



● 作者/Sarah Jacobs Gamberini

● 譯者/李永悌

● 審者/馬浩翔

社群媒體武器化

Social Media Weaponization

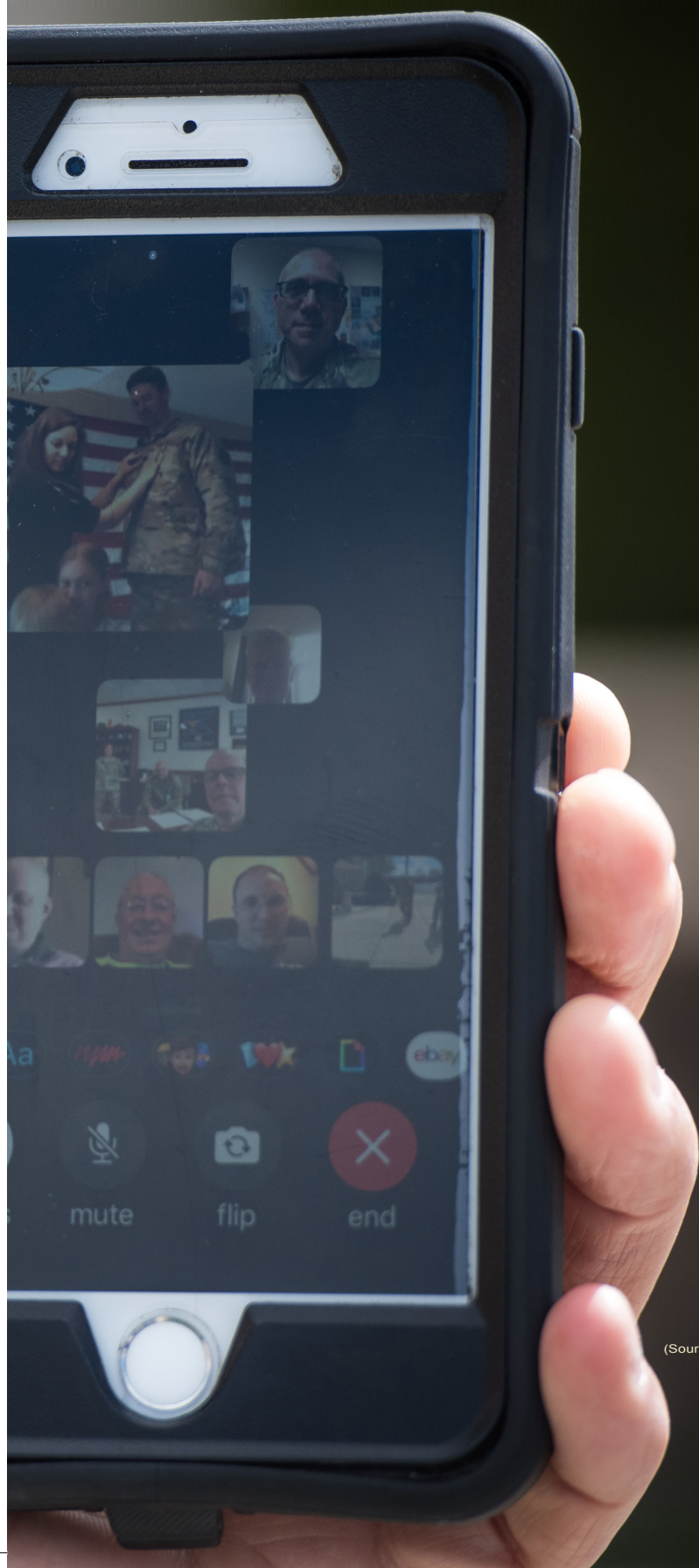
取材/2020年第四季美國聯合部隊季刊(*Joint Force Quarterly*, 4th Quarter/2020)

政府應致力提升人民社會媒體素養，教育其認識資訊攻擊與分辨假資訊，避免敵人利用社群媒體擴大歷史傷痕與歧見，破壞和諧與穩定。

在全新的大國競爭時代，美國面臨來自諸多領域、不分傳統戰爭與和平界線的敵人。美國的競爭對手經常以低於引發軍事反應門檻的方式從事活動，其中也包括資訊戰場。外國行為者於網路暗中發動資訊作戰導致戰爭界線模糊，將迫使美國作戰與社會消化資訊的方式改變。早在社群媒體問世之前，俄羅斯即已透過影響力與脅迫戰術，不僅能以無所不在的方式接近目標，還有足夠能力就一系列敏感社會問題，包括公共衛生問題，掌控敘事(Narrative)與操弄群眾的內心與思想。

俄羅斯長久以來試圖投射權力與影響力，同時運作技術與地緣政治等不利條件。有鑑於其歷史和與諸多國家毗鄰的地理位置，俄羅斯認為自己經常面臨四面楚歌之境，特別是遭到西方國家圍堵。自蘇聯解體低潮以來，俄羅斯即致力重新平衡權力，同時降低美國的影響力。惟在缺乏對等傳統軍事力量的情況下，俄羅斯轉而尋求以其他不對稱優勢補強對美國的競爭。社群媒體提供了操縱敘事與擴大社會分歧的獨特工具，以前所未見的方式削弱美國。儘管俄羅斯將資訊武器化(Weaponization of Information)絕非新鮮事，俄羅斯的假資訊(Disinformation)、公共衛生危機與生物事件(Bioevents)漏洞等作為，同時為美國帶來全新且令人憂心的國土





2020年6月5日，美空軍第27特種作戰聯隊公共事務播音員威廉斯(Marcel Williams)下士於新墨西哥州加農(Cannon)空軍基地的「團結集會」(Gathering for Unity)活動中分享其族群遭受種族歧視的經驗。(Source: USAF/ Lane T. Plummer)

(Source: US Air National Guard/ Tony Harp)



