其他研究

DOI:10.6237/NPJ.202210_56(5).0008

論中共「網路戰」人才培育體系(譯作)

China's Human Capital Ecosystem for Network Warfare

作者：麥克雷諾茲(Joe McReynolds)、露絲(LeighAnn Luce)
譯者：劉宗翰

本篇取材自美國陸軍戰院出版品2021年《共軍2.0版人員》(The People of the PLA 2.0)，本文屬公開出版品。

提　　要：

一、中共成立「戰略支援部隊」是為了統合C4ISR體系，並打造一支能在資訊化戰場打勝仗的軍隊；在其成軍後，與「網路戰」人才培育相關的組織、院校、研究機構及人才招募管道也發生變化，凸顯中共高層意在達成「網路強國」的戰略目標。

二、共軍在網羅資訊暨網路人才的管道已產生一定的改變，如非指揮職的網路安全名額已開放給女性、廢除「文職幹部」改為「文職人員」制度、廢除「國防生」改為「直招士官」管道；至於大學、研究所及博士在課程安排及錄取員額上，「不約而同」都採取一些彈性調整和獎勵措施，以吸引人才就讀，俾利畢業後為共軍所用。

三、儘管各項資訊計畫雖然能委外合作，借助民間的人力資源，但實情是共軍仍需要常規且長期受管控的人力，而非短暫的委託合作關係。再者，共軍在吸引人才上的不爭事實是軍方待遇仍低於民間，人才外流使共軍先前的投資白白浪費；最後，共軍是否能在組織重組過程中做好傳承，這也是一大隱憂。

關鍵詞：網路戰、人才培育、文職人員、戰略支援部隊

壹、前言

共軍近幾年在各個軍事單位與國防工業進行一連串的改革，其目標之一是藉由建立完善的「指揮、管制、通信、資訊、情報、監視與偵察」(C4ISR)體系來支援資訊作戰，以創建一支能在資訊化戰場「打勝仗的軍隊。改革作為之一是在2015年底成立「戰略支援部隊」(以下稱「戰支隊」)這個新軍種，做為能在「資訊戰」(共軍稱「信息戰」)中獨立作戰的部隊；這意味著共軍須在資訊領域(尤其是網路空間)取得優勢，這問題也將成為思考戰略與組織規劃的「重中之重」。此外，網路是一項「攻守兼備」的工具，共軍及情報部門已用來從事一系列行動，如產業諜報，情蒐、影響力行動及戰場空間整

備。

共軍在「網路戰」的作戰方式、準則發展及兵力規劃，因為在資訊不透明情況下，鮮少為外界所知；因此「網路戰」武器的發展情形也同樣難為外人知曉。此項武器雖是戰爭中的一小部分，但卻可能在一場衝突中扮演決定性關鍵角色，誠如中共國防工業學者所言，它們是資訊戰中的「利刃」。[1]檢視共軍「網路戰」人才體系的培養、獲得及如何部署網路武器，可以提供一個機會來理解中共「資訊戰」的能力。資訊戰場由於涵蓋網路空間、電磁及心理等領域的獨特性，也讓各種人才匯聚於此；而藉由分析人才，讓我們得以理解其「網路戰」的發展與能力。此外，由於從事網路武器發展所需的技能教育與民間資訊業有高度重疊，故共軍在招聘網路人才較其他人才來得透明許多。若將網路武器想像成「利刃」，則我們的一些疑惑，應能從鍛造利刃的工匠身上找出答案。

共軍在資訊暨網路的人才體系已產生下列改變：一、2015年底「戰略支援部隊」的成軍只是一連串組織改革的開頭；二、將「軍民融合」提升至國家戰略層級，發起「民進軍」的倡議，從而擴大部隊接觸民間人才的管道；三、「文職幹部」制度已不符時代需求，改以「文職人員」制度替代；四、共軍以往專注於「網路戰」與「電子戰」的科技學術研究機構改隸於「戰支隊」下；五、中共在學術機構廣泛改組過程中，已賦予像是「軍事科學院」等機構新的面貌。總體而言，共軍正在進行大規模的人才體系重組，以因應未來的資訊化作戰。本文研究目的為檢視中共「網路戰」人才培育體系之發展趨勢，從中指出其窒礙與制度性矛盾問題，同時也發現共軍逐漸在招募文職與軍職人才之間取得一定的平衡。

貳、網路武器的特性形塑共軍人才需求

網路武器是共軍平、戰時不可或缺的常規武器之一，但由於其具有多項特性，使之難以納入共軍傳統的國防研發暨獲得體系內，這也直接影響發展網路武器所需的人才，特性歸納如后：

一、共軍網路攻擊的研發和執行者雖然負責電腦網路的攻擊，但並不會與他們的職位名稱或是職涯、教育路線相對應，這種情形在共軍其他軍事領域同樣很常見。儘管共軍並未在公開文獻上載明這些職位的明顯區分，但發展網路攻擊工具的人與運用工具的人往往會一起在某個特定的軍事單位工作，這些職位上的人似乎有類似的職涯路線，而且也來自相同的軍事與民間教育體制。這些共同性在其他國防部門難以看見，這種情況就像是研發與工程人員在一起生產戰機，並和戰機飛行員共享軍事單位、職涯路線及教育背景。為釐清從事網路武器的發展與「網路戰」人員的教育與職涯狀況，本文後續將檢視這兩個主題以獲得全貌。

二、共軍並不承認有發展任何特定的網路武器，但「戰略支援部隊」成軍後，凸顯其有一支從事網路攻擊的部隊。網路武器的

註1：程永生，《軍事高技術與信息化武器裝備》(北京：國防工業出版社，2009年)，頁373。

進展要比一般國防研發暨獲得計畫的進展來得更不透明；因此，要證實傳聞及理解組織結構和人員的職涯發展等都實屬不易。由於缺乏關於網路武器發展的資訊，我們更應儘可能蒐集瑣碎與片段的資訊，以組成一個有意義的整體圖像，不過完整度仍取決於資料公開的多寡。

三、網路武器除本質上經常是模組化外，也須不斷發展、更新及修正，否則將無法持續維持其效力；再者網路武器的生產、測試、修改，以及轉作某特定目的使用，這種壽期循環的快速性與持續性，不同於傳統的國防研發暨獲得計畫。我們可預期中共新式海軍船艦在多年後下水服役，但網路武器像是「零日漏洞」(Zero-Day Exploit)[2]的網攻效力，可能就只有數天或數小時；共軍一旦使用，就會被發現其攻擊來源路徑，對手一定會立刻採取反制措施。「時間迫切性」拉近組織內網路武器研發與使用者之間的距離，形成兩者在職涯路線上有所重疊，這在其他國防部門並不常見。

