● 作者/Richard L. Manley ● 譯者/余振國 ● 審者/丁勇仁

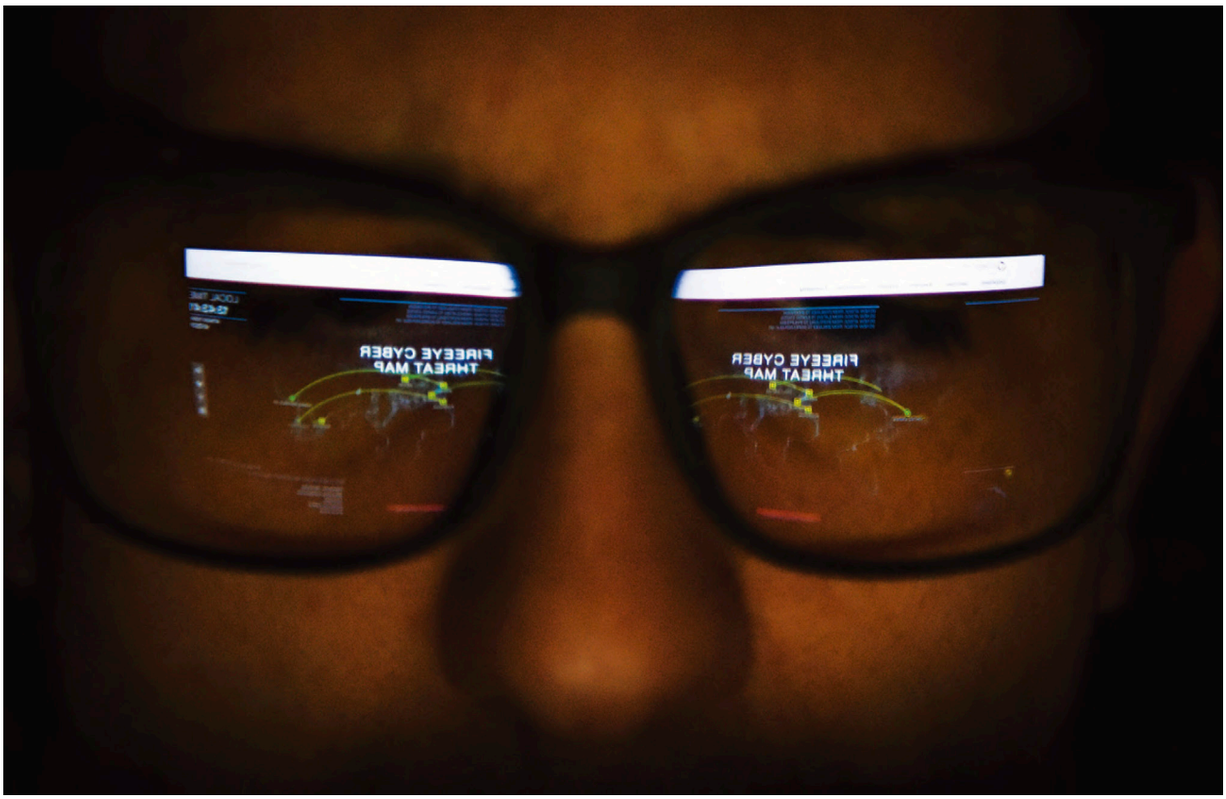
暗地行動：未來的網路作戰

Cyber in the Shadows: Why the Future of Cyber Operations Will Be Covert

取材/2022年第三季美國聯合部隊季刊(*Joint Force Quarterly*, 3rd Quarter/2022)

網路作戰除了能讓弱勢行動者在對抗強勢行動者時獲得不對稱優勢，也可使強勢行動者在不造成實體衝突狀況下，影響同級對手的政策，這些都歸功於網路作戰的隱密能力。隨著現代社會與網路的關係愈形緊密，隱密之網路作戰對於國家安全威脅也與日俱增。

(Source: Shutterstock)



2021年12月5日，在阿肯色州小岩城空軍基地，第189空運聯隊通信小隊愛德華(Jochen Emrich)上士以系統評估現實世界網路威脅。(Source: US Air National Guard/Jonathan Porter)

