專載

DOI:10.6237/NPJ.202004_54(2).0009

論社群網路安全－新興國家安全威脅

Social Cybersecurity: An Emerging National Security Requirement

作者：卡萊(Kathleen M. Carley)博士為電機電子工程師學會會士、貝斯科(David Beskow)為美陸軍中校。
譯者：黃依歆小姐

本篇取材自《美國軍事評論雙月刊》(Military Review)，2019年3-4月號，並為美國官方出版品，屬公共領域著作。

提　　要：

一、隨傳播科技發展與社群媒體普及，由網路安全引發的威脅層出不窮，而目前最新的作戰手段係利用人工智慧(AI)等高科技，影響軍隊基層官兵、民眾的想法，進而動搖社會結構，達到「不戰而屈人之兵」的效果。而其中又以中共、俄國對他國的操作最為明顯。為因應此新興國安威脅，特譯介本文介紹相關機動形式，期望我軍同仁提高警覺並回應此一迫切安全議題。

二、網路安全議題面臨典範轉移：「資訊作戰」手段由「科技駭入科技」進化為由「科技駭入人類心靈」、攻占人們認知與想法。這類戰場關於時下人類生活所依附的社群媒體平臺，戰略效果比擬二戰時的實體「閃電戰」。

三、在民主開放的地區，由於資訊流通自由，上述安全威脅會更為嚴重。近年來我方受到假資訊影響的案例屢見不鮮，在加強相關作戰能力之外，加強國軍與人民數位媒體素養、提升社群媒體「識讀」能力，將事實查核精神普及國軍同仁，才是數位時代中克敵之良方。

關鍵詞：社群網路安全、社群媒體、網路機器人

壹、前言

「社群網路安全」是國家安全議題的新興次領域[1]，將影響未來傳統及非傳統戰爭的所有大小層面，並導致不同的戰略結果。社群媒體安全係「一個新興的科學領域，聚焦於描繪、理解並預測網路時代中人類行為轉變，與隨之而來的社會、文化及政治變化，並在以網路為媒介的資訊環境中，面臨正在發生或迫近且變動的社群網路威脅下，建

註1：國家安全研究領域包含「經濟安全」、「能源安全」、「實體安全」、「環境安全」、「網路安全」等等，「社群網路安全」係國家安全研究領域中的新興次領域。

立維持社會以其本質續存所需的網路基礎設施。」[2]今日的科技能讓國家與非國家行為者，皆能以演算法的速度操縱全球意見市場，而這點正在改變各個層面戰爭的場域。當我們最近透過「混合戰」(Hybrid Warfare)的視角來分析「資訊作戰」時，我們會發現「資訊作戰」本身就是目的。「俄羅斯國家通訊社」的國際新聞特派員基謝列夫(Dmitry Kiselev)指出「資訊作戰是主要的戰爭型態。」[3]在攻擊、擾亂、扭曲並分化其他競爭國與組織的社會、文化與價值時，資訊是用來強化論述的有力工具。行為者[4]藉由在國家機構內部，弱化信任、摧毀國家價值的共識，並跨越國際社群，打破對這些價值的承諾，能夠在一場戰爭還沒開打前就預告下一場勝利。事實上，鑑於偶發的衝突已轉變成持續的威脅，俄羅斯參謀本部的高階領導人紛紛表示，「戰爭都還未宣告，但卻已經開始了。」[5]

在國力的元素中，資訊正在強化它的地位。戰略通常會透過國力的元素，包括外交、資訊、軍事與經濟等加以檢視。如今，科技得以運用一種過去無法想像的範圍與精細程度，讓國家與非國家行為者延伸他們在資訊領域的力量。這種新興的「資訊閃電戰」將會與第二次世界大戰初始的實體「閃電戰」擁有一樣的戰略效果。

「社群網路安全」與傳統的網路安全在技術本質上有所不同。傳統的網路安全是人類運用科技來「駭入」科技，目標是資訊系統；但「社群網路安全」則是人類運用科技來「駭入」其他人類，目標是人類與集結這些人類的社會。以上網路研究的典範轉移[6]與「認知駭入」(Cognitive Hacking)有關。這種新興「資訊作戰」考量到達成最廣泛的傳播，而選用網路媒體，專精於研究目標行銷、心理學與說服技巧，利用私人與政府機構的政策落差與對社會科學的理解，以部署具有戰略效果之資訊行動。

「社群網路安全」本質上是跨領域的計算社會科學(Computational Social Science)。「融合政治學、社會學、傳播科學或組織科學、行銷、語言學、人類學、鑑識、決策科學與社會心理學。」[7]這個領域的

註2：Kathleen M. Carley et al., “Social Cyber-Security,” in Social, Cultural, and Behavioral Modeling: 11th International Conference, SBPBRiMS 2018, Washington, DC, USA, July 10-13, 2018, Proceedings, ed. Halil Bisgin et al. (New York: Springer, 2018), pp.389-394。

註3：Joshua Yaffa, “Dmitry Kiselev Is Redefining the Art of Russian Propaganda,” The New Republic (website), 1 July 2014, https://newrepublic.com/article/118438/dmitrykiselev-putins-favorite-tv-host-russias-top-propogandist, accessed 14 November 2018。

