第八章　戰略支援部隊的網路戰能量

吳宗翰、洪嘉齡 *

壹、前言

2017 年 10 月 18 日，習近平在中共十九次全國代表大會報告時提出新時代國防和軍隊建設「新三步走」的發展戰略，指出全軍要「到 2020 年基本實現機械化，信息化建設取得重大進展」；「到 2035 年基本實現國防和軍隊現代化」；「到本世紀中葉時建成世界一流軍隊」。[1] 2019 年 7 月，中共《新時代的中國國防》白皮書指出網路空間屬於國家主權範圍，是國家重大安全利益，並將其與核力量、太空等同並列同為戰略高點。而早在 2014 年第一次召開中央網絡安全和信息化領導小組會議上，習近平就說「沒有網絡安全，就沒有國家安全；沒有信息化，就沒有現代化。」[2] 信息化的目標、網路空間防禦，皆為中國人民解放軍戰略支援部隊的職責要點。《新時代的中國國防》白皮書同時指出，戰略支援部隊是「新質作戰能力的重要增長點」，將「按照體系融合、軍民融合的戰略要求」促進新型作戰力量加速發展、一體發展。[3] 由此顯見戰略支援部隊的重要性。

長期以來，受限於資料的侷限性，外界對於戰略支援部隊的真實面貌始終有限而碎片化，研究者只能透過零星的資訊拼湊。雖偶有研究報告或學術期刊等文獻，多聚焦在組織面的介紹，少有著墨於技術、手法

* 吳宗翰，國防安全研究院網路安全與決策推演研究所助理研究員；洪嘉齡，國防安全研究院網路安全與決策推演研究所助理研究員。

1 〈如何加速推進國防和軍隊建設　習近平強調新「三步走」戰略〉，《中國共產黨新聞網》，2021 年 3 月 11 日，http://cpc.people.com.cn/xuexi/BIG5/n1/2021/0311/c385474-32049007.html。

2 〈習近平親自出馬　主掌中國網絡安全〉，《BBC 中文網》，2014 年 2 月 27 日，https://www.bbc.com/zhongwen/trad/china/2014/02/140227_china_xi_web_security。

3 〈《新時代的中國國防》白皮書（全文）〉，中華人民共和國國務院新聞辦公室，2019 年 7 月 24 日，http://www.scio.gov.cn/ztk/dtzt/39912/41132/41134/Document/1660318/1660318.htm。

層次。[4] 本篇主旨在於梳理戰略支援部隊，著重在其網路戰（cyberwarfare/cyber operation）能力面向，並列舉可能是其部隊行動的近期案例，提供有關研究最新文獻。

貳、戰略支援部隊與其網戰部門

解放軍戰略支援部隊成立於 2015 年 12 月 31 日，為解放軍在陸、海、空、火箭之外的第五軍種。這一變革，不僅意味著解放軍多了一軍種，更深刻的意涵在於解放軍將太空、網路、電子甚至心理等非實體領域納入同一戰場框架。根據中共黨媒的介紹，戰略支援部隊為解放軍全軍提供「資訊支撐和戰略支援保障」，作用在於擔當全軍的「資訊傘」，它「將與陸海空和火箭軍的行動融為一體，貫穿整個作戰始終。」具體的說，戰略支援部隊的核心任務在於透過網路與電磁領域作戰（戰略）或協助（支援）各軍兵種聯合行動，項目涵蓋偵察、預警、通信、指揮、控制、導航等，以期在戰事中取勝。[5]

雖然戰略支援部隊是一個與陸、海、空、火箭同等級的軍種，但是在「軍委管總、戰區主戰、軍種主建」的格局下，由於其隸屬於中央軍委聯合作戰指揮中心，因而在指揮體系上會隨著任務屬性的改變而異動。[6] 表面上看，戰略支援部隊主職支援與防護，實際上，由於其轄下部門包括情報人員與網軍駭客部隊，對外主動出擊亦是重點。尤其，隨著解放軍益發