目前網路衝突型態看起來與傳統衝突型態非常相似。然而，因網路領域造成傳統大國間情勢的變動，乃科技使潛在行動者具有不對稱優勢。國家力量中此一新要素，使較弱國家能夠在單極或多極世界中「越級挑戰」，能與大國競爭或衝突。阿奎拉(John Arquilla)將這種新環境描述為一場「資訊革命」，且「意味著網路戰爭將興起，這種戰爭結果將不會由兵力大小及部隊機動性所決定。」[1] 網路作戰依然會遵照托夫特(Ivan Arreguín-Toft)的戰略互動理論，讓強勢行動者有充分自由度可以進行間接競爭，減少傳統意義上的肢體衝突。[2] 網路也讓弱勢行動者在不產生重大風險情況下，迫使強勢行動者增加競爭的花費。強者繼續將網路領域取得的影響，整合到其教條式的對外政策，無論是軍事上還是其他方面，都最大限度地發揮分層效應。網路這個新競爭領域的結果已經有幾十年學理了，但讓這個領域變得難以預測的原因，是科技創新速度及現有可用科技的變化。

本文將討論網路作戰對行動者在網路領域進行戰略互動所帶來的影響，提出在大國競爭中使用網路的案例，並解釋網路作戰如何為較弱勢行

動者提供不對稱優勢。本文內容將側重於吉爾斯(Keir Giles)、卡森(Austin Carson)與亞瑞米洛(Keren Yarhi-Milo)，以及馬內斯(Ryan Maness)與嘉特納(Margarita Jaitner)等人，對於俄羅斯聯邦和中華人民共和國等修正主義國家行動者使用網路作戰的研究。本文將展示網路是如何讓這些行動者「位居弱勢也能有效發揮」，以支持其各自的混合戰及超限戰理論。在討論完修正主義國家之後，本文將舉例說明北韓等惡棍國家在網路上的戰略互動，描述該國在與南韓及美國的鬥爭中身為弱勢行動者所享有的不對稱優勢。從夫炯旭(Hyeong-wook Boo)、中島(Ellen Nakashima)及松恩(Paul Sonne)的著作可以解釋網路作戰，如何讓惡棍國家在不需要為傳統衝突加溫情況下向對手施加壓力。最後，本文與阿奎拉的立場相反，儘管網路作戰可以提供不對稱優勢，但未來的使用必然是以秘密或隱蔽方式，以避免越界而造成武裝衝突。

修正主義國家的運作

隨著俄羅斯聯邦繼續向西擴張領土的目標，以阻撓北大西洋公約組織(NATO)的東擴，俄羅斯政府明白，如果北約與東歐國家聯合起來，該聯盟就可以匯聚更多戰鬥力，並在軍事支出上享有優勢。俄羅斯為了對抗這種結果，已將科技納入其傳統形式的「積極措施」中，以確保心理作戰能提供欺敵優勢。這種利用政治與心理戰的能力，使俄羅斯能夠在西方聯盟與有意加入聯盟者的心中製造疑慮。例如，在2014年入侵烏克蘭期間，「俄羅斯人巧妙地使用簡訊，來打擊烏克蘭前線部隊士氣，其中甚至在簡訊中提到烏克蘭官兵在基輔的妻子與孩子。」[3] 網路戰術之運用使敵戰鬥人員心煩意亂且士氣低落，在戰場上為俄羅斯軍隊創造明確的心理優勢。俄羅斯透過網路資訊作戰來塑造戰場，可以防止敵對盟國軍事力量的強化，並在聯盟內部製造疑慮。

這些強軍的戰術不僅體現在軍事實力上，而且在政治作戰場域也得到充分發揮。關於俄羅斯在2016年美國大選期間所部署的積極措施有相當多的報導，這項行動所造成的潛在效應是使許多美國人不斷懷疑美國制度的有效性。馬內斯及嘉特納對此的解釋是：「俄羅斯的政治干預是為了讓敵對國家內部造成長期分裂，俄羅斯希望將這種分裂擴散出去，並加劇任何可能發生的衝突，最終破壞對手政治體系的穩定，以及削弱人民對政府與機構的信任。」[4] 莫斯科一直使用這種增加不信任的戰略已經長達數十年，然而網路環境提供的優勢，將確保這些行動在沒有被阻止前會繼續積極進行。