註4：譯者註：本文所指「行為者」包含做出行為的國家、非國家(個人、團體、組織、企業等等)不同類型。

註5：Stephen Townsend, “Accelerating Multi-Domain Operations: Evolution of an Idea,” Modern War Institute at West Point, 23 July 2018, https://mwi.usma.edu/accelerating-multi-domain-operations-evolution-idea/, accessed 14 November 2018；Valery Gerasimov, “The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations,” Military Review 96, no. 1 (January-February 2016), pp. 23-29。

註6：譯者註：「研究典範」(paradigm)、「典範轉移」係指科學哲學家孔恩(Thomas Kuhn)所提出的概念，現今普遍運用於各種學科中。簡而言之，典範是讓我們能分析各種科學或理論的方法、概念、架構的工具，但隨時間累積，傳統的典範會被新的典範所取代，因此產生科學革命，這個過程稱之為「典範轉移」。在本文中，作者指出傳統的網路研究典範(科技駭入科技)已經轉移為新的社群網路安全典範(科技駭入人的認知)。

註7：ibid.1.

許多學者運用計算社會科學的工具如網路分析、空間分析、語意分析與機器學習，應用於個人、對話層次，一直到更廣的社群。若美國國防部欲「保衛國家的安全並在海外維持美國的影響力」，美國的軍事領導人必須瞭解「社群網路安全」這個新興學科，以及它如何影響軍隊、國家與價值觀[8]。以下將介紹與定義這門新學科，首先簡短地討論其歷史成因與讓其得以運作的社會科技變化，最後討論現今正蓬勃發展之「社群網路安全」的各種「機動形式」。在探討的過程中，我們將詳細說明「社群網路安全」與傳統網路作戰的相似與相異點。

貳、回顧：俄羅斯的資訊閃電戰

「俄羅斯正在進行資訊作戰史上最為驚人的資訊閃電戰。」－摘自2014年北大西洋公約組織威爾斯峰會[9]，美國空軍退役上將布里德勒(Philip Breedlove)

俄羅斯的國家宣傳機器以往只針對國內及前蘇聯的衛星國家[10]，但現在已經開始對國外的目標進行攻擊。2013年，俄國參謀總長格拉西莫夫(Valery Gerasimov)上將把「資訊作戰」定義為俄國戰爭的重要面向，他在其所發表知名文章〈科學的價值在前瞻〉(The Value of Science is in the Foresight)中，有做進一步闡明[11]。西方將該文章視為對烏克蘭危機的解釋，且錯把該危機看作是俄國軍隊遂行「混合戰」的開端。但這篇文章其實旨在說明他對「阿拉伯之春」的觀點，以及對美國在南斯拉夫、伊拉克和阿富汗征戰的看法[12]。在格拉西莫夫眼中，「阿拉伯之春」和美國所主導的中東地區同盟，都深深仰賴傳統軍力以外的資源來形塑事件，特別在「資訊作戰」上著力甚深。而武力角色只是最後關頭的臨門一腳罷了。

格拉西莫夫在研究了這些衝突後，嘗試加速他著手進行中的「資訊作戰」倡議，他說「資訊作戰」大幅增加「不對稱作戰」的機會，以削弱敵人的作戰潛力[13]。這些行動都與傳統的蘇聯國家安全委員會(KGB)的「積極手段」有關。KGB前特務卡盧金(Oleg Kalugin)少將把這些行動描述為「弱化西方、在各種西方社群同盟間挑撥離間(特別是北約)、在盟國間製造不合、削弱美國在歐洲、亞洲、非洲與拉丁美洲人民心中的形象，且得以進一步為可能發生的戰爭，做好必要準備。」[14]卡盧金所言強調了俄國「資訊閃電戰」的關鍵角色之一，即在每一條裂縫間尋找任何能夠插針的機會，試圖在一國之內或同盟國間進行分化，這包含了在政黨、種族、宗教、國家與其軍隊、國家與其盟國

註8：“Legacy Homepage,” U.S. Department of Defense, https://dod.defense.gov/, accessed 16 November 2018。

註9：Peter Pomerantsev, “Russia and the Menace of Unreality: How Vladimir Putin is Revolutionizing Information Warfare,” The Atlantic (website), 9 September 2014, https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/ accessed 14 November 2018。.

註10：譯者註：指當時的波蘭、匈牙利、保加利亞、羅馬尼亞、東德等等。

註11：Gerasimov, “The Value of Science is in the Foresight.”

註12：Charles K. Bartles, “Getting Gerasimov Right,” Military Review 96, no. 1 (January-February 2016): pp. 30-38.

註13：Ibid。

註14：Steve Abrams, “Beyond Propaganda: Soviet Active Measures is Putin’s Russia,” Connections: The Quqrterly Journal 15, no. 1 (2016): pp. 5-31.

