中共網路戰攻擊手段與能力之研析

作者簡介

王清安中校，中正理工88年班、通資電正規班175期、陸院98年班、戰院暨戰研所107年班；曾任排長、連長、營長、群參謀主任，現任馬防部通資組長。

提　要

一、網路攻擊能力，已成為衡量國家網路戰實力綜合象徵。2017年，美國評估中共網路攻擊能力，已具有癱瘓美國國家境內部分電網能力，此舉意味著中共網路攻擊能力，已從竊取它國數據資料的網路大國，走向具有研發電腦病毒能力的網路強國。

二、本文研究發現，隨著中共網路科技的進步，其網路攻擊手段，已從阻斷式服務攻擊(DDos)拒止他國網路正常使用，到運用先進持續攻擊手段(APT)操控它國輿情，已對我國家安全產生嚴重威脅。

三、因應中共網路攻擊型態的改變，國軍應擴編電腦緊急應變小組、擴大網路人才徵選範圍及採購新型網路偵察裝備，以提升國軍資通安全防護能力。

關鍵字：網路攻擊、網路戰、病毒、網路駭客

前　言

隨著網路科技的發達，網路攻擊的對象已從平時竊取他國重要軍事、商業機密；戰時癱瘓敵國軍事指管通資系統及國家關鍵網路基礎設施，發展為平、戰時合一，利用網路大數據資料庫，掌握敵國重要網路輿情資訊，進而顛覆他國政權，達到不戰而屈人之兵的作戰模式。根據2018年美國約翰霍普金斯大學國際研究學院的教授Seth G.Jones研究表示：考量傳統和核戰爭可能的成本和風險，未來戰爭將朝向政治戰爭發展，其手段運用將包括軍事、外交、經濟，及公共廣播和心理戰等，以實現國家利益目標。如俄羅斯利用攻擊性網路計畫，隱蔽其軍事行動。同時，再利用歐洲和跨大西洋的裂縫，支持民粹主義運動，破壞歐盟和北約的凝聚力。[1]此外，《2018年全球風險報告(The Global Risks Report 2018 13th Edition)》更指出，攻擊性網路能力，所造成不確定性的錯誤評估，將可能觸發1個報復性回應，如國家關鍵基礎設施系統受到網路攻擊，導致中斷基本服務，其結果可能將引發連鎖反應，造成擴大衝突。[2]由網路攻擊型態的改變，凸顯出網路攻擊已威脅到國家安全與利益。換句話說，無法掌握網路攻擊的作戰型態，極可能會因誤判情勢導致國際衝突，甚至發生相互攻擊的網路戰爭。

然而，我國網路安全正面臨中共強大的威脅。根據2018年4月5日我國《自由時報》披露，2017年我國公部門遭網路攻擊成功案例共計360件；其中高達八成的網路攻擊來自中共網路部隊。另外，我國資安處長簡宏偉更表示，2016～2017年，中共網路部隊攻擊臺灣公部門的次數雖然降低，但攻擊成功率卻是提高。[3]不僅如此，中共網路攻擊能力更是日益增加，根據2017年美國防部出版的《網路嚇阻的任務力量(Task Force On Cyber Deterrence)》指出，中共網路戰能力已對美國的網路、資訊等關鍵基礎設施產生威脅，其影響已衝擊到美國的重要利益及軍事反應能力。同時，中共網路戰還具有利用網路社群媒體，破壞美國政治體制(如選舉)和社會凝聚力。[4]在我國軍、民網路設備及作業軟

1　Seth G.Jones, "The Return of Political Warfare," Center for Strategic and International Studies, February 2018,pp.3-4,https://www.csis.org/analysis/return-political-warfare,檢索日期2018年6月16日。

2　The World Economic Forum, "The Global Risks Report 2018 13th Edition," pp.33,http://www3.weforum.org/docs/WEF_GRR18_Report.pdf,檢索日期2018年6月16日。

3　李欣芳，〈中國網軍強攻我公部門〉《自由時報》(臺北)，2018年4月5日，版1。

4　Department of Defense Science Board, Task Force On Cyber Deterrence(WASHINGTON, DC：Office of The Secretary of Defense Pentagon, February, 2017),pp.4-9.

體長期依賴美國的同時，探討中共網路攻擊能力更顯重要。基此，本文首先瞭解網路攻擊的定義。其次，探討中共網路攻擊的戰略構想及網路攻擊手段。第三，評估中共網路攻擊能力。最後，提出策進之道，以強化國軍資電防護能力。

