● 作者/Laura Rosenberger ● 譯者/張彥元 ● 審者/洪琬婷

打造更安全網路空間

Making Cyberspace Safe for Democracy

取材/2020年5-6月美國外交事務雙月刊(*Foreign Affairs*, May-June/2020)

民主國家視資訊爲掌握在人民手中的力量。威權體制則視資訊流通爲威脅，故以操縱公衆言論等手段，對內鞏固權力，對外削弱對手。民主陣營面臨此不對稱態勢，應找出資訊競爭下可維護民主價值之最佳方案。

隨著2020年美國總統大選開跑，俄羅斯干預選舉的傳聞又再次甚囂塵上。2016年，俄羅斯的駭客行動以及利用社群媒體操縱美國公眾言論之舉，讓美國的決策者措手不及。四年後，官員仍未完全理解，那些攻擊行為反映著地緣政治競爭局面的變化。若視2016年俄羅斯意圖影響美國大選之舉為個案，美國恐顧此失彼。換句話說，在廿一世紀，敵對國家在資訊領域競爭程度與在其他領域的對抗程度相比，不遑多讓。

民主國家視資訊為掌握在人民手中的力量，思想、新聞和輿論的自由流通與開放，促進了審議式民主(Deliberative Democracy)。威權國家則認為此種模式屬於威脅，將資訊視為對其政權之危害，故而必須由國家控制與引導之。專制政權透過監視、審查及資訊操縱等手段，對內鞏固其權力，對外則削弱民主競爭對手之影響力。

美國及其民主盟邦尚未適應此一現實情況，採取被動回應，僅求克服現有問題，而未運籌帷幄求取致勝之道。資訊領域的困境已然浮現，民主政體所承受的內外壓力日增，而威權國家卻在全世界站穩腳步。嶄新型態的大國競爭不一定在戰場或圓桌上進行；它將會在智慧型手機、電腦、其他連網設備及

資訊競爭茲事體大。圖為美陸戰隊網路指揮部，負責網路作戰攻勢與守勢等任務。(Source: DVIDS)

資訊機房發生。許多民主國家對資訊通常採取放任態度，使其難以與他國一爭高下。

民主政體陷入了兩難，倘若在資訊競爭中不採取主動態度，在國內易遭受打擊，在國外則將陷入不利之處境。然而若以錯誤方式採取積極和強勢作為，則民主政體可能淪於模仿專制國家高壓行徑，並創造出獨裁者所企圖嚴格管控的環境。

資訊競爭茲事體大。倘若威權體制勝出，各國在管制資訊和塑造公眾觀感等方面將更加箝制。管理資訊基礎設施之全球規則也將偏向威權而非民主體制，從而限制美國發揮影響與投射力量之能力，亦削弱了政府體系。世界會變得更加專制、更不民主。

決策者必須保護民主的資訊空間，俾能保障民主國家之運行並捍衛現有生活方式。在資訊時代欲保護美國國家安全，瞭解資訊競爭本質、確立成功願景，並發展新戰略以實現該願景，至關重要。

打一場資訊戰爭

中共、俄羅斯與美國截然不同，前兩者早已將資訊競爭納入國家安全戰略的重要部分，並將網路空間(支撐網際網路的基礎結構，例如可能容易遭受侵駭之伺服器及電腦系統等)以及資訊空間(可能遭國家進行監視、蒐集、刺探以及扭曲的數據和公眾觀感等範疇)之各項作為，列為優先事項。中共及俄羅斯均強調擁有網路空間之主權，旨在透過監看或控管作為，將資訊流通限制在國境之內。值此同時，這兩國雖採取不同手段，但均已發展出操控國外資訊的方法。中共和俄國也正致力發展人工智慧(以下簡稱AI)等新興科技，企圖取得領先地位，因這些科技將在未來對地緣政治競爭產生重大影響。