之間，一個分裂的國家自然會在抵禦攻擊的能力上居於下風。

俄羅斯「資訊作戰」的新興作為早在前蘇聯時代的宣傳行動中就可見端倪。1951年，耶魯大學法學教授拉斯威爾(Harold Lasswell)概述了蘇聯的宣傳機器(繼承者是目前的俄國安全機器)：「主要的戰略目的，旨在節省保護及擴展俄國菁英權力的物質成本，不論在國內外皆然。這樣的宣傳是在爭奪人類的心靈，從蘇聯的觀點來看，只有爭奪物質資源支配權，大眾的心靈才有可能被塑造與影響。因此，俄羅斯宣傳的目標不是在一個既定的國家內以和平的方式說服大多數人民，以做為占領的前奏；反之，是要累積能達到共識的物質資源，成功影響意識形態上的少數族群……，蘇聯的宣傳家與他們的代理人能夠毫無節制地說謊與歪曲事實，因為他們大部分都對人類的自尊需求無感，……而這都是在鞏固現在與未來的克里姆林宮菁英的權力[15]」。

這種慣用的手段一直延續至今，其在建立一個極小核心的同時，分化了所有反對組織與機構，並時時刻刻都在利用假訊息帶來的效果。然而時至今日，科技已讓這樣的手段達到規模與距離上都是1951年蘇聯難以想像的境界。

俄羅斯發展這些手段不是偶然的。早在2003年，俄羅斯科學院(Russian Academy of Sciences)就進行了基礎研究，要發展「資訊作戰」的高階應用數學模型，與其社會應用型態。研究員們結合社會科學與數學模型以進行如「社會中的謠言與資訊宣傳的數學模型」的研究，在這些論文宣稱是為防禦目標的同時，相關攻勢作戰的應用，早已悄然進行。

這樣的作戰行動與日益演變成為核心的「政治技術操作師」(Political Technologist)有關。這些人是政府內、外的領導者，他們瞭解人類、政治、軍隊與科技領域互相關聯的本質。運用這種對「多領域」的理解，他們發展並合作塑造許多行動，運用網路與科技領域來影響社會、政治與軍事領域。舉例而言，在2018年美國期中選舉前，莫斯科的「政治技術操作師」馬可維奇(Alexander Malkevich)就建置一個位於莫斯科的網站(www.USAreally.com)[16]，其任務是散布一個扭曲的敘事內容，並進行煽動，目的是在美國人民間製造不合；最終整起事件被主流美國新聞媒體報導，或至少受到美國主流新聞聚合網站的關注[17]。他本人在推特帳號上的個人簡介寫著，「記者，媒體人，對生活有熱情的人，不怕在俄羅斯境內工作，以俄羅斯之名。」[18]這就是個典型的政治技術操作師。

註15：Harold D Lasswell, "The Strategy of Soviet Propaganda," Proceedings of the Academy of Political Science 24, no. 2 (1951):pp.66-78。

註16：Tim Johnson, "Exclusive: 'Little Russian Media Project' Tries to Turn America against Itself," McClatchy, last updated 10 June 2018, https://www.mcclatchydc.com/news/nation-world/national/national-security/article213403299.html, accessed 21 December 2018。

註17：譯者註：整合各種新聞來源至其單一網頁供瀏覽的大型入口網站、搜尋引擎或社群網站，如Yahoo!、Google、LINE等。

註18：Alexander Malkevich (@McCevich), "Journalist. Media man. A person who is interested in life. And he is not afraid to work in the regions of Russia. And in the name of Russia [in Russian]," Twitter, https://twitter.com/McCevich, accessed 21 December 2018。

參、戰略重心轉移

二十世紀充斥著戰史上最對稱的戰爭及「動能戰」(Kinetic War)[19]，隨時序進入二十一世紀，在越過冷戰競賽數十年後，大量「不對稱」與「非動能」衝突開始浮現。在第一次世界大戰期間，各國只為了幾碼的實體領土而犧牲無數人命；今日，許多行為者發展了複雜的機制，要在不知不覺間贏取人類領域的「那幾碼」(Yards)，而這很可能進一步讓他們贏得實兵作戰的勝利。

今日的地理因素很重要。例如美國在太平洋與大西洋上分別建立了其最大的兩個安全機制[20]，至今未有變動；克里米亞(Crimea)被俄羅斯併吞[21]，大部分原因是因為黑海港口的戰略重要性(及能源考量)[22]；阿富汗的動盪將會持續的原因，部分也是因為其地理位置[23]。地理確實很重要，而且也會一直重要下去；然而，包含科技的許多因素，已將局面轉向人類身上。

在反恐戰爭中，美軍內部曾一度激辯這樣的議題轉向，經過數年的爭論，多數人似乎同意在2009年《小型戰爭期刊》(Small Wars Journal)一篇文章所言：「美軍在反叛亂(Counterinsurgency)作為上必須發揮其效能，最大的改革之一就是將戰略重心從實體領域轉向戰爭中的人類面向。」[24]現在已公認這是在反叛亂上的變革趨勢，但仍待觀察這樣向人類領域的轉向，將如何改變大規模作戰與戰鬥。

由於科技賦予人群得以分散行動的能力，他們進行組織並推翻了許多既存的專制政權；「阿拉伯之春」過後，將人群視為戰略重心有了全新的意義。這些行動震驚了世界，使東、西方的領導人皆開始研究相關議題，它們強調了人類面向的權力，以及社群媒體動員人群的力量。軍事期刊中的許多文章都記載了這些行動，特別是聚焦於賦予這些行動權力的社群媒體上。2013年格拉西莫夫於俄國的《軍工快遞》(Military-Industrial Courier)周刊也發表一篇研究西方的文章，提出「混合戰」與「灰色戰」(Grey Warfare)的起源，但這比較像是其對「阿拉伯之春」的個人感想(就像對在伊拉克、阿富汗與南斯拉夫衝突的感想一樣)，而不是要試圖去創造一種新型態的戰爭[25]。