中共與俄羅斯同一掛，試圖透過整合網路作戰來顛覆全球規範。中共的超限戰概念使其能夠結合國力所有要素來向對手施壓，而結合網路作戰之後，無疑能使中共更加主導這種競爭步調。當中國共產黨從內部認知自己在科技上落於人後，就開始一場全球性的智慧財產權盜竊行動，以人為方式來提高自己技術水準。如今，中共積極鎖定以美國軍事承包商與基礎設施為盜竊目標，藉此來提高自己能力。戴維森(Philip S. Davidson)上將在美印太司令部任職聽證上表示：「中共正在對一系列平臺進行投資，這包括低噪音潛艦，

配備先進武器及新式感測器……當中共需要無法自行研發的科技時，通常都會透過網路來進行竊取。」[5] 這些評論是在中共駭客攻擊「關於潛艦戰的高度敏感資料」後所發表的，凸顯了中共駭客攻擊的嚴重性。[6] 儘管美國施加壓力且進行外交互動，但中共似乎準備繼續其網路間諜活動，同時靠著競爭對手經濟與自己經濟糾纏在一起這點作為安全措施，以防止對手果斷採取行動。中共願意積極利用技術在國內監視及控制自己人民，同時向潛在的專制國家出口類似科技，這些做法應該會讓自由國家感到特別擔憂。

惡棍行動者與不對稱優勢

北韓及伊朗等惡棍國家，以及暴力極端主義組織都依靠網路作戰的不對稱優勢，但它們在這方面各自有不同程度的成功。北韓在2014年對索尼公司採取強硬手段的脅迫作為，導致國際社會認為雖然北韓限制電影《名嘴出任務》上映的既定目標沒有達成，但一個積弱國家也可以在網路中找到脅迫的途徑。然而這次被大幅報導的攻擊只是夫炯旭所描述，「對南韓及美國極複雜網路攻擊中的一小部分。由對熱門網站的簡單DDoS攻擊(分散式阻斷服務攻擊)與電子郵件伺服器的駭客攻擊開始，這類網路攻勢作戰採用稱為先進持續性威脅(Advanced Persistent Threat)的先進科技」。[7] 這些侵略性攻擊是北韓與更強國家進行戰略互動的一部分。惡棍國家這種具危險性的行動之所以可以繼續進行下去，是因為實力更強的國家希望維持在較低的衝突水準。惡棍國家在網路上所要承擔的風險，就是行動能否繼續下去是取決於更強國家想要維持低衝突狀態的意願。如果強勢國家覺得放任這類活動繼續進行已經不再符合其利益，則直接衝突就比承受攻擊成為更佳選擇，屆時弱勢國家就無獲勝希望。這種狀況所造成結果，就是網路作戰力度必須被保持在一個可接受限度之下，因此限制網路行動所能造成的決定性。

網路作戰的未來：朝「隱密性」方向發展

要想利用網路作戰作為一種改變的機制，實現所望之政策，就需要有能力合理地阻斷行動者的參與。這種互動就是國際關係中所說的「前臺和後臺」，其中「只能看到前臺者，可能無法看到或誤解行動，會向那些進出後臺者放大傳遞的資訊及訊號」。[8] 那些瞭解後臺並能收到完整資訊者，會更清楚理解一個行動或事件的全般意涵。透過這種方式，可以在目標及無法歸責於該行動贊助者之間進行某種形式的溝通。

這可以解釋一個實力更強國家如何將網路作戰納入整體嚇阻戰略，但一個實力較弱國家如何才能在網路上進行決定性行動？就定義而言，弱勢國家在外交、資訊、軍事及經濟能力方面都不如強大競爭對手，而其作戰只能在可承受暴力或壓力的限度下進行。當一個強大國家認為讓一個弱國在網路上競爭不再符合其最佳利益時，這個弱國該做出甚麼反應？加茲克(Erik Gartzke)解釋說，網路攻擊的相對風險係數「很低，主要是因為那些有權干預，以阻止或懲罰刺激性行為的人往往沒有動機阻止這些行為」。[9] 本文認為網路活動愈來愈需要被隱藏的立場，在很大程度上是