4 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (2018, Washington: National Defense University Press); Rachael Burton and Mark Stokes, *The People's Liberation Army Strategic Support Force Leadership and Structure* (2018, Project 2049 Institute); Elsa Kania and John Costello, The Strategic Supprt Force and the Future of Chinese Information Operations, The Cyber Defense Review (2018), pp. 105-121; Adam Ni and Bates Gill, The People's Liberation Army Strategic Support Force: Update 2019, *China Brief*, Vol. 19. No. 10, May 2019, https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

5 邱越，〈專家：戰略支援部隊將貫穿作戰全過程　是致勝關鍵〉，《人民網》，2016 年 1 月 5 日，http://military.people.com.cn/BIG5/n1/2016/0105/c1011-28011251.html；倪光輝，〈揭秘我軍首支戰略支援部隊（國防視線・深化國防和軍隊改革進行時）〉，《人民網》，2016 年 1 月 24 日，http://military.people.com.cn/BIG5/n1/2016/0124/c1011-28079245.html。

6 林穎佑，〈中共戰略支援部隊的任務與規模〉，《展望與探索》，第 15 卷第 10 期，2017 年，頁 105。

重視信息戰、心理戰與認知戰的不對稱作戰效果，戰略支援部隊亦承擔相關任務。[7] 需要注意的是，戰略支援部隊雖屬於廣義中共網軍的一環，但後者還包括公安部、宣傳部、民兵等單位。

戰略支援部隊的成立涉及習近平發動軍改前後解放軍多重部門與人員的整併整合。根據媒體報導與研究文獻的整理，戰略支援部隊已知轄下有航天系統部、網絡系統部、電子／電磁系統部與軍事情報部門等，各自底下再分單位，彼此分工又合作。總體而言，其目的在於利用資訊技術鏈結各作戰力量，使其形成完整的作戰體系。當前，占據網路空間與電磁頻譜的制高點已被解放軍視為獲得軍事優勢的重要手段。在此思維下，戰略支援部隊是使解放軍達到「網電一體戰」不可或缺的一環。

2017 年 7 月，網絡系統部（又稱網絡空間部隊）正式成立於戰略支援部隊編制中，負責部隊在網路空間的防禦與對外打擊。該部門整合過去負責無線電監聽、偵察的總參謀部技術偵察部（總參三部）及負責雷達系統的原總參謀部電子對抗部（總參四部）以及原來的總參謀部信息化部（即總參五部），該部內設有「信息安全局」單位，負責網路作戰進攻與防護。因而，一般認為原來總參三部下轄的 12 個業務局與部隊也均重新編隸為戰略支援部隊中。此外，根據《漢和防衛評論》過去的報導，該部門中名為「總部直屬信息作戰力量」的單位負責集結解放軍中的駭客專家，專門研製各種病毒與邏輯炸彈，用於網路攻擊。簡而言之，網絡系統部的運作包括研發、偵察、防護、攻擊等，形成完整的鏈。[8] 有關戰略支援部隊及其他網軍部隊基本架構圖可見圖 8-1。

自成立以來，戰略支援部隊首兩任司令員高津與李鳳彪均非資通訊相關背景出身，其任命可能著重於資歷或解放軍全軍布局原因。不過，此一現象可能已經被打破。甫於 2021 年 7 月 5 日新上任的司令員巨乾生主要

7　王清安，〈中共網軍發展對本軍威脅評估之研究〉，《陸軍通資半年刊》，第 127 期，2017 年 4 月，頁 4-26；〈從中共「網電一體戰」探討共軍戰略支援部隊作戰能力〉，《海軍學術雙月刊》，第 54 卷第 3 期，2020 年 6 月，頁 81-92；朴昌熙，〈中共解放軍信息戰能力之評析：以臺灣想定為例〉，《國防雜誌》，第 36 卷第 2 期，2021 年 6 月，頁 1-50。

8　尹俊傑，〈網路戰　漢和：共軍駭客部隊增加〉，《中央社》，2016 年 1 月 4 日，https://www.cna.com.tw/news/acn/201601040303.aspx。