與國家安全威脅。

美國是多樣、多元且民主的國家。這些特質是美國立國的原則，也是其作為國家的優勢。惟對包括俄羅斯等美國的敵人而言，這些特質反而成為可資利用的潛在弱點。俄羅斯影響力作戰(Influence Operations)的戰略目標之一為削弱美國及其盟國的力量；俄羅斯認為，這些國家的活動過於接近其勢力範圍，亦即其所稱的「近鄰國家」(Near Abroad)。¹ 俄羅斯屢次運用眾所周知的影響力戰術散布假資訊，企圖削弱美國的民主社會並詆毀美國在世界舞臺上的聲譽。² 從2016年介入美國總統大選，到2020年新冠病毒全球大流行期間散播假消息，俄羅斯不斷利用假資訊分化美國，加深美國國內的不和並破壞其體制。由於俄羅斯以此方式鎖定公共衛生問題，對美國人民與醫療體系將產生重大影響。目前全世界正與「資訊傳染病」(Infodemic)與新冠病毒疫情奮戰，兩者皆需要採全社會(Whole-of-Society)動員才能有效解決。³

遭受圍困的俄羅斯

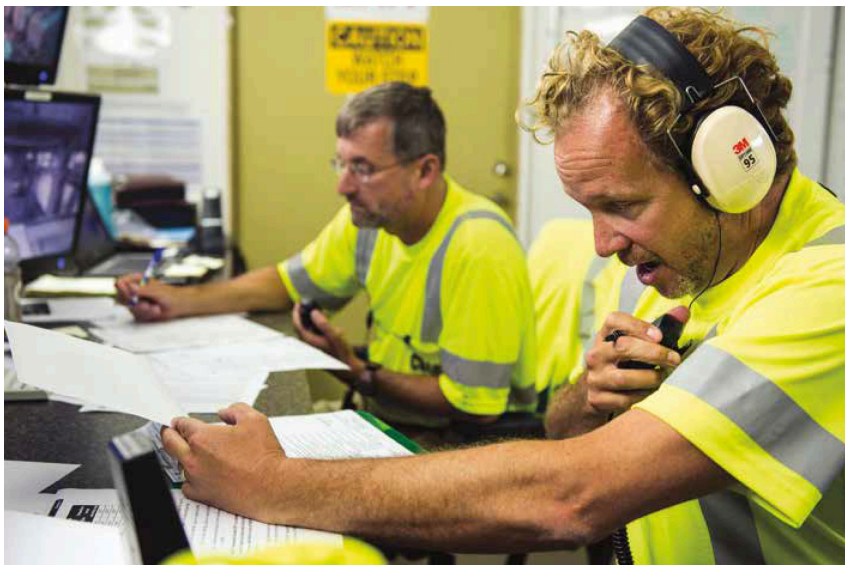
數個世紀以來，俄羅斯曾經歷條頓騎士團(Teutonic Knights)、拿破崙與納粹德國的攻擊，以及自冷戰結束後美國與北大西洋公約組織(North Atlantic Treaty Organization, NATO，以下簡稱北約)的蠶食。俄羅斯認為美國、北約與歐盟致力削弱其國力，消除其勢力範圍，並確保美國與西方國家擁有單方面長期優勢。⁴ 此種判斷係因俄羅斯堅信美國已違背其前國務卿貝克(James Baker)在蘇聯解體後表示北約「絕對不會東進一步」的承諾。⁵ 俄羅斯宣稱，西方國家於烏克蘭革命期間的「干預行

為」，已進一步證實美國與北約過分介入其影響範圍。⁶ 俄羅斯將此種對其近鄰國家的蠶食鯨吞視為無法接受的公然侮辱。⁷

俄羅斯認為，西方國家的優勢表現在社會與文化(例如西方國家的娛樂產業試圖取代俄羅斯的文化、價值觀與語言)、政治(西方國家在俄羅斯與前蘇聯煽動「顏色革命」[Color Revolutions])與軍事(美國以擴張北大西洋公約組織在地理上包圍俄羅斯，並以飛彈防禦系統與軍事基地在技術上圍困俄羅斯)等層面。此外，俄羅斯長久以來憂心自己的科學與技術落後西方國家。有時俄羅斯就某些防禦平臺做到勢均力敵，但整體上卻是苦苦追趕在後，故其極度仰賴傳統大規模毀滅性武器，例如為數可觀的核子武器庫存，藉以抵銷美國的常規武力。俄羅斯在民用技術方面亦同樣落後。而其背後隱藏著大量且令人憂心的人口與健康難題(因非自然因素，包括普遍存在的酗酒問題，導致出生率持續降低與死亡率增高)。⁸ 這些因素導致俄羅斯認為自身始終處於遭受圍困與物資匱乏的狀態。

當前俄羅斯世界觀的形成與發展，大多以前總理普里馬科夫(Yevgeny Primakov)拒絕美國霸權、追求多極世界，並重新將俄羅斯打造為前蘇聯地區主要區域大國的信條為基礎。⁹ 冷戰結束後，俄羅斯必須以精算與創造性等方式平衡其經濟、軍事與技術劣勢，俾與美國競爭，並儘可能利用較非常規的戰爭工具，包括於資訊領域從事隱蔽行動。

冷戰期間，前蘇聯採取積極措施，以有異於間諜與反情報活動的脅迫方式來影響各國。這些積極措施包括假資訊、政治影響行動與控制媒體與訊息傳遞，其目標在於污衊與影響西方國家，同時呼



2014年6月16日，隸屬美國政府的雷角號(MV Cape Ray)貨櫃船厄齊塢生化中心(Edgewood Chemical Biological Center)控制室作業員，於西班牙羅塔海軍基地(Naval Station Rota)確認與記錄當前行動資料，該貨櫃船於改裝後派往東地中海處理敘利亞化學戰劑。(Source: USN/ Desmond Parks)

應俄羅斯當前戰術。¹⁰ 西方國家為此類作戰與其他尚未達實際動武門檻的措施賦予不同名稱，包括俄羅斯的不對稱、模糊地帶、混合或新一代作戰等。惟跨領域作戰(Cross-domain Warfare)一詞較能反映當前俄羅斯塑造安全環境的方法，亦即運用整合諸般軍事與非軍事工具的作法達成其戰略目標。¹¹

俄羅斯認為阿拉伯之春(Arab Spring)事件係由西方國家煽動，為因應此一運動，格拉西莫夫將軍(Valery Gerasimov，現為俄羅斯總參謀長)曾公開討論如何在