因為加茲克的著作：重新審視穩定—不穩定悖論。這個問題重點在於較弱行為者對較強行為者做出反應的能力是否有可信度。卡森與亞瑞米洛解釋道：「隱密行動是可以理解的，因為它包含一系列顯著的質性門檻，這些門檻就可代表行動發起人的決心。」但他們強調，這些訊息必須是「可信的」。[10] 一個弱勢行動者對強勢行動者展現決心的可信程度，在確認雙方互動穩定性(或不穩定性)具有重大作用。

網路中的穩定—不穩定悖論

冷戰時期的嚇阻理論大多是建立在相互保證毀滅概念之上。由於核武大國間之全面衝突後果相當嚴重，擁有核武的國家都明白，除了用來作為嚇阻外，核武基本上不是一種可動用的戰略。從這種嚇阻效果中就誕生穩定—不穩定悖論，該悖論假設：「擴大核嚇阻實際上可能會導致暴力等級較低的行動自由度增加。」[11] 從此悖論中，史奈德(Glenn Snyder)想出美國與蘇聯間之戰略互動的假設「顧慮到大規模報復所造成的威脅，蘇聯可能會覺得，可以進行一系列小規模冒險而不會受到懲罰的行動，儘管這些行動客觀看來將有引發某種報復的可能性」。[12] 由於為防止這些低強度衝突而需採取行動會造成巨大後果，採此戰略的國家自然會適應這個競爭環境，在這個環境中只要採取的進攻行動不超過可接受門檻，就可以被執行。當時對此狀況的問題是：可接受門檻究竟是什麼？以及被逼對手的忍耐程度？

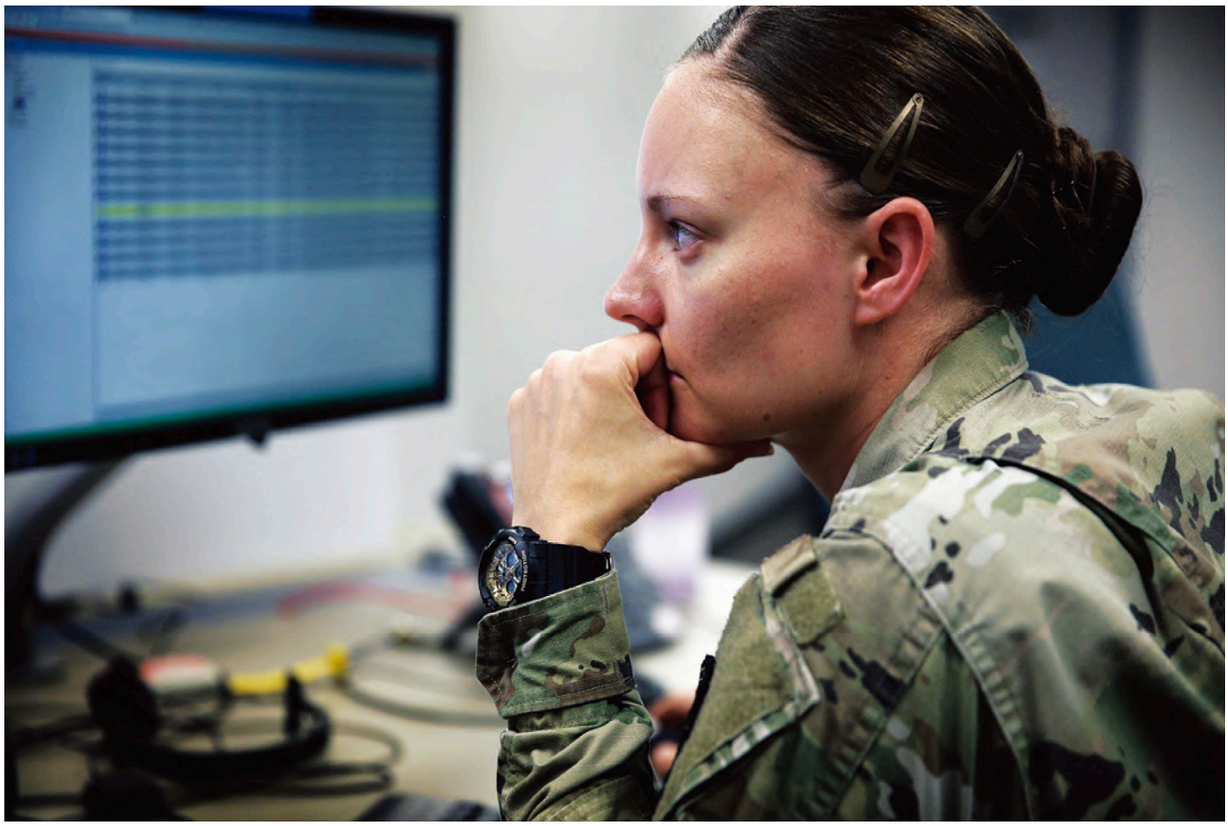
最近，加茲克在近期重新審視穩定—不穩定悖論，並將其應用於網路環境中。表1解釋該理論與網路作戰「隱密性」有關的應用。假設該模型是成立的，則我們可以用以下邏輯看待未來的網路作戰：