一如其外交政策之大部分內容，俄羅斯在網路戰與資訊戰之界定上均採防禦性措辭，且認為美國早已利用資訊支援俄羅斯境內之異議人士。其2016年之資安準則正式將「保護俄羅斯資訊主權」列為社會維穩之核心項目。俄羅斯干預他國選舉之行為，僅為大規模策略的一小部分，此策略目的在於破壞目標國家政治與社會制度、企圖操控該國民眾之心理，並依俄羅斯國防部2011年提出的文件〈資訊空間下武裝部隊作業概念〉所述，迫使「目標國做出有利於其敵對勢力的決定」。

俄羅斯操縱資訊者之目的通常不是要說服他人、傳播觀點和意識形態，而是散播造成混亂與崩潰的種子。其目的乃是給人一種事實並不存在的印象，從而破壞民主國家的信任和權威。這些操縱者在社交媒體上炒作極端觀點、陰謀論以及懷疑民主制度等論點。俄羅斯官方支持的媒體也協助散播這些論述。例如，當俄羅斯特工被指控在英國毒害前俄羅斯情報官員斯克里帕爾(Sergei Skripal)和其女兒之後，俄羅斯官員利用推特傳播其他勢力才是背後主謀的各種可能說法，暗示不可能查明罪魁禍首，而俄羅斯官媒和其秘密網路組織則對這些說法加以鼓吹唱和。

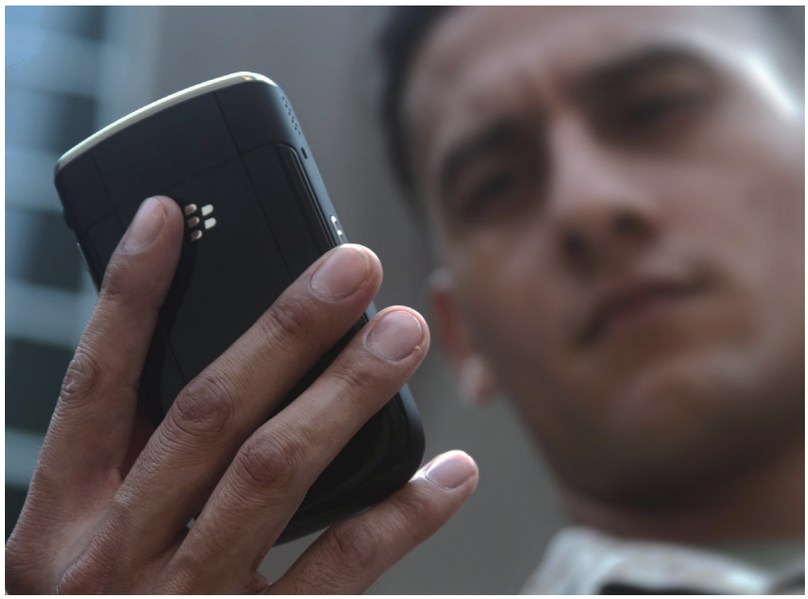
在中國大陸，當局同樣致力於嚴格控制國內的資訊流通，同時也操縱資訊以影響海外社會。中共要求國內所有單位密切合作，來保護網路空間和資訊空間；透過審查異議與限制外國科技廠商

進入中國大陸，以建立「和諧的網路」；對外提倡「中」式網路主權和「防火長城」概念。中共建立「國家互聯網資訊辦公室」等數個機構以推動資訊戰略，並制訂管控網路與資訊空間之整合性措施，共軍在其中亦肩負多項任務。

上述協調一致的資訊戰略係由高層發起。中共領導人習近平曾強調「話語權」(Discourse Power)的重要性，亦即創造和傳播符合國家利益的論述並壓制威脅國家的言論。例如，中共相關企業先前在許多非洲國家買下獨立媒體，繼而鼓勵刊載有利中共的論點並消除負面內容。2019年，中共政府相關人士曾在臉書、推特和YouTube等社群媒體上操縱香港抗議活動的相關言論。中共官員和媒體也曾試圖引導有關2019年底新型冠狀病毒疫情爆發的報導；他們壓下防疫失敗的新聞(將3位華爾街日報記者驅逐出境以報復該報刊載中共起初隱瞞疫情的社論)、散播陰謀論(指稱病毒係由美國生化武器攻擊所造成)，並利用美國總統川普在疫情問題處理上缺乏透明度，以妝點中共成為疫情處理的優等生。