俄羅斯防止類似動亂發生。格拉西莫夫在其演說中提到資訊管制為致勝的關鍵。¹² 這場被誇大為俄羅斯軍事準則的演講確實描述了俄羅斯應如何在軍事、政治、網路與資訊戰等多重領域，同時進行作戰以實現戰略目標。2019年3月，格拉西莫夫在演說中談到作戰將轉移至資訊領域，並將資訊科技列為「最有發展潛力的武器之一」，不僅可暗中用在「至關重要的資訊基礎設施，還可用於對付國家的人民，直接影響國家安全狀況。」¹³

資訊只不過是跨領域作戰的

一環。這項俄羅斯構想的另一項重要論述，就是主張習慣上戰時與平時的分野已不復存在。這些模糊的界線已於演說或準則的範圍以外出現，例如俄羅斯以低於美國武裝衝突門檻的方式——於克里米亞(Crimea)及東烏克蘭(Eastern Ukraine)的「小綠人」(Little Green Men)武裝份子、於敘利亞的「獨立」私人軍事團體、於英國使用諾維喬克(Novichok，前蘇聯於冷戰時期研發的化學武器)神經毒劑，以及為數眾多的網路攻擊——進行此類惡意活動，此外還表現在秘密活動的本質與其他更多方面。惟由於俄羅斯矢口否認並運用烏賊戰術，使其責任歸屬與涉入程度陷入爭論，因而得以免於遭受軍事行動反制。

舊影響力作戰準則，新媒體工具

俄羅斯當前領導人擔憂，美國的資訊科技優勢讓其與盟國得以破壞俄羅斯的社會、文化與政治體制，作為其範圍更廣大的鬥爭方式之一，來確保西方國家地緣政治優勢。¹⁴ 克里姆林宮將資訊視為新式武器，並將所有平臺



上的各式資訊視為可資武器化的潛在力量來源。俄羅斯認為，西方國家正運用各式資訊科技對抗俄羅斯——包括透過衛星電視與網際網路，以俄羅斯視為公開反對國家的訊息持續轟炸該國人民，以及以社群媒體作為協調激進份子與間諜於前蘇聯國家從事反抗活動的工具。最後，俄羅斯將美國的太空、情監偵及其他資訊科技系統視為網路化軍事能力，其目的在概括瓦解所有科技適應性不佳的敵人。

俄羅斯採取數種方式應付此類資訊時代的威脅。該國致力打造「俄羅斯專用」網際網路，期能創造出類似中國大陸的俄羅斯版「防火長城」。¹⁵ 俄羅斯的新聞與宣傳工具(例如其國營電視網今日俄羅斯電視臺[RT]，以及諸如史普尼克[Sputnik]等線上「新聞」聚合服務[aggregator])即用於反制西方國家的有線電視新聞。¹⁶ 此外，俄羅斯在擁有自己的資訊作戰軍事系統之前，將同時以實體(例如反太空能力)與網路攻擊等方式威脅西方國家的資訊戰系統。¹⁷ 最後，俄羅斯政府積極從事的網際網路活動已遍及社群媒體領域，運用大量



2020年5月19日，美國加州馬奇空軍後備基地(March Air Reserve Base)美空軍第452後勤戰備中隊的運輸系統士官，準備將由美國國際開發總署(U.S. Agency for International Development)提供的50具通風器運往俄羅斯莫斯科。(Source: USAF/ Keith James)

俄羅斯網軍(Web Brigades)、酸民農場(Troll Farms)與自動化網路機器人四處進行宣傳活動與大量張貼主題標籤。¹⁸

俄羅斯善用社群媒體機器影響敵國與其人民，符合其認為任何資訊皆可利用的觀點。俄羅斯網路酸民(trolls)運用線上敘事的力量，置重點於鎖定團體凝聚力散發簡單訊息，如此一來其訊息就會被外國的目標分享並進一步擴散。¹⁹ 他們已深刻理解到強烈的情緒可在網路上迅速蔓延，而在正確的提示下，人們只喜歡主張與鞏固根深蒂固的觀念。²⁰

雷同於前蘇聯積極措施，俄羅斯社群媒體武器化的目的在煽動混亂，製造對美國體制不信任，並鎖定該國既有之分歧。這一切讓美國更難以在較傳統的領域建立反制俄羅斯的統一因應作為。

錯誤資訊與假資訊活動

美國人經常面對各類來自國內、外消息來源的假新聞。網路上的假資訊不勝枚舉，包括臉書好友出自善意卻未經思考分享自認為真的錯誤資訊(Misinformation)，以及更具惡意與針對性，

以刻意混淆與欺騙為目的之宣傳內容。因此，瞭解假資訊與錯誤資訊間的差異極為重要。假資訊是以惡意與故意為之的方式製造並散播虛假資訊，而錯誤資訊則是不慎傳播的錯誤內容。兩者皆為俄羅斯所倚重的工具。例如，讓不知情的網路用戶散播假資訊，即可從事惡意的錯誤資訊宣傳。

比爾蓋茲在1995年被問及有關在當時新興的「網路」上散播假資訊的問題時提到，拆穿假新聞相當容易，因為會有更多人查核在朋友之間傳遞的事實與資訊，這是更加值得信任的資訊交換活動。²¹ 然而就目前所知，讓錯誤資訊活動成功進行與假新聞蓬勃發展的，正是此種社群媒體的特質。另一項讓網路影響力作戰相當成功的重大挑戰是，資訊一經散播與消化吸收，就很難從人的思想中撤回。讓社群媒體在聯繫、分享與組織方面非常有效的工具，與讓惡意行為者濫用與操弄的工具完全相同。這項事實——加上對不待驗證研究與事實查核的即時新聞需求、社群媒體平臺分享的便利性，以及最能挑撥離間的主題往往極度情緒化的現象(例如公共衛生與種族關係)——讓美國成為此類社群媒體武器的完美目標。

俄羅斯運作社群媒體的模式有脈絡可循：找出有爭議的問題、運用網路機器人與酸民在各式社群媒體平臺散布製造分裂言論、擴大爭端與加深不和。²² 俄羅斯最為人所知的影響力作戰之一，就是介入2016年美國總統大選。惟莫斯科當局的影响力作戰並不僅止於美國大選，並已成為持續針對美國民眾進行的蓄意活動之一。在多樣、多元化的社會中，可用來借題發揮的社會歧見不計其數。