- 美國作為獨強國家，可以繼續制定網路作戰的規則。當美國想要影響那些國力相對強大並能進行報復的修正主義者時，只要收得到後臺的資訊，就可以在隱密性方面找到網路作戰的優勢。在對付惡棍國家時，如果需要，美國可以公開採取行動，藉此發出明確訊息來進行嚇阻，如果針對特定目標或個人，則可以隱密地採取行動。美國還可以透過確定哪些網路攻擊是其願意忍受，以及美國報復(實體攻擊)的網路「底線」在哪裡，來定出可接受的網路活動門檻。
- 想要影響美國的修正主義國

表1 網路中的戰略互動模型

檢設序列	強勢行動者	弱勢行動者
強勢行動者	網路中隱密互動	網路中公開互動
弱勢行動者	網路中公開互動	網路中隱密或公開互動

Source:爰引自Michael Krepon, "The Stability-Instability Paradox," *Arms Control Wonk*, November 2, 2010, available at <https://www.armscontrolwonk.com/archive/402911/the-stability-instability-paradox/>



2021年5月24日，美網路司令部網路國家任務部隊成員於馬里蘭州米德堡(Fort George G. Meade)參加訓練及戰備演習。(Source: US Army/Josef Cole)

家應透過使用代理人和替代者來發展出適當的隱密行動方案，以合理化其推諉藉口，並確保其網路作戰保持在美國公開報復的門檻之下。對修正主義國家而言，若與其他修正主義國家或與惡棍國家相互競爭時，它們須根據其對手之傳統武力強度，來選擇採取隱密或公開行動的方式。

- 惡棍國家應儘可能保持隱密，除非其認為來自各國的支持可以抗衡更強大國家傳統武力的報復。關於這方面之案例是北韓對索尼進行的駭客攻擊事件。雖然它並未完全達成其預期目標，但北韓確實向對手發出一個嚇阻訊息並有效表達其能力。

網路邊緣政策

1962年10月，兩個全球多極化的超級大國因為古巴飛彈問題而完全處於核戰邊緣。每位世界領導人都面對著一位看似毫不動搖的對手，除了要防止現代文明不久終結之外，無論是甘迺迪(John F. Kennedy)還是赫魯雪夫(Nikita Khrushchev)似乎都沒有要先妥協的動機。這兩個核子超級大國都需要向對方及自己民眾證明，競爭規則正在被

重新定義。這種重新定義幾乎要終結世界。在這場危機之後，人們認知在這個核武世界中的衝突將跟過去有所不同──超級大國試圖相互損害會產生新的後果，因此制定新遊戲規則是有其必要，結果是創造出一個隱密活動的時代，可以在避免直接傷害的同時又允許施加間接壓力。雙方都不想重蹈古巴飛彈危機的覆轍，因此雙方都進入一個隱密行動的現狀。

當我們想到核子時代初期的教訓，我們應該想到類似情況似乎最有可能發生在數位時代。隨著重新定義新規範及標準，似乎很自然會有一段「試探」彼此能力的時期。我們同樣也能理所當然認為，在網路戰力方面會出現某種程度的邊緣政策。格林伯格(Andy Greenberg)在2019年8月於《連線》(*Wired*)雜誌的文章中，就斷言這種邊緣政策已經發生：