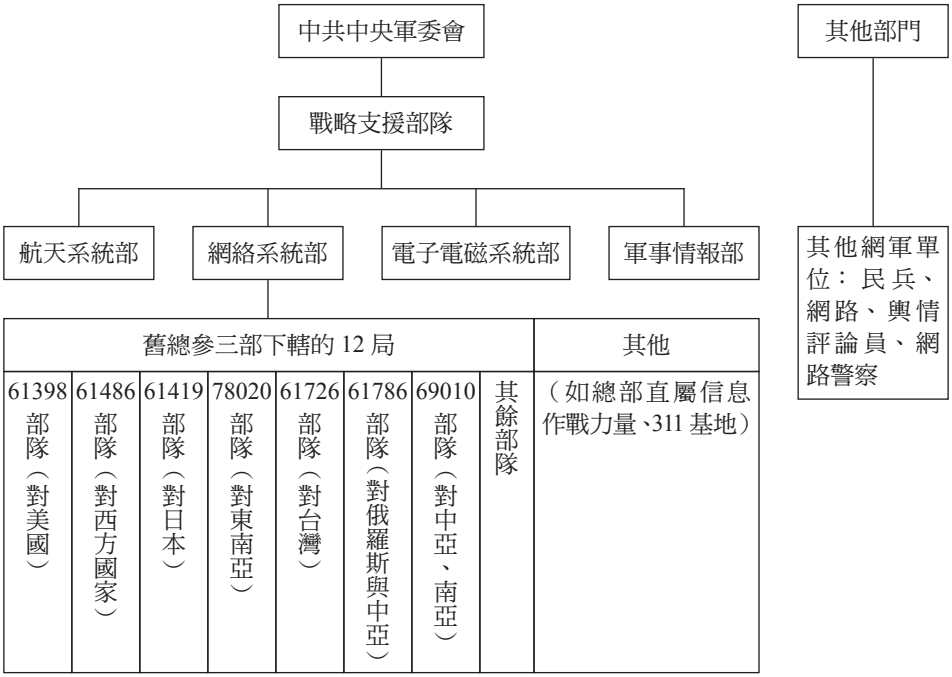

圖 8-1　戰略支援部隊及其他網軍架構圖

資料來源：作者自製。

為技術背景，擔任過總參謀部技術偵察部副部長，也擔任過戰略支援部隊網絡系統部的司令員，充分熟悉網路作戰特性。他的任命可能預示戰略支援部隊今後將更重視技術專業領導，進一步整合內部資源，在現有基礎上強化聯合作戰與爭取戰場優勢。

參、戰略支援部隊網路作戰攻擊手法與近期案例

網路戰結合實體作戰的各類型戰術戰法，足以成為現代戰爭中影響勝負的關鍵。網路攻擊的發動可能著眼於不同目的而有程度之別；可能是為了潛伏情蒐，也可用以約束影響目標者的行動，還可以透過阻斷對方運用網路和資訊系統的能力，為己方爭取更多優勢。透過將原有總參謀部門的

情報、電子、網路等部門橫向整合，解放軍戰略支援部隊的網攻能力咸信目前已經具備專精各類型網攻手法，亦能混合運用，對我國政府機關、重要關鍵基礎設施、產業供應鏈構成威脅。

在軍事領域，隨著載台、載具與武器設備數位化日深，解放軍對我網路空間、電磁頻譜安全性與軍事指管通網情監偵防護的威脅性更是不在話下。此外，由於戰略支援部隊亦肩負資訊戰、心理戰、認知戰等任務，假訊息的議題近來亦已成為網路防護中極被重視的一環。[9]

戰略支援部隊發動網路攻擊的方式與多數資安事件大同小異，主要有透過事先針對被攻擊對象的相關情資蒐集，找到可能破口，再依據需要攫取重要機敏情資，或者入侵被攻擊對象系統植入惡意程式，或者藉由事先偵獲的系統獲軟體漏洞直接攻擊，破壞系統。有關具體手法舉例簡述如下：

