中共解放軍「戰略支援部隊」之發展對我陸軍威脅評估 - 以網路作戰部隊為例

作者／王清安上校

提要

一、2015 年 12 月 31 日，中共解放軍將原太空部隊、網路部隊及電子對抗部隊，整併為「戰略支援部隊」，並直屬於中共中央軍委指揮成為第五個軍種。組織的改革，勢必對中共網路空間作戰運用產生影響。

二、本研究發現，中共網路作戰部隊整併至「戰略支援部隊」後，其網路戰略將從被動防禦轉向「平戰結合、偵防一體化」的主動防禦；其作戰效能將提升網路空間整體戰力、強化聯合作戰效能與增加網路戰略嚇阻能力。

三、因應中共網路作戰部隊組織調整，本研究建議我陸軍應提升軍民網路安全合作機制，採購抗干擾、機動性強的通資系統；建構 AI 人工智慧網路安全防護，強化網路攻防課目演練等二項，以提升我陸軍通資安全防護能力。

關鍵詞：戰略支援部隊、網路作戰部隊、網路攻擊。

前言

2015 年，《中國的軍事戰略》指出：面對網路空間的威脅，中共解放軍應加快網路空間力量建設，以確保國家安全和社會穩定。[1]同年 12 月 31 日，中共軍委主席習近平主持「戰略支援部隊」成軍典禮時表示：「戰略支援部隊」是維護中共國家安全的作戰力量。同時更是新型態聯合作戰能力的增長點。[2]此外，2017 年曾擔任美國雷根總統的國防特別顧問艾利森(Graham Allison)亦揭露出：中共網路攻擊能力，已具備可暫時削弱美國在網路空間的反擊能力；其攻擊目標更包含了關鍵的指、管、通、資、情、監、偵等系統。[3]由中共網路作戰部隊發展的意圖及能力，凸顯出中共解放軍的網路戰實力不容忽視。同時，也意味著網路作戰部隊的成立，對中共解放軍提升聯合作戰能力，至關重要。

---

[1] 中華人民共和國國務院新聞辦公室，〈中國的軍事戰略〉《解放軍報》(北京)，2015 年 5 月 27 日，版 4。
[2] 馮凱旋，〈習近平向中國人民解放軍陸軍火箭軍戰略支援部隊授予軍旗並致訓詞〉《解放軍報》(北京)，2016 年 1 月 2 日，版 1。
[3] Graham Allison, “How America and China Could Stumble to War,” National Interest, http://nationalinterest.org/feature/how-america-china-could-stumble-war-20150, (April 12, 2017), 2017/10/10.

2016 年，我國安局研判中共解放軍「戰略支援部隊」有助於網路戰力提升。同時該部隊在整合太空、網路與電子戰任務後，對爾後中共解放軍在遂行整體作戰具有一定的助益。[4]隔年，美國防部出版的《2017 中共解放軍軍力與安全發展報告(Military and Security Developments Involving the People's Republic of China 2017)》更明確指出：「戰略支援部隊(Strategic Support Force, SSF)」為中共解放軍遂行聯合作戰，提供資訊鏈結保障；同時未來台海衝突中擔負起極為重要之角色。[5]因此，隨著中共網路作戰部隊移編至新成立軍種的「戰略支援部隊」後，將投射出對我國網路安全產生更大威脅。同時，對我陸軍通資安全亦產生嚴重衝擊。因此，本文採「文獻分析法」，首先瞭解網路空間之定義及對軍事作戰影響。其次探討該部隊發展背景、編組與特、弱點。最後評估對我陸軍通資安全防禦能力之威脅，據而提出策進作法。

網路空間之概述

隨著網路科技的發達，網路空間已從物理空間的關鍵資訊基礎設施，擴及到網路行為體的資訊用戶。

一、網路空間之定義

(一)美國

作戰環境為依作戰任務及指揮官意圖所界定之範圍。根據 2013 年 2 月 5 日，美國國防部發布的《網路空間作戰聯合條令》(Cyberspace Operations)指出：自由、開放的網路空間是資訊、通訊科技等基礎設施的網際網路所建構而成；其包括電信、網際網路及控制、辨識數據資訊之網路協定的伺服器，與資訊用戶終端的電腦系統。同時，網路空間區分為物理網路(The Physical Network)、邏輯網路(The Logical Network)及網路行為體(Cyber-persona)等三個層次，每一層都可以進行網路空間作戰。[6]另外，美軍為強化聯合作戰效能，於 2017 年 1 月 27 日，新出版的《聯合作戰 JP-3.0》更指出：網路空間是由資訊、通訊等基礎設施組成；其中包括網際網路、電信網路及電腦內的作業系統與處理器。[7]由美國防部網路空間界定的範圍，已透露出美國網路作戰企圖，將涵蓋其兵力投射範圍。同時，網路空間防禦範圍也從資訊終端用戶的作業系統，到機動載具的接收器，均為網路空間防禦範圍內。

---

[4] 國家安全局，〈從國防部成立第四軍種之必要性探討網路駭客之侵擾對政府及民間資訊安全防範之挑戰〉《立法院第 9 屆第 1 會期外交及國防委員會第 19 次全體委員會議》(臺北)，2016 年 5 月 11 日，頁 2。

[5] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2017," May 15, 2017, pp.81.

[6] United States Department of Defense, Joint Publication 3-12 (R) Cyberspace Operations(Washington:United States Department of Defense, February 5, 2013), pp.I-2- I-3.

[7] "Joint Publication 3-0, Joint Operations," Defense Technical Information Center, 17 January 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf, pp.IV-2.

(二)中共

網路空間對軍事層面的影響，已從網路、資訊等關鍵基礎設施擴及到個人決策。根據 2013 年劉興等人研究表示：網路空間區分為物理、資訊、認知及社會等四個領域；其中社會領域為文化域，其目的為影響人員的價值觀。[8]另外，2014 年 5 月遠方更指出：網路空間還包括電磁域，如無線電電子訊號與位元域，如作業系統。[9]此外，2015 年 2 月任職「南京陸軍指揮學院」的趙秋梧副教授表示：網路空間為網際網路、通信實體線路、電腦作業系統，及電腦晶片中的處理器所建構的新型社會生活虛擬空間。[10]因此，網路空間所界定範圍應包括物理空間的網路、資訊等關鍵基礎設施、國際規範的網路協議及資訊用戶外，還有電磁頻譜。換言之，中共解放軍的網路空間作戰，即為網路戰與電子戰的結合。

因此，美、中兩國在網路空間的定義共同點為網路空間中的物理層、認知層及邏輯層，而不同點為中共網路空間包括電磁頻譜空間及影響個人意識型態的宣傳戰、心理戰。換言之，中共國防武力所形塑的網路空間，將較以往的網路戰、電子戰或太空戰的空間，更為複雜、廣泛及立體，對軍事作戰也產生影響。

二、網路空間對軍事之影響

隨著軍事領域對網路的倚賴，獲取網路空間的制高點，將可確保軍事行動自由及提升聯合作戰效能。

(一)確保軍事行動自由

隨著移動式無線電寬頻網路，已可提供聯合作戰所需戰場圖像的平台。只要癱瘓敵方之網路、資訊等關鍵要點，即可確保我方軍事行動自由。根據 2013 年偉恩(Wayne W.)指出：由於網路與電信基礎設施的無線電應用日益擴展，使得商用和軍用系統愈來愈依賴兩者發展。同時，也使得電子戰與網路空間彼此關聯愈趨緊密。[11]另由於電磁干擾對太空衛星、遠距離載(具)台和指揮中心等之數據共享或通連影響愈來愈大，電磁頻譜已為現代戰爭中最重要領域之一。[12]此外， 2017 年 10 月哈里森(Todd Harrison)亦表示：網路攻擊已對衛星造成極大的威脅；其主要原因是透由網路攻擊可控制衛星與關閉通信網路，還可以損壞其電子設備，最後摧毀衛星。另方面還可針對衛星與地面接收站間數據鏈路、遙控鏈路及終端用戶與網路電話等實施網路攻擊。[13]因此，隨

[8] 劉興、藍羽石，《網路中心化聯合作戰體系作戰能力及其計算》(北京:國防工業出版社，2013 年 6 月)，頁 2-3。
[9] 遠方，〈網路空間的戰爭脆弱性〉《中國資訊安全》，第 5 期，中國資訊安全測評中心，2014 年 5 月，頁 114。
[10] 趙秋梧，〈論網路空間戰爭的特徵及其本質〉《南京政治學院學報》，第 31 卷第 2 期，2015 年 2 月，頁 81。
[11] Wayne W and Grigsby Jr, 梁正綱譯，〈網路電磁作業:統合地面作戰之致勝關鍵(CEMA: A Key to Success in Unified Land Operations) 〉《國防譯粹》(臺北)，第 40 卷第 2 期，國防部政務辦公室，2013 年 2 月，頁 32。
[12] 宋吉峰譯，〈反制「停滯」美軍未來電磁頻譜作戰優勢(上)〉《青年日報》(臺北)，2016 年 7 月 19 日，版 7。
[13] Todd Harrison, Zack Cooper, Kaitlyn Johnson, and Thomas G. Roberts, “Escalation and Deterrence in The Second Space Age,” Center for Strategic and International Studies October 2017, pp.15-16.