註19：譯者註：簡言之「動能戰」指涉實體戰爭(可見的槍砲火力)，「非動能戰」則牽涉非實體戰爭(外交、網路、輿論戰等)。

註20：Peter Zeihan, The Accidental Superpower: The Next Generation of American Preeminence and the Coming Global Disorder (New York: Twelve, 2014)。

註21：譯者註：Steven Lee Myers and Ellen Barry, “Putin Reclaims Crimea for Russia and Bitterly Denounces the West”, The New York Times, March 18, 2014, https://www.nytimes.com/2014/03/19/world/europe/ukraine.amp.html。

註22：John Biersack and Shannon O’ Lear, “The Geopolitics of Russia’s Annexation of Crimea: Narratives, Identity, Silences, and Energy,” Eurasian Geography and Economics 55, no. 3 (2014):pp. 247-269。

註23：Robert D. Kaplan, “The Revenge of Geography,” Foreign Policy, no. 172 (2009): pp. 96-105。

註24：James A. Gavrilis, “A Model for Population-Centered Warfare: A Conceptual Framework for Analyzing and Understanding the Theory and Practice of Insurgency and Counterinsurgency,” Small Wars Journal, 10 May 2009, accessed 14 November 2018, http://smallwarsjournal.com/blog/journal/docs-temp/241-gavrilis.pdf。

註25：Bartles, “Getting Gerasimov Right.”

許多其他國家與非國家行為者觀察到這些改變，並開始尋找在網路空間中操縱這些行動的方法。透過「資訊作戰」，許多國家與行為者已經實際操縱過自己的人民或組織，進而尋求擴展相關經驗至國外人口與社會上[26]。直接針對社會的基本結構展開行動，意即瞄準一個國家真正的重心，在戰爭的戰術與戰略層級都會產生關鍵影響，而這也代表著「社群網路安全」這個新興領域的濫觴。

肆、讓改變發生

在人類溝通與社會資訊流上的兩個改變（去中心化、不需要實體存在），使得社群網路威脅得以發生。首先，科技去除了影響社會所需的實體接近需求，而資訊流的分散則減低了進入的成本。義大利國際政治研究所政治學家瑞吉(Fabio Rugge)總結道：「對操弄資訊的顛覆性效果來說，網路空間是一個相當有力的加乘因子；因為它提供了高度連結性，極短的等待時間、低進入成本、眾多不須經由媒介的傳播點，以及能夠全然不顧實體距離與國家疆界之隔閡。最重要的是匿名性與無法歸罪於攻擊者，都造就了網路空間成為一個灰色地帶。」[27]

一、去中心化

過去30年以來，我們觀察到資訊流快速地去中心化。傳統的政府、大型組織，以及一些大型媒體控制了紙媒(報紙等印刷媒體)、廣播及電視新聞報導。這些機構控制了資訊的流動方向，通常是將資訊一致地傳播到整個社會當中。然而隨著部落格、微網誌與社群網路的興起，現在世界上多數人反而是分散地在社群媒體上取得資訊[28]。創造網路上的爆紅內容，常享有低進入門檻與財務誘因，且匿名性也相對使人願意去完成。這樣的去中心化，降低了外部行為者的攻擊成本，也不容易被發現與歸罪。

控制資訊流動的品質，目前也呈現去中心化的趨勢。使用者可以逕自進行事實查核，而不需靠記者去完成。對那些生長在新聞普遍受信任年代的使用者而言，數位新聞時代中的事實與非事實混雜並存，這使他們感到無所適從，特別是當這些扭曲事實的目的，是在加強他們固有的偏見時更是如此。傳統的新聞商業模式需要事實，如果報導失真的狀況屢見不鮮，記者會失去工作，而新聞機構也難以持續獲利；然而，社群媒體的商業模式奠基於整體流量與廣告，在關注事實查核上並不費心。這樣的情況近年來有緩慢的改變，由於「推特」與「臉書」兩大社群巨擘在清除散布假新聞帳號進度緩慢，2018年8月兩公司的股價便應聲下跌。

最近，全球的立法機關都致力於找到管控新聞品質的方法，然而這都牽扯到審查與言論自由降低的敏感議題。在某些情況下，這會是一場絕對性災難，特別是社群媒體公

註26：Lasswell, “The Strategy of Soviet Propaganda.”