網路攻擊定義

網路攻擊能力來自網路科技發展及網路部隊執行能力。

一、美方

網路攻擊，即為削弱、摧毀敵國網路防禦的能力。根據2013年曾任美國網路司令部副局長Danelle Barrett少將等3人研究表示，網路攻擊為網路部隊透過電腦與網路所採取的攻擊行動，其目的以干擾、拒止、削弱或摧毀敵國電腦軟、硬體及電腦中的數據資料。[5]另外，2014年美國防部所出版的JP3-12《網路空間作戰聯合準則(Joint Publication 3-12(R), Cyberspace Operations)》更指出，網路攻擊依攻擊目的區分為拒止(Deny)及操控(Manipulate)。拒止為造成敵國暫時或永久性無法正常使用網路系統，其拒止還可以依照敵國使用網路系統程度，區分為降級(Degrade)、中斷(Disrupt)和摧毀(Destroy)3種類型。另外，操縱(Manipulate)為控制或改變對方的數據資訊及網路系統，以擾亂敵國指揮系統產生錯誤決策。[6]因此，網路攻擊為運用網路攻擊技術，使敵方無法正常使用資訊系統，進而操控敵國電腦數據資料，使其決策錯誤。

二、中共

網路攻擊為通過使用網路命令或軟體，非法進入當地或遠程用戶主機系統，獲取、修改、刪除用戶系統的資訊，其後果使敵方網路系統服務被拒絕，簡稱為服務拒絕；同時使敵方網路資訊為我所用，稱為資訊竊取。[7]另外，根據2001年中共《戰役信息作戰指揮研究》指出，利用軍、民網路戰力，對敵網路實施多種攻擊，其手段為運用網路病毒、精準武器打擊及高能電磁脈衝攻擊等手段，對敵網路進行攻擊，並且利用網路駭客入侵他國數據資料庫竊取、修改和控制指揮和武器系統。[8]故中共網路攻擊的定義，為利用軟、硬殺手段，以阻止敵國正常使用網路資

5 Nancy brown, Danelle Barrett, and Jesse Castillo，〈訓練官兵網路戰力(Creating cyber warriors)〉，《國防譯粹》，第40卷第4期，國防部政務辦公室，2013年4月，頁49。

6 U.S.Joint Chiefs of Staff, "Joint Publication 3-12(R)Cyberspace Operations,"(Washington, D.C.2013), pp.II-5,http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf,檢索日期2018年6月8日。

7 徐小岩，《信息作戰學》(北京：解放軍出版社，2002年，頁47。

8 楊根源，《戰役信息作戰指揮研究》(北京：國防大學出版社)，2001年，頁23。

訊，透過網路駭客竊取他國數據資料庫，以供我方使用。

總而言之，美、中兩國對網路攻擊的定義，相同點在於運用網路攻擊，以拒止、操控它國網路系統，使其數據或網路系統無法正常使用，藉由破壞設備，以達暫時或永久的影響；同時，操控網路數據以影響指揮官決策判斷。不同點在於，中共網路攻擊的資訊竊取，與美國的操控敵國數據資料有所不同，中共側重於掌握敵國數據資料，而美國則強調改變或控制他國數據資料(如表1)。

中共網路戰攻擊之戰略目的與手段探討

隨著網路空間為第五個作戰空間，網路攻擊的作戰效益已可提升軍事實力，其網路攻擊戰略目的為發揮網路戰不對稱作戰優勢，進而削弱敵國戰力。

一、中共網路攻擊之戰略目的

(一)發揮不對稱作戰優勢

網路空間是繼陸、海、空及太空的第五個戰場。由於網路空間被認為是弱勢國家謀求以小搏大、以弱勝強的絕佳戰場。和平時期，運用網路滲透潛伏他國資訊系統，偵察獲取情報；戰時，針對軍隊作戰基礎設施實施網路攻擊。[9]根據2002年，曾任中共解放軍少將的網路戰專家戴清民表示，沒有一種網路防禦技術上能取得領先，只有新的網路攻擊手段產生後，才能尋求相應的防禦措施。作為資訊技術落後的國家，只有強化網路攻擊能力，才

表1　美國與中共網路攻擊與目的差異對照表

區分／對象	網路攻擊目的	網路攻擊目標
美國	使敵國網路系統無法正常使用(拒止)，如金融、交通、軍事。另外，運用網路病毒，操控它國資訊系統，提供或改變數據資料。	拒止：運用網路駭客，使用分布式拒絕服務攻擊(DDoS)，使敵國網路伺服器被網際網路流量壓制，其系統能力將被降級或被拒絕，或網路中斷服務。 操控：運用電腦病毒，平時入侵敵國資訊系統內部設備，衝突階段或戰時癱瘓敵國系統。
中共	使敵國網路系統無法正常使用，如金融、交通、軍事(服務拒絕)。另外，運用民間網路駭客對敵國實施資訊竊取，以利衝突或戰時，網路部隊發動網路攻擊。	平時，運用網路駭客，針對敵國重要資料庫，實施資料竊取。戰時，利用網路病毒，並用硬殺手段，對敵國關鍵基礎設施實施網路攻擊。

資料來源：作者整理並參考Nancy brown, Danelle Barrett, and Jesse Castillo，〈訓練官兵網路戰力〉(Creating cyber warriors)，《國防譯粹》，第40卷第4期，國防部政務辦公室，2013年4月，頁49; U.S.Joint Chiefs of Staff, Joint Publication 3-12(R), Cyberspace Operations(Washington, D.C.2013), p.II-5。