中共外交官向來發言謹慎，近期則在網路上採取更為強硬的態度，許多中共官員也開始利用推特在中國大陸境內遭封鎖的現況，將推特作為霸凌外界的管道。中共外交部發言人趙立堅是一位特別挑釁好鬥的外交官，藉由嘲笑美國對新疆人權問題的關切，為中共侵犯人權之行為辯護，也因而招致負評。他多次以美國種族歧視問題為例，辯稱美國才有人權問題，而不是中共。與此同時，中共加強脅迫力道控制海外言論，對許多企業施壓，要求避開「敏感」話題，否則將無法繼續在中國大陸經商。2019年，由於休士頓火箭隊總經理推文支持香港反送中運動，多家中共企業竟以終止合作贊助和轉播等手段對美國NBA實施報復。NBA為保住大陸市場，火速向中共道歉。在此事件發生前，萬豪酒店、賓士汽車，以及多家航空公司均曾遭遇類似情況。中共官員還因為負面報導而威脅外國媒體，例如，中共駐瑞典大使因媒體報導中共拘禁異議書商而威脅瑞典媒體。中共並於2020年3月發布驅逐美國《紐約時報》、《華盛頓郵報》和

美國NBA因休士頓火箭隊總經理推文支持香港反送中運動，曾遭中共終止合作與贊助。圖為NBA賽事一景。(Source: AP/達志)



俄羅斯政府是否透過其企業發表之變臉程式FaceApp蒐集全球人臉辨識資料，引發不少質疑。(Source: DVIDS)

《華爾街日報》所有記者的決定，據推測是中共為報復川普政府決定限制其官媒駐美人數之舉，也造成這場全球新聞自由戰爭更趨白熱化。

全面開戰

中共和俄羅斯將網路安全與資訊安全視為一體的兩面，俾利在多個層面上控制和操縱資訊。在中國大陸，政府與私營部門在開發與應用新科技方面，合作比以往更為密切。北京與莫斯科除為新興科技挹注大量資本外，並以國家戰略利益為依歸，主導科技發展。

中共與俄羅斯企業已開始發展可供全球使用之新科技和應用程式。2019年，俄羅斯公司設計並發布了一款備受歡迎之變臉程式FaceApp，但俄羅斯政府是否可能透過該程式從全世界蒐集人臉辨識資料則引發質疑。該程式演算法亦可透過資料訓練用以優化或查禁特定內容，如在中國大陸境內最新資訊監管規定中已採用這項資訊管制功能，且顯然透過抖音(TikTok)等流行影音分享平臺而將此功能擴及全球。

北京正在其「社會治理」(Social Governance)範疇內開發AI監視科技，如新疆省穆斯林少數民族所遭受的待遇即為例證。這些少數民族受到科技全面監視，若有不忠誠之嫌，即被迫進入集中營。此外，北京也將監視科技應用於全中國大陸，並搭配根據個人行為表現評分的「社會信用體系」(Social Credit)。與此同時，北京正在向其他國家出口監視科技。這些科技通常被稱為「安全城市」(Safe City)計畫，據稱可提供高科技公共安全系統。儘管俄羅斯在AI發展方面落後中共，但俄羅斯總統普丁已試圖迎頭趕上，大力投資研究AI並擴大與中共之合作夥伴關係。