註27：Fabio Rugge, “ ‘Mind Hacking’ : Information Warfare in the Cyber Age,” Analysis No. 319, Italian Institute for International Political Studies, 11 January 2018, https://www.ispionline.it/en/pubblicazione/mind-hacking-information-warfare-cyber-age-19414, accessed 14 November 2018。

註28：Elisa Shearer and Jeffrey Gottfried, “News Use Across Social Media Platforms 2017,” Pew Research Center, 7 September 2017, http://www.journalism.org/2017/09/07/news-use-across-socialmedia-platforms-2017/, accessed 14 November 2018。

司的平臺可提供人們標記假資訊或惡意訊息之用。因為若這種功能是開放使用的，不管是透過應用程式介面(API)或網頁/手機介面，傳播假訊息的機器人程式也可以用演算法的極快速度，標記所有正確訊息為假，造成災難性的損害。

二、不需要實體存在

在歷史的洪流中，影響力的發揮有賴實體的存在或至少實體的接近性。要影響古羅馬社會的重心-即古羅馬廣場的集會談話內容，需有一位行為者或代理人親身出現於廣場，或至少要身在羅馬城，這個人要可清楚辨識且積極參與討論，就算是在祕密行動中，也需要實體的存在。這樣的需求適用於二十世紀前半段，當時收音機與傳單興起，並不需要直接的實體存在，但仍需一定程度的接近性；礙於地理疆界的限制，就算是神通廣大的蘇聯宣傳行動，仍大幅侷限於東歐與亞洲。網際網路的出現則鬆綁了這樣的限制，多數社會在自由且開放的環境中交流，使網路空間中的行動者得以從世界各個角落參與行動，不受國界限制，那些重視言論自由與開放意見市場的國家，更容易受到這些威脅的攻擊[29]。世上公認最封閉的國家－北韓，反而最不受網際網路社會操縱的影響，要直接影響北韓社會，仍然需要實體存在或地理接近性。

開放社會對於透過科技進行社會操縱的脆弱性會更嚴重，因為大部分的戰略性資訊行動，都在全球社群媒體平臺上進行，而這些平臺都是私人擁有，且在政府的直接監控範圍之外(儘管仍透過法規影響)。所有的社群媒體公司都在它們的平臺上審查內容，但這些審查的動機聚焦於改善全世界最多人的使用者經驗，並不是以任何單一國家的國家安全做為考量。在商場上，對任何議題選邊站都是不妥當的，因為這會使其流失某部分的顧客基礎。政府的內容審查會被認為是涉及黨派立場，且違反它們自己所擁護的言論自由，而現在也已出現交由公正第三方來審查內容的作為。截至目前為止，這些行動所關注的層面太窄，且容易遭人規避。第三方審查的案例之一是「社會科學行動」(Social Science One)，這是一個跨越政治光譜介於學術研究者、私人產業與資金間的創意性夥伴關係，目的在促進社群媒體數據的第三方研究，同時保留這些數據的個人隱私，而這樣的行動多還在初期發展階段。

伍、社群網路的機動形式

就像在實體領域和傳統的網路領域上，社群網路領域也提供了許多的「機動形式」。在這個領域中，敵人可以操縱資訊與網路兩者，這些網路可以是社交網路(例如A和B是朋友)、對話網路(B回信給A)，或是資訊網路(A和B都分享了主題標籤#NATO[30])。

註29：Robert F. Baumann, “A Central Asian Perspective on Russian Soft Power: The View from Tashkent,” Military Review 98, no. 4 (July-August 2018): pp. 50-63。

註30：譯者註：主題標籤(hashtag)是網路網路上的資料標籤類型之一，普遍運用於臉書、推特、Instagram等社群網站的貼文中，用來連結所有相同標籤主題的貼文，使用戶在社群平臺上搜尋內容更加容易。使用者可以在自己貼文內加上任何主題標籤，幫助他人更快找到自己的貼文；運用熱門的主題標籤，也能使自己的貼文被更多用戶看見。主題標籤通常由一個「#」加上一個詞、單字、或無空格的一句話組成。

附表：社群媒體安全的機動形式(BEND模式)

分類	網路機動		資訊機動	
	社群網路操縱		知識網路操縱	
	可以做些什麼來影響正在說話的人/可以做些什麼來影響誰聽誰說		可以做些什麼來影響正在討論的事情	
正面	支持 Back	增加某意見領袖重要性的行動	承諾 Engage	開始討論相關並適宜的主題
	建立 Build	創造一個團體(或貌似一個團體)的行動	解釋 Explain	提供細節或闡述某主題的討論
	連結 Bridge	在兩個或多個團體間建立連結的行動	鼓勵 Excite	給團體歡樂/幸福/振奮/熱情的討論
	刺激 Boost	壯大某個團體，或使其看起來有成長。	加強 Enhance	鼓勵團體繼續討論某主題的討論
負面	抵銷 Neutralize	限制意見領袖的效能，例如減少潛在或真正追踪、回文或關注的人數。	去除 Dismiss	討論為何某主題不重要
	隔離 Nuke	使某個團體逐漸解散的行動	扭曲 Distort	改變某主題主要訊息的討論
	窄化 Narrow	使某團體與其他團體隔離的行動	打擊 Dismay	帶給團體憂慮/哀傷/憤怒的討論
	忽視 Neglect	縮小某個團體，或使其看起來規模變小了。	擾亂 Distract	討論某個完全不同且不相關的主題

資料來源：David M. Beskow, Kathleen M. Carley, “Social Cybersecurity: An Emerging National Security Requirement”, Military Review,99 no.2 (March-April 2019):123.

