



● 作者/John Antal ● 譯者/章昌文 ● 審者/黃依歆

2019年美「中」網路軍備競賽

The Cyber Arms Race in 2019

取材/2019年7-8月德國軍事科技月刊(*Military Technology* , July-August/2019)

“FIGHT'S ON!”

WED FEB 05 2020 036
04:23 09:23 14:23 19:23 23:53
JAPAN HAWAII PACIFIC EASTERN ZULU RFBHNN



全球網路軍備競賽正如火如荼展開。(Source: USMC/Jacob Osborne)

爲能在未來衝突中勝出，國家須在網路空間中取得優勢。因此，美「中」在近五年內相繼成立司令部層級的指揮單位，以建構全面的網路攻防能力。

現代國家及其軍隊都倚賴網路，且當幾乎所有相互連結的裝置形成物聯網(Internet of Things)時更是如此。在物聯網中，無論是精密或簡單的裝置，都會蒐集資料。而這些互相連結的每一個裝置，從船艦、戰鬥機、智慧型手機到烤麵包機，都將成為惡意網路攻擊的入口。隨著全球科技應用擴大，當物聯網成為現實，攻擊面將呈指數增長，網際空間領域更大幅擴張。由於每一個裝置都可能成為網路攻擊入口，許多國家投資數十億美元建立網路防禦，同時，各國也投資發展攻擊性網路武器。在一個幾乎無法遏止網路攻擊的時代中，擁有最佳網路防禦和最強網路攻擊武器的國家，將具備極大的優勢。

網路空間是一個關鍵戰爭領域，對其他領域包括陸地、海上、空中和太空具有阻擾效應。在未來戰爭中，這五個領域全在互相競爭，而網路戰爭或許是用來打擊其他四個領域的首要武器。網路戰讓民族國家、私人企業和個人能以有效、代價低和不認帳的方式攻擊重心，因此，透過檢視美國和中共在此面向上的發展，即可輕易證實網路軍備競賽加劇的事實。

中共戰略支援部隊

所有戰法都是以欺敵為基礎，而最佳欺敵法是在敵人不知己身處戰爭的情況下開戰。儘管中共極力否認，但其對美國和歐洲的網路戰爭早已開打。在反覆且造成重大損失的攻擊後，美國和歐盟仍未將中共的舉動稱為戰爭，但近期發生的重大事件或許得另當別論了。



區域情勢 REGIONAL

2010年1月，中共對谷歌發動了一次網路攻擊，竊取其機敏的智慧財產，谷歌隨後抗議，但卻未採取進行任何實質行動。2012年，英國航太系統公司(BAE Systems)遭到源自中共的駭侵，駭客竊取了F-35聯合打擊機的關鍵數據。2014年，美國司法部長宣布共軍人員駭入美國鋼鐵公司(US Steel Corp.)、鋼鐵工人聯合工會(United Steel Workers Union)、美國鋁業(Alcoa)、阿勒格尼科技(Allegheny Technologies)、太陽能世界

(Solar World)和西屋電氣公司(Westinghouse)。2015年，中共的網路攻擊竊取了美國國防承包商數兆位元組的機敏資料，並駭入美國人事管理局(Office of Personnel Management)，竊走2,200萬名美國人的重要資料。此次攻擊嚴重到被稱為「網路珍珠港」。當美國專注在俄國2016年的駭侵時，中共支持的駭客突破世界最大的遠端控制及桌面共享軟體供應商——德國軟體公司TeamViewer，並駭入了兩家位於紐約的著名律師事

務所，偷走近300萬美元。2017年，美國司法部以駭侵穆迪分析(Moody's Analytics)、西門子(Siemens AG)和全球定位系統開發商天寶導航(Trimble)電腦系統為由，起訴中共網路安全公司博御信息技術公司(Boyusec)所僱用的三名中共公民。2018年12月，中共駭客破解歐盟的通信系統，讓中共得以讀取數年來累積的機敏外交與經濟情報。2018年，中共駭入一家美海軍承包商，竊走6,140億位元組的數據。2019年5月，隸屬