著軍事系統對網際網路的依賴，搶佔網路空間制高點將可阻止、削弱敵人優勢，確保自身軍事行動自由。

(二)提升聯合作戰效能

作戰效能即為以最少的成本獲取最大的功效。根據 2010 年溫茲(Larry K. Wentz)指出：為提升美軍聯合作戰效能，美國防部依任務需求在網路空間區分為業務、作戰及情報等三種區域。同時，情報網路不完全由國防部管理，與美國情報機構共同管理。[14]另外，因應日益嚴重的網路攻擊威脅及確保美軍在網路空間的優勢，美國防部已規劃結合民間企業力量以提升網路戰攻、防能力，確保其太空通信、影像資源等數據安全。[15]不僅如此，為提升美軍先發制人的作戰能力，將整合太空科技與網路空間之情蒐能力，優先對敵 C^4ISR 等目標遂行攻擊以削弱敵防空能力，進而擾亂、摧毀敵指揮系統與重要目標。[16]因此，提升網路空間作戰能力，將可擴大作戰空間的接戰能力，提升遠距離精準打擊能力，以滿足聯合作戰任務需求。

中共「戰略支援部隊」之網路作戰部隊發展背景與編組

隨著網路空間作戰型態與軍事戰略的改變，網路作戰部隊亦須做組織改革。

一、網路作戰部隊發展背景

誰能控制網路空間的制高點，誰就能掌握戰爭的主動權。根據 2013 年中共解放軍國防大學所出版《網路空間安全戰略研究》指出：網路空間納入聯合作戰體系後，將可提高整體作戰效能；其中，網路戰與電子戰相結合，可實現網電一體化聯合作戰。同時，網路空間與實體攻擊相結合，亦可提高戰略嚇阻能力和火力打擊效能。[17]另外，2015 年 2 月中共解放軍《陸軍指揮學院》副教授趙秋梧更表示：網路空間中的戰爭，是資訊社會依託於網路空間而進行對抗和衝突的一種嶄新形式，較網路戰不同的是虛擬網路空間中更加依賴電磁頻譜。同時，在多個領域通過網路平臺進行作戰，才能獲取行動的自由權。[18]另值得注意，中共解放軍已觀察到 2014 年俄羅斯入侵克里米亞，曾運用網路空間的假消息，搭配傳統軍事武力成功之案例。因此，面對新型態的網路空間作戰，中共解放軍已意識到，已往分散於總參四部的電子偵察部隊、總參三部的網路部隊、總裝備部太空部隊將無法贏得未來的戰爭勝利。簡言之，因應未來的複合式作戰型態，整合網路、太空、電子戰等部隊是勢在必行。

---

[14] Larry K.Wentz，李健、嚴美譯，《網路戰-美軍稱霸全球的第五戰場》(香港：新點出版公司，2010 年 12 月)，頁 15-16。

[15] 黃文啓譯，〈肆應潛在威脅 美國重塑軍事實力(中)〉《青年日報》(臺北)，2015 年 11 月 25 日，版 7。

[16] 李華強譯，〈美、日、澳海上安全合作 聯防亞太區域(中)〉《青年日報》(臺北)，2016 年 5 月 18 日，版 7。

[17] 黃藝，《網路空間安全戰略研究》(北京：國防大學出版社，2013 年 3 月)，頁 52。

[18] 趙秋梧，〈論網路空間戰爭的特徵及其本質〉《南京政治學院學報》，第 31 卷第 2 期，南京政治學院學報雜誌社，2015 年 2 月，頁 82-83。

除此之外，軍事編裝的變革除因應戰爭型態的調整還須考量國防戰略。2012年底，中共軍委主席習近平出席首次《深化國防和軍隊改革》常務會議時表示：為實現中華民族偉大復興，須建設強大的國防軍隊，改革國防和軍隊是實現這個戰略佈局的重要支撐。[19]另外，2013 年，《中國武裝力量的多樣化運用》更強調：打贏資訊化條件下的局部戰爭，須搶占太空、網路空間等戰略制高點。[20]此外，2015 年 11 月 24-26 日，中央軍委主席習近平出席「中央軍委改革工作會議」更強調：推進高效統一指揮部隊，以形成「軍委管總、戰區主戰、軍種主建」的新格局。[21]由中共國防改革及軍事戰略訴求重點，已透露出中共解放軍面對未來聯合作戰，奪取網路空間的制高點對其國防武力之重要性。換句話說，要確保中共解放軍贏得未來戰爭，就須提升網路空間整體戰力。

二、中共網路作戰部隊編組

2015 年 12 月 31 日，中共軍委主席習近平於中共解放軍軍委八一大樓主持「戰略支援部隊」成軍典禮時強調，「戰略支援部隊」要建設為一支體系融合、軍民融合現代化的部隊。[22]同時，「戰略支援部隊」將整合過去負責無線電監聽、偵查的總參謀部技術偵察部(總參三部)、雷達系統的總參謀部電子對抗部(總參四部)，及總參謀部訊息化部(總參五部)。[23]

(一) 編制單位

原總參謀部之「技術偵察部」下轄網路部隊及第 56(江蘇計算技術研究所)、58(中國電子工業集團研究所)研究機構，移編到「戰略支援部部隊」下轄之「網路系統部門(Network Systems Department, NSD)」。[24]同時，更換為「中國人民解放軍戰略支援軍網路空間作戰部隊」(簡稱戰支三部)。[25]另外，值得注意的是，總政聯絡部情蒐單位納入戰略支援部部隊，以強化網路心理戰能量。[26]因此，網路作戰部隊的編制部隊，應包含原網路部隊及總政聯絡部情蒐部門。

---

[19] 〈改革強軍 奮楫中流-習主席和中央軍委運籌設計深化國防和軍隊改革紀實〉《解放軍報》(北京)，2015 年 12 月 31 日，版 1。

[20] 謝奕旭，〈由習近平宣示裁軍談大陸的國防現代化〉《展望與探索》，第 13 卷第 10 期，法務部調查局，2015 年 10 月，頁 20-21。

[21] 〈習近平在中央軍委改革工作會議上強調 全面實施改革強軍戰略 堅定不移走中國特色強軍之路〉《解放軍報》(北京)，2015 年 11 月 27 日，版 1。

[22] 馮凱旋，〈習近平向中國人民解放軍陸軍火箭軍戰略支援部隊授予軍旗並致訓詞〉《解放軍報》(北京)，2016 年 1 月 2 日，版 1。

[23] 〈戰略支援部隊作用 中共黨媒：致勝關鍵〉《中央通訊社》，https://www.cna.com.tw/news/acn/201601240213.aspx，(2016 年 1 月 25 日) ，2017 年 10 月 15 日.

[24] John Costello, “The Strategic Support Force: Update and Overview,” Jamestown., https://jamestown.org/program/strategic-support-force-update-overview/, (December 21, 2016) , 2017/10/15.

[25] 〈獨家：原總參三部併入戰略支援部隊 正式改名網路空間作戰部隊〉《博聞社》，https://bowenpress.com/news/bowen_58905.html，(2016 年 1 月 19 日)，2017 年 10 月 15 日.