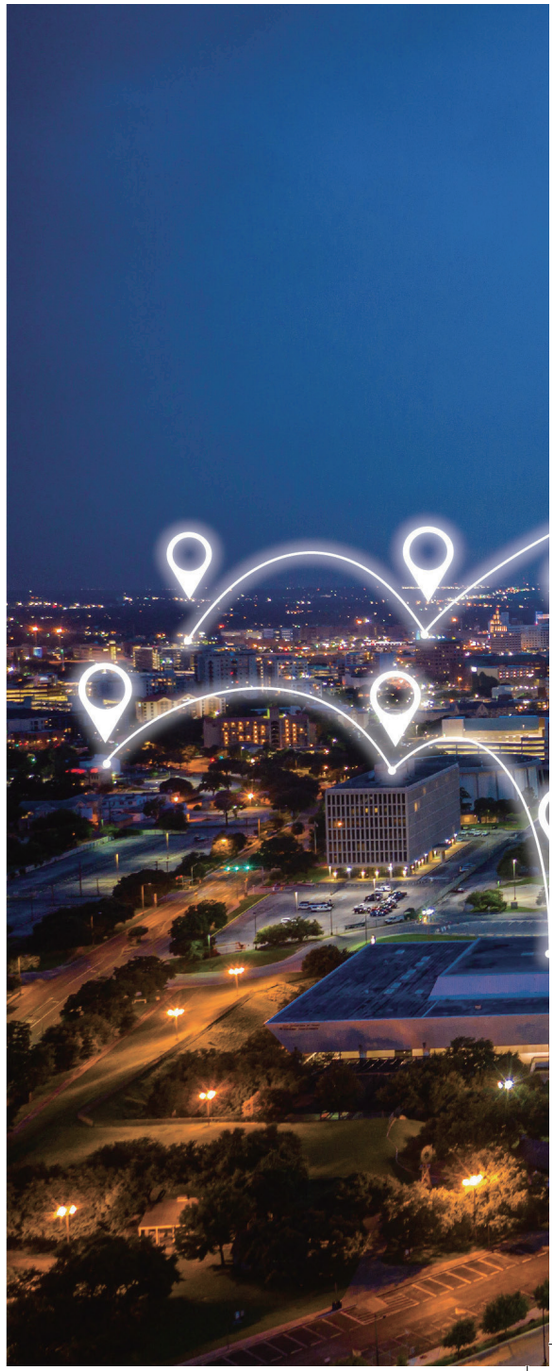
開發人員為強化演算法並提供機器學習所需資料，對各種來源資料之需求程度與日俱增。中共與俄羅斯之科技出口使兩者得以在資訊平臺、應用程式以及監視系統等方面，打造全球資訊架構，蒐集更多數據，以加強訓練AI應用程式與發展更為精確的方法管控資訊。中共所謂的「數位絲路」(Digital Silk Road)為一科技平

臺，表面上是為支撐其以基礎設施和投資所驅動之「一帶一路」倡議，事實上乃是對外出口網路和平臺科技，並藉以主導他國資訊管理基礎設施和規範的手段之一。中共向全世界推廣5G行動通訊設備之作為，將使其電信公司得以蒐集大量數據，且相關資訊可與中共黨國各單位分享。中共政府長期支援華為這家銷售電信設備、智慧型手機以及電子產品之科技公司，把華為養成了世界級巨獸。中共也在西方民主國家散布其監視科技。法國城市馬賽(Marseille)目前正與其中興通訊公司合作建立公共監視網路。雖然中共是全球資訊基礎設施的較大出口國，但俄羅斯公司也朝向包括伊拉克與墨西哥等許多國家，出口成本較低的網路監控技術。