9　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》(北京)，480期，中國國防科技信息中心，2017年1月，頁48、49。

能威懾他國不輕啟網路戰。[10]此外，根據2016年美國《外交政策委員會(American Foreign Policy council)》所出版的1份報告指出：中共運用網路攻擊目的，對內為穩定其政權合法性；對外利用網路間諜，對美國政府和國防承包商實施網路攻擊，以作為未來美、中兩國發生衝突中，延遲和中斷部署美國戰術指管通資系統，開創中共解放軍戰略態勢。[11]故中共運用網路攻擊，其戰略目的即為創造以弱勝強的絕佳戰場。

(二)建立攻防兼備的網路空間作戰體系

要奪取網路空間制高點，除運用網路攻擊瓦解敵方網路系統外，還須防範敵方對我方實施網路反擊。根據2001年中共《戰役信息作戰指揮研究》指出，網路戰具有攻中有防、防中有攻的作戰特性。一方面，全面防護是確保我方資料、資訊系統和資訊武器裝備不受敵攻擊、摧毀。另一方面，進攻是最好的防禦，綜合運用資訊作戰進攻和防禦力量攻擊敵人，成為保護自己最有效的途徑。[12]此外，建立攻防兼備的網路空間作戰體系，才能實現網路空間利用效果最大化。同時，將網路空間作戰與傳統武力手段結合，才能增強常規作戰力量，實現作戰效果的最大化。[13]不僅如此，根據2013年《中國武裝力量的多樣化運用》指出：要打贏資訊化條件下的局部戰爭，就須搶占網路空間等戰略制高點。[14]因此，建立攻防兼備的網路作戰體系，將有助於中共解放軍提升軍事實力。

二、中共建立網路攻擊手段

影響網路戰場作戰成敗的關鍵在於誰優先掌握網路情報，運用網路攻擊手段，摧毀敵人特定目標及削弱敵作戰能力，故網路攻擊手段為達到戰略目的的重要作為。

(一)蒐集網路情報

要制敵機先，首先須掌握敵國軍事動態。根據2010年James C.Mulvenon研究指出，網路情報蒐集為資訊優勢的基礎，作戰開始前攻擊敵之網路預警系統；戰

10 載清民，《直面信息戰》(北京：國防大學出版社)，2002年，頁60。

11 Richard M.Harrison, "Strategic Primer: Cybersecurity," American Foreign Policy Council, 2016 Spring Volume 2, 檢索日期April 1, 2016,pp.6-7.

12 同註8，頁90～93。

13 張兵城，〈美軍網路空間作戰主要方式與特點〉《國際研究參考》(北京)，第11期，國際研究參考出版社，2017年，頁36。

14 中華人民共和國國務院新聞辦公室，〈中國武裝力量的多樣化運用〉http://www.scio.gov.cn/zfbps/ndhf/2013/Document/1312844/1312844_9.htm。

役開始後，網路戰的主要任務為攻擊敵方的偵察系統進行資訊欺敵，並掩護我方作戰意圖及防護我軍部隊發動攻擊。[15]此外，培養專業化的作戰力量，運用解放軍的網路藍軍，提高對網路意識形態鬥爭訓練，並提升網路空間戰略情報研究中心能量。同時，運用網路民間公司力量，如百度Baidu、阿里巴巴Alibaba、騰訊Tencent等，發揮網路大數據資料蒐集、分析和運用能力和影響力，以提供戰略決策和運行之支撐。[16]故建立軍民網路空間作戰體系，平時透由民間網路公司大數據分析能力掌握敵國輿論及敵國軍事部署；戰時，運用網路攻擊對敵國軍事設施及網路用戶實施攻擊，提升軍事整體作戰效能。

(二)摧毀敵人特定目標

隨著國家基礎建設、金融發展及軍事作戰朝向數位化發展，網路攻擊提供兵不血刃的最佳攻擊途徑。根據2002年中共《信息作戰學》指出，網路攻擊程序為，首先破壞敵指揮控制系統的防火牆實施網路攻擊，癱瘓敵指揮系統。其次，破壞敵方指管數據鏈路，使其難以協調。第三，強占敵網路重要站台，在敵未偵察前關閉站台造成敵網路空間全局或局部混亂。最後，攻擊敵網路通信、電力等基礎設施，使敵國境內的關鍵基礎設施癱瘓。[17]此外，根據2012年曾在美國國防部情報局及戰爭學院發表過網路安全議題的Jeffrey Carr指出，中共解放軍建立攻防兼備的網路攻擊方式，綜合運用軍事、政治、經濟、外交等多種手段，以贏得未來戰爭勝利，其手段包括為物體破壞、電磁頻譜優勢、網路戰及網路心理戰。[18]因此，中共網路攻擊即為運用網路病毒或駭客，以干擾、癱瘓敵國軍、民電腦網路無法正常使用，以支持軍事任務遂行。