一、網路釣魚（Phishing）：此種攻擊是一種社交工程，它指的是透過電子通訊方式騙取遭攻擊對象的機敏訊息。此種手法通常透過電子郵件或者假網站。

二、擺渡攻擊（Ferry）：此種攻擊主要透過行動儲存裝置進入物理隔離之網路竊取資料或從事其他惡意行動；該攻擊往往搭配木馬程式（Trojan horse）。

三、分散式阻斷服務攻擊（distributed denial-of-service attack, DDoS）：此種攻擊的目的是使遭攻擊目標無法繼續提供服務。攻擊者利用大量（事先入侵的）電腦同時連線網站，藉由傳送大量封包阻塞網路頻寬，使系統效能負荷過大而無法正常運作。

四、網路大砲攻擊（Great Cannon）：此攻擊衍生自網路長城（Great Firewall），主要綁架特定流量，針對對象發動分散式阻斷服務攻擊。

9 溫貴香，〈假訊息意圖撕裂台灣　總統：全民提防認知作戰〉，《中央社》，2021 年 4 月 16 日，https://www.cna.com.tw/news/aipl/202104160089.aspx；游凱翔，〈調查局影片遭曲解學者：中共認知戰手法升級〉，《中央社》，2021 年 4 月 18 日，https://www.cna.com.tw/news/firstnews/202104180076.aspx。

五、進階持續性滲透攻擊（advanced persistent threat, APT）：此種攻擊預先針對目標進行長期觀察分析，掌握受攻擊對象的動態資訊，再對其發動客製化的攻擊；攻擊者往往採取多重複雜的手段，包括社交工程，針對可能的漏洞入侵滲透。APT 攻擊的過程可能很長、多階段且隱密。

至於發動心理戰或認知戰，其過程與一般網攻類似。差別在於，前者透過訊息蒐集、傳播手段，影響受眾心理狀態或透過改變受眾認知達到目的。對戰略支援部隊來說，網、電、心理戰為一體、相互關聯，可以有組合搭配進攻。

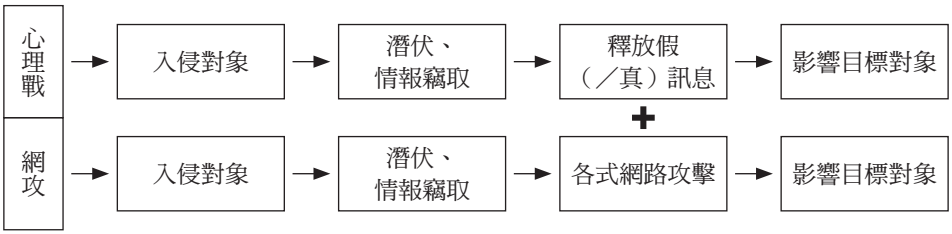

圖 8-2　心理戰與一般網攻路徑圖

資料來源：作者自製。

受限於資料，本文不擬具體指出戰略支援部隊究竟在具體的人、事、物上採取何種攻擊手法與步驟。不過，透過對相關資安報告或媒體報導的整理，本文以下列舉出 2020 年以來戰略支援部隊可能涉及的網攻事件。值得一提的是，這些網攻行動未必全然只由戰略支援部隊執行，事實上很可能也涉及雇傭駭客或與其他網軍的協力攻擊。本節最後亦整理出可能與戰略支援部隊相關的 APT 團體。

首先，2020 年 5 月我國中油與台塑公司先後遭到勒索病毒攻擊。由於時值 520 總統就職前夕，時機敏感。經調查局研析整起事件後，認為與中共駭客組織 APT41（別稱 Double Dragon；Barium；Winnti；Wick Panda；Wicked Spider）—— 該組織被認為與戰略支援部隊之一 —— 高度相關，