除了數位基礎設施，中共與俄羅斯也正在其他國家建構傳統的媒體網，將官媒頻道拓展至非洲、拉丁美洲以及中東，同時與傳媒發展夥伴關係，以散播有利此兩國之內容。例如，中共已投資南非之獨立媒體；其「四達時代」傳媒集團已在非洲30個國家開展業務。這些媒體多半擁有廣大的網路聲量。中共國營媒體企業控制了一部分成長飛快的臉書粉絲專頁(Facebook Pages)；俄羅斯在YouTube的英語頻道「今日俄羅斯」(Russia Today)則累積了高度人氣。中共與俄羅斯的官媒合作日益增加；特別是在批評美國方面，雙方經常一鼻孔出氣。例如，俄羅斯官媒衛星通訊社(Sputnik)與中共《環球時報》和新華社之間，簽有合作協議，相互分享阿拉伯文與西班牙文報導內容。俄羅斯衛星通訊社與新華社也彼此唱和，指責美國煽動在香港和俄羅斯的抗議活動。

控制架構

政府對數位網路架構的控制也讓獨裁者得以限制其國內的資訊流通。俄羅斯依據2019年生效之「網路主權法」(Sovereign Internet)將國內網路流量集中管理，並建立類似中共「防火長城」的節點(chokepoints)，讓莫斯科可將俄羅斯境內的網路完全與境外隔絕。許多國家，從伊朗等專制政體到印度等民主國家，在面對動盪時均曾關閉網路以限制資訊流通。中共發展獨立的網際網路根系統(Internet root system，係導引網路流量之數位機制)，是為其邁向「分叉互聯網」(Bifurcation of



the Internet)之途上關鍵的一步。藉由發展控制部分網際網路之能力，中共可將網路連線轉變為地緣政治武器，迫使各國遵從其條款和條件，例如威脅中斷提供他國的5G行動通訊服務，此種手段亦可能在其未來地緣政治操控上發揮影響力。

數十年來，美國及其盟邦致力發展自由開放的網際網路，現在中共和俄羅斯則提出了另一種模式。其可控之「主權網路」願景，可給予採用的政府極大控制權。2019年秋，俄羅斯與中共等國家聯手，促成聯合國大會支持國際網路犯罪條約草案，該案以國家主權和審查制度為架構，使政府可強力監管網路資訊內容。儘管美國反對，但該

美國及其盟邦致力發展自由開放的網際網路。例如近期美國國防部選定聖安東尼聯合基地等12處，發展5G行動通訊科技。(Source: DVIDS)

聯合國決議案在許多非洲，亞洲和拉丁美洲國家支持下得以通過。中共和俄羅斯拉攏了此大團體的許多成員，包括蒙古、奈及利亞和南非等國。故「新美國」(New America)智庫的學者稱這些國家為「數位決策者」(Digital Deciders)。迄今，這些國家尚未表態將採取民主式或專制集權式的網際網路。

此外，北京正與他國合作，發展以中共法律為藍本之「主權網際網路」法律架構，支持由政府對資訊流通進行更嚴格的管制。此架構下法律多著墨於審查制度與移除敏感內容，並要求數據資料必須儲存於特定國家內，可說是樹立了保護主義的壁壘，讓政府得以遂行監查。這些法律時常搭配中共科技與網路基礎設施的進口。北京亦經常對外國官員進行媒體與資訊管理以及資料使用方面的訓練。

民主的困境

美國在研析網路世界架構等許多方面，態勢均處落後。華府視資訊競爭僅為戰術層級之競爭，且未能體認到這些競爭有三種整合層面：資訊(言論的傳播、控制和操縱)、架構(傳輸、排序和蒐集資訊的系統和平臺)，以及管理(法律與規範，在特定情況下可包括內容、數據和科技等相關標準)。況且，美國仍未明瞭網路與資訊空間領域日漸整合，而中共和俄羅斯卻已了然於心。