四、攻勢網路武器與防衛資訊安全科技發展的複雜度是其他國防部門未見的，雖然大部分防範傳統武器系統的科技，都須理解「彈道物理學」(Ballistic Physics)的原理，但攻勢與防禦科技的研發者彼此都鮮少交集；網路防禦還須架構在防範從未見過的威脅源上，並等到惡意程式碼發動攻擊後，才能真正判定其破壞程度。因此，要建立有效的網路防禦，國家需事先預測並找出「網路戰」的攻擊源。網路攻防的研發彼此交織在一起，也影響中共的人才需求及其與民間資訊安全企業的互動。具備民間資訊科技或受過資訊安全教育的研究人才，已可直接招聘至軍中，無須經漫長轉換至國防技術工作的過程，所以民間的編碼與軟體技術也藉此整合至共軍的攻擊武器庫之中；然而，這種與民間共享招聘科技人員意味著須直接與民間企業競逐人才。

五、網路武器通常蘊含社會工程的元素，例如一些攻擊源可能需要目標方在毫無戒心的情況下，接收電子郵件並點選郵件中的連結至有毒網站，或是讓對方在無意間開啟惡意的附加檔案，這種方式就是「魚叉式網路釣魚」(Spear Phishing)。而在網路武器的人才體系中，具適當文化與知識背景的國防或情報語言學家不可或缺，因為要用對手熟悉的語言和風俗民情，才能讓人「上當」。

六、網路武器在平時主要從事諜報作為，同一組人馬、設施及攻擊手段，同樣也能用於情蒐與戰場空間整備，這種共享資源為共軍開啟戰略的可能性，但也構成獨特的指揮與人員挑戰。共軍「網路戰」人員待遇明顯比不上民間資訊企業，根據西方資訊安全分析人員指出，更多時候共軍特定人員會使用軍事設施來為軍外的客戶蒐集資訊。[3]

參、共軍網路戰單位重組、人才培育與待遇

為發展網路武器與訓練資訊作戰人員，

註2：譯者註：「零日漏洞」攻擊就是利用尚未修補的軟體、韌體或硬體設計的漏洞進行攻擊，駭客或犯罪集團會針對某項廠商尚未釋出修補更新(或者廠商根本不知道)的漏洞進行概念驗證攻擊或植入惡意程式。

註3：Mandiant Intelligence Center, APT1: Exposing One of China's Cyber Espionage Units, February 18, 2013, https://www.fireeye.de/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf，檢索日期：2022年7月1日。

表一：中共「戰略支援部隊」組織編制表

職能部門	直屬單位	下屬院校
◎參謀部、政治工作部、紀律檢查委員會 ◎網絡系統部(納編前總參三部，下轄網軍61398部隊【對美】、61486部隊【對西方國家】、61419部隊【對日】、78020部隊【對東南亞】、61726部隊【對臺】、61786部隊【對俄、中亞】、69010部隊【對中亞、南亞】，及前總參四部主體) ◎航天系統部 ◎裝備部(未確定)、後勤部(未確定)	◎戰略支援部隊特色醫學中心(三級甲等醫院) ◎311基地(從事三戰工作：輿論戰、心理戰、法律戰) ◎電子對抗旅	◎航天工程大學(隸屬航天系統部) ◎信息工程大學(隸屬網絡系統部) ◎網絡系統部第56研究所

資料來源：參考John Costello and Joe McReynolds, China’s Strategic Support Force: A Force for a New Era (Washington: National Defense University Press, 2018), p.11；蘇紫雲、洪瑞閔主編，《2021國防科技趨勢評估報告-中共新世代軍事科技評估》(臺北市：五南書局)，2021年12月，頁86，由譯者彙整製表。

共軍成立各式不同的機構，如各軍種下轄的「技術偵察局」、各編號研究所及軍事學術機構；而人才體系主要集中在「中央軍事委員會」(以下稱「軍委會」)下，由「國防科技大學」(以下稱「國科大」)，「信息工程大學」(以下稱「信工大」)，前總參三部(技術偵察部)、四部(電子對抗)，前總參第56、57、58研究所，「電子工程學院」等機構來管理，變化歷程概述如后：

一、單位重組

(一)「戰略支援部隊」成軍(如表一)與軍事學術機構改組之後，其人才體系制度產生不同變化。在2015年底「戰支隊」成立之前，中共網軍是按照任務類型之偵察、攻擊、防禦、心理戰分組，如網路間諜和信號情報，由前總參三部負責；進攻性網路行動和電子對抗由前總參四部負責；「心理戰」由前總政指導；軍事網路安全大部分由前總參的信息化部負責。[4]以往中共網軍編制在總參三、四部、雷達部之下，易發生任務重疊與組織衝突，「戰支隊」則統合前總參三、四部的網軍。原總參四部執行網路攻擊的「電子作戰部隊」改編至「戰支隊」的「網絡系統部」，前總參四部的總部則改隸至聯合參謀部下成為「網絡電子局」，可能負責監督整體網路戰與電子戰、[5]「電子工程學院」是前總參四部的主要教育機構，也改置於「國防科技大學」下，並轉型更名為「電子對抗學院」、「信息工程大學」也移至「網絡系統部」，並整合其他相關重點領域的教育機構。

(二)前總參之下的各編號研究所或許是最不尋常的改變，雖然在「國防科技大學」成軍後納編相關的研究所，但2017年中，數個研究所又回歸直屬軍委會的「軍事科學院」(下稱軍科院)；值得注意的是，前總參「第54研究所」已更名為「網電對抗研究所」，隸屬於軍科院「系統工程研究院」。根據共媒報導，該院已定位成共軍科研的龍頭，因為其將軍事理論的傳統工作與國防科研做

註4：譯者註：龍率真，〈網路癱瘓目標國，中共威脅全球警戒〉，青年日報，2021年8月29日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1439867&type=forum，檢索日期：2022年7月3日。

註5：John Costello and Joe McReynolds, China’s Strategic Support Force: A Force for a New Era (Washington, DC: National Defense University Press, 2018).

結合；[6]再者此波重組意味著已化解先前「軍科院」與「國防科技大學」之間的分歧，並由「國科大」專注人員訓練與核心國防科研。共軍認為這種轉型符合軍方所需，也貼近軍事戰略中的科技發展路線，至於各編號研究所則轉為注重工程與能力測試的研究。

總體而言，「戰略支援部隊」已與中共戰略研究體系密切連結，如高層人員會在該部隊與軍科院間調動，該部隊首任司令高津，前一職務即為軍科院院長，這多少都會使人聯想官僚政治問題，所以在共軍改革過程中，也可能造成一定程度的影響。

二、人才遴選

院校人才來自直接招募、「直招士官」或「文職幹部」等不同管道。雖然這種軍事網路的工作可以借助具相關資訊技能的民間人士，但軍事科技院校的網路人才培育計畫仍持續進行，不管是在培養實際從業者或從事研究工作者方面；因此，檢視「網路戰」人才的遴選、培育及留用至關重要。以下列舉「國防科技大學」與「信息工程大學」的案例，希冀藉由理解「網路戰」人才培育在大學、碩士、博士各層級的學術路線，獎勵結構及招生政策，以及「戰略支援部隊」的留營與士氣問題，進一步評估中共「網路戰」的工作人力需求。