2019年於中國大陸浙江省舉行的「世界互聯網大會」(World Internet Conference)。(Source: Reuters/達志)



中共情報機構的駭客入侵美國國家安全局，隨後發現中共自2016年以來就一直在使用工具擷取該局資料。而這些發生在公共領域、曝光有限的攻擊行為，只是中共攻擊美國和歐盟網路行動的冰山一角。

儘管這些駭入行動部分可能是中共民間犯罪分子所為，但共軍顯然部署專門作戰單位，持續遂行網路攻擊和諜報，為中共取得對美國和西方國家經濟與軍事優勢的部分作為。2019年1月，美國聯邦調查局反情報處助理處長普里斯塔普(Bill Priestap)在參議院司法委員會的聲明中表示，「中共從美蘇的冷戰理解到的重要經驗是：經濟實力是國力基礎，美『中』間的競爭，就算不會完全決定，也將大幅影響美國的經濟實力。」中共目標是窮盡一切手段贏得此長期的戰爭，從而成為主導世界的強權。

共軍為協調其網路行動，在2015年成立了戰略支援部隊。該部隊統合了共軍在太空、太空反制和網路空間的作戰行動，由單一司令部管轄所有網路部隊。根據2018年10月美國國防



共軍戰略支援部隊的徽章。該軍種成立於2015年12月，結合網路、太空和電子戰任務，目標是一體化共軍內部於關鍵戰鬥領域的行動。

(Source: Military Technology)



美國網路司令部的徽章。該司令部負有整合網路空間行動指揮、強化國防部在網路空間的戰力，及統合與加強國防部網路專業之任務。

(Source: Military Technology)

大學科斯特洛(John Costello)和麥克雷諾茲(Joe McReynolds)的〈中共戰略支援部隊：一支新世代兵力〉(China's Strategic Support Force: A Force for a New Era)研究，其中提及，「藉由整合資訊戰多項專業領域為單一軍種、結合網路諜報與進攻行動、統合資訊戰戰役計畫作為及兵力發展，同時一體化資訊作戰的指揮與管制責任，戰略支援部隊改進了共軍遂行資訊作戰的能力。」該報告繼續寫道，「相較於美國網路司令部，戰略支援部隊的網路系統部負責的作戰範圍更為廣泛，包括

動能、網路空間、太空、電磁和心理作戰。」中共也進行網路諜報來竊取及複製西方科技，並用中國大陸的公司來取代發展這些科技的企業。

在戰爭中，共軍希望網路部隊能癱瘓敵方作戰網路，並破壞其指揮、管制、通信、資訊、情報、監視與偵察系統，以便取得並維持衝突中的優勢。2013年出版的專書《戰略學》寫道，「凡此其中，掌控資訊是作戰時獲取主動的基礎，缺少資訊優勢將難以有效籌劃制空與制海戰鬥。」

惡意程式碼是網路武器的精



髓所在。用在電子伏擊的預置程式碼，這是中共所稱的「殺手鐮」，這是一種將對手的強項變成弱點的構想。中共專家白邦瑞(Michael Pillsbury)主張，「這個殺手鐮是中共百年馬拉松軍事戰略的關鍵要件。」最近美國禁用華為公司及其5G網路科技，多半是擔心會創造出一個可能暗藏中共殺手鐮、隨時準備出擊的系統。華為執行長、億萬富翁任正非原為共軍軍官與中共黨員，他的公司雖宣稱是員工持股，但因中共國家安全法，華為必須應中共政府要求交出其資料。知名的北京維權律師莫少平表示，「中共有法律，但無法治。」西方國家是否願意將其5G網路交到中共手中，並甘冒讓華為充當共軍諜報工具的風險？