儘管華府於2018年發布「國家網路戰略」(National Cyber Strategy)指出了資訊作戰的威脅以及威權國家對開放網路引起之挑戰，但其大部分內容仍聚焦於傳統的網路安全觀點，侷限於網路的運作。2020年，由負責設計新戰略以保衛美國網路空間的兩黨聯合跨政府機構「網路空間日光室委員會」(Cyberspace Solarium Commission)發布了一份報告，此舉使美國向前邁出了數步。該委員會雖已建議美國在開發新興科技與反制資訊作戰等方面，應採取更為協調一致的作為，但並未著墨於如何管理資訊與數據資料等議題。2017年，時任美國國防部長馬提斯(James Mattis)堅認，美軍應認知到資訊在廿一世紀戰爭與大國競爭中所扮演的重要角色。雖然美國民間機構多有參與網路空間管理與資訊戰略制定，但其僅在軍事領域內耕耘，並未發展為整合性國家戰略，俾利於資訊空間遂行競爭。全球資訊戰大多發生於民用網路，且以平民百姓為目標，然此領域不屬於美國政府傳統管轄範圍之內。迄今，華府未能運用有系統的方式，與私營部門和民間社會相互合作。

美國等民主國家不能套用中共和俄羅斯之方法，也必須採取有效方法從事資訊競爭，並且不扭曲資訊或箝制民主開放的社會。若民主國家開始管制資訊內容並加強控制網際網路架構，則民主體制將受到破壞。在資訊戰中，堅守民主價值不僅是對的事情，也是戰勝獨裁政體所不可或缺之要素。

資訊競爭係由於民主體制與威權國家根本上的不對稱所導致。獨裁者在控制和操縱資訊方面看到了巨大的利益，然而對民主國家而言，如此行徑會侵蝕其體制與價值的基礎。民主國家依賴自由開放政治言論的同時，為對手提供了侵入其資訊生態系統之機會。這樣的生態使民主國家在

因應敵手之惡意作為上受到限制。若民主國家採取北京和莫斯科的戰術，或接受威權國家將此競爭定位為資訊戰，則意味著民主國家屈服於獨裁政體且競相沉淪，必將導致失敗。民主政體的挑戰在於挫敗專制主義，而不是隨之起舞。

外國勢力並非對自由與開放之公共網路空間唯一的威脅。一些資訊環境遭到入侵且混亂，充斥著仇恨言論、極端主義以及虛假資訊，這些情況已從內部削弱了民主政體，且腐蝕了其所自稱的高道德標準。從白人至上主義(White Supremacist Manifesto)、反疫苗陰謀論的散播、政客傳播深度偽造(Deepfakes，以下簡稱深偽)技術影片、網路上婦女所遭受的騷擾，以及民選領導人利用社群媒體傳布謊言等種種亂象可知，在網際網路平臺上瘋狂轉傳和極端之內容大量增加，鼓勵和健康之民主言論相左的行為。

美國開創之新數位經濟在欠缺足夠保護下，可能戕害其長期以來對隱私權與個人權利的保護。學者祖柏芙(Shoshana Zuboff)所稱之「監控資本主義」(Surveillance Capitalism)，亦即民間科技公司將人們使用經驗轉換為新經濟之燃料；此行為縮小了民主體制與中共等專制政體在數位科技應

2017年，時任美國國防部長馬提斯堅認，美軍應認知到資訊在廿一世紀戰爭與大國競爭中所扮演的重要角色。圖為美空軍人員執行資訊系統作業。(Source: USAF/George Goslin)

用方面的差距。之所以形成「監控資本主義」係由利益所驅使，而中共無所不在的監控系統則是為了鞏固政府控制。而這兩種監控形式均以蒐集海量資料為優先，可引導並塑造民眾之觀點。由於民主政府未採取行動來限制監視科技使用，這些工具在許多民主國家中，正在侵蝕隱私權範疇的臨界點；例如，監視學生在其宿舍中之生活作息，或透過社群媒體蒐集圖像進行人臉辨識。儘管有些城市已禁止使用人臉辨識科技，但如倫敦等其他城市卻正採用這項科技。華府在規範新興科技上採取放任態度，對改善當前情況並無助益。當民主政體無法提出明確替代方案以區隔威權政體之作法，大眾將益發認為美國所開發的數位科技與中共正發展之相關科技，兩者間並無差異。