其目的在展示其可於關鍵時刻癱瘓我民生服務引起恐慌之能力，網路練兵與警告意味濃厚。[10] 2020 年 6 月澳洲總理莫里森（Scott Morrison）公開表示，澳洲數個月以來遭遇複雜的「國家級」駭客發動大規模網路攻擊，政府和民間企業都是被鎖定的目標。儘管莫里森未明言所指的國家行為者是誰，但多數報導認為所言就是中共。[11] 2020 年 10 月，媒體報導中共駭客組織 RedEcho 攻擊印度電網，導致孟買（Mumbai）大停電。一般認為，由於時值當時中印邊界情勢緊張，兩軍對峙，該駭客組織的目在於警告恫嚇印度政府。資安公司報告揭露，RedEcho 與 APT41 行為有諸多雷同之處。[12]

2021 年 3 月，中共駭客組織 Hafnium 透過微軟 Exchange Server 漏洞發動四項零時差攻擊，遭到微軟揭露。7 月中旬，美國及其全球盟友包括五眼聯盟（Five Eyes）、歐盟（EU）、北約（NATO）與日本等在內同步發表聲明，譴責中共政府在全球從事「不負責任的惡意網路活動」並隨後起訴 4 名中共駭客嫌疑人。英國國家網路安全中心（National Cyber Security Centre）也在其聲明中指出中共國務院與涉及對微軟 Exchange Server 實施駭客行動的 Hafnium 組織相關，並點名中共國家安全部就是 APT31 與 APT40 兩個駭客組織的幕後主使者。[13]

另一方面，有關心理戰與認知戰的實例亦有數起，共通處在於均是意圖製造國際事件損我國形象，甚至外交關係。2020 年 4 月，流傳台灣人向世衛組織秘書長譚德塞道歉的大量文章。後經調查為中共網民自導自演、刻意炒作。2020 年 12 月，網路再流傳調查局函請總統府研討與美國推動

10 翁芊儒，〈調查局完整揭露中油、台塑遭勒索軟體攻擊事件調查結果〉，《iThome》，2020 年 8 月 12 日，https://www.ithome.com.tw/news/139331。

11 “Australia cyber attacks: PM Morrison Warns of ‘Sophisticated’ State Hack,” *BBC NEWS*, June 19, 2020, https://www.bbc.com/news/world-australia-46096768.

12 “China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions,” *Recorded Future*, February 28, 2021, https://www.recordedfuture.com/redecho-targeting-indian-power-sector/.

13 John Hudson and Ellen Nakashima, “U.S., Allies Accuse China of Hacking Microsoft and Condoning Other Cyberattacks,” *Washington Post*, July 19, 2021, https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html.

網路泰國民主革命的假公文，而後被證實為曾赴中共受網路水軍訓練的劉姓男子等人散布。2021 年 9 月，資安公司杜浦數位安全（TeamT5）被指接受台灣政府授意非法蒐集日本民眾個資以及企業重要人士的機敏資訊。經查證為出自中共之網路假訊息。[14]

從趨勢言，全球資安事件在過去一年間數量不斷創紀錄。疑似為中共各路網軍的攻擊也變得更機動、更具侵略性。在全球籠罩在以中美對抗為主的態勢下，網路空間儼然已是如火如荼的戰場。[15]

表 8-1　推估與戰略支援部隊相關之 APT 團體

名稱	攻擊的部門或產業	目標說明	台灣受害紀錄
APT1（61398）	政府、國防、非政府、研究、關鍵基礎設施、民生娛樂、高科技	橫跨多領域，但多集中於政治、經濟、軍事情報	有
APT2（61486）	政府、研究	多集中於衛星航空產業	
APT3	國防、航空、太空、建築、製造業、高科技，電信、交通運輸	多針對先進技術領域的公司	
APT10（menuPass）	政府、國防、航空、太空、能源、金融、醫療、製藥、高科技、媒體、電信	多針對政府與企業；對象尤以日本居多	有
APT18	國防、航空、太空、建築、工程、教育、醫療、高科技、電信、生物技術	多針對政府、企業、人權團體	