(三)削弱敵國作戰能力

網路空間已成為第五個作戰空間，搶占其制高點將有利於嚇阻敵國不輕易發啟網路戰爭。根據2000年中共出版的《IT戰爭》指出，運用網際網路獲得情報

15 James C.Mulvenon, Murray Scot Tanner, Michael S.Chase, David Frelinger, David C.Gompert, Martin C.Libicki, Kevin L.Pollpeter，國防部史政編譯局譯，《中共對美國軍事變革之反應(Chinese Responses to U.S.Military Transformation and Implications for the Department of Defense)》，(臺北：國防部史政編譯局，2010年，頁102。

16 王聖飛、劉明崢，〈網路國防與網路意識形態鬥爭話語權〉《今傳媒》(陝西)，2016年第3期，陝西人民出版社，2016 年3月，頁36。

17 同註7，頁272、273。

18 Jeffrey Carr, Inside Cyber Warfare: Mapping the Cyber Underworld 2nd Edition(USA: O'Reilly Media, 2012年,p.173.

優勢，並破壞敵人資訊系統使其網路攻擊能力減弱，配合威懾性的網路宣傳震撼敵人戰鬥意志，以達成網路嚇阻之戰略目的。[19]另據2009年美國外交軍事研究辦公室(The Foreign Military Studies Office, FMSO)前任分析師Timothy L.Thomas表示，中共網路戰戰略為運用網路嚇阻、封鎖、節點破壞、系統癱瘓等攻勢行為，以獲取網路空間作戰優勢或預防網路攻擊，為劣勢一方掌握戰爭主動權。[20]故運用網路攻擊削弱敵國作戰能力，以達嚇阻敵國不輕易發動戰爭。

總而言之，中共網路攻擊戰略為運用軍、民網路空間作戰體系，於平時利用網路大數據資料庫，掌握敵國輿論動態，以及對敵國實施數據資料竊取。衝突或戰爭發起後，運用網路部隊攻擊敵國伺服器，造成敵國網路系統癱瘓，並對敵國實施網路宣傳與網路戰略威懾；隨後利用軟、硬殺攻擊手段，癱瘓敵國網路空間作戰重心，進而達到敵國指管通資鏈路中斷，引起國家政治、經濟危機(如圖1)。

中共網路攻擊能力評估

網路攻擊能力的強、弱，決定於網路部隊及網路科技的發展。

一、軍民網路合作，提升網路空間作戰體系攻擊效能

隨著網路科技的發展，網路戰場已不分平、戰時，其參戰人員也無法區分平民與武裝人員。根據2014年中共國防科技所刊載文章指出，由於網路戰的作戰力量廣泛而且高度分散，網路戰作戰編組應將網路偵察、攻擊、防禦力量等結合起來，形成軍隊主導、民間支援、軍民聯合的國家體系，全面提升國家網路空間戰略威懾能力。[21]另外，2016年我國銘傳大學助理教授林穎佑亦指出，2015年底中共解放軍，將過去總參謀部三部的網路部隊與總參二部的電子情報部隊整合成為「戰略支援部隊」後，並在中央統一指揮下，其網路攻擊部隊已包括解放軍體系及國安體系。同時，中共網路攻擊目標，已從社交工程的APT攻擊(Advanced Persistent Threat, APT)，開始改為針對網路設備實施網路攻擊，如路由器的韌體。[22]此外，根據2018年美國蘭德公司最新報告表示：中共戰略支援部隊為支持中共解放軍搶占網路

19 張軍主編，《IT戰爭》(北京：科學出版社)，2000年，頁35。

20 Timothy L.Thomas，李育慈譯，〈中共網路偵察(China's electronic long-Range reconnaissance)〉，《國防譯粹》(臺北)，第36卷第7期，國防部政務辦公室，2009年7月，頁20、21。