(一)大學計畫可說是中共「網路戰」人才體系的重點。雖然大學生較研究生缺少技術知識，但他們在這段時期的學術專長，將決定未來會占哪些職缺；其中區別是未來有人是作戰指揮路線，有人是專業技術路線。大學生數量眾多，畢業後自然形成「網路戰」的人力主幹。共軍也注意到招募人員的問題，自2014年起，共軍的科技教育機構開始要求大學新生年齡為17至20歲，除非是預備役軍官與其他特定的新生。許多與「網路戰」相關的學術機構，傳統上都只招男性或只接受極少數女性，但過去幾年來已出現變化，一些非指揮職的網路安全名額已開放給女性；[7]然而，招募的女生多半是在「網路戰」領域內學習語文專業技術。共軍的科技大學也試著要確保國內各區錄取人數的平衡，所以各省(市)錄取分數高低，也不盡相同。[8]

(二)共軍的各科技院校也對下列對象給予一定比例的優先錄取，如擁有共軍所需的專業技能者、曾獲頒國家級的學術獎項者，以及現役軍人子女和因公犧牲、烈士子女可在一定比例範圍內優先錄取。[9]錄取生都需進行「邁爾斯－布里格斯性格分類指標」(Myers-Briggs Type Indicator)的心理測驗，以區分出受測者的個性類別。[10]共軍也重視新生的政治立場，他們在前一個學校的

註6：馬浩亮，〈建軍90週年：軍校改革三院校作龍頭引領新格局〉，大公網，2017年7月29日，http://news.takungpao.com/mainland/focus/2017-07/3477971_wap.html，檢索日期：2022年7月5日。

註7：蔡鵬程等人，〈2018軍校招生，你需要的訊息在這裡〉，解放軍報，2018年6月29日，http://www.mod.gov.cn/topnews/2018-06/29/content_4818065.htm，檢索日期：2022年7月7日。

註8：吳昊，〈2013年信息工程大學全國錄取分數線〉，中國軍網，2014年4月23日，http://www.81.cn/rdzt/2014/0421bkjx/2014-04/23/content_5878152.htm，檢索日期：2022年7月8日。

註9：〈2013年解放軍電子工程學院招生簡章〉，騰訊網，2013年7月18日，https://xw.qq.com/amphtml/20130718013619/2013071801361900，檢索日期：2022年7月9日。

註10：〈研究生招生〉，中共戰略支援部隊信息工程大學招生信息網，2019年9月7日，http://zhaosheng.plaieu.edu.cn/channels/252.html；北京教育考試院，〈軍隊院校招收學員體格檢查標準〉，陽光高考，2018年6月12日，https://gaokao.chsi.com.cn/gkxx/zc/ss/201806/20180612/1697224935.html，檢索日期：2022年7月10日。

表二：中共「國防科技大學」概況表

	設置院所計文理學院、計算機學院、電子科學學院、前沿交叉學科學院、智能科學學院、系統工程學院、空天科學學院、國際關係學院、信息通信學院、電子對抗學院、氣象海洋學院、軍事基礎教育學院、研究生院、第63研究所。
簡介	■位於湖南省長沙市，直屬軍委會的綜合性大學，原「985工程」、「211工程」(即民間知名大學院校統稱)重點建設大學。 ■2014年後，中共教育部逐漸淡化「985工程」、「211工程」，並自2015年起就不再提及。 ■2017年9月，「雙一流」(世界一流大學和一流學科建設)名單正式公布，已將「985工程」、「211工程」教育建設項目納入。

資料來源：參考〈共軍國防科技大學〉，維基百科，https://zh.wikipedia.org/zh-tw/共軍國防科技大學，檢索日期：2022年7月25日，由譯者彙整製表。

政治考核必須在入學時一併轉移，通常新生並不一定已加入共產黨，故在入學時要繳交入團志願書。[11]

三、院校招生與課程安排

(一)「國防科技大學」(如表二)為「網路戰」提供兩個主要的非指揮職學術課程，分別是「軟件工程」與「網路工程」，前者訓練學生從事網路戰的軟體開發與分析能力；後者是讓學生理解並學習網路技術。至於「電子對抗學院」(前身為電子工程學院)提供指揮職(作戰軍官)與非指揮職(技術軍官)一系列學術課程，非指揮職技術軍官的課程包含「信息工程」(著重於軍事網路的攻防)和「網路工程」(著重於民間網路之安全)，而該學院的電子對抗指揮與工程課程則是針對通信網路和資訊系統之攻防。[12]

(二)「信息工程大學」(如表三)則提供另一種面向的課程安排，屬非指揮職的網路工程，致力於培養男、女性的網路攻防技術幹部，至於提供的指揮職課程為信息安全與工程，其中大多數的新進學官都是指揮軍官而非技術專業人員。[13]另一方面，共軍大學講授「網路戰」的師資一直都是由「文職幹部」擔任而非軍職，因為軍官畢業後往往須接受預劃派職，但共軍在轉型過程中將「文職幹部」廢除並轉成「文職人員」體制，或許將影響軍方大學內原本教育體制的平衡。

(三)中共國防科技院校的碩、博士班深

註11：〈2012級新生相關問題說明〉，共軍戰略支援部隊信息工程大學招生信息網，2014年3月20日，https://web.archive.org/web/20150222054248/http://zhaosheng.plaieu.edu.cn/a/benkezhaosheng/2014/0320/283.html.，檢索日期：2022年7月11日。

註12：〈招生簡章〉，共軍國防科技大學研究生招生信息網，2021年10月21日，http://yjszs.nudt.edu.cn/index/index.view.，檢索日期：2022年7月12日。

註13：〈走進信大〉，共軍戰略支援部隊信息工程大學招生信息網，2022年6月19日，http://zhaosheng.plaieu.edu.cn/channels/249.html.，檢索日期：2022年月日。

表三：中共「信息工程大學」概況表

■教學管理機構：基礎部、信息系統工程學院、地理空間信息學院、密碼工程學院、網絡空間安全學院、數據與目標工程學院、洛陽校區、研究生院、信息技術研究所、外訓大隊、信息作戰指揮系。
■直附屬機構：職業教育中心、教學考評中心、教研保障中心、服務保障中心、警通勤務隊。

簡介	■位於河南省鄭州市、洛陽市。 ■2017年，以原信息工程大學、外國語學院為基礎重建而成，隸屬「戰略支援部隊」網絡系統部。 ■外國語學院改為信息工程大學洛陽校區，外語類系部撤併。

資料來源：參考〈共軍戰略支援部隊信息工程大學〉，維基百科，https://zh.wikipedia.org/zh-tw/共軍戰略支援部隊信息工程大學，檢索日期：2022年7月25日，由譯者彙整製表。