14 黃彥棻，〈中國認知作戰新手法！鎖定臺灣資安公司製造假新聞，挑撥臺日政府關係〉，《iThome》，2021 年 9 月 23 日，https://www.ithome.com.tw/news/146834；蕭博文，〈台灣人涉散布中國網軍假訊息　首宗網路國安案件〉，《中央社》，2021 年 12 月 11 日，https://www.cna.com.tw/news/firstnews/202012110028.aspx；蕭博文，〈中國網民冒充台灣人承認攻擊譚德塞還道歉〉，《中央社》，2020 年 4 月 10 日，https://www.cna.com.tw/news/firstnews/202004100033.aspx。

15 Nicole Perlroth,〈中國是如何成為美國主要網路威脅的〉，《紐約時報中文網》，2021 年 7 月 20 日，https://cn.nytimes.com/technology/20210720/china-hacking-us/zh-hant/。

表 8-1　推估與戰略支援部隊相關之 APT 團體（續）

名稱	攻擊的部門或產業	目標說明	台灣受害紀錄
APT19（別稱 Deep Panda）	政府、國防、能源、教育、金融、電信、製造業、高科技、醫藥	多針對政府與國防領域；其團體亦多針對智囊團以及政治異見人士	
APT26	政府、非政府、航空、太空、國防、能源、金融、電信、農糧、醫療保健	多針對在航空、國防與能源行業具有競爭力的企業	
APT30（別稱 Naikon Team）	政府、國防	多針對政治、經濟、軍事數據竊取；對象多集中於東協國家	
APT40	政府、國防、工程、製造、航運、物流	多針對與海事技術相關領域，被認為與中國海軍密切	
APT41（別稱 Barium、Winnti、Wicked Panda、Wicked Spider Group）	政府、國防、建築、教育、能源、金融、醫學、高科技、製造、石化、零售、電信、運輸、娛樂	多領域；香港爆發反送中事件時候也頗活躍	有
Blacktech	政府、建築、金融、媒體、醫療保健	多集中於東亞地區	有
Tonto Team	政府、國防、金融、媒體、IT	2019 年以前多針對韓國，俄羅斯和日本；之後多針對蒙古與俄羅斯	有
Mustang Panda	政府、非政府、航空	多以非政府組織為目標，且常使用蒙古語	有
RedDelta	政府	多針對政府部門；自 2020 年起被發現常攻擊梵蒂岡與天主教有關的組織	

資料來源：整理自 Gulshan Rai, “Cyber DNA of China-Deep,” Focussed and Militarised, Vivekananda International Foundation, March 23, 2021, https://reurl.cc/1oeR7W; Adam Hlavek, “The China Threat, In Brief,” IronNet, January 10, 2021, https://reurl.cc/r1LWAk; “Groups,” MITRE|ATT & CK, https://reurl.cc/95V8qn; “Advanced Persistent Threat Groups,” MANDIANT, https://reurl.cc/EZGdvR; APT list, CYBER INTEL MATRIX, https://reurl.cc/NZqe8Q。

肆、小結

網路戰被解放軍視為取得「信息戰」勝利的重要關鍵。根據國防部《110 中共軍力報告書》指稱，「解放軍現階段已具備對第一島鏈以西區域進行軟、硬殺電子攻擊、通信阻絕與遮沒等能力，還可結合中共網軍啟動有、無線之全球網路攻擊，足以癱瘓國軍防空、制海及反制作戰體系的能力」，我國國防情勢顯然已面臨嚴峻挑戰。[16] 促使解放軍能力持續快速增長的要素，戰略支援部隊顯然是不可忽視的一環。

自 2020 年以來的趨勢，可見各類型網攻事件頻繁，手法也不斷翻新。另一方面，針對心理為主的攻勢亦有成長，尤其，本文發現多起事件企圖損及我國政府形象及與友盟關係。我國安相關單位實需要審慎應對，有必要對戰略支援部隊展開更全面而深入的研究。

16 楊清緣，〈國安危機！國防部 110 年中共軍力報告書揭共軍已全般掌握我軍事動態〉，《Newtalk 新聞》，2021 年 9 月 1 日，https://newtalk.tw/news/view/2021-09-01/629400。