21 田成信、張峰、江飛，〈網路戰對作戰的影響及對策〉《國防科技》(北京)，第35卷第5期，國防工業出版社，2014年10月，頁104。

22 於下頁。

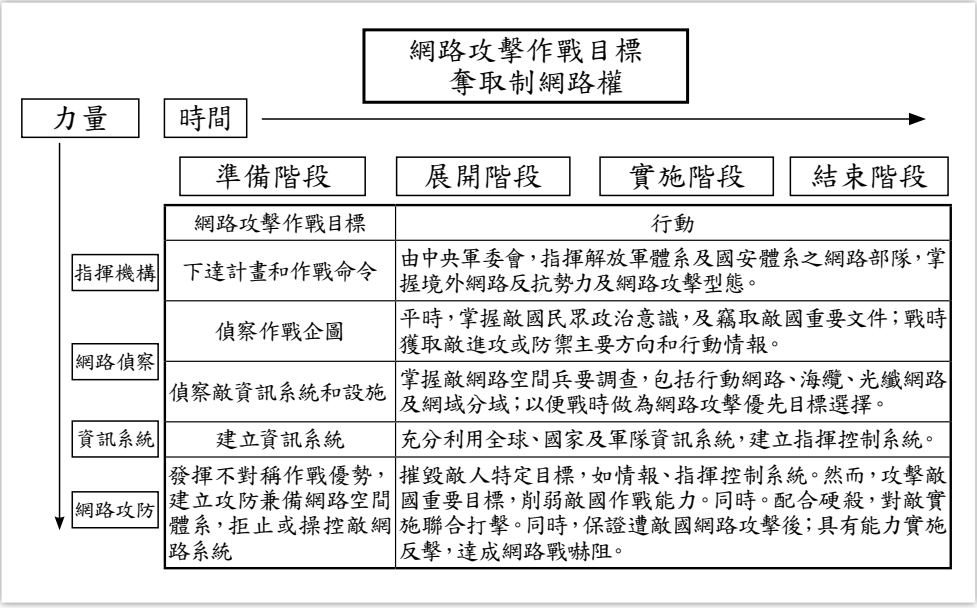

圖1　中共網路攻擊戰略構想圖

資料來源：作者整理並參考徐小岩主編，信息作戰學(北京：解放軍出版社，2002年，頁301；張軍主編，《IT戰爭》，(北京：科學出版社，2000年，頁35；曹正榮、吳潤波、孫建軍，《信息化聯合作戰》，(北京：解放軍出版社，2006年，頁120；Timothy L.Thomas，李育慈譯，〈中共網路偵察(china's electronic long-Range reconnaissance)〉，《國防譯粹》，第36卷第7期，國防部政務辦公室，2009年7月，頁20、21。

、電磁頻譜及戰略心理等制高點所設立；該部隊已針對癱瘓敵國的網路、資訊等關鍵基礎設施加強準備。[23]

除此之外，為因應未來網路作戰需求，中共解放軍應針對網路資訊安全的密碼學與民間大學等研究機構合作研究。[24]2016年，中共為強化動員社會力量參與維護網路安全，成立「網路空間安全協會」。該協會包括了中共境內主要網路科技企業和科研機構。[25]此外，2017年「戰略支援部隊」與中國科技大學、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所大學簽訂「協定」。[26]不僅如此，2017年底中共中央「軍民融合發展委員會辦公室」和解放軍相關部門指導下，成立「網路空間安全軍民融合創新中心」，並由民間網路公司令奇虎

22　林穎佑，〈中國近期網路作為探討：從控制到攻擊〉《臺灣國際研究季刊》(臺北)，第12卷第3期，臺灣國際研究學會出版，2016年／秋季號，頁60～62。

23　Jeffrey Engstrom, Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare(California RAND Corporation, 2018).p120.

24　劉玉青、龔衍麗，〈網路戰時代的安全威脅及對策研究〉《情報探索》(福建)，第11期，2014年11月，頁63。

25　中華人民共和國國家互聯網網路信息辦公室，〈中國網路空間安全協會成立〉，http://www.cac.gov.cn/2016-03/26/c_1118448623.htm，2018年6月8日。

26　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〉，http://news.xinhuanet.com/politics/2017-07/12/c_1121308932.htm，檢索日期2018年6月8日。

360負責。該中心負責網路國防安全智庫服務和創新技術產業服務，以落實網路強軍戰略之目標。[27]另外，根據2018年4月底美國資安業者Protect Wise研究發現證實，美國、日本、韓國的網路高科技業者與中國大陸境內的維吾爾族、西藏等所遭遇的網路攻擊，為中共解放軍所支持的網路駭客所為。同時，該駭客組織隸屬於中共情報組織，且這些中共駭客組織已經做到彼此連結、資源共享的地步，如Winnti，PassCV，APT17，Axiom，LEAD，邪惡的熊貓等。[28]

另外值得注意的是，根據2017年美國防部向國會報告《2017中共軍力報告》時指出：網路空間已成為中共解放軍作為國家安全和戰略競爭的新領域；其解放軍網路部隊，平時任務負責捍衛網路安全。戰時，協助解放軍先期掌握敵軍動態，發揮資電優勢確保戰場勝利。[29]另外，根據2018年3月6日美國國家情報總監柯茨(Dan Coats)出席美國聯邦參議院軍事委員會的「全球威脅(Worldwide Threats)」聽證會時表示，中共的網路攻擊能力已整合到解放軍中，其作戰範圍已威脅擴大到美國軍事和民用系統等基礎設施。[30]事實上，中共網路部隊的攻擊能力，可以癱瘓敵國軍事決策能力，早在2015年曾任美國國務院和商務部的James Andrew Lewis即研究證明，中共與俄羅斯正加強網路政擊能力，以癱瘓敵國在武器系統操作的軟體及指揮與管制系統，影響它國決策系統無法正常工作。中共運用先進的網路科技滲透他國網路空間，以延誤修復時效，降低軍事反擊能力。[31]由美國對中共網路攻擊能力的

27 張新、楊利程，〈我國「網路空間安全軍民融合創新中心」成立〉，http://www.81.cn/gnxw/2017-12/27/content_7886012.htm，檢索日期2018年6月8日。

28 Catalin Cimpanu, "Chinese Cyberspies Appear to be Preparing Supply-Chain Attacks,"https://www.bleepingcomputer.com/news/security/chinese-cyberspies-appear-to-be-preparing-supply-chain-attacks/，檢索日期2018年6月8日。