造教育計畫，在持續培養資訊暨網路研發人才上扮演要角，學成後多從事高階研究計畫或是進入「戰略支援部隊」與隸屬「軍委會」的相關機構服務。至於各院校為吸引特殊的資訊網路人才，都會在研究所層級建立各自的招生管道。

1.「國科大」為網路攻防研究的領頭羊，有眾多關於「網路戰」的博士研究課程，中共中央政府對該校相當重視，並自「十-五年計畫」起提供網路攻防研究的經費補助。一般而言，關於網路攻防的學術出版品往往由「電子對抗學院」主導並與計算機、信息通信、電子科學等學院產製。[14]在「計算機學院」內的「網絡與信息安全研究所」從事的網路攻防研究，甚至包含高階資訊戰運用的太空網路研究。[15]至於博士課程設計目的，似乎也不像是為了要讓文職人才進入軍方博士體系，申請人規定須為軍事碩士應屆畢業生或是已取得碩士學位的軍隊在職人員，而且從過去幾年的觀察顯示，該校關於網路攻防的總錄取名額已增加3倍之多，凸顯共軍積極經營的努力。[16]

2.「信工大」長期以來都保留博士名額給無軍事背景的人，包含提供全額獎學金給從原「985工程」院校中獲得碩士文憑的學生，而為招募應屆碩士與現役軍人，申請條件還開放給已擁有碩士學位、或曾從事相關領域工作經驗達6年(含)以上的軍職人員。[17]

註14：〈院所發文〉，共軍國防科技大學研究生招生信息網，2022年7月9日，http://yjszs.nudt.edu.cn//pubweb/homePageList/recruitStudents.view，檢索日期：2022年7月13日。

註15：〈網絡與信息安全研究所〉，共軍國防科技大學，2010年6月28日，http://web.archive.org/web/20120209160356/http://www.nudt.edu.cn/ArticleShow.asp?ID=46，檢索日期：2022年7月14日。

註16：〈博士研究生招生簡章〉，共軍國防科技大學研究生招生信息網，2021年12月1日，http://yjszs.nudt.edu.cn/pubweb/homePageList/detailed.view?keyId=12145，檢索日期：2022年7月15日。

註17：〈共軍信息工程大學研究生院〉，共軍戰略支援部隊信息工程大學，2014年2月25日，http://zhaosheng.plaieu.edu.cn/a/yanjiushengzhaosheng/2014/0225/304.html，檢索日期：2022年7月16日。

此外，還打造一項特殊人才選拔計畫，報考碩士生如能具體展現攻勢網路戰技能，如參加「奪旗資訊安全競賽」獲得區域賽前三名、發現並提交漏洞入選信息安全「國家漏洞庫」、個人在網路安全領域有特殊專長並取得突破性成績，任一條件均可直接參加複試。[18]一般而言，相較共軍其他教育機構的徵選，該校對現役軍官的碩士入學資格評估較寬鬆。[19]

3. 中共的國防科技院校或各編號研究所的博士班入學不同於全國聯招，考試內容由各院校自定、報考人員管制於兩日內完成，以及須在入學考試中名列前茅才會錄取。[20]與大學生的審查機制一樣，兩校的所有博士申請者都須通過標準意識形態查核表中所列的標準，如優良品德操守、政治可靠度及清白法治紀錄。[21]

(四)除科技人才之外，「網路戰」也需要語文人才，各院校不只有安排標準的科技專業英文課程，還開設軟體工程與網路安全等課程，如「外國語學院」在2017年併入「信工大」，並更名為「信息工程大學洛陽校區」，以替「戰支隊」培育網路武器生產與部署所需的語文人才，並提供各種不同語系(特語)的課程；在語文訓練上，置重點於科技軍官而非指揮或支援的課程，還定期聘請外籍師資進行語文訓練。[22]另一種有效的訓練方式，係借助在中國大陸的外國公民來訓練軍方人員，俾利遂行國家未來所交付的諜報行動，這種作法也是世界各國的國防語文院校一貫的作法。洛陽校區雖然扮演主要語文人才培育的角色，但「信工大」主校區也提供碩士語文訓練課程，同樣培育該部隊「網絡系統部」在作戰時所需的語文專才。[23]從「戰支隊」與各軍種「技術偵察局」所要求的職位技能顯示，即使是技術參謀人員也須在工作上定期使用英語。

(五)「網電對抗研究所」雖然主要從事網路武器發展，但也招收碩士並授予學資。儘管總參以下各編號研究所的招生過程與課程安排，較諸其他國防科技院校更不透明，但一般仍遵循標準的軍事院校申請程序，亦須通過相關考試規定標準。

四、網路人才待遇

(一)共軍在培育網路人才方面一直存在關於薪資、福利及工作環境等問題，因為具有資訊相關專業的人才在民間同樣也很受歡迎，雖然共軍已建立相關津貼制度，但公家

註18：〈網絡空間安全學科碩士研究生特殊人才，選拔工作報名通知〉，共軍戰略支援部隊信息工程大學，2018年3月26日，http://web.archive.org/web/20180405050413/http://zhaosheng.plaieu.edu.cn/contents/252/912.html，檢索日期：2022年7月17日。

註19：〈公布2014年博士研究生入學考試軍人考生最低錄取分數線〉，共軍戰略支援部隊信息工程大學，2014年3月28日，http://web.archive.org/web/20140720151016/http://zhaosheng.plaieu.edu.cn/a/yanjiushengzhaosheng/2014/0328/307.html，檢索日期：2022年7月18日。

註20：同註17。

註21：同註17。

註22：〈共軍外國語學院〉，搜狗百科，https://baike.sogou.com/v11026509.htm，檢索日期：2022年7月19日。

註23：〈2014年碩士研究生招生專業目錄〉，共軍戰略支援部隊信息工程大學，2014年3月20日，http://web.archive.org/web/20140720145959/http://zhaosheng.plaieu.edu.cn/a/yanjiushengzhaosheng/2014/0320/290.html，檢索日期：2022年7月20日。

表四：駭客名稱分類表

名　稱	定　義　說　明
灰帽駭客 (Gray Hat)	一名駭客或電腦保安專家，他們有時可能會違反法律或道德標準，但不具黑帽駭客的惡意意圖。
黑帽駭客 (Black Hat)	在未經允許情況下擅自入侵他人系統，欲獲取利益之駭客，通常製造惡意網站、入侵他人網站，讓使用者系統感染惡意軟體
白帽駭客 (White Hat)	具道德感的駭客或電腦保安專家，專門從事滲透測試及其他測試方法，確保資訊系統安全，通常是取得客戶同意後的合法行為。
藍帽駭客 (Blue Hat)	軟體公司會與藍帽駭客合作，在軟體發布之前，尋找軟體的安全性漏洞。與白帽駭客的區別在於軟體公司將安全性測試委外給外部公司中的藍帽駭客執行，不過他們也可以被視為白帽駭客。
腳本小子 (Script Kiddie)	專門利用他人開發的腳本程式進行攻擊的網路滋事者，他們通常不懂攻擊程式的原理，也無法自行撰寫攻擊程式。真正的駭客有時候會看不起這些人，因為駭客通常被認為能用自己開發的工具進行駭客攻擊。
激進駭客 (Hacktivism)	激進駭客(或稱為紅帽駭客)進行駭客攻擊來表達政治、意識形態、社會或宗教訊息，目的不是金錢或個人利益，如維基解密(WikiLeaks)和匿名者行動(Anonymous)。