[26] 林穎佑，〈共軍軍改對亞太區域的威脅與影響〉《中共研究》，第 50 卷第 4 期，中共研究雜誌社，2016 年 7 月，頁 147。

除此之外，2016 年底中央軍委給某大隊「模擬室」記集體一等功。該模擬室在第二代衛星通信裝備、全軍首支作戰部隊通資裝備電磁相容試驗和聯合頻譜管理系統研製等，獲軍隊科技進步獎 19 項。[27]另據 2017 年卡尼亞(Elsa Kania)指出，為因應未來資訊戰爭的需求，提升網路科技創新能量，將原第 54、56、57 和 58 研究機構全部移編至「戰略支援部隊」。[28]因此，網路作戰部隊，還包含具有科技研發能力的部隊。

(二)非編制單位

隨著網路空間擴及到國家安全領域，軍、民網路科技整合有利於網路空間戰力提升。根據 2016 年石格爾(Adam Segal)表示：中共「華為」和「中興」等民間通信公司與中共解放軍合作甚密，已危害美國的網路、資訊等關鍵基礎設施；其主要理由為 2011 年美國政府已調查出代號 SHOTGIANT，是「華為通信」為中共解放軍可以癱瘓敵國所需後門程式。[29]事實上，根據 2013 年《美國眾議院》出版報告指出：「華為」和「中興」等民間通信公司，已提供中共情報機構可以癱瘓、竊取敵國網路重要資情之惡意軟、硬體等程式。[30]不僅如此，2013 年卡查瑟芙(Boris Kazantsev)亦表示：中共在網路空間技術層面發展上，以扶植本土網路科技產業為目標。同時更規範要進入中國大陸市場，外商企業須讓中國網路科技公司入股，如聯想收購 IBM。[31]除此之外，名為中國熊貓網路駭客組織，其網路攻擊能力也愈來愈強；攻擊目標包含外國的領使館、國防承包商等。[32]因此，在軍民融合支持下，將可提升其網路空間整體戰力。

另外值得注意的是，隨著網路空間作戰範圍擴大，網路科技所需的技術層面也隨之提高。根據 2015 年中共網路專家的惠志彬指出，中共解放軍應摒棄駭客部隊的國際不利影響，積極整合軍隊、企業和民間力量，組建精英化的網路空間安全保障和威懾部隊，推動中共網路空間的防護和對抗能力。[33]2017 年 7 月 12 日「戰略支援部隊」分別與中共科技大學、上海交通大學、西安交通大學、北京理工大學、南京大學、哈爾濱工業大學等 6 所大學，以及航太科技集團公司、航太科工集團公司、電子科技集團公司等軍工企業，簽訂戰略合作框架協定，以縮短高科技人才培養週期。[34]此外，名

---

[27] 梁蓬飛、張能華，〈軍委聯合參謀部給某大隊模擬室記集體一等功〉《解放軍報》(北京)，2016 年 11 月 15 日，版 2。

[28] Elsa Kania ,"China's Strategic Support Force: A Force for Innovation?," The Diplomat, https://thediplomat.com/2017/02/chinas-strategic-support-force-a-force-for-innovation/, (February 18, 2017), 2017/10/15.

[29] Adam Segal, "China, Encryption Policy,and International Influence," A Hoover Institution Essay Series Paper No. 1610, https://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf, pp.8.

[30] U.S. House of Representatives, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE Paperback(U.S:Create Space Independent Publishing Platform, June 19, 2013), pp.3

[31] Boris Kazantsev, "How to Counter America's Digital Hegemony," Strategic-Culture, https://www.strategic-culture.org/news/2013/11/23/how-to-counter-americas-digital-hegemony.html (November 23, 2013), 2018/2/14.

[32] Marzie Astani, and Kathryn J. Ready, "Trends and Preventive Strategies For Mitigating Cybersecurity Breaches in Organization," Issues in Information Systems, Vol.17, Issue II, 2016, pp.210.

[33] 惠志斌，《全球網路空間信息安全戰略研究》(上海:中國出版集團，2015 年 4 月)，頁 231。

[34] 李國利、宗兆盾，〈戰略支援部隊與地方 9 個單位合作培養新型作戰力量高端人才〉《新華社》，http://news.

為「3+1 計畫」，已在中共西安交通大學等一些機構實施試行。該計劃為將徵選網路人才擴及到高中職，待完成三年課程後，至企業實習 1 年。這些優秀畢業生將至中共解放軍「戰略支持部隊」服務。[35]故在民間大學、企業與中共戰略支援部隊合作下，將可提升網路戰部隊整體素質。

不可諱言，隨著網路科技的發展，電子信號偵蒐/反偵蒐、干擾/抗干擾，對網路空間的影響日趨重要。故要確保網路空間整體安全，便須考量電子對抗部隊及太空部隊發展。原總參謀部四部「電子對抗與雷達部」下轄的戰略級或國家級電子戰部隊，以及第 54 研究所(中國電子科技集團公司)，移編至「戰略支援部隊」。[36]另外，為強化電子情報能力，原總二部下轄的圖像衛星及戰略無人機隊，移編「戰略支援部隊」，以提升網路空間中的電磁頻譜管制能力。[37]另外，原總裝備部之「國家航天局」涉及太空軍事用途部分及衛星發射基地併入新成立的共軍戰略支援部隊。[38]負責航空航天的「航天偵察局」(61646 部隊)（The Aerospace Reconnaissance Bureau, ARB），以及航天研發中心，工程設計研究所研究機構，移編至戰略支援部隊。另外，總參五部「信息化部」(Informatization Department, INFID)的衛星通信總站(61096 部隊)(Satellite Main Station, SMS)被納入「戰略支援部隊」。[39]故在電子戰部隊及太空部隊整併於戰略支援部隊後，將使網路空間作戰部隊更專注於網路攻、防任務。

總而言之，中共網路作戰部隊，編制單位包含為原網路部隊、原總政聯絡部與某大隊「模擬室」。另外，非編制單位包含華為、中興等通信民營公司、網路駭客組織，以及中國科技大學、上海交通大學、西安交通大學、北京理工大學、南京大學、哈爾濱工業大學等 6 所大學，網路作戰部隊編組圖，如圖一。

中共解放軍遂行網路空間的部隊，不僅有專業的網路空間作戰部隊。另外，平時建制於各戰區下的網路部隊。中共聯合參謀部下設有 4 大局，分別是信息通信局、導航局、作戰局、戰場環境保障局。[40]「信息通信局」為原「信息化部」(簡稱總參五部)重組單位，除原第 61 研究所轉移到「中央軍委裝備發展部」及衛星通信總站(61096 部隊)移編「戰略支援部隊」外，餘保留部隊成立「中央軍委聯合參謀部信息保障基地」，負責軍委聯合信息保障、資訊安全和情報傳播的責任。[41]「信息通信局」負責網路戰

---

xinhuanet.com/politics/2017-07/12/c_1121308932.htm，2017/10/20。

[35] Zi Yang, “China Is Massively Expanding Its Cyber Capabilities,” National Interest, https://nationalinterest.org/blog/the-buzz/china-massively-expanding-its-cyber-capabilities-22577, (October 3, 2017), 2017/10/17.

[36] 同註 24。

[37] “China Reorients Strategic Military Intelligence,” IHS Jane's Military & Security Assessments Intelligence Centre, https://www.janes.com/images/assets/484/68484/China_reorients_strategic_military_intelligence_edit.pdf, 2017/ 10/17, pp.3.