針對這些挑戰，歐洲官員已開始呼籲採行新方法加以因應。法國總統馬克宏(Emmanuel Macron)表示，希望尋求一個「新途徑」，而非政府允許民間公司制訂具重大社會與經濟影響力之決策的「加州式自由網路」，也不是由政府推動創新並掌控一切的「中共式網路」。法國與歐盟官員已開始分別闡述此第三方案的原則，包括許多可行的概念。但是，由於此方案架構係著眼於保護歐洲「主權」，不禁使人想起北京與莫斯科的華麗辭藻，且方案未能明確區隔出民主模式。對美國官員而言，最感困擾的是，歐洲官員正尋求新模式以使其國家疏遠美國，而非致力於建構更

美軍持續提醒軍人及其眷屬，慎防不肖分子利用社群媒體進行詐騙或侵犯個人隱私權。(Source: DVIDS)

廣泛的民主架構。由於美國拒不處理自身的缺點且正在退出世界舞臺，因此並未參與這些重要討論。

尋求謙虛的力量

美國不應繼續將領導權讓與私營部門，而必須致力解決棘手問題，在保護民主價值觀之際權衡取捨，保持國家科技競爭力，並在防止資訊落入專制政權手中的同時，保持相對開放之資訊流通。此外，華府必須謀求在不傷害美國公司創新能力或破壞自由市場的情況下，與私營部門間強化合作之道。

美國不應僅專注於反制虛假資訊和技術專制主義，而必須採取更積極的態度，建設有利於民主國家的資訊生態系統。為達此一目標，美國需要與民主夥伴共同合作，開發合乎時代且展現民主原則的資訊模式，並且不由公司或政府，而是由個人管理其蒐集與運用相關資訊之方式。為了在資訊競爭中勝出，華府必須將政府機構編組並賦予資源，同時，特別在新興科技方面，政府與私營部門之間需發展新的合作方式。

在採取作為之同時，美國必須抱持謙虛態度，承認其對資料隱私權與科技監管的冷漠態度，使其建立自由開放網際網路願景之路困難重重。勇於承認疏失，繼於國內強化對隱私權之保護與對科技公司之規範等作為，華府才有機會與歐洲諸國，特別是民主盟友共同打造多邊聯盟。各國應繼續支持自由開放的網際網路，以反制專制政權

作者認為美國應持續參與國際網路重要討論。圖為2018年9月28日，美國於聯合國大會第73屆會議期間，與各國召開部長級會議討論國家網路責任議題。(Source: US State Department)

為謀求控制而散播「主權網路」，此事至關重要。與此同時，惡意行為者正利用民主之權利與自由以破壞民主，民主國家亦必須對此有所認知並加以因應。美國在制定新架構時，須優先考量數據資料的隱私權，並讓演算法透明化，使民眾個人可自行決定網路隱私權限。另外，此架構更應能平衡政府、科技公司以及個人之間的權力。這些措施將與威權體制所採取之模式形成鮮明對比，提供具吸引力的替代方案，並防止更多國家遭中共未來「分叉互聯網」的誘惑。

上述作為成功與否，有賴美國政府重新調整其處理問題的方式。美國不應模仿中共或俄羅斯的架構；但是，美國政府目前並無任何單位有權限權力或資源可因應全面資訊競爭。美國國家安全會議(National Security Council)應規劃一個由文官體系領導之跨部會方案，採取網路、資訊與新興科技相關整合作為，同時亦應協調各政府相關機構，並與私營部門發展新的合作機制。美國國防部已將資訊競爭列為優先要務，國會亦已賦予其新權力，俾利於資訊環境中遂行軍事行動。例如於2018年期中選舉前，向美軍已知的俄羅斯網路特工先期發送警告訊息。但是國防部在資訊競爭所扮演之角色應有所節制，若將此競爭軍事化，盡如威權主義者之所願將資訊變成武器，不啻將正中其下懷。