資料來源：參考〈駭客是什麼？〉，NordVPN，2020年10月25日，https://nordvpn.com/zh-tw/blog/heike-shi-shenme/，檢索日期：2022年7月22日，由譯者彙整製表。

資源畢竟較有限。一位擁有信息工程碩士的網路武器發展者，在2006至2008年間以「羅西鳥」(Rocy Bird)的化名於網路上發表一系列貼文，抱怨在某「技術偵察局」的工作既單調乏味又與社會隔離，[24]還指出自己做的比同年紀在共軍工作的人相對較好，但薪資跟同學在進入民間企業相比根本少的可憐；況且還生活在上海這樣高物價水準的城市，甚至指出上級長官為「一己之私」，捨棄共軍為共同利益而犧牲奉獻的精神。誠如2013年「麥迪安網路公司」(Mandiant Corporation)的報告指出，共軍61398部隊和前總參三部(技術偵察部)的人員往往會在外兼差，從事白帽與灰帽駭客的網路活動來提升收入，有些甚至還會從事低階的網路犯罪或駭客活動，以賺取額外收入(如表四)。[25]

(二)鑒於從事資訊專業人員的薪資待遇較低，共軍在2011年起讓擔任技術偵察專業技術職務的人員(包含從事技偵專業工作的軍、文職幹部)可以支領「技偵專業崗位津貼」，這些人員為從事密碼破譯、情報分析、臺情分析、綜合校譯、話報偵聽、技偵發展研究、信號分析、技偵裝備、開發應用技偵專用計算機、偵收測向監聽等專業人員。[26]至於該崗位津貼的人員及等級，由前總參三部直屬局或相當於直屬局的單位、軍種「技術偵察局」及其情報部負責審批並備案；其中，「技術偵察局」人員屬於一等標準者

註24：Barbara Demick, “China Hacker’s Angst Opens a Window onto Cyber-Espionage,” Los Angeles Times, March 12, 2013, http://articles.latimes.com/2013/mar/12/world/la-fgchina-hacking-20130313，檢索日期：2022年7月21日。

註25：David E. Sanger, David Barboza and Nicole Perlroth, “Chinese Army Unit Is Seen as Tied to Hacking Against U.S.,” The New York Times, February 18, 2013, https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html，檢索日期：2022年7月23日。

註26：〈官兵生活待遇200問〉，中國軍網，2011年10月9日，http://www.mod.gov.cn/service/2011-10/09/content_4303211.htm，檢索日期：2022年7月24日。

，經審批後還可以額外獲得年終績效獎金。[27]這種激勵制度的給付名目為補貼、獎金或津貼，以減少支領者的稅務負擔。[28]至於「戰支隊」成軍後，便已完全承接前總參三部的權責。

肆、戰略支援部隊與文職人才體系

數十年來，共軍「網路戰」計畫在與民間經濟接觸後，已歷經數種不同模式的轉變，這種轉變多因科技人才多匯集在民間。共軍早期與既不可靠又無政府主義的「愛國駭客」接觸，因而認為應持續建立更可靠的人才體系，至於內部作法是擴展共軍教育體制的訓練與研究；外部作法是與民間資訊安全企業進行往來。習近平在2013年將「軍民融合」提升至國家戰略層級，使其重要性等同於軍事與經濟發展，接著在2015年底進行「軍改」，這也開啟「戰略支援部隊」如何重新運用文職人才的新時代。[29]2017年起，在改革過程中逐步產生重大改變，如招聘人員從「文職幹部」、「國防生」轉為重視「文職人員」和「直招士官」。

一、從招聘文職幹部轉向文職人員

(一)過去幾年來，「戰支隊」改招聘「文職人員」至軍中服役，或許最大影響是讓「文職幹部」計畫走向終點，這是過往文職專業技術人員進入部隊及共軍科技研究領域的主要手段。依《共軍文職幹部條例》規定，文職幹部是被任命為初級以上專業技術職務或辦事員級以上職務，不授予軍銜的現役軍人，穿著與現役軍官相同的軍服，擁有與共軍階級對等的文職階級與職等，按照工作性質區分專業與非專業技術。「軍改」後，軍隊人員只包括軍官、軍士、義務兵、「文職人員」四種。[30]就「戰支隊」的觀點而言，進入文職體系意味著一種更接近軍隊的生活型態。[31]

(二)姑且不論「文職幹部」對「戰略支援部隊」的價值為何，其存在已引起當局決策者、媒體和公眾的強烈負面觀感，如共軍體系中存在大量「文藝將軍」，也就是文藝工作者的專業技術職等只要晉升至三級以上(一級相當於中將，二級相當於少將，三級相當於大校)時，就成為文職將軍；然共軍對此解釋為「有職無銜」，只享受相應待遇，並無軍銜的管理和指揮功能，非實質意義上的將軍。[32]另一個案例是「文職幹部」開豪車、炫富的照片在網路上傳播，更招致國家主席習近平的譴責。中共希冀藉由轉型成「文職人員」體系，改善該部隊獲得專業人才問題及消除奢華腐敗風氣。[33]

(三)共軍「文職人員」體系旨在容納未

註27：同前註。
註28：同註24。
註29：〈學習貫徹習近平強軍思想，開創文職人員工作新局面〉，人民網，2018年1月24日，http://military.people.com.cn/n1/2018/0124/c1011-29783604.html，檢索日期：2022年7月25日。
註30：龐慶雲，〈戰略支援部隊某部20餘名在編現役幹部轉改文職人員紀實〉，《解放軍報》，2018年7月11日，http://military.workercn.cn/32821/201807/11/180711090317195.shtml，檢索日期：2022年7月26日。
註31：白萬綱，〈軍民融合的六大動因〉，《國資報告》(北京：中國經濟出版社)，2018年第4期，頁32。
註32：〈再見，文職幹部，謝謝你們〉，騰訊網，2017年11月15日，https://xw.qq.com/cmsid/20171115A04WXU00，檢索日期：2022年7月28日。
註33：王劍宇，〈軍改動態：中共大規模調整軍隊文職人員體系〉，大紀元時報，2017年11月11日，http://www.epochtimes.com/gb/17/11/10/n9827902.htm，檢索日期：2022年7月29日。