[38] 鍾承翰，〈淺析中共發展航太科技戰略意涵〉《青年日報》(臺北)，2016 年 1 月 24 日，版 7。

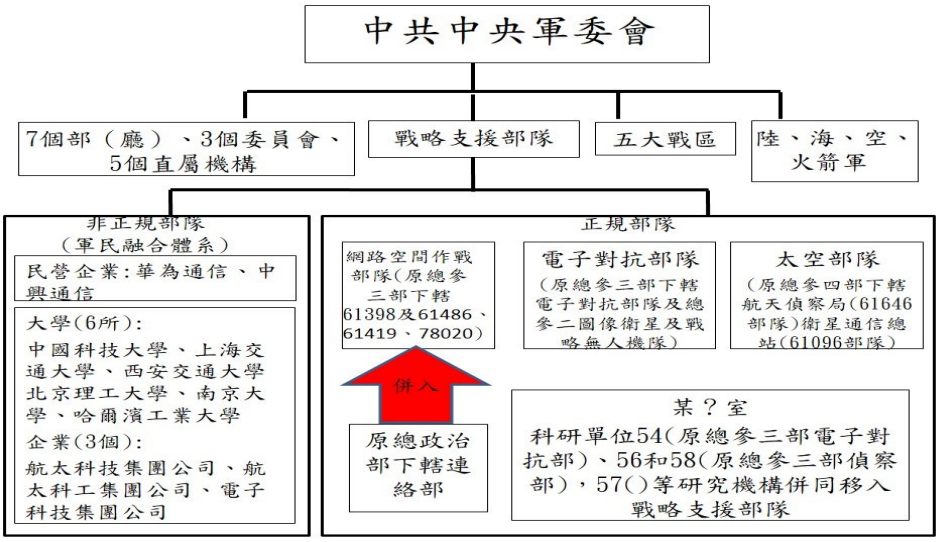
[39] 同註 24。

[40] 陳建瑜，〈軍委聯參部 神祕 4 大局曝光〉《旺報》(臺北)，2016 年 4 月 17，版 6。

[41] 註 24。

進攻與防護，在各戰區的軍級單位成立信息化辦公室及下屬「信息戰分隊」，專責駭客部隊的網路攻擊。[42]根據 2016 年 11 月報導證實：中共解放軍在國防科技大學召開全軍首期網路管理骨幹培訓班。其對象為來自全軍師、旅級以上的50餘名網路管理幹部，實施 2 個月網路新技術新應用、網站運行維護等訓練。[43]

圖一 網路作戰部隊編組圖



資料來源：參考自惠志斌，《全球網路空間信息安全戰略研究》(上海：中國出版集團，2015 年 4 月)，頁 231；張楊、劉笛〈戰略支援部隊組織首批畢業國防生軍政集訓〉《解放軍報》(北京)，2016 年 11 月 7 日，版 2；李國利、宗兆盾，〈戰略支援部隊與地方 9 個單位合作培養新型作戰力量高端人才〉《新華社》，http://news.xinhuanet.com/politics/2017-07/12/c_1121308932.htm，2017 年 7 月 12 日；梁蓬飛、張能華，〈軍委聯合參謀部給某大隊模擬室記集體一等功〉《解放軍報》(北京)，2016 年 11 月 15 日，版 2。

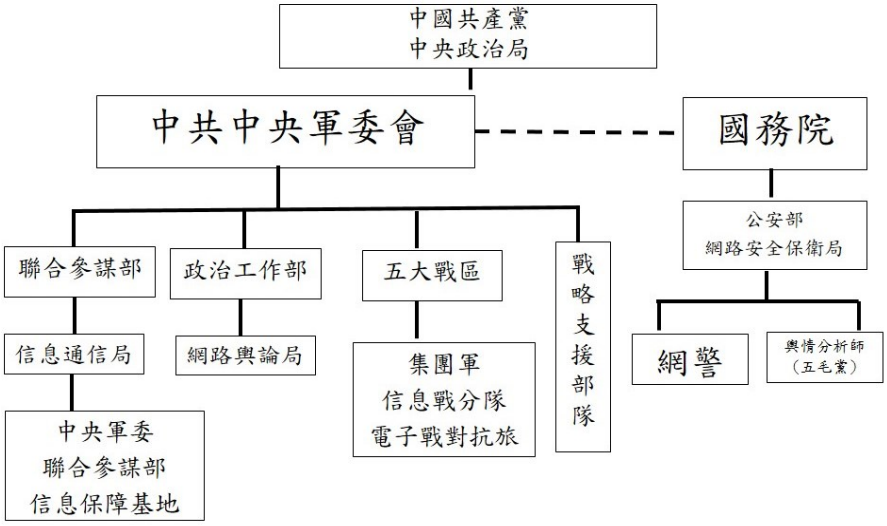
另外值得注意的是，原總政戰部軍改後「中央軍委政治工作部」，其所屬的 5 個局包括：群眾工作局、宣傳局、組織局、幹部局及網路輿論局；其網路輿論局與解放軍報合開專欄，名為「過好網路關時付關新探索新實踐」，介紹讓部隊利用「互聯網+」創新政治教育經驗，解決「互聯網進軍營矛盾難題」的問題。[44]故網路空間的意識形態管制，已成為中共解放軍管理重點。

除此之外，為因應網路空間作戰的複雜性，中共解放軍在各戰區組建各級「網路作戰指揮中心」，負責網路空間作戰準備與指揮，形成軍委聯指、信息作戰集群、網路作戰群等三級網路空間作戰指揮體系。[45]「戰略支援部隊」平時未部署至各戰區，視

[42] 尹俊傑，〈網路戰 漢和：共軍駭客部隊增加〉《中央通訊社》，https://www.cna.com.tw/news/acn/201601040303.aspx, 2016 年 1 月 4 日。
[43] 王握文，〈全軍首期網路管理骨幹培訓班開班〉《解放軍報》(北京)，2016 年 11 月 10 日，版 2。
[44] 潘維庭，〈軍改成績單 政治工作部 5 局亮相〉《旺報》，2017 年 2 月 6 日，版 A8。
[45] 黃藝主編，《網路空間安全戰略研究》(北京：國防大學出版社，2013 年 3 月)，頁 65。

狀況支援各戰區遂行作戰。[46]2016 年 10 月 19 日中共東部戰區演習中，中共解放軍首支電子對抗旅，承訓了 3000 多名專業人才，為全軍電子對抗部隊提升整體戰力。[47]因此，中共遂行網路空間作戰人員，還包括各戰區中的網路戰及電子對抗部隊。(如圖二)

圖二 中共解放軍遂行網路空間作戰部隊編組圖



資料來源：參考自陳建瑜，〈軍委聯參部 神祕 4 大局曝光〉《旺報》(臺北)，2016 年 4 月 17 日，版 6；黃藝，《網路空間安全戰略研究》(北京：國防大學出版社，2013 年 3 月)，頁 65。尹俊傑，〈網路戰 漢和：共軍駭客部隊增加〉《中央社》，2016 年 1 月 5 日；John Costello, “The Strategic Support Force: Update and Overview,” Jamestown., https://jamestown.org/program/strategic-support- force-update-overview/, December 21, 2016；王握文，〈全軍首期網路管理骨幹培訓班開班〉《解放軍報》(北京)，2016 年 11 月 10 日，版 2；潘維庭，〈軍改成績單 政治工作部 5 局亮相〉《旺報》，2017 年 2 月 6 日，版 A8；郭崇德，〈多維偵察讓戰場變得透明-第 47 集團軍某旅參加跨區實兵對抗演習見聞〉《解放軍報》(北京)，2016 年 8 月 30 日，版 1；代烽、李勇，〈「電磁利劍」從幕後走向前臺〉《解放軍報》(北京)，2016 年 10 月 19 日，版 1。

評估中共「戰略支援部隊」之網路作戰部隊能力

評估網路作戰部隊能力，必須瞭解其網路戰略構想。同時透由各國威脅評估進而檢視其網路戰能力。

一、戰略構想

(一)平時

誰掌握戰爭面的主動權，誰就擁有戰爭優勢。根據2016年美國情報局於參議院情報專責委員會報告《全球威脅評估(Worldwide Threat Assessment)》指出：中共解放軍之網路空間作戰意圖，為運用網路偵察手段掌握它國重要人物動態或公眾情緒。於衝

[46] 揭仲，〈中共推動軍事變革對臺灣之影響〉《中共研究》，第 50 卷第 4 期，中共研究雜誌社，2016 年 7 月，頁 149。
[47] 代烽、李勇，〈「電磁利劍」從幕後走向前臺〉《解放軍報》(北京)，2016 年 10 月 19 日，版 1。

突階段時，散佈虛假資訊或修改對方數據資料，進而引起敵國決策中錯誤。[48]此外，根據2017年陳森表示：和平時期，運用網路滲透潛伏它國資訊系統獲取戰時所需的情報，以利掌握先機開創有利態勢。[49]故和平時期，中共解放軍將運用網路偵察手段，以便先期掌握該國戰爭面及軍事情報需求，以利開創後續有利態勢。