2019年有內部洩露文件透漏，俄羅斯考慮鎖定美國最深沉且歷史最悠久的裂痕之一：種族問題。這些文件顯示，俄羅斯考慮對一批非裔美國人進行作戰與陰謀破壞訓練，之後將這些人員送返美國，於美國南方建立泛非洲主義(Pan-African)國家，俾實際上分裂美國。這項從未頒布的計畫企圖「破壞美國內部狀況的穩定」。²³ 俄羅斯有認知，奴隸制度與其造成的數百年不平等是美國的原罪，也是可資利用的終極裂痕。俄羅斯在2016年美國總統大選之前，即已針對非裔美國人士進行影響力作戰，²⁴ 近期則是以主題標籤洗版推特網站——一種用於削弱相關內容正當性的技術——之方式利用「黑命關天」(Black Lives Matter)運動，進而占據作為抗議活動期間相互聯繫方式的社群媒體平臺。²⁵ 值得注意的是，俄羅斯的目標鮮少會針對任何問題表態支持任一方，而是煽風點火與火上加油——美國的自取滅亡將成為俄羅斯的大獲全勝。

俄羅斯資訊戰戰術目標並不固定，使其難以捉摸與反制。2020年6月，俄羅斯進行長達六年之久的大規模假資訊活動遭到揭露。該行動運用新方法鎖定西方國家與烏克蘭，議題的範圍從否認俄羅斯在國際體育賽事中使用禁藥，到更大規模歌頌俄羅斯與其政府，並凸顯美國與北約對其他國家的侵略與干預。²⁶ 這項命名為「續發傳染」(Secondary Infektion)²⁷ 的行動係向「感染行動」(Operation Infektion)致敬，猶如重啟1980年代冷戰時期的假資訊活動，當時蘇聯即利用惡意訊息宣傳美軍研發愛滋病毒作為戰爭工具的陰謀論。²⁸ 值得特別關注的是，俄羅斯在續發傳染行動期間使用



的方法為大量「分身」帳號(“Burner” Accounts)，這些帳號於發布單一誤導性推文後即棄之不用。相較於以往建立具有追隨者、信譽力與公信度的社群媒體帳號的作法，此舉代表俄羅斯認定美國人民毫無媒體素養、無法辨別假新聞，也不願做比單獨推文還要更深入的研究。鮮少有人會花時間追查資訊來源，而截至目前為止，俄羅斯的假說已證實為真。²⁹ 如同瞭解俄羅斯的目標與方法般，社群媒體代價低廉與無所不在的本質，已讓假資訊活動能視需要轉移與適應社群媒體演算法的變化。此外，社群媒體還能釋放大量虛假與有害的資訊，即便成果微不足道，卻還是能產生巨大影響。

擴大公共衛生爭端

俄羅斯顯然知道如何找出、利用與擴大美國的政治壓力與國家的種族創傷，加上其他的裂痕與歧見。公共衛生是美國另一個爭議激烈的領域，也是俄羅斯鎖定的理想目標。公共衛生問題同時關係著個人與社會，因此任何相關主題的討論往往充滿情緒，並渴望盡速獲得資訊。相較於中立客觀的機構，人們通常更信賴朋友、家人或意見領袖(Influencer)在健康方面所給予的建議。美國國家衛生研究院(National Institutes of Health)的研究發現，「美國每十位網路使用者當中，有八人會上網搜尋健康資訊」。³⁰ 這讓諸如新冠肺炎(COVID-19)或麻疹等公共衛生問題，成為俄羅斯社群媒體武器化的理想目標。此種具有離間性與情緒性的武器可實際削弱美國的力量。

反疫苗接種(anti-vaxxers)運動所信奉的理念是

最好不要接種疫苗，否則最壞的情況將造成包括自閉症和癲癇發作等身體傷害。對政府當局的嚴重不信任，加上網路上存在的回音效應，造成錯誤資訊在朋友圈迅速傳播，益發助長如此運動。由於所有關於疫苗的假新聞皆極為成功，故實際上更難以反制。諸如麻疹等疾病已被視為過去早已根除的歷史遺跡，而且不會觸及現代美國社會。惟美國部分地區正經歷自1992年以來最多的麻疹病例，而極大比例的人口卻選擇不接種疫苗。³¹ 疫苗可透過群體免疫(Herd Immunity)奏效，惟仍須視疾病的傳染性而定；當社會上一定比例的民眾接種疫苗後，即可保護少數因各種原因而無法接種疫苗的人士(例如兒童、懷孕婦女與其他弱勢族群)。

就傳染性如麻疹等疾病而言，群體免疫只有在大約94%的人口接種疫苗後才會發生；甚至連疫苗接種人數的微量變化，都有可能導致此一已於2000年宣布在美國境內絕跡的疾病死灰復燃。³² 對疫苗的錯誤恐慌，將導致先前已銷聲匿跡的疾病削弱社會大眾的健康。³³ 如今，全世界正致力應付引發嚴重特殊傳染性肺炎的新型冠狀病毒，但社會上大多數人卻不願瞭解如何保護自己與周邊社群。若美國人民一再反對支持為何口罩與保持人身距離(physical distancing)為良好預防措施的科學見解，即可預見一旦有疫苗可用，就會有人對其表示懷疑。由於疫苗研發頗有成就，美國已陷入虛假的安全感。

在外敵尚未試圖將其擴大前，這些公共衛生危機即足以駭人聽聞。美國《公共衛生期刊》(*Journal of Public Health*)披露——由普里格欽(Yevgeny Prigozhin，俄羅斯總統普丁[Vladimir Putin]的摯友)