表五：《共軍文職人員條例》職位說明表

定義說明	文職人員是指在軍民通用、非直接參與作戰，以及社會化保障不宜承擔的軍隊編制職位下從事管理工作和專業技術工作的非現役人員，列為軍隊成員之一。
職位設置	依2017年修訂的《條例》區分： ◎管理職位：指擔任領導職責或者管理任務的工作職位，由高至低分為部級副職、局級正職、局級副職、處級正職、處級副職、科級正職、科級副職、科員及辦事員等九級。 ◎專業技術職位：指從事專業技術和技能工作，職位要求具有相應的專業技術、技能水準和能力，分為高、中、初級職位，由高到低設一至十三級。 ◎修訂前後差異在於設置文職人員領導職位，文職人員可擔任單位、機關部門或業務部門領導職務。

資料來源：參考〈共軍文職人員〉，維基百科，https://zh.wikipedia.org/zh-tw/共軍文職人員，檢索日期：2022年7月25日，由譯者彙整製表。

來幾年更多的文職專業技術人員，希冀從2017年的4萬人，逐漸擴充超過20萬人。[34]依《共軍文職人員條例》（下稱《條例》）規定，人員不著軍服或擁有準軍事階級，享有跟政府部門聘雇人員同等的權利與義務。[35]這種制度既擴大「文職人員」的職位範圍，又改善薪資待遇，以吸引並留住人才，而且學術與科研人員還能獲得特別待遇。[36]一些在辛苦偏遠地區或是其他特別艱困單位的特殊職位，甚至不會要求「文職人員」和軍人一樣全天候部署。《條例》中也提出招錄聘用的最高年齡限制，初級職位為35歲、中級為45歲，甚至在戰時規定渠等在必要時須轉為現役人員（如表五）。[37]

（四）先前招聘文職至「戰支隊」與「技術偵察局」往往透過特定的方法，但《條例》公布的作法修正為在統一的門戶網站公開招聘資訊。這類似美軍的人才求職網站，而「戰支隊」在成軍時就用這種方式，在30個地區公告招聘1,037位專業技術人員（主要是科研與技術工程），還包含如學術、醫務和財政管理等專長人員。[38]「文職幹部」可以選擇轉換成「文職人員」體系或是退出軍中，雖無法得知多少人選擇在這體制下繼續工作，但中共官媒曾指出有「戰支隊」某部20多名「文職幹部」已申請轉「文職人員」。[39]雖然「戰支隊」的「文職人員」薪資已有所改善，但報導同樣指出，待遇仍普遍低於私人資訊企業。

二、鎖定學術界的招聘計畫改革

（一）「國防生」計畫在2017年終止前，向來是「戰支隊」招募民間大學人才的主要管道之一。該計畫讓大學生可以透過直接辦理轉服役或報考國防科技碩士班等方式從軍

註34：Patrick Boehler, "No More Singing Generals and Dancing Majors in Chinese Military: Xi Jinping," South China Morning Post, August 27, 2013, https://www.scmp.com/news/china-insider/article/1299752/no-more-singing-generals-and-dancing-majors-chinese-military-xi，檢索日期：2022年7月30日。

註35：同註29。

註36：同註33。

註37：同註32。

註38：〈戰略支援部隊面向社會公開招考文職人員宣傳公告〉，搜狐，2018年7月16日，http://www.sohu.com/a/241546660_164555，檢索日期：2022年8月1日。

註39：同註30。

，也是共軍從民間大學挑選更多軍官從軍的重要作為之一。[40]由於「國防生」計畫旨在吸引並維持高素質的新成員，其中包括為頂尖人才提供特殊表現獎學金，及提供優待碩士入學給軍方相關大學的畢業生。[41]招募管道主要是針對原「985工程」、「211工程」知名院校中的學生，而且對於其中一些相對較不嚴格的院校則壓低錄取名額。[42]學生在完成計畫中的學業後，會預劃派職並授予官階，作法等同於「信工大」與其他國防科技院校的畢業生。[43]然因成效不彰，共軍決定終止計畫並轉往文職人才招聘的作法；[44]其中的問題如獎學金金額不高，每人每年約僅獲得1萬人民幣(折合臺幣約4萬5,000元)，不足以吸引大學畢業生興起參軍念頭，[45]而選擇「國防生」計畫的學生，在受訓與看到實況後，往往選擇打退堂鼓；也有在進入部隊服役後，發現無法適應軍中文化的現象。[46]

(二)共軍從民間大學的招募也不只有「國防生」，在「戰略支援部隊」成軍以前，前總參三部即在數個知名的科技校園招募，讓在「國防生」計畫之外的民間大學生也有機會加入共軍，並以中尉任官。[47]此外，前總參三、四部也會網羅已在民間科技院校中完成學位的人員入營，這意味著「國防生」計畫在2009年實施之前，就存在其他的管道，亦凸顯共軍長期以來即致力從民間招募人才至軍中。當然共軍也採取「多管齊下」方式將學術界人才引進軍中，除從「文職幹部」轉變成「文職人員」制度，「戰支隊」還擴大招募管道，如2018年時，即引進來自21個省(市、自治區)、百餘所普通高等院校、四成以上取得本科學歷之570名直招士官，來補實特殊技術職缺，並進行為期13週「由民轉軍」的入伍訓練。[48]

三、戰略支援部隊在民間大學的招募

(一)雖然「信工大」的碩士名額大多保留給軍職，但隨著時間過去，既有的軍職與非軍職比例已開始產生變化；[49]值得注意的是，共軍學術機構已著手制定規則，招收一

註40：〈青年學生政策答記者問〉，共軍戰略支援部隊信息工程大學，2014年5月28日，http://zhaosheng.plaieu.edu.cn/a/zhaoshengzhengce/2014/0528/323.html，檢索日期：2022年8月2日。

註41：同前註。

註42：同前註。「985工程」為綜合實力、學科教育及科研，處於領軍地位和一流水準的大學院校；「211工程」是「21世紀的100所重點大學」，自中國大陸各地挑選出約100所高等學校設定為重點高校，這些學校可優先獲得中共的教育資金補助。

註43：同前註。

註44：〈2017年起不再從普通高中畢業生中定向招收國防生〉，中國軍網，2017年5月26日，http://www.81.cn/zggfs/2017-05/26/content_7620030.htm，檢索日期：2022年8月3日。

註45：同註40。

註46：Ying Yu Lin, “One Step Forward, One Step Back for PLA Military Education,” The Jamestown Foundation, April 24, 2018, https://jamestown.org/program/one-stepforward-one-step-back-for-pla-military-education/；〈國防生贖身記〉，端傳媒，2016年9月23日，https://theinitium.com/article/20160923-mainland-paramilistudent/，檢索日期：2022年8月4日。

註47：〈國家安全部VS總參三部〉，天涯社區，2009年10月16日，http://bbs.tianya.cn/post-188-567594-1.shtml，檢索日期：2022年8月5日。

註48：〈戰略支援部隊570名直招士官來了〉，中共國防部，2018年8月31日，http://www.mod.gov.cn/power/2018-08/31/content_4823804.htm，檢索日期：2022年8月6日。