(二)戰時

誰能掌握較多的情報，誰就能掌握較多的作戰優勢。中共解放軍網路作戰部隊的成立，即為搶佔網路空間之制高點所進行的組織調整。根據2017年美國國防部所出版的《中共解放軍軍事評估報告》指出，「戰略支援部隊」的戰略構想為將網路戰、電子戰和心理戰爭視為一體，作為實現資訊優勢的必要組成部分；其重要手段為削弱對手在戰爭中獲取、傳播，處理和使用資訊的能力，迫使美國軍艦、飛機在網路空間中無法通聯傳輸數據。[50]此外，根據2017年8月1日《慶祝中國人民解放軍建軍90周年》受閱梯隊證實；「資訊作戰群」作戰任務為加快融入全軍聯合作戰體系，關鍵領域實現跨越發展。同時掌握複雜電磁環境下戰場主動權；其部隊包含信息支援方隊、電子偵察方隊、電子對抗方隊及無人機方隊。[51]故戰時，中共網路作戰部隊以癱瘓敵國指揮與管制系統，並以網路宣傳戰獲取國際戰爭的話語權，同時確保聯合作戰通聯順暢。

承上所述，中共網路作戰部隊成立後，將於中共解放軍遂行聯合戰役作戰時，編組「資訊作戰群」受戰役部隊作戰管制，以確保戰役部隊通聯順暢。另外，回顧中共解放軍網路戰略目標。根據中共2002年《信息作戰學》表示：針對戰役所需的網路偵察、攻擊和防禦，應考量目標、力量、行動、時間及網路空間等五個要素實施調整。同時密切協調各軍、兵作戰所需，以達成資訊作戰目標。[52]另外，2007《信息化戰爭論》更指出：隨著網路科技運用，未來的戰場將是陸、海、空、天、網、電一體的立體戰爭，應強化網、電偵察與反偵察、干擾與反干擾，以強化戰略威懾能力。[53]不僅如此，2010年《信息戰爭：第四空間的角逐和博奕》更指出，網路戰為利用電腦網路系統獲取敵方情報，破壞敵方資訊系統，獲取我方所需的軍事和情報能力。同時透由控制資訊的傳播，以獲取戰爭的主動權。[54]因此，中共解放軍遂行聯合戰役時，「戰略支援部隊」將編組「資訊作戰群」配屬聯合戰役部隊，以獲取網路空間相對優勢，置重點於敵軍事指管與通資系統的癱瘓。同時，協助戰役部隊獲取太空與網路空間所建

---

[48] National Intelligence, “Worldwide Threat Assessment of the Us Intelligence Community,” Senate Select Committee on Intelligence, 2016, pp.2-3.

[49] 陳森，〈廓清網路安全殘缺認知，務實推進網路國防建設〉《現代軍事》，480 期，中國國防科技信息中心，2017 年 1 月，頁 48-49。

[50] Office of the Secretary of Defense, “Military and Security Developments Involving the People’s Republic of China 2017,” May 15,2017, pp58-59.

[51] 〈慶祝中國人民解放軍建軍 90 周年閱兵解說詞〉《解放軍報》(北京)，2017 年 8 月 1 日，版 3。

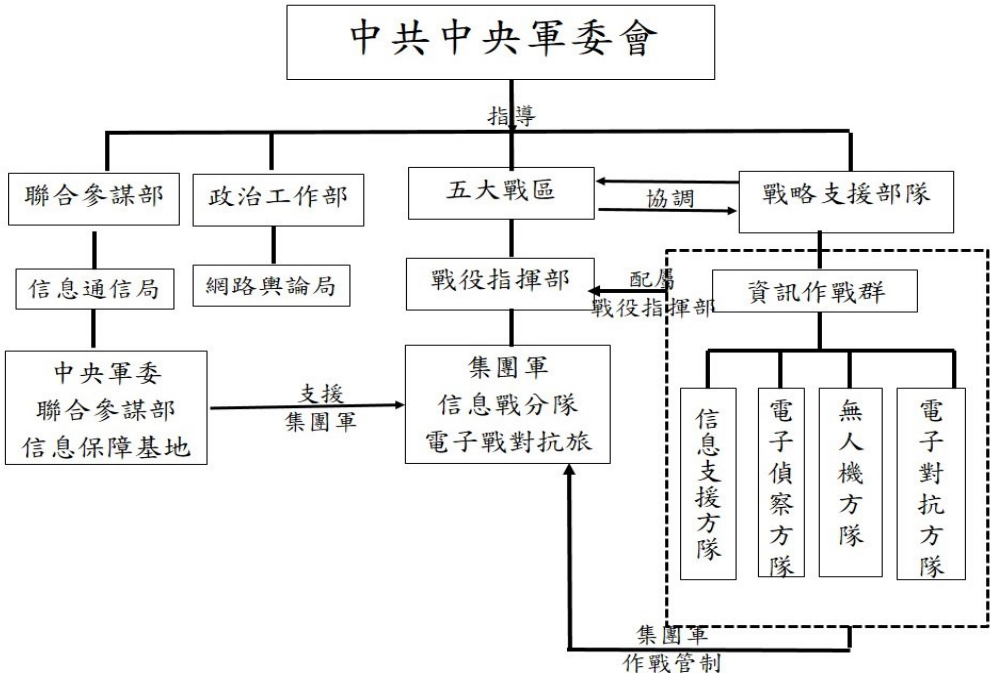
[52] 徐小岩、許金裕，《信息作戰學》(北京:解放軍出版社，2002 年) ，頁 258-266。

[53] 蔡仁照，《信息化戰爭論》(北京:國防大學出版社，2007)，頁 303-305。

[54] 陳寶國，《信息戰爭:第四空間的角逐和博奕》(北京:中國發展出版社，2010 年)，頁 350-351。

構出的通聯系統。此外，依戰況需求擇派任務分隊，受集團軍作戰管制(如圖三)

圖三 中共解放軍戰時遂行網路空間作戰指揮與管制圖



資料來源：參考自〈慶祝中國人民解放軍建軍 90 周年閱兵解說詞〉《解放軍報》，2017 年 8 月 1 日，版 3；徐小岩、許金裕，《信息作戰學》(北京：解放軍出版社，2002 年) ，頁 258-266；蔡仁照，《信息化戰爭論》，(北京：國防大學出版社，2007)，頁 303-305；陳寶國，《信息戰爭：第四空間的角逐和博奕》(北京：中國發展出版社：2010)，頁 350-351。

二、特、弱點

中共網路作戰部隊能力組織變革後，對其作戰能力必然產生特、弱點：

(一)特點

1. 提升網路空間整體戰力

因應未來多領域的作戰空間型態的轉變，要提升作戰效能就須集中指揮。根據 2016 年美國科斯特洛(John Costello)指出：中共網路作戰部隊的建軍構想，為實現平、戰結合及網路偵察、防禦一體化所做的調整。[55]另據 2017 年美國《資訊作戰：薩德系統將遭受到駭客攻擊(Information Warfare:Thaad the Hack Attack Magnet)》指出：中共解放軍的網路作戰部隊來自軍事資助的大學相關科系和民間網路高手，已直接提升中共網路戰能力；其網路空間攻擊方面，已對美軍進駐韓國的 THAAD 防空系統造成極大的威脅。[56]事實上，中共網路戰力早已是不容忽視。根據 2014 年美國《資訊作戰：網路戰主要大國(Information Warfare: Major Cyber War Powers)》曾揭露出：中共網路

[55] 註 24。

[56] "Information Warfare: Thaad the Hack Attack Magnet," Strategy Page, https://www.strategypage.com/htmw/htiw/articles/20170611.aspx, 2017/10/5.