主導，並於穆勒(Robert Mueller)針對俄羅斯干預美國大選的調查報告中指控的——俄羅斯網路研究局(Russian Internet Research Agency)，就是運用網路機器人與酸民散布有關疫苗接種假資訊的幕後黑手。³⁴ 該期刊在分析中提到，俄羅斯網路機器人與酸民在推特發布數量相當的支持與反疫苗推文。而其目標似乎是引發爭論，並讓人們各自選邊支持，進一步確立自身觀點。俄羅斯的目標是將爭論擴大與常態化，並牢牢地深化歧見。施打疫苗爭論的常態化對健康造成的後果可能並非俄羅斯的主要目標(這不過是副產品)，惟俄羅斯可能以冷酷無情的方式斷傷美國人民的健康，作為其影響力作戰的次要效果，這確實可惡至極。鑑於此類活動與俄羅斯總統的關聯性，意味著必須進一步關切該國將如何支持此類活動及其對美國的因應作為有何意義。儘管如此，否認與卸責是普丁在此一領域取得成功的關鍵。

新冠肺炎大規模流行期間，俄羅斯同樣對美國運用可預期的戰術挑起恐懼與混亂，並破壞

美國的因應作為。俄羅斯官方媒體、網路酸民與機器人散布虛假的敘事，包括各種病毒來源的陰謀論，諸如由移民引發、美國的生物武器，或美國製藥公司為圖利所製造，甚至該病毒本身就是騙局等。³⁵ 此外，中共的假資訊運用——歷史上一直著重在國內宣傳，並製造中共及其威權政府仁厚強大的說法——於疫情期間師法俄羅斯影響力作戰準則，從最初淡化與否認該疾病的宣傳式回應，到一切完全是陰謀論與假資訊，包括病毒係由美陸軍人員於類似奧運會的2019年世界軍人運動會期間傳入武漢等。³⁶ 這些作為更令人憂心俄羅斯影響力作戰對美國其他敵人的吸引力，並將持續作為眾多行為者的主要攻擊方法。

上述針對公共衛生的攻擊為美國國土與國家安全帶來威脅。反疫苗運動以擴大美國防疫的漏洞作為賭注。在預期一旦新冠肺炎疫苗問世後將如何如法炮製時，美國必須考量因來自國內、外有關疫苗的惡意訊息造成的影響。除了散播對美國醫療體系(例如包括疾病管制與預防中心[Centers for Disease Control

and Prevention]等醫院/檢測與政府組織)的質疑，這些活動還會造成對基礎科學(例如人們不願戴口罩以及可能不相信未來的疫苗)的懷疑。俄羅斯藉由擴大公共衛生爭端與不表態支持任何一方，讓以往否定疫苗與防疫基礎科學的非主流討論成為常態。由於與這些傳染病相關的科學事實可信度因有意或無意的謊言而降低，美國醫療體系正面臨信任危機。

反疫苗運動的擴大將帶來更長遠的影響。除了健康與體制問題外，亦造成美國醫療體系的損失和與隔離衍生成本。對於在這場危機中負擔過重的醫療保健專業人員，以及必須投入時間與資源反制此類假資訊的地方、州與聯邦政府而言，該運動是種干擾。此外，自然或國際生物威脅(包括因外敵炒作訊息而加劇的自然生物威脅)恐將抑制美軍對國外投射武力的能力。新冠病毒大流行凸顯美軍部隊感染如新冠肺炎的疾病時有多麼脆弱，而美國的敵人對此威脅已有新的體認。³⁷ 美國亦仰賴軍方的協助來擴充國內醫院病床容量，這些已造成資源過度消耗，也代表



理論上可部署的部隊更少。³⁸

反疫苗者的數量與/或影響力若增加，將削弱美國應付任何形式生物威脅——無論自然或人為——的能力。未來生物武器已不太可能是歷史上可武器化的戰劑，且更有可能針對平民。生物戰劑必須滿足造成廣泛與大規模影響所需數量與傳播方式，因此一直難以武器化。隨著冷戰時期大規模計畫的威脅性已不若恐怖威脅，以往裝滿生物戰劑的試管掉入地鐵的生物威脅狀況想定，已由真實世界中令人不安的疫情大規模流行場景所取代。

俄羅斯與其他美國的敵人當然已注意到美國對抗新冠病毒的漏洞。這一切代表對未來生物武器的全新憂慮，而其效果可進一步透過資訊戰加以實現。這些針對公共衛生的無差別資訊攻擊，顯現俄羅斯如何利用美國國內歧見，甚至到了危害公共衛生的地步。這些公共衛生攻擊亦凸顯美國面對的對手是多麼殘酷。美國在某種程度上必須認真思考此類對公共衛生的干擾，是否是由外敵所造成的生物威脅。

反制影響力作戰的影響

敵人擴大了準戰爭構成要素概念，每日於各種平臺對美國及其人民發動不對稱作戰。儘管俄羅斯針對衛生事務發動的資訊戰影響甚鉅，美國尚未將這些社會攻擊明定為戰爭，因此不致於引發軍事層級的回應。美國必須以全面性、全政府的解決方案反制這些行動，並在解決方案中加入全體社會意識。政府與企業可提高門檻，讓假資訊活動更加困難，民眾則可更有效獲得資訊，了解如何辨識錯誤與假資訊，進而降低其效果。縱使無法完

全遏止假資訊，其共同效果仍可導致俄羅斯的影響力降低。這項適用社會各個階層的解決方案必然錯綜複雜，且自始至終都需要具有高媒體素養且見多識廣的民眾配合。

政府可從旁協助，但無法單獨解決假資訊問題，也無法單獨解決公共衛生挑戰。2020年美國《國防授權法》(National Defense Authorization Act)要求美國國家情報總監(Director of National Intelligence)成立惡意外國影響力應對中心(Malign Foreign Influence Response Center)，針對外國影響力問題進行情報部門的協調與整合；惟截至撰寫本文時，該中心仍未獲授權成立。³⁹ 過去，美國致力在部分政府機構反制俄羅斯的訊息傳播，惟其通常僅限於處理公開宣傳活動，而不是現下面臨的低階社群媒體濫用游擊戰。冷戰期間，美國積極措施工作小組(Active Measures Working Group)的成立，不僅為了反制蘇聯的假資訊，也為了提升社會的敏感意識，使其能認識俄羅斯對社會的干擾。⁴⁰ 此種反制假資訊的全政府積極作為似乎可以及時恢復，或許可採用惡意外國影響力應對中心的模式。即便如此，不僅單靠政府本身勢必不足，只有情報部門參與也絕對不夠。美國國務院的全球接觸中心(Global Engagement Center)刻正致力識別、揭露與反制假資訊，惟如未能讓美國人民與美國的敵人有更深的認識，就無法完全成功。⁴¹