註49：〈共軍信息工程大學2013年博士研究生報考須知〉，百度文庫，2012年12月7日，http://wenku.baidu.com/view/3ea518136bd97f192279e9b0.html；〈信息工程大學2020年碩士研究生招生簡章〉，中國軍網，2019年10月8日，http://www.81.cn/big5/201311jxjjh/2019-10/08/content_9644873.htm，檢索日期：2022年8月7日

些較年輕的非軍職人員，該作法凸顯網路人才培育朝更年輕的族群發展。共軍也認知到較年輕的人員往往比前一個年代的資深軍官更精通專業技術，尤其在發展「資訊戰」能力時，比其他軍事領域更注重拋棄資歷、等級觀念，如前總參第54研究所多年前就要求六成的研究專案，須由35歲以下研究人員來主導的政策。

(二)除一般招收計畫外，共軍也發展一系列規模較小、為招收高階人才而量身訂製的特殊方案。「信工大」研究生招生辦公室負責制訂高階人才的專案招生，每年有數十位知名科技大學的頂尖研究生，透過免試推薦方式，直接就讀碩士班；[50]且申請者都來自原「985工程」、「211工程」的重點院校。此外，民間重點科技大學的頂尖學生，有時候會在大學生涯早期就被共軍選上，並於技術偵察單位服兩年義務役，役滿後返回校園繼續完成學業。自2011年起，這些返校者更獲得學費補償、補助或學貸還款補助等獎勵，以彌補中斷學業的代價，至於相關規定均明列在公布的辦法中。[51]

(三)一些高級研究員或是各軍事研究所的領導人，還在頂尖民間科技大學的資訊安全、網路工程、計算機科學等學門擔任兼職的博士生導師，如前總參第54研究所的知名高級研究員郭世澤就曾在中國科學技術大學、北京郵電大學、武漢大學擔任博士生導師，[52]這些委任職位不僅可以當成知識共享機制，也成為共軍任務所需與招聘優秀人才的手段。另一種招聘從事「網路戰」優秀人才的方式，為網羅在競賽中脫穎而出的學生。2008年起，共軍軍事院校與民間重點大學合作舉辦特別競賽，以挖掘優秀的資訊安全人才，其中最知名且行之有年的案例為「全國大學生信息安全比賽」，主要是由從事網路攻防研究的軍事與民間卓越中心所策劃，如「國科大」、「信工大」、四川大學、海軍工程大學、電子科技大學、北京郵電大學等。[53]該比賽在防禦重點與人才發掘方面，足以與「全美大學生網路防禦大賽」(U.S. National Collegiate Cyber Defense Competition)媲美。[54]

四、資訊科技與安全公司參與網路戰

(一)「戰支隊」與其前身總參三、四部一樣，也與民間資訊科技與資訊安全公司建立委外研究的機制；尤其中共近幾年強調「軍民融合」政策也朝向更深度的整合，甚至增加與私人企業的資金與範圍合作。如從事資訊戰研究機構的「網電對抗研究所」，從事企業單位委託項目時，將一些主要是網路攻防科技的研究案委託給具適當研發能力的民間公司與大學，意在使用民間人力資本來協助網路武器之開發。不同的公司及個人參

註50：同前註。

註51：該規定為「應徵入伍服義務兵役高等學校在校生學費補償、國家助學貸款代償及退役復學後學費資助暫行辦法」，參見〈2012年高校畢業生應徵入伍預徵工作啟動〉，中國政府網，2012年4月19日，檢索日期：2022年8月8日。

註52：趙少華、唐克美等〈眾多文藝界領導專家助陣中外首工美術館〉，網易新聞，2011年3月28日，http://web.archive.org/web/201905121436 24/http://news.163.com/11/0328/16/708FDCEF00014AEE.html，檢索日期：2022年8月9日。

註53：〈競賽章程〉，全國大學生信息安全競賽，http://117.78.33.202/competitioncharter，檢索日期：2022年8月10日。

註54：“History of CCDC, National Collegiate Cyber Defense Competition,” https://www.nationalccdc.org/index.php/competition/about-ccdc/history，檢索日期：2022年8月11日。

與網路武器發展，主要是透過管道來出售網路漏洞的知識、或是發展共軍所需使用的工具，惟這種合作並非總是「直來直往」。過去中共一些頂級「白帽駭客」表示，在公司承接軍事委託專案後經常面臨一些重大的阻礙因素，如在2012年時，某位世界頂尖的資安漏洞駭客指出，中共願意支付給外部從事「零時差」及其他漏洞攻擊者的金額異常偏低，主因係軍方內部研究網路漏洞攻擊能力大幅提升，再加上許多私人研究者願將技術（也可能是以轉讓或是強制方式）賣給共軍的國防與情報機構牟利。

（二）私人企業也發現在與民間大學和國營學術機構（如前總參第54研究所）競爭軍方研究專案時處於劣勢。一所民間大學可能同時有許多國防研究專案在進行，而一間民營公司不會優先選擇軍方合作，即在於軍規採購的規範與標準存在高昂的固定成本，弄不好甚至還會破壞公司在國際市場上的名聲，這些都可能是阻礙與軍方建立合作關係的因素。因此，中共的「軍民融合」政策顯然有意改善採購合約體制，消弭民間企業的擔憂，至於「戰支隊」「網絡系統部」所負責的網攻任務，也有與外部的資訊科技公司簽約做人員訓練。[55]此外，外部資訊科技安全公司也經常協助培育軍內的「資訊戰」民兵單位，並擔任防禦者角色，以改善中共關鍵基礎設施的韌性，俾因應危機或戰爭發生。[56]

五、民間大學參與網路戰的研發計畫

（一）共軍長期以來委託民間科技大學從事「網路戰」研發計畫與訓練軍方的技術偵察人員；對這些學校而言，這些委託案其實是「有利可圖」。某大學就表明與「技術偵察局」之間的委託關係，將可獲得額外預算，並有助學校的各項計畫執行。[57]委託給民間大學的國防項目可區分為縱、橫向，兩者呈現出不同的態樣，前者涉及軍委會、軍（兵）種、國防集團、政府部會等將專案直接委託民間大學執行；後者涉及民間大學協助軍事機構進行自主研發、協助籌組軍事機構子專案的代表團、接受軍方將主計畫中的子計畫及軍轉民項目進行委託研究。[58]

（二）雖然各所學校在執行委託項目的過程有些許不同，但一般而言，學校都會設置「國防軍工科研項目管理辦公室」（簡稱「軍工辦」），做為接受軍方專案的窗口，執行專案管理、軍民專家學者之間的聯絡橋樑。[59]實務工作的執行則在各學校內的國防軍

註55：Andy Greenberg, “Shopping for Zero-Days: A Price List for Hackers’ Secret Software Exploits,” Forbes, March 23, 2012, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/，檢索日期：2022年8月12日。

註56：Mark Stokes et al., The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure (Arlington, VA: Project 2049 Institute, November 11, 2011).

