得人民幣五毛錢酬勞的那些人)，他們拿錢加入線上社群，對付反對共產黨的內容、宣揚黨的重大工作、或是制止敏感內容。

暴力極端組織同樣運用網路治國作為宣傳手段，也做為徵召及激化的重要機制，社群媒體多半成為這些宣傳方法的場所。不過，諸如真主黨(Hizballah)等技術更專精的一些團體，也創作了應用程式來招募信徒及散播意識形態。其他諸如錫納羅亞同業聯盟(Sinaloa Cartel)、敘利亞電子軍(Syrian Electronic Army)等與政府關係密切的那些非國家團體，同樣製作了YouTube影片、建立推特帳號，當做影響當前事件論述的修訂者工具，或是宣傳其承諾團體內的成員可享受富裕的生活方式。

網路審查

國家利用網際空間來操控並審查內容(如同先前的探討)，網路審查會得出各種結果，而依其條件規範，達成的預期成果依舊會含糊不清。取決於網路審查的深度和廣度，其可能會激起、反而不是撲滅動亂。例如，委內瑞拉在2014年打算審查推特，卻引發更多對政府的抗議。在2014年的抗議展開和戒嚴法頒布過後，泰國同樣曾試圖審查各種社群網站。近期，土耳其在一次安全會議上的錄音資料外流後，升高了對YouTube的防堵，隨後的政治危機，導致其於2014年增加了對網路的審查，此舉所激起的抗議，依舊困擾著埃爾多安(Recep Tayyip Erdogan)政府。同樣地，魯哈尼最近取締Instagram，臉書及推特也都成為在伊朗正式禁止的社群媒體管道。諷刺的是，魯哈尼自己還是個頻繁的Instagram用戶，擁有大批追隨者。最後，在塞爾維亞一世紀以來最糟的幾次洪患之後，該國政府因處置失當，激起了直言不諱的網路言論。為了回應此一事件，塞爾維亞政府用網路審查制度管制言論，移除凸顯政府行動錯失、或公然批判政府的網站。

先前案例都聚焦在以網路審查作為限制反政府內容的手段，中共雖然使用相同手段，但採取了略為不同的做法。近期一本哈佛刊物中的文章〈中共的網路審查是如何容許政府批判但卻讓集體表達噤聲〉(How Censorship in China Allows Government Criticism but Silences Collective Expression)，[5] 分析了各種社群媒體的資料，發現中共網路審查的主要目標，是在防範社會動員。先前案例所聚焦的是限制反政府的修辭，而中共領導階層更有可能是在檢查任何可能導致群眾動員的內容，並不理會談話的內容。此種以防範任何類似社會動員為目標的傾向，顯露在2014年的「1989年天安門廣場大屠殺25周年紀念日」當中，中共的網路審查封鎖了主要的社群媒體管道、直接或間接與天安門有關的查詢，目標就在防止任何類似的社會動員。

攻勢網路攻擊

在網路治國範圍偏激的一端，一名行為者攻擊性的使用網路手段，完成其懲罰性的治國用途。攻勢網路手段在嚴重性上變異極大，它們本身就包含了範圍廣泛的治國手段，按理可將其劃分成四個清楚的領域：置入(例如：惡意程式)、阻斷(分散式阻斷服務攻擊[DDoS])、移除(網路諜報活動)、摧毀(諸如關鍵資訊或基礎設施)。2009年，阿拉伯聯合大公國靠著部分國營的電信公司「阿聯酋電信」(Etisalat)，要求其黑莓機用戶更新渠等話機以提供更佳服務，因而得以將間諜軟體安裝在裝置中，使政府未經同意即可取得私人資訊。親政府的敘利亞電子軍(一個結合鬆散的駭客團體)做得更加過分，除了其他網路攻擊外，還執行「陰暗彗星」(Dark Comet)和「黑色幽靈」(Blackshades)等惡意程式來對付反政府的活動分子。儘管尚不清楚其與阿薩德(Bashar al-Asad)政權是否有直接聯繫的實力，但該非國家團體確實具有政府代理人功能，且力求在國內攻擊反政府的活動分子，他們其他諸多手段類似綠色革命(Green Revolution)期間伊朗用來對付其人民的那些做法，而許多分析師認為，敘利亞使用的是伊朗設計的攻擊軟體，2012年在敘利亞史無前例的2天網際網路封鎖期間，阿薩德政權使用的可能就是類似的手段。