為反制假資訊，美國政府可採取的最有效措施之一就是傳遞前後一致的訊息，並就假資訊與公共衛生傳遞口徑統一，並且以科學為基礎的訊息。在嘗試於英國使用諾維喬克暗殺斯克里帕爾(Sergei Skripal)後，俄羅斯提出了數百種相互矛盾



2014年3月10日，烏克蘭鎮暴警察金鷹部隊(Berkut)於克里米亞半島(Crimean Peninsula)入口處的檢查哨部署兵力。(Source: Sasha Maksymenko)

的敘述來混淆、偏離與否認其參與其中。英國則是發出說法一致、以科學為基礎的訊息來協助揭露俄羅斯訊息活動中的謊言與前後矛盾，而不是只有見招拆招，試圖反駁每一項謬誤。⁴²

此外，美國必須大肆宣揚俄羅斯包括資訊作戰領域的跨領域惡行。美國必須以針對性制裁、於多邊論壇進行國際性譴責，以及其他不對稱應對措施直接回應這些威脅。儘管俄羅斯試圖否認其在上述活動中扮演的角色，美國與其盟國應在諸如聯合國安全理事會(United Nations Security Council)等場合上提出證據，以展示這些不良行為者與

俄羅斯政府間的關聯。由於俄羅斯在聯合國安理會中擁有否決權，預料將不會通過任何決議，惟如此高能見度的行動將向世界昭告俄羅斯的惡意活動，並可能號召其他國家協助阻止此一惡意行為者。美國不僅須透過方法，還須透過效果來評估俄羅斯的活動。若俄羅斯的社群媒體干擾活動導致社會大眾的身體羸弱，則美國必須考慮將這些行為視為更近似生物攻擊，而非網路攻擊。

產業夥伴將在這項解決方案中扮演重要角色。作為此類錯誤資訊與假資訊傳播平臺大本營的矽谷(Silicon Valley)，致力

在言論自由與股東壓力以及假新聞危害間求取平衡，惟也因此對社群媒體網站上發動的資訊戰參與度仍顯不足。身為民主社會，美國將無法遏止此種威脅，惟須接受此類虛假內容確實存在，並置重點於讓企業與使用者有能力識別與揭露此類內容。在新冠肺炎疫情中，推特採用新系統來識別與注意可能被認為危險或散播未經證實資訊的文章與貼文。2020年6月，推特網站中對中共外交部官員趙立堅宣傳生物武器陰謀論的推文進行了事實查核。儘管此種社群媒體監管措施帶有審查制度與箝制言論自由的疑慮，而「見招拆招」的做法亦成效不彰，但這卻是個好的開始，能讓使用者注意到所有推文，即便發布自經過驗證的帳號，也必須抱持正向存疑態度予以閱讀。⁴³

隨著社群媒體不斷演進成包括如抖音等更為視覺化的平臺，諸如由人工智慧合成的深偽(Deepfake)等「被操弄媒體」(Manipulated Media)的標記就顯得相當重要。儘管這也意味著巨大挑戰，惟隨著令人信以為真的深偽技術不斷進步，其反制技



術亦將不斷提升。科技公司刻正投資開發可在圖像遭更改時顯示其跡象的方法，例如在圖像加上水滴，明白標示受媒體操弄的標誌。⁴⁴ 此外，亦可利用演算法來評估文章標題是否與內容不符，藉以警告使用者並阻止其僅依據標題就分享誤導性資訊。⁴⁵ 將這些技術納入社群媒體平臺，讓被操弄媒體遭進一步分享之前進行標記，將可減緩假資訊擴散，同時有助於建立具有正向存疑態度與提升媒體素養的社會。為維護取得所有資訊的自由，美國必須確保使用者擁有可協助辨識與反制假資訊的必要工具。

為有效反制俄羅斯假資訊而須進行的最重要改變，就是教育美國民眾並賦予其識讀能力，使其能夠辨別與忽略俄羅斯的假資訊。採取嚇阻行動無法阻止或延緩俄羅斯散布假資訊的作為，因此美國應置重點於教導人民防範俄羅斯影響資訊領域的企圖。公共衛生危機期間反制假資訊的挑戰，在於平衡對高媒體素養社會的需求；高媒體素養社會極度重視假資訊的偵測，同時以平等方式發自內心地信



2018年8月4日，美陸戰隊於敘利亞哈金(Hajin)支援堅定決心行動(Operation Inherent Resolve)訓練期間發射81公釐迫擊砲。(Source: USAF/ Corey Hook)

任醫療體系。美國必須投資媒體素養的養成，並循序教育民眾瞭解這些針對性活動的方法與目標。除了讓民眾察覺俄羅斯在這些針對性資訊攻擊中扮演的角色，美國人民也必須評估其他未來在美國社會中可能以此方式遭到鎖定的裂痕。

在俄羅斯眼中，多元化就是美國的弱點。為反駁這種說法，美國必須就其多元主義展現實力，並致力消弭歧見，避免成為社群媒體武器化的理想目標。俄羅斯正不斷加深美國社會既有的裂痕——分化、分歧與弱化。特別是面對總統大選與現代大規模流

行疾病，所有美國人民都必須提高警覺，質疑資訊出處，並特別注意美國社會中成為此類攻擊主要目標的裂痕與歧見。美國正成為日益兩極化的國家，為能撫平創傷與裂痕，進而防範俄羅斯社群媒體武器化的影響，美國仍有漫漫長路要走。