註57：Rob Sheldon and Joe McReynolds, “China’s Cyber Militia System,” in China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, ed. Jon Lindsay et al. (Oxford, UK: Oxford University Press, 2015).

註58：Shannon Van Sant, “China’s Freelance Hackers: For Love of Country (and Proof That Propaganda Works),” CBS News, July 15, 2013, http://www.cbsnews.com/news/chinas-freelance-hackers-for-love-of-country-and-proof-that-propaganda-works-57592999/，檢索日期：2022年8月13日。

註59：〈上海理工大學國防軍工科研項目管理辦法〉，上海理工大學信息公開網，2018年10月16日，https://xxgk.usst.edu.cn/2018/1016/c8850a164086/page.htm，檢索日期：2022年8月14日。

工科研生產基地或類似機構，該處所不僅為學校列管單獨執行委託案，且還具備儲存機密資訊的能力。軍方委託案的執行工作被視為是機密，因此相關參與人員須遵守2007年頒布的《國防科技工業涉密人員保密管理暫行辦法》，[60]意味民間研究人員可能須先接受安調，據信這些在民間大學經安調過的研究人員，有些人也會被共軍指派來檢視網路產業諜報活動、提供遭竊資訊的專業知識，並在科技領域提供協助與指導。

伍、結語

在過去十年間，共軍在領導人與高階將領支持下，已建立強健的人才體系支援其「網路戰」計畫，而人才體系的整合來源眾多、且不再只依賴單一的管道。這種轉變雖部分反映網路武器對比戰機、戰艦及飛彈發展，僅需較少資本及密集度較低的廠房設施，但也代表共軍致力於國防研發與國防工業現代化的成效之一；值得注意的是，其資訊暨網路人才體系刻正進行變革及重組。

當然共軍仍持續面臨一些挑戰，如從事「網路戰」的專業人才受到民間更優渥待遇的吸引，在役滿後都轉投民間企業；儘管共軍不斷尋找新管道來讓民間企業人才協助「網路戰」武器之開發，但實情是「戰略支援部隊」從事的各項「資訊戰」計畫，更需要常規且受管控的人力，而非這種委託合作的關係。

人員編制變動或更迭並不全然是壞事，「老一派」人的離開才能有空間容納年輕一派的數位人才，並引進現代的技術與創新思維。隨著共軍從事「資訊戰」的單位朝向愈來愈專業化，如何留住訓練有素人才以保持「資訊戰」量能也成為重點工作。因為人才流失意味著共軍先前投資在這些人身上的訓練與教育都白白浪費；此外，共軍在「組織再造」過程中，能否做到保留或傳承一些科技軍官的經驗，或在「網路戰」人才培育的一些作為，能否在未來幾年獲得成效，這些都仍有待後續觀察與驗證。

陸、譯後語

中共「網路部隊」也稱為「網軍」，兩個知名的網軍為前總參三部下屬的61398部隊與61486部隊，在「軍改」後已併入「戰略支援部隊」，而「網路戰」被共軍視為取得「資訊戰」勝利的關鍵。至於作戰構想則是整合「網路戰」與「電子戰」的「網電一體戰」，[61]藉由將病毒、邏輯炸彈及惡意軟體等武器植入敵方戰場資訊網路內部，採取「滲透控網、超載廢網、傳染癱網」等行動，達成戰場指管中斷，甚至癱瘓整體作戰體系。[62]鑒此，相關人才培育是維持資訊暨網路能力與能量的要素，本文作者就指出共軍在網路人才培育上轉型後的優、劣勢，可供

註60：〈國防科工委在京召開國防科技工業安全保密專題會〉，中國政府網，2007年7月19日，http://www.gov.cn/gzdt/2007-07/19/content_690568.htm，檢索日期：2022年8月15日。

註61：王清安，〈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》(臺北市)，第54卷，第3期，2020年6月1日，頁82-86。

註62：譯者註：龍率真，〈網路癱瘓目標國，中共威脅全球警戒〉，青年日報，2021年8月29日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1439867&type=forum，檢索日期：2022年8月16日。

國軍相關資訊從業人員參考。

網路人才具有軍民通用的特性，因此優秀人才不管是在民間資訊企業或是軍方都「不可或缺」，民間所提供的薪資與福利誘因相對比軍方優渥，但民間資訊人才都有其工作時效性；過了時效性後就會被新的人所取代，那是因為民間企業為撙節人事成本，多以新進人員的「低薪資」來取代資深人員的「高薪資」；然而國軍的資訊部門卻不會有這個問題，「長留久用」與「保障工作」或許是國軍招募資訊暨網路人才的優勢之一。

我國平均每月受3,000萬次以上的網路攻擊，當中來源主要是中國大陸，這已讓資訊安全成為另一個戰場。[63]國軍雖已成立「資通電軍」，俾有效提升資訊作戰能力，但其動能仍須時時與民間密切接軌、整合民間技術與能力，才能發揮實質戰力；而更重要的是「人如何招得進來，又留得下來」，因此做好進階教育訓練仍是當務之急。近期在美國眾議院議長斐洛西(Nancy Pelosi)訪臺後，中共對臺發動網攻事件，並讓總統府、國防部及外交部網站造成短暫中斷，這類攻擊示警及嚇阻意味濃厚，雖未造成實質損失，但吾人不容輕忽以對。「網攻」手法不斷推陳出新，國軍應不斷精進學習，面對未來中共可能發起的網路攻擊，國軍平時應做好遭遇大規模網攻之應變準備。因為現今與網路連結的系統與設施眾多，一旦部分或全面停擺所造成的效應「不容小覷」，政府部門與國軍單位應及早做好防範的準備。 ⚓

註63：譯者註：鄭閔聲，〈指尖上的防衛戰〉，《今周刊》(臺北市)，第1180期，2019年7月31日，https://www.businesstoday.com.tw/article/category/80392/post/201907310022/，檢索日期：2022年8月17日。

作者簡介：

麥克雷諾茲(Joe McReynolds)為國際SOS公司智能方案解決組的首席網路分析師，「詹姆斯頓基金會」(Jamestown Foundation)中共安全研究研究員，中共網路與情報研究院共同創辦人，並在2019年時擔任日本防衛省與慶應義塾大學的客座研究員。

露絲(LeighAnn Luce)為獨立分析師，專門研究中共國防電子與資訊科技，目前任職於一家軟體公司，先前在國際SOS公司特別計畫處擔任高級工程師，以及曾在國防集團公司(Defense Group, Inc)情資研究分析中心擔任技術分析助理副主任(Associate Deputy Director)。

譯者簡介：

劉宗翰中校，國防大學管理學院93年班、政治大學外交系戰略所碩士104年班。曾任排長、《國防譯粹》月刊主編，現服務於國防部政務辦公室暨軍事譯著主編。