一、BEND[31]機動形式

每一種資訊行動所追求的最終狀態都不同。傳統「資訊作戰」會加強支持所欲敘事(Narrative)[32]、減少支持「反敘事」(Counternarrative)。其他作戰則不論敘事為何，只追求騷動增加和信任降低的最終狀態。這樣的騷動是用來製造社會分裂。每一種最終狀態都是由BEND機動形式所構成(如附表)。

BEND機動形式解釋了一名行為者如何能夠操縱意見、想法與資訊的自由市場。這樣機動形式建立在大西洋理事會數位取證研究實驗室(Atlantic Council Digital Forensic Research Lab)資深研究員尼莫(Ben Nimmo)所稱之去除、扭曲、打擊及擾亂的典範上[33]。BEND模式係以兩個對立的觀點來區分機動的形式。

二、網路機動(Network Maneuver)

網路機動係對現行網路的操縱，在這些機動當中，敵人會去標定一個社群網路(指網路上的社會與談話連結投射)。網路機動的形式如下：

(一)吸收意見領袖

爭取線上意見領袖的認可與交流，並利用其影響力來散播自己的敘事。

註31：BEND模式的名稱，取自附表中四類機動形式的英文首字母之縮寫。

註32：敘事(narrative)為社會學、傳播學、廣告學、語言學常見名詞，是人類思考和組織知識的方法。簡言之，其指涉一套說故事的方式，包含其內容腳本、意識形態、核心訊息等等。例如超商飲料品牌「左岸咖啡館」的電視廣告敘事，就在傳達巴黎的意象，藉由廣告影像的鋪陳，要將觀眾帶到法國巴黎左岸；而「喝左岸咖啡館包裝飲料就能身在巴黎」就是其品牌所欲傳達之敘事。

註33：Ben Nimmo, “Anatomy of an Info-War: How Russia’s Propaganda Machine Works, and How to Counter It,” Central European Policy Institute 15 (2015)。

(二)建立社群

建立某個議題、想法或興趣的社群，並將某項敘事植入該社群中。這曾經在烏克蘭成功實現過，藉由成人內容分享帳號所建立的青年社群，在其中注入反烏克蘭與支持俄羅斯的論述。

(三)縮短距離

植入某團體的想法至其他團體。這樣一來，敵人將能夠識別甲與乙兩個社群，敵人可將乙團體的想法注入甲團體，作法是先對甲團體進行滲透，再慢慢加入來自乙團體的轉推文或分享內容，藉此縮短兩團體之間想法的落差。

(四)虛偽的一致性

提出錯誤概念、提倡某既定內容係代表群眾的共識，因此應被認定為大家所接受的概念或信仰。

三、資訊機動(Information Maneuver)

資訊機動係操縱資訊及網路空間中資訊的流動或相關性。資訊機動的形式如下：

(一)誤導

在事件的脈絡中引進不相關、且帶有分歧意見的話題，目標是轉移討論的走向。

(二)綁定主題標籤(Hashtag)

將內容與論述與不相關的流行話題或主題標籤連結在一起。

(三)煙幕技法

同時在語義上與地理上散播遮掩其他行動的內容。

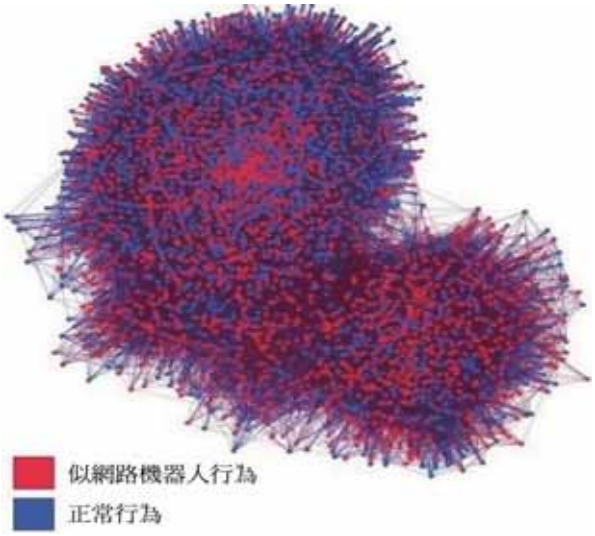
(四)扭轉風向

積極擾亂或吸收一個多產的線上討論。

陸、網路機器人係戰力加乘因子

在「資訊作戰」的領域中，「網路機器人」(Bots)運用於戰力加乘因子的案例日益增加，它們利用機器學習及人工智慧(Artificial Intelligence，AI)技術遂行針對性、即時性的資訊交易，並留下高操縱性的關鍵對話，供人類操作者運用。在這樣的背景下，這些人類行為者通常會被稱為「酸民」(Trolls)，雖然他們與電腦(機器)行為者的手法都是在網路上製造歧見，但兩者是不同的概念。