戰能力已成為美國最大的威脅者之一;其中,中共網路攻擊目標已入侵澳洲情報機構、印度政府網路部門及美國民間企業。[57]故在中共網路作戰部隊移調至戰略支援部隊後,其網路戰略將調整為「平戰結合、偵防合一」,將有助於網路空間攻擊能力的提升;其網路攻擊目標,也從入侵政府部門及民間網路擴及至美國軍方網路系統。

2. 強化聯合作戰效能

未來聯合作戰成敗關鍵,在於聯合資訊作戰環境能否提供安全、可靠的通資系統。根據 2016 美國學者費爾(Phillip C.)表示:網路作戰部隊可提高中共解放軍遂行聯合作戰的能力。[58]同年底,印度夏爾馬少將亦表示:該部隊於戰爭期間,可提供參戰單位網路和情報需求。同時,更有助於強化解放軍的海、空軍兵力投射。[59]此外,2017 年法比(Michael Fabey)更指出:中共解放軍為強化聯合作戰網路空間作戰效能,已針對新型態的作戰構想「綜合網路電子戰(Integrated Network Electronic Warfare, INEW)」加強準備;其作戰手段將運用電子戰和網路戰,對敵國發起電子戰與網路攻擊。同時運用網路攻擊隔離敵人,以彌補空中距離無法保護的作戰空間。[60]由上述網路戰能力,透露出中共的網路作戰部隊,將可提供戰役部隊所需指揮鏈路需求。同時,運用網電一體化作戰,以削弱敵國軍事資電作戰優勢,進而確保其軍事行動自由。

3. 提升戰略嚇阻能力

戰略嚇阻即為預防衝突,使敵人相信遭反擊後的下場,將不符合攻擊成本,迫使敵人不輕易動武。根據 2016 年 8 月 29 日中共軍委主席習近平視察「戰略支援部隊」時指出:「戰略支援部隊」為新型作戰力量,全面提高威懾和實戰能力。[61]同年,美國蘭德公司所作的研究報告指出:未來美、中兩國若發生戰爭,中共解放軍反制作為,其中一項作戰手段即可能為運用網路攻擊,以癱瘓、破壞美軍 C4ISR 系統。[62]此外,根據 2017 年美國官方出版的《網路嚇阻行動任務》報告指出:中共網路攻擊能力已有顯著增加,已使美國的網路、通訊等關鍵基礎設施處於危險之中。[63]同年,美國學者艾利森研究亦指出:中共解放軍網路作戰部隊將運用虛擬網路空間中的代理伺服器,

---

[57] "Information Warfare: Major Cyber War Powers," Strategy Page, https://www.strategypage.com/htmw/htiw/20140313.aspx, (March 13, 2014), 2017/10/15.

[58] Phillip C. Saunders and Joel Wuthnow,黃文啟譯,〈中共軍事組織變革〉《國防譯粹》(臺北),第 43 卷第 10 期,國防部政務辦公室,2016 年 10 月,頁 34-35。

[59] Major General BK Sharma, Brigadier Sandeep Jain & Dr Roshan Khanijo, "Analysis of China's Military Reorganisation," United Service Institution of India (USI), January 12,2016, pp2-8.

[60] Michael Fabey, "China Looks to Wage "Hybrid" Electronic War," Center for Strategic and Budgetary Assessments, http://csbaonline.org/about/news/china-looks-to-wage-hybrid-electronic-war, (February 15, 2017), 2017/10/15.

[61] 王士彬、安普忠、鄒維榮,〈習近平在視察戰略支援部隊機關時強調擔負歷史重任 瞄準世界一流 勇於創新超越努力建設一支強大的現代化戰略支援部隊〉《解放軍報》(北京),2016 月 8 月 30 日,版 1。

[62] 黃文啓譯,〈美「中」大戰分析聚焦作戰準備及軍事交流、整備(上)〉《青年日報》(臺北),2016 年 9 月 20 日,版 7。

[63] Department of Defense Science Board , "Task Force On Cyber Deterrence," (Washington, DC：Office of The Secretary of Defense Pentagon, February, 2017), pp.4-6.

偽裝網路攻擊來源使美國誤判情勢。同時，中共網路戰的能力已可以暫時削弱美國的反擊能力。[64]不僅如此，2018 年 6 月 13 日美國國家情報總監柯茨(Dan Coats)更表示，美國聯邦、州和地方政府等網路關鍵基礎設施，遭受嚴重損害的風險正逐漸擴大，其威脅來源國家之一，為中共網路作戰部隊。[65]因此，中共網路作戰部隊具有癱瘓敵國網路關鍵基礎設施後，已直接提升網路戰略嚇阻能力。

(二)弱點

1. 通資系統整合雙頭馬車

要確保聯合作戰，各載具、作戰部隊與指揮所須能相互構連。2016 年 1 月 1 日，中共國防部新聞發言人楊宇軍表示，「戰略支援部隊」成立，有利於優化軍事力量結構，提高綜合保障能力。[66]然就，2017 年卡尼亞研究表示：由於「戰略支援部隊」負責網路空間的建設。同時新任中央軍委聯合參謀部「信息通報局」亦要承擔起主要責任。在雙頭馬車帶領下，中共解放軍 C^{4}ISR 的發展將仍然面臨著的挑戰。[67]另外值得注意的是，2015 年 6 月達姆(John M.Dahm)曾提及：為確保美國聯合資訊環境的通連，美國防資訊系統局須對國防部通信負有全面性的責任。同時，還須負有管理網路標準，確保整體網路數據流通及商業衛星通信等服務。[68]因此，部門分散所造成影響，將會影響到未來中國解放軍聯合作戰互連互通的整合能力。

2. 網路人才欠缺

沒有網路人才就沒有網路科技發展，更沒有網路安全。根據 2017 年上半年《互聯網安全報告》指出，「中國大陸大學教育培養的資訊安全專業人才僅 3 萬餘人，而網路安全人才總需求量則超過 70 萬人(缺口高達 95%)。另當前中國重要行業資訊系統和資訊基礎設施需要各類網路資訊安全人才，將以每年 1.5 萬人的速度增加，到 2020 年相關人才需求將增長到 140 萬。但目前中國只有 126 所大學設立 143 個網路安全相關科系，僅占 1200 所理工院校的 10%。」[69]事實上，這個問題不是出現在中共解放軍，由於網路安全已影響到國家政治、經濟、軍事等領域，網路人才已成為政府與民間相互爭搶的對象。根據 2016 湯瑪斯(Ferdinand H. Thomas)指出，美國民間企業亦非常欠缺網路科技專業人員，均願意提供比軍中薪餉高三倍的優渥薪資，以做為吸引軍中優

---

[64] Graham Allison, “How America and China Could Stumble to war,” National Interest, http://nationalinterest.org/feature/how-america-china-could-stumble-war-20150, (April 12, 2017), 2017/10/15.

[65] 〈毀滅性網攻 柯茨警告已亮紅燈〉《青年日報》(臺北)，2018 年 6 月 15 日，版 6。

[66] 呂德勝，〈詳解深化國防和軍隊改革有關問題〉《解放軍報》(北京)，2016 年 1 月 2 日，版 3。

[67] Elsa Kania, “PLA Strategic Support Force: The 'Information Umbrella' for China's Military,” The Diplomat,” https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/, (April 01, 2017).

[68] John M.Dahm，劉慶順譯，〈美軍「聯合資訊環境」的挑戰與未來(Next Exit:Joint Information Environment) 〉《國防譯訊》(臺北)，國防部政務辦公室，第 43 卷第 2 期，2016 年 2 月，頁 20。

[69] 騰訊安全聯合實驗室，〈2017 年上半年互聯網安全报告〉，2017 年 8 月 8 日，頁 11-12。

秀高科技人員到其公司服務。[70]因此，網路人才不足對網路作戰部隊的戰力，造成很大的影響。

總體而言，中共「戰略支援部隊」之網路作戰部隊成立後，將有助於其網路空間作戰能力的提升。同時，納入戰役部隊作戰管制後，可確保其聯合作戰通聯暢通。此外，網路戰力提升後，將助嚇阻它國不輕易發動網路空間，以維護其網路安全、利益與主權，中共網路部隊軍改前、後比較表，如表一。

表一 中共網路作戰部隊軍改前、後比較表

區分 項目	軍改前網路部隊	軍改後戰略支援部隊 (網路作戰部隊)
戰略構想	一、平時：運用網路部隊，竊取敵重要機密資訊，提升軍事整體實力，如竊取 F-35。 二、戰時：運用網路戰力，癱瘓敵國網路、資訊等關鍵基礎設施，擾亂敵國軍事指揮與管制，阻止它國增援時效，開創聯合作戰有利態勢。	一、平時：利用網路部隊及利用民營通信、網路營運商，掌握它國重要人物情報及輿論，以利後續戰爭面的掌握。 二、戰時：運用網路部隊與電子戰部隊，癱瘓敵國網路空間，使它國無法接收正確資訊，獲取網路空間制高點優勢，提升聯合作戰效益。
戰略目標	一、網路、資訊等關鍵基礎設施。 二、敵軍事指揮管制通資系統。	一、網路、資訊等關鍵基礎設施。 二、敵軍事指揮管制通資系統。 三、敵重要人物情資及輿論。
組織	各軍區配屬一個網路部隊。	一、編制部隊：原網路部隊、原總政聯絡部及某大隊「模擬室」(研究機構)。 二、非編制部隊：華為、中興等通信民營公司、網路駭客組織，及中國科技大學、上海交通大學、西安交通大學、北京理工大學、南京大學、哈爾濱工業大學等 6 所大學。
指揮關係	直屬原總參謀部(三局)。	統歸中央軍委指揮。
戰役執行	由軍區內的網路部隊配屬該軍區戰役部隊執行。同時，協助戰役部隊之通信部隊建構網路安全防護。	戰略支援部隊成立資訊作戰群(信息支援方隊、電子偵察方隊、電子對抗方隊及無人機方隊)受戰區編成的聯合戰役部隊作戰管制。同時，依戰役部隊向敵發起聯合網電攻擊。