作者簡介

Sarah Jacobs Gamberini為美國國防大學國家戰略研究所大規模毀滅性武器研究中心政策研究員。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. Roy Godson, *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*, Hearing Before the Select Committee on Intelligence of the U.S. Senate, 115th Cong., 1st sess., 2017, available at <www.intelligence.senate.gov/sites/default/files/hearings/S%20Hrg%20115-40%20Pt%201.pdf>.
2. Adam Taylor, “Did Russia Interfere in Brexit? An Unpublished Report Roils UK Politics Before Election,” *Washington Post*, November 5, 2019, available at <www.washingtonpost.com/world/2019/11/05/did-russia-interfere-brexit-an-unpublished-report-roils-uk-politics-before-election/>; Filippa Lentzos, “The Russian Disinformation Attack That Poses a Biological Danger,” *Bulletin of the Atomic Scientists*, November 19, 2018, available at <<https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/>>; Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vols. I and II (Washington, DC: Department of Justice, March 2019), available at <www.justice.gov/storage/report.pdf>.
3. Tedros Adhanom Ghebreyesus, speech delivered to the Munich Security Conference, Munich, Germany, February 15, 2020, available at <www.who.int/dg/speeches/detail/munich-security-conference>.
4. Godson, *Disinformation*.
5. Svetlana Savranskaya and Tom Blanton, *NATO Expansion: What Gorbachev Heard* (Washington, DC: National Security Archive, 2017), available at <<https://nsarchive.gwu.edu/briefing-book/russia-programs/2017-12-12/nato-expansion-what-gorbachev-heard-western-leaders-early>>.
6. *Ukraine: Background, Conflict with Russia, and U.S. Policy*, R45008 (Washington, DC: Congressional Research Service, April 29, 2020), available at <<https://fas.org/sgp/crs/row/R45008.pdf>>.
7. Gerard Toal, *Near Abroad: Putin, the West, and the Contest Over Ukraine and the Caucasus* (New York: Oxford University Press, 2017).
8. David M. Adamson and Julie DaVanzo, *Russia's Demographic 'Crisis': How Real Is It?* (Santa Monica, CA: RAND, 1997), available at <www.rand.org/pubs/issue_papers/IP162.html>; Cheney Kalinich, “Russia: The Sickness of a Nation,” *The Yale Global Health Review* (Fall 2016), available at <<https://yaleglobalhealthreview.com/2016/12/21/russia-thesickness-of-a-nation/>>.
9. Eugene Rumer, *Primakov (Not Gerasimov) Doctrine in Action* (Washington, DC: Carnegie Endowment for International Peace, 2019), available at <<https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254>>.
10. Bureau of Public Affairs, *Soviet “Active Measures”: Forgery, Disinformation, Political Operations*, Special Report No. 88 (Washington, DC: Department of State, 1981), available at <<https://www.cia.gov/library/readingroom/docs/CIA-RDP-84B00049R001303150031-0.pdf>>.
11. Dmitry Adamsky, “Strategic Stability and Cross-Domain Coercion: The Russian Approach to Information (Cyber) Warfare,” in *The End of Strategic Stability? Nuclear Weapons and the Challenge of Regional Rivalries*, ed. Lawrence Rubin and Adam N. Stulberg (Washington, DC: Georgetown University Press, 2018).
12. Mark Galeotti, “The ‘Gerasimov Doctrine’ and Russian Non-Linear War,” *In Moscow's Shadows*, 2013, available at <<https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrineand-russian-non-linear-war/>>; Valery Gerasimov, “The Value of Science in Prediction,” *Voенно-Промышленнi Kuryer* 26, no. 840 (February 26, 2013), available at <www.vpk-news.ru/articles/14632>.
13. Valery Gerasimov, trans. Harold Orenstein and Timothy Thomas, “The Development of Military Strategy Under Contemporary Conditions: Tasks for Military Science,” *Military Review* (October 2019), available at <www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2019-OLE/November/Orenstein-Gerasimov/fbclid/IwAR18VUoZTZ15KB7AvBVyPEAQcQo5w-5myuymQPRqQ5qogem5JDR5PjsLCmA/>.
14. Carolina Vendil Pallin, “Internet Control Through Ownership: The Case of Russia,” *Post Soviet Affairs* 33, no. 1 (2017).
15. Jane Wakefield, “Russia ‘Successfully Tests’ Its Unplugged



- Internet,” BBC, December 24, 2019, available at <www.bbc.com/news/technology-50902496>.
16. Steven Erlanger, “Russia’s RT Network: Is It More BBC or KGB,” *New York Times*, March 8, 2017, available at <www.nytimes.com/2017/03/08/world/europe/russias-rtnetwork-is-it-more-bbc-or-kgb.html>; Nathan Layne, “U.S.-Based Russian News Outlet Registers as Foreign Agent,” Reuters, July 2, 2018, available at <www.reuters.com/article/us-usa-trump-russia-propaganda/u-s-based-russian-news-outlet-registers-as-foreign-agentidUSKCNIG201H>.
 17. “Russia Tests Direct-Ascent Anti-Satellite Missile,” *U.S. Space Command Public Affairs*, April 16, 2020; Michael Connell and Sarah Vogler, *Russia’s Approach to Cyber Warfare* (Arlington, VA: CNA, September 2016), available at <<https://apps.dtic.mil/dtic/tr/fulltext/u2/1019062.pdf>>.
 18. David Lee, “The Tactics of a Russian Troll Farm,” BBC, February 16, 2018, available at <www.bbc.com/news/technology-43093390>.
 19. Elizabeth Townsend, *Understanding Narratives for National Security: Proceedings of a Workshop* (Washington, DC: The National Academies Press, 2018), available at <www.nap.edu/read/25119/chapter/1>.
 20. Matthew Shaer, “What Emotion Goes Viral the Fastest?” *Smithsonian Magazine*, April 2014, available at <www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/>.
 21. Tom Huddleston, Jr., “In 1995, Bill Gates Made These Predictions About Streaming Movies and Fake News on the Internet,” CNBC, 2019/5/31, available at <www.cnn.com/2019/05/31/bill-gates-1995-predictions-about-streaming-movies-fake-news.html>; Bill Gates and Terry Pratchett, “GQ&A: Bill Gates Talks to Terry Pratchett About the Future, the Microsoft Revolution and How to Become a Billionaire,” *GQ*, July 1995.
 22. *The War on Pineapple: Understanding Foreign Interference in 5 Steps* (Washington, DC: Department of Homeland Security, 2019), available at <www.dhs.gov/sites/default/files/publications/19_0717_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf>.
 23. Richard Engel, Kate Benyon-Tinker, and Kennett Werner, “Russian Documents Reveal Desire to Sow Racial Discord—and Violence—in the U.S.,” NBC, 2019/5/20, available at <www.nbcnews.com/news/world/russian-documents-reveal-desire-sow-racial-discord-violence-u-s-n1008051>.
 24. Scott Shane and Sheera Frenkel, “Russian 2016 Influence Operation Targeted African-Americans on Social Media,” *New York Times*, December 17, 2018, available at <www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html>.
 25. Mark Scott, “Russia and China Target U.S. Protests on Social Media,” *Politico*, June 1, 2020, available at <www.politico.eu/article/russia-china-us-protests-social-media-twitter/>.
 26. *Secondary Infektion at a Glance*, 2020, available at <<https://secondaryinfektion.org/report/secondary-infektion-at-a-glance/>>.
 27. Ben Nimmo et al., *Graphika: Secondary Infektion*, 2020, available at <<https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf>>.
 28. Thomas Boghardt, “Operation INFEKTION: Soviet Bloc Intelligence and its AIDS Disinformation Campaign,” *Studies in Intelligence* 53, no. 4 (December 2009), available at <<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf>>.
 29. Lance E. Mason, Dan Krutka, and Jeremy Stoddard, “Media Literacy, Democracy, and the Challenge of Fake News,” *Journal of Media Literacy Education* 10, no. 2 (2018), available at <<https://digitalcommons.uri.edu/jmle/vol10/iss2/1/>>.
 30. C. Lee Ventola, “Social Media and Health Care Professionals: Benefits, Risks and Best Practices,” *Pharmaceutical and Therapeutics Journal* 39, no. 7 (July 2014), available at <www.ncbi.nlm.nih.gov/pmc/articles/PMC4103576/>.
 31. Centers for Disease Control and Prevention (CDC), “Measles Cases and Outbreaks,” available at <www.cdc.gov/measles/cases-outbreaks.html>.
 32. Sebastian Funk, *Critical Immunity Thresholds for Measles Elimination* (London: Centre for the Mathematical Model-