網路機器人係一個社群媒體帳號，運用一臺電腦自動遂行社群媒體任務。以推特(Twitter)的介面為例，一個機器人帳號可以自動推文、轉推、追踪、加好友、回文、引述並按讚。這種機器人可以利用有創意的方法來產生內容，不論是在網路上到處「爬文」(Scraping，並自動摘要這些文章)、轉推已存在的內容、操縱其他人類使用者製作的既有內容，或是透過人類輸入數據與人工智慧來創造自己的內容，都能達到可觀的結果。將這些內容製造出來以後，網路機器人可以進一步控制要推文的時間，使得表面上就像是人類帳號自己進行的一樣自然(又或者假扮人類帳號不是本次行動的主要目的，它們也能日以繼夜進行數千次行動，來達到其他目的)。最終，這些網路機器人會被組織成「機器人網路」或「殭屍網路」(Botnets)，有時也稱「殭屍網軍」(Bot Armies)或「聯合殭屍群」(Coordinating Bots)，彼此之間加好友、跟隨，甚至相互



附圖：網路機器人與人類操作者網路行爲分布圖

說明：圖為推特上圍繞瑞典近期選舉主要政治對話的網路行為，顯示雙方行為密切交織。

資料來源：David M. Beskow, Kathleen M. Carley, “Social Cybersecurity: An Emerging National Security Requirement”,Military Review, 99 no.2 (March-April 2019): P.125。

拉抬宣傳，呈現出在網路上受到歡迎的樣子。

運用網路機器人的理由相當廣泛，且能夠創造正面、擾亂或惡意的效果。正面的網路機器人案例包括個人助理系統，以及有向大眾告警天然災害的作用；擾亂性的殭屍機器人則散布垃圾郵件，內容可包括商業廣告或成人內容；有害的網路機器人則主要運用於宣傳、壓迫異己內容、恫嚇、網路入侵與操縱[34]。

雖然我們通常傾向將帳號分類為網路機器人或人類使用者，現實當中每個帳號有著自動化程度的不同，許多帳號並不是完全自動化的(亦即所有的網上活動都由電腦執行)，這些帳號仍有部分仰賴人為涉入，以產出微妙的人類對話內容；而電腦則負責在背後執行一定規模的任務。最後，網路機器人若再與人工智慧相結合，將能大規模、以演算法的速度執行極度複雜的作戰任務(如附圖)。

柒、結語

「新一代的戰爭將由『資訊作戰』與心戰所主導，尋求對軍隊及武器的優勢控制，並在道德上與心理上挫敗敵軍成員與人民。在目前資訊科技的革命當中，『資訊作戰』與心戰將會替未來的勝利打下基礎。」－摘自喬基諾夫(G. Chekinov)等人所著之《新一代戰爭本質》[35]

對任何國家而言，最大的戰略弱點係來自於其內部，而非外部。領導者必須瞭解「社群網路安全」，以防止這些內部弱點遭外部操縱。身為軍事領導者的吾人，更應瞭解未來「資訊閃電戰」的行動主軸之一，將會在我們、我們所捍衛的社會，與領導我們的

註34：Cristian Lumezanu, Nick Feamster, and Hans Klein, “#bias: Measuring the Tweeting Behavior of Propagandists,” Proceedings of the Sixth International Conference on Weblogs and Social Media (Palo Alto, CA: The AAAI Press, 2012), pp. 210-217; John-Paul Verkamp and Minaxi Gupta, “Five Incidents, One Theme: Twitter Spam as a Weapon to Drown Voices of Protest” (paper presentation, 3rd USENIX Workshop on Free and Open Communication on the Internet, Washington, DC, 13 August 2013), pp. 1-7; Rosie Alfatlawi, “Thousands of Twitter Bots Are Attempting to Silence Reporting on Yemen,” Al Bawaba: The Loop, 22 November 2017, accessed 16 November 2018, https://www.albawaba.com/loop/original-saudi-bots-yemen-suffering-1051564; Matthew Benigni and Kathleen M. Carley, “From Tweets to Intelligence: Understanding the Islamic Jihad Supporting Community on Twitter,” in Social, Cultural, and Behavioral Modeling: 9th International Conference, SBP-BRiMS 2016, Washington, DC, USA, June 28-July 1, 2016, Proceedings, ed. Kevin S. Xu et al. (New York: Springer, 2016), pp. 346-355。

註35：Sergey G. Chekinov and Sergey A. Bogdanov, “The Nature and Content of a NewGeneration War,” Military Thought 4 (2013): pp. 12-23。

文職領導階層之間進行挑撥離間的行動。一個內部缺乏信任的組織將會失去金援、減少運作，且喪失應有的行動力。

如果美國主要的任務之一係「維持美國在國外的影響力」，則需要找到倡導美國價值在國際自由意見市場的的角色，並能同時與公、私部門進行合縱連橫。這樣的影響力展現可以是網路上的互動，或是與前進部署排長的握手畫面。

軍事領導者必須在相關的資訊環境中，啟動確保機動自由的政策。一份最新的蘭德(RAND)報告〈監控社群媒體：以經驗教訓因應未來資訊作戰〉指出，美國國防部必須在政策上改弦更張，以在資訊領域中全力遂行道德機動[36]。大多數的「社群網路安全」運作人員(網路機器人的應用者與捍衛者)都使用應用程式介面與公開資料，以便取用並行動於這樣一個數據環境。換句話說，應用程式介面同時是進攻型或防禦性社群網路行動的切入點，在軍中，僅有特定政策或官方組織得以進入應用程式介面，其他機構則毫無權限。我們需要的是靈活的政策，能在變動的資訊環境中採取主動，同時保護網路上老百姓的個人隱私權，並繼續行使國防部(指美國)應有的權力。