29 Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China 2017,pp.35-39, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF,檢索日期2018年6月8日。

30 DIA Public Affairs Defense Intelligence Agency, "DIA Director Briefs Senate Armed Services Committee on Worldwide Threats,"http://www.dia.mil/News/Articles/Article-View/Article/1459039/dia-director-briefs-senate-armed-services-committee-on-worldwide-threats/,檢索日期2018年6月8日。

31 James Andrew Lewis, "U.S.-Japan Cooperation in Cybersecurity," Center for Strategic and International Studies, November 5, 2015,pp.6,https://www.csis.org/analysis/us-japan-cooperation-cybersecurity,檢索日期2018年6月8日。

評估，凸顯出中共已掌握網路攻擊拒止的實力。

因此，在中共推動軍民合作網路戰略下將有利於網路病毒程式的研發；其網路攻擊能力將從網路竊取提升至具有癱瘓敵國軍民網路之攻擊能力。同時，中共解放軍所扶植的網路駭客具有竊取敵國民間公司的程式碼，意味著中共網路攻擊能力將具有影響他國經濟能力。換言之，當中共網路部隊掌握到敵國網路科技之後門程式密鑰後，敵國資訊化設備將可能成為網路安全屏障的突破口，也投射出中共網路部隊具有搶占網路空間制高點的能力(如圖2)。

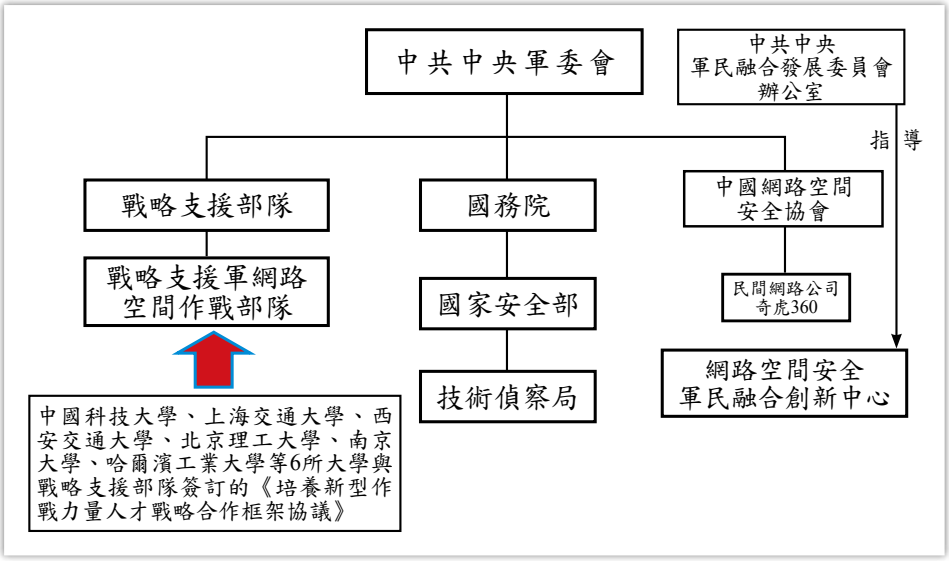

圖2　中共網路攻擊組織圖

資料來源：作者整理並參考林穎佑，〈中國近期網路作為探討：從控制到攻擊〉，《臺灣國際研究季刊》，第12卷第3期，2016年／秋季號，頁60～62。中華人民共和國國家互聯網網路信息辦公室，〈中國網路空間安全協會成立〉《中華人民共和國國家互聯網網路信息辦公室》，2016年3月26日，http://www.cac.gov.cn/2016-03/26/c_1118448623.htm〉;張新、楊利程，〈我國「網路空間安全軍民融合創新中心」成立〉，《中國軍網》，〈http://www.81.cn/gnxw/2017-12/27/content_7886012.htm〉。

二、攻擊目標從癱瘓敵國關鍵基礎設施擴及網民群眾

由於網路空間已擴及政治、經濟、文化及軍事等領域，網路攻擊影響層面已擴及到可降低敵國反應，並強化己方作戰效能。回顧中共網路攻擊行為，從2012年攻擊美國官方網站、新聞媒體，到2014年竊取美國人事部門的人事資料。至2017年美國防部《網路嚇阻的任務力量》指出，中共網路戰能力已對美國的網路、資訊等關鍵基礎設施產生威脅，其影響已衝擊到美國的重要利益及軍事反應能力。同時，中共網路戰還具有利用網路社群媒體，破壞美國政治體制(如選舉)和社會凝聚力。[32]不僅如此，2018年初俄羅斯宣布禁用中共民間網路公司所研發的網路社交軟體 —— 微信(We Chat)；其原因為用戶安

32　Department of Defense Science Board , Task Force On Cyber Deterrence(WASHINGTON, DC : OFFICE OF THE SECRETARY OF DEFENSE PENTAGON, February, 2017),pp.4-9