[70] Ferdinand H.Thomas，楊黎中譯，〈美陸軍網路部隊人才留用(Retaining Soldiers on a New Battlefield:An Army Plugged into Cyber Needs Talented Specialists)〉《國防譯粹》(臺北)，第 43 卷第 2 期，國防部政務辦公室，2016 年 2 月，頁 59。

作戰效益	網路作戰能力	提供網路情報，並有能力對它國實施局部網路、通訊等關鍵基礎設施的癱瘓。	網電一體聯合作戰。除可提供以往網路情報、攻擊能力外，在網路部隊、電子部隊整合，可強化網路空間安全。同時，對敵加強網路、電子及心理攻擊。
	支援聯合作戰	獲取資電作戰優勢，支援聯合作戰。	透過與太空部隊、電子部隊的橫向協調，確保其聯合作戰之網路空間通聯暢通。同時，加強軍事資料庫整合，與協助戰役部隊建構聯合作戰通資安全環境。
	戰略嚇阻	利用網路長城防火牆，監控、掌握它國網路攻擊態樣。同時，具有網路戰反擊能力，以癱瘓它國網路、資訊等關鍵基礎設施，以嚇阻它國使用網路攻擊。	除具備網路部隊任務外，凡針對它國對中國大陸國家境內，如網路接收器、無線電移動裝備實施干擾，即視為侵犯其網路主權。中共解放軍即可形塑師出有名的網路戰反擊，獲國際認同。

資料來源：作者整理。

中共網路作戰部隊對我陸軍通資安全防禦威脅評估及策進作為

搶佔網路空間制高點，已成為中共解放軍未來攻臺戰役中首要奪取的戰略目標。故檢視敵網路作戰部隊對我陸軍通資安全防禦之威脅，有利策進因應之道。

一、威脅評估

(一) 我陸軍指管通資系統面臨高風險的威脅

中共戰略支援部隊戰時將納編網路作戰部隊、電子偵蒐、干擾部隊與無人機部隊編成為「資訊作戰群」。未來臺海戰役中，任何無線電訊號源將成為中共「資訊作戰群」優先攻擊目標的首選。根據 2016 年我國《國家政策研究基金會》研究員揭仲指出：隨著中共解放軍網路作戰能量提升，運用網路、電子信號情報，將可嚴密監控第一島鏈以西之海、空域等情資能力。同時透過衛星導引對我國重要目標實施精準打擊。[71]另外，2017 年 9 月 26 日美國總參謀長(Chief of Staff Gen)Mark Milley 出席「武裝部隊空中和地面小組委員會(House Armed Services Air and Land Subcommittee)」聽證會更表示：美陸軍 WIN-T 通資系統計畫必須停止；其主要原因為面對中共解放軍的現代化，該系統太容易受到電子戰干擾和網路駭客攻擊而癱瘓。[72]不僅如此，2018 年 6 月中共網路部隊已在上海、北京完成史上最大規模的擴編。同時，該部隊配備了最新的硬體和軟體等網路作戰裝備，其作戰能力已可掌握全球特定目標，對敵實施從 Gbps 到高

[71] 揭仲，〈中共推動軍事變革對臺灣之影響〉《中共研究》，第 50 卷第 4 期，中共研究雜誌社，2016 年 7 月，頁 152。

[72] Colin Clark and Sydney J. Freedber JR., “Army Plans To Halt WIN-T Buy; Shuffle Network $$,” Breaking Defense, https://breakingdefense.com/2017/09/army-plans-to-halt-win-t-buy-shuffle-network/, September 27, 2017.

達 Tbps 高頻率「分散式阻斷式服務攻擊(Distributed Denial of Service, DDoS)」，其效益將使敵國網站全面癱瘓。[73]因此，中共網路作戰部隊併入戰略支援部隊後，將使原建制不同部門的網路部隊與電子戰部隊整併為「資訊作戰群」後，其網路空間作戰能力將對我陸軍網路、通信等系統產生極大威脅。不僅如此，我陸軍通資備援系統的陸區系統將面臨更大的威脅，由於該系統鈍重性及天線網極易成為電子戰及太空偵照目標，到戰時存活率將非常低。換句話說，未來台海戰役中，我陸軍的固定資訊機房及具有無線電信號源的高山站台，或備援指管通資系統，將受到更為嚴重的威脅。

(二)網路宣傳戰、心理戰，將衝擊我陸軍部隊精神戰力

不戰而屈人之兵，善之善者也。隨著網路空間的擴大，網路平民已成為網路攻擊目標的首選。根據 2015 年美國國防部公布《中共軍力報告》指出，中共解放軍在未來攻臺戰役手段之一，即透由網路部隊對臺發動網路戰攻擊；其攻擊目標為癱瘓我國政治、軍事與經濟基礎建設，進而引發臺灣執政當局恐慌。[74]另2017年美國格茨(Bill Gertz)亦表示：一項名為 2020 年中共解放軍攻臺秘密軍事計劃中，其中一項重要手段為中共解放軍利用網路平台之社群媒體，如臉書，對我國民眾進行心理戰，以削弱降低島上的戰鬥力。同時，大量使用網際網路傳播媒體，對我國民眾宣傳戰爭的代價，以侵蝕、分裂我國抵抗的意志。[75]此外，2018 年任職於我國中正大學的助理教授林穎佑更表示：中共解放軍未來攻臺戰役，可能運用網路媒體發佈錯誤消息，如傾中的政府接管軍隊，取代了現任政府。這個聲明無論合法性如何，都可能造成相當大的動盪，甚至會降低軍隊的戰鬥意志。[76]因此，在我國資訊基礎設施普及國軍募兵體制朝向「精簡常備、廣儲後備」發展下，中共網路作戰部隊於平時運用網路空間，掌握、分析我陸軍後備軍人在臉書的言論。戰爭開始前，極可能發佈假新聞、誤導動員報告時間、地點，進而影響我陸軍「編實動員、擴充動員、戰耗梯隊」。同時，併運用臉書的靠北長官社群發佈假新聞，煽動現役或備役對政府不滿言論，造成國軍官兵內部團結失衡，進而喪失抵抗意志。簡言之，運用網路散佈假新聞，將對我陸軍部隊的精神意志產生衝擊，進而影響我陸軍捍衛國土的決心。

二、策進作為

面對中共網路作戰型態的改變及網路戰力的提升，其攻擊目標已從網路竊取、中斷，轉變為同步運用網路戰及電子戰癱瘓敵國網路機房及無線電信號源等指管通資系

[73] 郭曉蓓，〈中共擴編網路部隊 試圖癱瘓特定網站〉《青年日報》(臺北)，2018 年 7 月 6 日，版 7。
[74] 王光磊，〈美公布中共軍力報告 聚焦臺海戰力部署〉《青年日報》(臺北)，2015 年 5 月 10 日，版 4。
[75] Bill Gertz, “China’s Secret Military Plan: Invade Taiwan by 2020,” Washington Free Beacon, http://freebeacon.com/national-security/chinas-secret-military-plan-invade-taiwan-2020/, 2017/10/20.
[76] Ying Yu Lin, “China’s Hybrid Warfare and Taiwan,” The Diplomat, https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/, January 13, 2018, 2018/2/14.