> 《紐約時報》在上週末報導中提及，美網路司令部比以往任何時候都更深入滲透到俄羅斯電力設施中，植入能夠破壞電網的惡意軟體，這或許是一種報復性措施，用來嚇阻俄國駭客的進一步網路攻擊。但從俄羅斯反應來看，這次駭客攻擊電網的消息可能已經直接產生反效果：就算克里姆林宮聲稱俄羅斯電網不受此類威脅影響，其依然警告這些入侵行為可能會升級為兩國之間的網路戰爭。[13]

對民用電網的網路攻擊影響尤其令人擔憂，因為有可能造成大量無辜生命損失的風險；雖然不像核子攻擊那樣立即致命，但如果以升級的方式進行，破壞程度及後續影響將無法估量。儘管俄羅斯已將限制性中等規模網路攻擊納入其混合戰戰略中，正如2014年克里米亞吞併事件所證明，但雙方都沒有完全理解這些類基礎設施攻擊對同等級競爭對手所造成的影響。

格林伯格又解釋道，這種網路邊緣政策的風險可能是由川普政府向俄羅斯發出嚇阻能力的作為所引起。前國土安全顧問博塞特(Tom Bossert)認為，當我們考慮到自身在電網攻擊中的脆弱性，就需要更加重視這種威脅升級的可能：「如果你全身都被澆上汽油，那就不要進行投擲火柴的比賽。」[14] 這裡又出現另一個悖論：我們要如何傳達自己具有隱密能力的訊息？公開機密的適當手段為何？

隱密性限制了邊緣政策

核子時代初期，當需要對無法與之開戰或開戰代價太大的對手做出反應，隱密行動一直是政策制定者的「第三選項」。根據卡森與亞瑞米洛的說法：「使用隱密行動來表明決心看起來是可行的，因為它對危機升級的風險會造成影響。」[15] 此一原則讓核子超級大國能藉推諉不知情而相互競爭，從而限制衝突升級的影響，並讓彼此有一條後路。因此，這種行為開始在網路空間中出現。伊朗秘密核子設施的震網(Stuxnet)匿名攻擊及俄羅斯對2016年美國總統大選的干預，都是獨立國家在網路領域中隱密競爭的例子。這些例子展示直接的隱密網路行動潛在能力，可在實現政策靈活性的同時，也能影響對手行為。但這就是網路潛力的極限嗎？是否有可以為網路衝突定下新規

2011年1月23日，突尼西亞共和國突尼斯的抗議者，於茉莉花革命(Jasmine Revolution)期間推翻前統治者班阿里(Ben Ali)。(Source: Idealink)

則的間接攻擊媒介？在冷戰期間，出現一系列代理人衝突，來作為獨立國家的戰場，如伊朗、越南、阿富汗、西藏及其他地方發生叛亂與游擊戰等衝突，獨立國家可以在這些地區讓對手付出代價並制定政策條款。那網路領域能否提供下一個隱密的戰鬥空間呢？

阿拉伯之春

阿拉伯之春的事件，成為網路串聯和社交媒體影響的案例研究。布萊克莫爾(Erin Blakemore)寫道：

> 從2010年12月開始，突尼西亞(Tunisia)爆發反政府抗議活動。到2011年初，這些抗議活動已經擴大蔓延且被稱為「阿拉伯之春」，這是一波抗議、起義和動亂的浪潮，在北非和中東的阿拉伯語國家中蔓延。支持民主的抗議活動由於社交媒體而迅速傳播，最終推翻突尼西亞、埃及、利比亞和

葉門的政府。[16]

即使政府試圖關閉通信網路、推特、臉書及YouTube等社交平臺，以切斷渴望變革民眾的支援，仍無法阻斷網路訊息傳播助長了支持民主的抗議活動。霍華德(Philip Howard)描述社交媒體與網路串聯力量，如何與革命有所關聯：「對民主有志一同者建立龐大的社交網路，並且組織政治行動，社交媒體成為爭取更多自由的重要工具之一。」[17]

在撰寫本文時，沒有任何國家或個體聲稱要為控制此社交媒體工具負責。網上的激進組織「匿名者」(Anonymous)確實聲稱提供技術支援與專業知識，但根據評估，這些訊息與內容的傳遞並非刻意安排，也並非由國外傳入。但是，如果將來主題及其內容可以主導呢？以前進行叛亂與政治行動需要有媒介互動，現在則可以透過社交媒體傳播，人們的不滿將受到入侵者所策動。俄羅斯在2016年美國總統大選中試圖進行政治操弄，就接近於此類的社交工程，但除了少數抗議與爭鬥外，其影響力主要集中在網路領域。隱密網路行動的潛力對社交工程學方面意義重大，尤其是當我們將之與已確立的社會運動理論研究結合在一起時。