總而言之，我們必須直接教育軍隊、間接教育社會，有關於現代資訊環境的去中心化特質、哪些存在有風險，並有獨立審視事實與意見的方法與手段，因為這些都是我們每天所接觸，而得以形塑我們的價值觀與態度的資訊。我們必須建立相關政策，捍衛「社群網路安全性」，尋求去除任何在軍隊與社會間挑撥離間的手段。美國國防部在跨部門行動中要勇於承擔責任，以對抗今日所面對的「資訊閃電戰」。相信在可預見之未來，「社群網路安全」也將會是一門顯學。

捌、譯後語

2018年日本關西機場事件，我主流媒體引用未經查證網路訊息、中共網站內容，影響後續網友在社群媒體平臺大量撻伐、轉發我駐日單位無作為訊息[37]，間接造成外交官自縊事件[38]，國人應記憶猶新。另外，在最近幾年的選舉中，網路操作也已經是大勢所趨[39]。根據瑞典哥德堡大學數位社會研究資料庫的數據，在全球179個國家或地區中，臺灣名列受境外假資訊攻擊的第一位[40]，我國家安全面臨相關威脅已是燃眉之急，相關

註36：William Marcellino et al., “Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations” (Santa Monica, CA: RAND Corporation, 2017)。

註37：譯者註：賴佩璇、劉宛琳，〈蘇啟誠之死 卡神楊蕙如雇網軍護謝長廷被訴〉，《聯合報》，2019年12月3日，https://udn.com/news/story/11311/4201436，檢索日期：2020年1月13日；吳珮如、陳建瑜，〈【卡神雇網軍1】護謝長廷轟大阪處「該死」楊蕙如遭起訴〉，《蘋果日報》，2019年12月2日，https://tw.appledaily.com/new/realtime/20191202/1671491/，檢索日期：2020年1月13日。

註38：譯者註：黃泓瑜，〈【2019事實查核工作坊／高雄場】報導一：情緒主導假新聞傳遞 悖離溝通本質〉，臺灣事實查核中心，2019年12月17日，https://reurl.cc/YlKmED，檢索日期：2020年1月13日。

註39：譯者註：王銘宏、戴毓辰，〈螢幕後的殺手：輿論操作與對抗〉，《蘋果日報》，2019年12月10日，https://tw.appledaily.com/highlight/20191210/EMTFJPJ7TLXBBFP3XL3SKWQJQE/，檢索日期：2020年1月13日。

註40：譯者註：林倖妃，〈【輿論戰爭，臺灣開打】一個帳號幾多錢，網軍價格全揭露〉，《天下雜誌》，第671期，2019年4月23日，https://www.cw.com.tw/article/article.action?id=5094849，檢索日期：2020年1月13日。

操作在未來只會更加細緻、且難以防範。

本文作者卡萊(Kathleen M. Carley)博士係最早探討「社群網路安全」科學的先鋒，她指出所有的社群媒體平臺主要目標有二：提供用戶和特定用戶的連結、提供用戶和特定內容的連結。對某些國家來說，藉由電腦程式控制的網路機器人大軍，能做為攻擊目標國家的低成本武器，運用演算法的優先定序決定哪些用戶能看到哪些內容，並自動大量反覆貼送、按讚追踪，以驚人的速度使其欲操控的訊息獲得同溫層之迴響。中共對臺所散布之特定訊息，也已建立某種特殊模式[41]。而共軍戰略支援部隊近期倡議採用具人工智慧功能的「網路輿情智慧引導」軟體，自動視情況調整並產生內容、適時運用貼文，便是進階「資訊作戰」的展現。

我國在民主開放的社會體制下，自然不會犧牲言論自由，以換取管控科技遏止相關內容的作法。然而軍方的軍事思維應正視並加入掌控社群媒體趨勢這一項，擴大編制專業團隊、即時監控並做出適當回應，同時努力培養國軍與人民的數位媒體素養才是正途。學者指出，掌握資訊流傳原因的主要因素還是在於人，而非科技[42]。透過網民、第三方事實查核機構培養人民媒體「識讀」能力，讓軍民對於去脈絡化、部分揭露、病毒式擴散的資訊有所警覺，並避免照單全收，才是數位時代中面對新興國安威脅的根本解方。

作者簡介：
卡萊(Kathleen M. Carley)博士為電機電子工程師學會會士(IEEE Fellow)。她是卡內基・美隆大學(Carnegie Mellon University)資訊工程學院資訊社會學教授、該校社會與組織系統運算分析中心(CASOS)主任，並擔任Netanomics公司營運長。
貝斯科(David Bescow)為美陸軍中校，曾任第82空降師與第4步兵師師長。他是卡內基・美隆大學電腦科學院博士候選人。

譯者簡介：
黃依歆小姐，淡江大學法文系92年班、巴黎第八大學文化與傳播學碩士2007年班，曾任《經濟日報》記者，現服務於國防部政務辦公室、《國防譯粹》副主編。

註41：譯者註：劉宗翰，〈論社群媒體的安全議題及因應之道〉，《海軍學術雙月刊》，第54卷，第1期，2020年2月1日，頁116-117。
註42：譯者註：同註38。