裝該軟體後，其個人位置地址將遭監控。[33]同年4月，美國國防部禁止美國軍人使用中共製造的華為手機。[34]此舉已凸顯出中共網路攻擊目標，已不再運用網路駭客，癱瘓敵國網站，而是擴及國家內部的網民用戶(如表2)。

除此之外，2018年4月中共國家主席習近平主持「全國網路安全和資訊化工作會議」時更表示，運用網際網路組織群眾、宣傳群眾、引導群眾、服務群眾，並加強網上輿論導向，推進網上宣傳理念。[35]另外，2017年中共國有媒體大量購買Facebook廣告，並在網路上大肆宣傳重要的外交活動。[36]故由中共強化網路攻擊宣傳行為，意味著網路心理戰已成為中共運用網路攻擊的重要手段。

總體而言，隨著網路科技的進步，影音串流、社群媒體已融入民眾日常生活中，網路空間的攻擊對象已從國家境內的網路、資訊等關鍵基礎設施，轉向為影響個人決策的網路媒體。中共網路攻擊能力已從拒止敵國網路系統正常運用、竊取他國重要資料，擴及至操控個人資料數據及癱瘓敵國部分關鍵網路基礎設施，也意味著未來衝突中，單靠軟體保護資料是不夠，其網路設備的硬體，將成為未來網路攻擊的重點目標。此外，據2016年美國愛達荷州國家實驗室任務支持中心出版《美國電力部門的網路威脅與脆弱性分析》(Cyber Threat and Vulnerability Analysis of the U.S.Electric Sector)表示，中共利用網路駭客對美國工業控制系統(Industrial Control System, ICS)實施網路攻擊，其效益除可收集情報外，還強化自身的網路基礎設施建設。[37]因此，在中共網路攻擊能力具備將網路病毒破壞化成網路戰攻擊武器的同時，凸顯出中共網路戰攻擊能力的提升；在網路技術的提升下，連帶也加強

33 高紫檀，〈俄羅斯宣布禁用中國通訊軟件微信〉《大紀元》，http://www.epochtimes.com/b5/17/5/5/n9110292.htm，2018年6月8日。

34 Paul Huang, "China-Made Huawei Phones Sold at US Bases Could Be Spying on American Soldiers,"https://www.theepochtimes.com/china-made-huawei-phones-sold-at-us-bases-could-be-spying-on-american-soldiers_2502960.html,檢索日期2018年6月8日。

35 張曉松、朱基釵，〈習近平在全國網路安全和資訊化工作會議上強調：敏銳抓住資訊化發展歷史機遇自主創新推進網路強國建設〉《解放軍報》(北京)，2018年4月22日，版1。

36 Paul Mozur, Mark Scott, "Facebook Faces a New World as Officials Rein In a Wild Web," https://www.nytimes.com/2017/09/17/technology/facebook-government-regulations.html,檢索日期2018年6月8日。

37 Mission Support Center Idaho National Laboratory, " Cyber Threat and Vulnerability Analysis of the U.S.Electric Sector," https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf,檢索日期2018年6月8日。

表2　中共網路攻擊行為遭美國揭露統計

年份	中共網路戰攻擊行為	攻擊目標
2012年	10月12日，美國遭中共實施電腦駭客攻擊，其遭攻擊目標為電網、交通、財政及政府系統。	電網、交通、政府財政系統
2013年	1月31日中共網路駭客入侵《紐約時報》電腦系統，竊取該報員工用戶及密碼。	《紐約時報》工作人員
2013年	2月1日《華爾街日報》遭中共網路駭客入侵。自2008年中共駭客攻擊美國新聞機構，包括報導有關中國領導人、中國政治法律問題的記者。	《華爾街日報》新聞機構
2013年	12月10日，中共網路駭客攻擊捷克共和國、葡萄牙、保加利亞、拉脫維亞和匈牙利等外交部電腦。	外交部電腦
2014年	7月10日，中共網路駭客入侵美國政府機構的人事管理辦公室部分數據庫，竊取系統聯邦僱員個人資訊。	政府部門系統
2015年	6月21日，中共網路駭客入侵目標為國防務承包商、能源企業和電子製造商。	國防務承包商電子製造商
2015年	9月23日，美國聯邦人事管理辦公室，遭中共網路駭客入侵竊取560萬聯邦僱員的指紋信息。	政府部門個人資料
2016年	3月26日，美國司法部起訴名為蘇斌(Su Bin)中共網路駭客。其目標為C-17數據運輸機等軍事機密資訊。	軍事機密資訊
2016年	4月，中共網路攻擊的目標是主要集中在美國政府和國防承包商;另在美、中衝突，中斷美軍指管通資系統。	國防承包商指管通資系統
2017年	2月，中共已具備對美國工業控制系統的攻擊的能力。	網路關鍵基礎設施
2017年	12月10日，中共情報單位利用「領英」交友平台，申請假帳號扮演顧問公司、智庫或學者，獲取個人資料。	政府官員帳戶
2018年	1-2月，中共駭客入侵美國海軍水下作戰中心(NUWC)合約商，成功竊取約614GB資料，其包含名為「海龍」的計畫、信號與感測數據、加密系統相關的潛艦無線電室資訊，以及美軍潛艦研發單位的電戰資料等。	軍事機密資訊