- ling of Infectious Diseases, October 19, 2017), available at <www.who.int/immunization/sage/meetings/2017/october/2_target_immunity_levels_FUNK.pdf?ua=1>.
33. CDC, "Measles History: Measles Elimination," 2018, available at <www.cdc.gov/measles/about/history.html>.
34. David A. Broniatowski et al., "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate," *American Journal of Public Health* (October 2018), available at <<https://ajph.aphapublications.org/doi/10.2105/AJPH.2018.304567>>.
35. Judy Twigg, "Coronavirus in Russia: How Putin's Disinformation Efforts Could Backfire at Home," *Bulletin of the Atomic Scientists*, March 31, 2020, available at <<https://thebulletin.org/2020/03/coronavirus-in-russia-how-putins-disinformation-efforts-could-backfire-at-home/>>.
36. Chris Buckley and Steven Lee Myers, "As New Coronavirus Spread, China's Old Habits Delayed Fight," *New York Times*, February 1, 2020, available at <www.nytimes.com/2020/02/01/world/asia/china-coronavirus.html>; Steven Lee Myers, "China Spins Tale that the U.S. Army Started the Coronavirus Epidemic," *New York Times*, March 13, 2020, available at <www.nytimes.com/2020/03/13/world/asia/coronavirus-china-conspiracy-theory.html>; Department of Defense, "7th International Military Sports Council: Military World Games," 2019, available at <www.defense.gov/Explore/Spotlight/CISM-Military-World-Games/>; Sarah Jacobs Gamberini and Amanda Moodie, "The Virus of Disinformation: Echoes of Past Bioweapons Accusations in Today's COVID-19 Conspiracy Theories," *War on the Rocks*, April 6, 2020, available at <<https://warontherocks.com/2020/04/the-virus-of-disinformation-echoes-of-past-bioweapons-accusations-in-todays-covid-19-conspiracy-theories/>>.
37. Daniel C. Payne et al., "SARS-CoV-2 Infections and Serological Responses from a Sample of U.S. Navy Service Members—USS *Theodore Roosevelt*, April 2020," *Morbidity and Mortality Weekly Report* (Washington, DC: CDC, June 12, 2020), available at <www.cdc.gov/mmwr/volumes/69/wr/mm6923e4.htm>.
38. Geoff Ziezulewicz, "The USNS *Comfort* Is Now Taking COVID-19 Patients. Here's What to Expect," *New York Times*, April 8, 2020, available at <www.nytimes.com/2020/04/08/magazine/hospital-ship-comfort-new-york-coronavirus.html>; Gamberini and Moodie, "The Virus of Disinformation".
39. National Defense Authorization Act for Fiscal Year 2020, 116th Cong., § 1790, January 3, 2019, available at <www.intelligence.senate.gov/legislation/damon-paul-nelson-and-matthew-young-pollard-intelligence-authorization-act-fiscal-1>; Amy Klobuchar et al., "Letter to Secretary Esper, Director Ratcliffe, Director Wray, General Nakasone, and Acting Secretary Wolf," U.S. Senate, 2020, available at <www.klobuchar.senate.gov/public/_cache/files/1/d/1d99087e-0a26-4242-a0cfa5867d208a18/D1FD0C7DAF-35260CBB-3D51CAB10A3324.062620disinformationletter.pdf>.
40. Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Strategic Perspectives 11 (Washington, DC: NDU Press, 2012), available at <<https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf>>.
41. Department of State, "Global Engagement Center," 2020, available at <www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/>.
42. Tom McTague, "Britain's Secret War with Russia," *The Atlantic*, December 3, 2019, available at <www.theatlantic.com/international/archive/2019/12/britain-russia-nato-disinformation/602836/>.
43. Nina Jankowicz, "Russian Trolls Are Only Part of the Problem," *New York Times*, January 25, 2018, available at <www.nytimes.com/2018/01/25/opinion/russian-trolls-fake-news.html>.
44. Fijoy Vadakkumpadan and Ye Liu, *Detecting Deepfakes and Disinformation* (Cary, NC: SAS, 2020).
45. Ibid.