美國網路司令部

為因應不斷增加的網路戰爭活動，美國增強了自身網路部隊，美國網路司令部(U.S. Cyber Command)在2018年5月4日成立，是美國國防部10個(編註：現為11個)聯合作戰司令部之一，肩負統一網路空間行動指揮的任務。美國網路司令部相信自己是在與時間賽跑，以期趕上中共、俄國和其他網路戰爭對手。其優先事項是建立新興網路戰爭能量。該司令部近期增添133個網路小組，由來自4個軍種約6,200名人員組成：13個防禦廣域網路攻擊的國家任務小組、68個優先防禦國防部網路及系統的網路防護小組、27個提供整合網攻以支援作戰計畫和應變作戰的戰鬥任務小組及25個提供分析與計畫援助的支援小組。此外，美陸軍已決定強化從旅級到部隊指揮部(Army service component command, ASCC)每個階層的網路與

電磁活動(Cyber and electromagnetic activities, CEMA)部門，這些新部門將規劃、同步並整合網路和電子戰行動，同時執行頻譜管理。

美國網路司令部的下個優先事項，是開發最先進的網路工具和基礎設施。創造「持續網路訓練環境」(Persistent Cyber Training Environment, PCTE)是手段之一，且與網路戰爭訓練關係至鉅。透過使用網路雲端訓練試驗場，持續網路訓練環境能解決對持久、務實訓練環境的迫切需求。2019年5月，這種訓練在「網路鐵砧」(Cyber Anvil)的72小時聯合演習中進行測試，是一種分散式集體和個別層級的訓練活動，旨在測試新裝備、戰術、技術與程序。「網路鐵砧」演習期間，在網路戰爭原型平臺上，士兵受訓進行直接規劃、準備與執行網路空間任務。另一個主要網路戰爭工具，是發展用於網路作戰、情監偵的「統一平臺」，以整合網路作戰的指揮、管制和戰鬥管理。諾格公司(Northrop Grumman)已贏得5,660萬美元的合約，擔任該統一平臺的系統協調者。單在2019年，網路司令部就耗費7,500萬美元升級美國網路空間兵力。

網路戰爭是一種代價低、可不認帳的非動能作戰表現，其終極目標是透過敵人的網路和電子系統，去影響政治、軍事或經濟結果。在衝突的全部面向，網路戰爭已成為一種用於偵察、擴張戰果、截斷、犯罪、干擾、誤報、拒止和破壞的關鍵武器。隨著有更多智慧型裝置連接到物聯網，每一個裝置都會變得更聰明，且遭到攻擊的可能性也會大幅增加。正如《連線雜誌》(Wired magazine)創辦人凱利(Kevin Kelley)所指陳的，「(人工

智慧)將賦予不能動的物體生命,就像一個世紀前電力所為;我們先前電氣化的每件物品,現在都要將其智能化。」全球安全專家、芬氏安全公司(F-Secure)研究總監哈普寧(Mikko Hyppönen)指出,每一個智慧裝置都必須被視為一個弱點。網路中的裝置愈多、組織愈龐大,可供對手利用的網路戰爭選項就愈多。偵測並回應這些攻擊,是現代軍事部隊研究與訓練的主要工作。

在過去戰爭中,缺乏空中優勢幾乎不可能獲勝。但要在未來衝突中勝出,國家就必須在網路空間中取勝。因此,競奪更強攻勢、守勢網路戰

爭能力,是沒有一個現代軍事部隊輸得起的比賽。逐漸明朗的是,要在網路空間中取得優勢,需要機器學習和改善人工智慧。網路軍備競賽,攸關能否成為人工智慧領頭羊,而最終勝出的國家,將可主宰整個戰爭領域。

作者簡介

John Antal係兵法學者,著有與軍事議題相關的14本著作與數百篇雜誌文章,且擔任德國莫希峰出版社(Mönch publications)長期撰稿人。

Reprint from *Military Technology* with permission.



隨著不同任務與網路相連,弱點也隨之增加。

(Source: USAF/Quinn Jacobson)