今日，外交斡旋多半並非在閉門會議內進行，而是見於公共場所。因此，美國必須使外交人員在訊息傳遞方面，擺脫官僚主義傳統之緩慢步調，使其可藉由參與公共事務來作為核心任務之一，整合科技做為拓展觸角之工具，從而能在現代的資訊空間中保持靈活。美國官員應利用公開報導與贊助獨立媒體等方式，揭露威權主義者之惡性與強制性資訊活動。美國政府及民間領袖必須反制境外的資訊審查，支持受獨裁政體威脅之公司，並將未公開之自動審查科技公諸於世。華府應在多邊管理體系中發展網路空間與資訊空間之民主原則，藉以遏止威權體制模式之擴張。此外，美國應投資其公民社會，保護自

美國國防部已將資訊競爭列為優先要務。圖為2019年12月，美海軍舉辦論壇，邀請民間企業專家共同研討並精進海軍資訊管理作為。(Source: USN/Kevin Casey)

由與獨立媒體，並支持有關資訊空間之研究。

在此項工作中，私營部門扮演了重要角色，包括實現公私合作之新模式。科技公司和傳統媒體必須理解惡人如何將其商務轉變為地緣政治的戰場。與此同時，政府則不應將科技競爭視為一場價值中立(values-neutral)之搶占主導權活動。舉例而言，若將在AI系統方面的競爭視為軍備競賽，則系統之發展將產生與民主治理及價值觀完全相悖之風險。相反地，政府及私營部門應共同推動創新，以促進言論自由與隱私權的民主價值，保護自由市場，制止惡人篡改資訊的企圖，並提供具競爭力的替代方案以取代威權政體發展之科技。政府和私營部門可就符合倫理之方式使用面部辨識科技發展相關原則，並刻正合作發展科技，用以檢測深偽技術影片，亦即經AI編造之不實影音。

由於基礎研究經費的節節下降以及中共在促進創新上的積極參與，美國在新科技發展方面正面臨落後的風險。政府應將如AI及量子運算等新興科技列為優先事項，並籌募資金俾與民間企業合作研發，同時，致力加強培訓和吸引海外頂尖科學家與工程師。美國亦應限制可能嚴重妨礙民主治理與人權的科技，首先是暫停使用面部與步態識別技術，因這些科技需要受到明確規範所監督以防止遭濫用；其次則是更嚴格的使用和管理AI。對於個人隱私權問題，亦可能有科技解決方案：例如，更尖端的機器學習模式或可減少對大量個人數據資料之依賴。美國及其民主盟邦亦應優先考慮採取多邊方式，與私營部門合作，俾利加強影響國際電信聯盟(International Telecommunication Union, ITU)等國際標準制定機構，尤其在該聯盟指導全球新興科技使用之方面。

美國迫切需要在資訊競爭中採取主動。隨著科技演進以及更多國家採行數位威權戰略，未來的挑戰將愈形艱難。隨著資訊空間遭破壞、分割和嚴格管制的情況日益嚴重，美國將更難擁有彈性來反制外部威脅。由於冰箱、汽車以及咖啡機等多種電器已可連網，而成為物聯網的一部分，數位科技將更深入的管理人類日常生活。更糟糕的是，對數位科技的依賴將有風險扭曲對現實之認知，如深偽技術可導致大眾失去對現實的共識。隨著威權體制科技及資訊管理模式的傳播，民主政體在此範疇的行動空間將愈顯促狹。

最後，網路空間競爭的成功與否，最大障礙可能是國內民主制度的退化。將資訊作為武器使用且不顧民主治理原則的國家領導人，將使其社會失去彈性，不但發展不出取代威權模式的資訊選項，更將加速邁向獨裁者所圖謀劣化資訊空間之途。在資訊競爭中，倘若美國領袖未具體推動民主願景，這願景終將難以企及。

作者簡介

Laura Rosenberger現任保衛民主聯盟計畫(Alliance for Securing Democracy)主任以及德國馬歇爾基金會(German Marshall Fund of the United States)資深研究員。她曾於美國國家安全會議與國務院任職。