在霍華德關於社會運動的開創性著作中提出，社會運動有四種類型，如表2說明，其中增加對網路影響傷害性的項目。

隨著網際網路逐漸成為現代日常生活的一部分，研究人員開始關注上網民眾受到的影響，以及其分享不滿的能力。在1990年代後期，由於社交媒體是一個剛起步的企業類型，波爾塔(Donatella della Porta) 與迪亞尼(Mario Diani)在關於該主題的基礎著作中將社會運動定義為：「透過成員的共同信念與團結所形成的非正式網路，經由各種形式的抗議動員以支持對特定社會問題的立場表達。」[18] 在2003 年，迪亞尼進一

表2 社會運動的四個類型

類型	焦點	案例	網路影響的傷害性	網路傷害性示例
選擇運動	部分個體改變	母親反對酒後駕車	高—個人很容易被社交媒體操縱	反疫苗運動支持者、洗衣膠囊食用者、出生地運動
救贖運動	全部個體改變	宗教運動	中—沒有反擊式論述就難以進行群體變革	白人至上主義者、孤狼式恐攻分子、反法西斯成員
改革運動	部分社會變革	婦女選舉權運動	中—影響具有共同不滿的現有群體，比說服人們改變群體更容易	美國政黨、體育迷
革命運動	全面社會變革	革命	低—全面的社會變革需要在網路領域之外採取行動。網路有策動環境以表達不滿的功能	2016年美國大選、阿拉伯之春、俄羅斯在克里米亞的網路活動

Source: Nick Lee, "The Four Types of Social Movements," *Medium, August* 2, 2019, available at https://medium.com/@nicklee3/the-four-types-of-social-movements-8db910192573.

步強調社交媒體對社會運動的影響：「激發網路模型的新社會運動是不需要對成員資格做設限，其為分散、動態、沒有正式等級的制度，並有賴於行動者認同社會運動的觀點、立場及目標。」[19] 正是在這種描述中，隱密行動的機會出現了。一個去中心化、沒有領導人，以自身觀點解釋真相，透過對於這些原則的共同信念來取得動力，並且缺乏明確階級制度的網路，這為有意或無意的操縱提供一個機會。

一個有動機且企圖間接影響競爭對手行動的國家，可以利用這種日常使用的網路結構，來散播假情報及欺敵，從而推動社會運動。這種方式可以體現在競爭對手的盟國、重要貿易夥伴、商品供應商的社會大眾中，或直接體現在自己國家的民眾。故意傳播錯誤資訊或放大反國家論述，可能會在前臺進行譴責和施壓，同時透過幕後的隱密行動來控制論述。雖然這不是一種創新的隱密行動概念，但它是一種新的傳播方法，也是利用不知情的代理人來進行隱密行動的新機會。在「阿拉伯之春」例子中，我們不難想像一個國家或國家集團在散布民主思想的動機下，隱密地控制向突尼西亞、埃及及敘利亞傳送訊息，操縱反國家言論的基調、節奏及傳播，就像一個軍事將領對戰役進行協調一樣。透過這種方式，隱密的行動者可以在幕後調整訊息傳遞的基調與內容，以便在進行艱難談判時加大壓力，或在做出讓步時撤回壓力，同時對於自己參與能夠保持合理的撇清，並管理狀況升級的風險。

總結

隨著社會開始接受網路世界的事實，當強者試圖嚇阻較弱的對手，網路攻擊的後果很可能會加大。網路攻擊為較弱行動者帶來的優勢，可以經由在實體領域造成的結果而被緩解。這些結果很可能會促使網路競爭轉向透過代理人及替代者所進行的秘密活動。網路作戰的影響將會是塑造在衝突中獲得競爭優勢的環境，但網路作戰的成果很可能無法製造出決定性結果。反之，將網路作戰納入其他形式的戰略互動，包括成為戰時功能中一種支援性工作，就像當前的隱密行動被納入政策塑造機制一樣。無論是在網路中還是戰爭中，隱密社會運動與操縱的潛力，優於公開行動的風險。風險判斷在隱密行動領域中占有重要地位，即使只是一種可能全面成功的形塑行動。