這些案例說明國家運用網路棍棒對付其本國人民有日益盛行的趨勢。當然，攻勢網路治國並不僅限於在國內實施，網路攻擊顯然也成為國家間權力政治的一種手段，在北韓和南韓、俄國與喬治亞，以及印度與巴基斯坦間的各種衝突與爭端中都表露無疑。在這些案例中，類似於敘利亞電子軍進行網路攻擊的做法，非國家團體與國家政府緊密結盟，實際執行網路的攻擊，由於網際空間歸因不明確的屬性，升高了國家間衝突的複雜性。在執行那些使用高度技術性且複雜的攻擊手段(諸如奧林匹克運動會[Olympic Games]、德國的R2D2木馬程式[Trojan]、俄國的CosmicDuke)時，國家當然具有優勢。同樣的，目前國家間使用諸如摧毀伊朗納坦茲(Natanz)核子反應爐的Stuxnet、攻擊沙烏地阿拉伯沙特阿美(Saudi Aramco)石油公司的Shamoon病毒等破壞性網路手段互動時，仍然是被壟斷的。Shamoon感染了該公司四分之三的個人電腦，雖然在影響石油供應前就被阻止，但對沙特阿美公司的攻擊，使該公司必須更換其數以萬計的個人電腦，一般認為源頭就是來自伊朗。

鑑於網路領域不對稱的本質，儘管在非國家行為者運用時，顯然其規模和範圍會有極大落差，但這些手段不會只屬於國家行為者的範疇。中共駭客近期利用「心臟出血漏洞」(Heartbleed bug)竊取健康紀錄，而目標百貨(Target)和尼曼馬庫斯精品百貨公司(Neiman Marcus)的資料外洩，或許是以跨國企業為目標的網路諜報活動最顯著的成功案例。匿名者(Anonymous)這個去中心化、結合鬆散的駭客團體，以國家和非國家行為者做為下手對象，對以色列政府進行分散式阻斷服務攻擊，並用其在網路的成就支持「阿拉伯之春」運動。不過，政府對該團體的影響展開了反擊，英國政府對匿名者的分散式阻斷服務攻擊，或許是首個政府介入分散式阻斷服務行動的公開事例。隨

著這些案例的持續披露，每當有新的揭露，都為網際空間內攻勢網路治國潛能的增強提供了實例。不過，歸因議題使誤解在網際空間內的影響程度加劇，將更難理解這些手段的實例化對國際關係造成的長期影響。

結論

本文初步概述網路治國的架構──和各種可供國家與非國家行為者運用的手段──以探索並理解日益增長的網路治國運用與可能影響，提供一個更有架構性與細密的做法，由於重要性日增，而網路治國對國家安全的可能影響，仍有大部分皆未經探究，況且這早就該做了。做為治國手段的網路，曾被它過分強調的軍事層面所佔據，此種著重於網路攻擊的表現，忽視了此一關鍵領域的細微本質，及其在地緣政治上更廣泛的運用。網路治國儘管強有力且具破壞性，但絕不只是由情報或攻擊能力所構成。分析人員和決策者同樣需開始將網路治國視為不只是少數情況下有用的個別攻勢手段，而是當成可與其他更傳統的治國形式分庭抗禮，包括吸引強制的軟硬實力連續體、由國家和非國家運用的一種治國型態。在網際空間運用更具固定體系的一種治國模式，有助於安全和政治領導人使網路治國的作用更趨穩固，並促進更深的理解，同時也能增加國際社會對網路治國，以及網際空間明顯影響國家安全與地緣政治的認識。

是該結束過分關注於將網路作為主導攻擊手段的時候了，這不僅造成根本上的不穩定，還加劇安全困境，而且也忽略了國家在該領域內的各種作戰方式。對用網路治國的檢驗，也會從科技界與戰略研究學界間增加的協調中獲益。與其在國際體系中的重要性相較，此一領域的科技本質，可能是造成網路治國不受關注的原因之一。儘管依舊處於一個領域的草創時期，擁有網路治國的架構，將更能對行為者如何善用網際空間做一整體思考，也最適合為將來科技──政策關係的研究開路，並因而促進對此科技干擾影響全球事務的方式，能有更多面向的理解。

作者簡介

Andrea Little Limbago博士，係一家名為終局(Endgame)的安全情報分析軟體公司首席社會學家。

Reprint from *Joint Force Quarterly* with permission

註釋

1. Joseph S. Nye, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly 5* (2011), 19.
2. Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).
3. World Bank, *Information and Communication for Development: Maximizing Mobile* (Washington, DC: The World Bank, 2012).
4. World Bank, *World Development Indicators* (Washington, DC: The World Bank, 2015)，參見網頁<http://data.worldbank.org/products/wdi>.
5. Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107 (May 2, 2013)，參見網頁<http://gking.harvard.edu/files/gking/files/censored.pdf>.