統。基此，我陸軍通資安全防禦應著重於強化軍民網路安全合作機制及建構 AI 人工智慧網路安全防護等，以確保指管通資系統暢通。

(一)提升軍民網路安全合作機制，採購抗干擾、機動性強的通資系統

網路安全不能有軍種本位主義。同時，網路安全環境須建構在聯合資訊安全環境中，透過產、官、學界合作以建構有效的防禦網路。「外防突襲」的網路攻擊，關鍵要素在於網路節點的安全防護。然而，隨著 2017 年 7 月我陸軍各作戰區資電群，外(離)島通資連移編至新成立的資通電軍指揮部後，我陸軍通資安全防護人力與預算均面臨不足的問題。事實上，我陸軍為彌補光纖覆蓋率不足，運用民營通信，如中華電信軍租網路，提供單位語音、數據等服務已行之有年。基此，我陸軍網路節點防護方面，應建構於軍、公、民營通資系統的基礎，並集中預算資源，以升級現行網管裝備及作業電腦。同時，針對資訊機房、光纖網路維護權責，建議國防部整合陸、海、空軍等網路安全需求，並納入國家整體聯合網路安全環境，以期建立共同標準、中央管控機制。另外，要搶佔網路空間的制高點，網路人才便是關鍵，故我陸軍應推動各聯兵旅與地區大學建教合作，針對網路科系或具有理工背景職校，優先納入我陸軍通資部隊召募對象，以提升我陸軍資電整體戰力。

不可諱言，我陸軍為強化內部網路安全防禦，近年來已在各營區安裝「營區資訊安全管理系統(BNS)」，透由 ARP 監控軟體可 24 小時監控營區內部任何一部電腦 IP 位置，有效防範內部網路攻擊。然此缺點為固定網段一旦遭敵掌握後，其部隊位置也隨之曝光。基此，網路空間的機房、訊號節點隱真示假，是提高戰時存活率的不二法門，故應建請國防部核予我陸軍備用頻率及網段，俾利我陸軍各作戰區(防衛部)，通過預置虛擬網路和假中心節點，並結合固定、機動和隱蔽部署，以反制敵人平時偵蒐、干擾。戰時，誤導敵國對假目標進行攻擊。另外，我陸軍應落實資料庫虛擬化，通過多重備份，確保戰時指揮體系能夠快速恢復。除此之外，隨著網路空間作戰型態是虛擬與實體攻擊的結合，面對中共解放軍網路作戰部隊的威脅，我陸軍應向國防部爭取預算，採構具有抗干擾、防網路攻擊、機動力強的通資系統裝備，以符合未來作戰實需。

(二)建構 AI 人工智慧網路安全防護，強化網路攻防課目演練

網路安全不能建構於被動防禦，惟有降低人為因素才能確保網路安全。隨著網際網路的社群媒體，如臉書、Line，已成為國人日常生活的工具。然而，自由的網路空間，其個人資訊的隱私、言論，也提供了有心人士，掌握其個人動態最好的平台。雖然，我陸軍要求所屬官、士、兵，進入營區之智慧型手機均不可為中國大陸製，且須安裝 MDM 管制軟體以防範非法入侵。但隨著網路戰爭型態的改變，網路社群媒體已成為中共網路作戰部隊平時偵蒐的對象。因此，我陸軍應建議國防部將人工智慧系統(AI)納入採購，透過電腦機器人的觀察、定位，及時監控假消息的傳播，以嚇阻敵國

實施網路宣傳戰、心理戰。

除此之外，要落實官兵網路安全教育，透過法制教育要求官兵網際網路言論行為。同時，持恆推展政治作戰文宣工作，以強化官兵抗敵意志。另方面，網路攻防戰除持續納入兵推課題演練外，我陸軍應積極向國防部爭取至國外參訓員額，如陸威專案時建議比照南韓與美國實施網路風暴演習(Cyber Storm)，參加跨國網路演習或以觀察員實習，以提升我陸軍網路空間整體戰力。

結論

因應網路空間日益威脅嚴重，美、俄等軍事強國均積極強化網路部隊建軍。同時，研發網路病毒及高科技的反衛星手段無非是希望搶佔網路空間的制高點。同理，中共解放軍之網路作戰部隊的成立，亦是要奪取網路空間的制高點，以強化其聯合作戰效能。該部隊成軍後將直屬中共中央軍委指揮，網路戰略從原被動防禦，轉向為「平戰結合、偵防一體」主動防禦。新編成網路作戰部隊，將可提升網路空間整體戰力，進而增加戰略嚇阻能力。同時，強化聯合作戰效能。但令人驚訝的是，美、俄等國為強化軍事作戰能力，依太空及網路空間，分別建構太空司令部與網路司令部。然而，中共解放軍竟將其整合為一。此舉組織改革，勢必也帶動其網路作戰方式的改變。因此，面對一個不斷強大的中共解放軍，無論編制上、作戰思維有所改變之網路作戰部隊，我陸軍須提升軍民網路安全合作機制，採購抗干擾、機動性強的通資系統；建構 AI 人工智能網路安全防護，強化網路攻防課目演練，俾利我陸軍遂行國土防衛任務。

參考文獻

一、 徐小岩、許金裕，《信息作戰學》(北京：解放軍出版社，2002 年)。
二、 陳寶國，《信息戰爭：第四空間的角逐和博奕》(北京：中國發展出版社，2010 年)。
三、 蔡仁照，《信息化戰爭論》(北京：國防大學出版社，2007 年)。
四、 黃藝，《網路空間安全戰略研究》(北京：國防大學出版社，2013 年 3 月)。
五、 惠志斌，《全球網路空間信息安全戰略研究》(上海：上海世界圖書出版公司，2015 年 4 月)。
六、 《國防部業務報告》，立法院第 9 屆第 4 期，2017 年 10 月 11 日。
七、 趙秋梧，〈論網路空間戰爭的特徵及其本質〉《南京政治學院學報》，第 31 卷第 2 期，2015 年 2 月。
八、 遠方，〈網路空間的戰爭脆弱性〉《中國資訊安全》，第 5 期，中國資訊安全測評中心，2014 年 5 月。
九、 黃基禎、陳瑞龍〈共軍軍事組織變革戰略意涵之解析〉《中共研究》，第 50 卷第 4

期，中共研究雜誌社，2016 年 7 月。
十、 揭仲，〈中共推動軍事變革對臺灣之影響〉《中共研究》，第 50 卷第 4 期，中共研究雜誌社，2016 年 7 月。
十一、 Larry K.Wentz 主編，李健、嚴美譯，《網路戰-美軍稱霸全球的第五戰場》(香港：新點出版公司，2010 年 12 月)。
十二、 Wayne W and Grigsby Jr, 梁正綱譯，〈網路電磁作業：統合地面作戰之致勝關鍵(CEMA:A Key to Success in Unified Land Operations) 〉《國防譯粹》(臺北)，第 40 卷第 2 期，國防部政務辦公室，2013 年 2 月。
十三、 US DOD，余忠勇譯，〈2014 年中共軍事安全發展(Military And Security Developments Involving The People's Republic of China 2014)〉《國防譯粹》(臺北)，第 42 卷第 5 期，國防部政務辦公室，2015 年 5 月。
十四、 Larry M.Wortzel，章昌文譯，〈評論中共軍事現代化及其網路活動〉《國防譯粹》(臺北)，第 41 卷第 10 期，國防部政務辦公室，2014 年 10 月。
十五、 Phillip C. Saunders and Joel Wuthnow，黃文啟譯，〈中共軍事組織變革〉《國防譯粹》(臺北)，第 43 卷第 10 期，國防部政務辦公室，2016 年 10 月。
十六、 Office of the Secretary of Defense," Military and Security Developments Involving the People's Republic of China 2017," May 15, 2017.
十七、 Todd Harrison, Zack Cooper, Kaitlyn Johnson, and Thomas G. Roberts, Escalation and Deterrence in The Second Space Age(Center for Strategic and International Studies), October 2017.
十八、 Elsa Kania, "China's Strategic Support Force: A Force for Innovation?," The Diplomat, https://thediplomat.com/2017/02/chinas-strategic-support-force-a-force-for-innovation/, (February 18, 2017), 2017/10/15.
十九、 Department of Defense Science Board, Task Force On Cyber Deterrence (Washington, DC:Office Of The Secretary Of Defense Pentagon, February, 2017).

作者簡介

王清安上校，中正理工學院 88 年班、英儲班 91 年班、陸軍通信電子資訊學校通資電正規班 96 年班、國防大學陸軍學院 98 年班、戰爭學院暨戰略與國際事院研究所 107 年班，曾任排長、連長、營長、參謀主任、通資組長，現任陸軍通信電子資訊訓練中心學員生總隊部總隊長。