間接網路作戰的優點是使行動者有機會用非致命方式競爭，並延續我們使戰爭更加精確，並避免大規模人員傷亡的趨勢。這種行動造成的威脅是因安全需求所產生的限制性，對充滿技術的現代世界所造成的影響，以及讓一個超連結的世界被暴露於網路作戰造成的傷害性。在對手的國界內設計一個促進社會變革的環境，同時增加衝突升級的可能，這證明網路作戰對於強者及弱者至關重要。

作者簡介

Richard L. Manley二級准尉目前為海軍研究院國防分析所的理學碩士候選人。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. John Arquilla, "Cyberwar Is Already Upon Us," *Foreign Policy*, February 27, 2012, available at https://foreignpolicy.com/2012/02/27/cyberwar-is-already-uponus/.
2. Ivan Arreguín-Toft, "How the Weak Win Wars: a Theory of Assymetric Conflict," *International Security* 26, no. 1 (Summer 2001), available at https://web.stanford.edu/class/polisci211z/2.2/Arreguin-Toft%20IS%202001.pdf.
3. Keir Giles, "Assessing Russia's Reorganized and Rearmed Military," Carnegie Endowment for International Peace and the Chicago Council of Global Affairs, Task Force on U.S. Policy Toward Russia, Ukraine, and Eurasia, May 4, 2017, available at https://carnegieendowment.org/files/5.4.2017_Keir_Giles_RussiaMilitary.pdf.
4. Ryan C. Maness and Margarita Jaitner, "There's More to Russia's Cyber Interference than the Mueller Probe Suggests," *Washington Post*, March 12, 2018, available at https://www.washingtonpost.com/news/monkeycage/wp/2018/03/12/theres-more-torussias-cyber-meddling-than-the-mueller-probe-suggests/.
5. Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *Washington Post*, June 8, 2018, 5.
6. Ibid.
7. Hyeong-wook Boo, "An Assessment of North Korean Cyber Threats," in *The Kim Jong Un Regime and the Future Security Environment Surrounding the Korean Peninsula* (Tokyo: National Institute for Defense Studies, 2017), available at http://www.nids.mod.go.jp/english/event/symposium/pdf/2016/E-02.pdf.
8. Austin Carson and Keren Yarhi-Milo, "Covert Communication: The Intelligibility and Credibility of Signaling in Secret," *Security Studies* 26, no. 1 (January 2, 2017), 124–156, available at https://doi.org/10.1080/09636412.2017.1243921.
9. Jon R. Lindsay and Erik Gartzke, "Coercion Through Cyberspace: The StabilityInstability Paradox Revisited," in *The Power to Hurt: Coercion in Theory and in Practice*, ed. Kelly M. Greenhill and Peter J.P. Krause (Oxford: Oxford University Press, 2018), 40.
10. Carson and Yarhi-Milo, "Covert Communication."
11. Michael Krepon, "The StabilityInstability Paradox," *Arms Control Wonk*, November 2, 2010, available at https://www.armscontrolwonk.com/archive/402911/thestability-instability-paradox/.
12. Glenn Herald Snyder, *Deterrence and Defense* (Princeton: Princeton University Press, 2016).
13. Andy Greenberg, "How Not to Prevent a Cyberwar with Russia," *Wired*, June 18, 2019, available at https://www.wired.com/story/russia-cyberwar-escalation-power-grid/.
14. Ibid.
15. Carson and Yarhi-Milo, "Covert Communication."
16. Erin Blakemore, "What Was the Arab Spring and How Did It Spread?" *National Geographic*, March 29, 2019, available at https://www.nationalgeographic.com/culture/topics/reference/arab-spring-cause/.
17. Catherine O'Donnell, "New Study Quantifies Use of Social Media in Arab Spring," *UW News*, September 12, 2011, available at https://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/.
18. David Zimbra, Ahmed Abbasi, and Hsinchun Chen, "A Cyber-Archaeology Approach to Social Movement Research: Framework and Case Study," *Journal of Computer-Mediated Communication* 16, no. 1 (October 1, 2010), 48–70, available at https://academic.oup.com/jcmc/article/16/1/48/4067637.
19. Ibid.