資料來源：Elsiabeth Bumiller , "Panetta Warns of Dire Threat of Cyberattack,"http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html;Thom Sharnker, "Pentagon Is Updating Conflict Rules in Cyberspace,"http://www.nytimes.com/2013/06/28/us/pentagon-is-updating-conflict-rules-in-cyberspace.html;Michael S.Schmidt, "Chinese Hackers Pursue Key Data on U.S.Workers,"https://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html;David E.Sanger, "Attack Gave Chinese Hackers Privileged Access to U.S.Systems,"
https://www.nytimes.com/2015/06/21/us/attack-gave-chinese-hackers-privileged-access-to-us-systems.html; "German intelligence unmasks alleged covert Chinese social media profiles,"https://www.reuters.com/article/us-germany-security-china/german-intelligence-unmasks-alleged-covert-chinese-social-media-profiles-idUSKBN1E40CA;Helene Cooper, "Chinese Hackers Steal Unclassified Data From Navy Contractor,"https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html

其網路防禦能力(如表3)。

中共網路攻擊對我國軍之威脅及策進之道

要確保國軍網路安全，著眼於外在網路安全防禦體制及內部防護作為。

一、對國軍網路安全防護之威脅評估

(一)國軍網路安全對外防禦，面臨更為嚴重的挑戰

要構建網路安全防護體制，即須透由層層防禦縱深。然而，據2018年4月底《中國時報》報導，我國內政部網站遭

表3　中共網路攻擊能力評估表

區分／能力	效益	影響
拒阻	在軍民合作網路戰略支持下，其網路程式密碼學能力得到提升，間接強化電腦病毒研發能力。中共網路攻擊能力，將從運用網路駭客對敵國政府部門、新聞傳播電台，竊取它國外交、軍事等重要資料，如F-35，提升至具有暫時或永久性癱瘓敵國網路系統無法正常使用。	電腦病毒研發能力提升後，將具有癱瘓敵國關鍵網路基礎設施能力。同時，間接強化網路嚇阻能力，使他國相信無法承受網路反擊，以致不敢輕啓戰事。並且竊取他國商業、外交、軍事等機密，有助於國防武力、商業競爭力等綜合國力提升。
操縱	利用進階持續性滲透攻擊，掌握他國網路用戶輿論，進而顛覆它國政權。	掌握國際輿論力量，運用文攻武嚇搶占國際話語權，以形塑師出有名的正義戰爭。同時，利用民粹主義提升國內民族團結。

資料來源：作者自行整理。

中共網路駭客攻擊，期間長達2天後，我國行政院資安處、內政部戶政司無法掌握駭客攻擊來源。同時，內政部所委外廠商仍無法承諾網頁何時恢復運作。[38]同年，我國國防大學黃基禎博士出席美國華府「戰略暨國際研究中心」發表臺灣網路安全報告時指出，境外對臺灣的網路攻擊已從脆弱的目標轉為有價值的目標，攻擊來源也從個別駭客變為有組織的團體。[39]由我國網路安全所面臨中共的網路攻擊威脅，凸顯出中共已清楚掌握我國軍、民共構的網路空間。換言之，我國網路安全防禦將面臨被動局面。因此，國軍在無前緣網路安全防禦縱深下，須強化自身網路對外監控能力。

(二)智慧型手機，已威脅軍隊內部網路安全

隨著智慧型手機的開放，網路社群媒體及影音串流已成各國運用網路攻擊的最佳手段。未來中共解放軍在臺海戰役中，其中一項重要手段為運用網路有限攻擊，對臺灣島內實施網路心理戰，以引起國內民眾恐懼，並瓦解百性對國家領導人的信心。[40]另外，根據2018年4月底《聯合新聞網》報導，中共戰機繞臺影片上傳至網路平台，其目的為中共解放軍企圖形塑強大軍事實力，以嚇阻他國不輕啟戰端。[41]此外，2018年初我國媒體披露，一款Strava Labs推出的運動追蹤App，[42]因可記錄用戶走過路徑地圖，其可能已暴露臺

38　張理國，〈內政部網頁癱2天查嘸攻擊來源〉http://www.chinatimes.com/newspapers/20180428000458-260118，檢索日期2018年5月11日。

39　曹郁芬、涂鉅旻，〈境外網攻臺灣升級〉《自由時報》(臺北)，2018年1月7日，版1。

40　胡文玲譯，〈中共軍事現代化與臺海軍事平衡(下)〉《青年日報》(臺北)，2015年10月15日，版7。

41、42　於下頁。

灣飛彈陣地位置。雖然，事後我國防部發表聲明予以否認。[43]故智慧型手機成現代人隨身必須物品後，已提供中共網路部隊運用網路心理戰更多的平台。尤其我國境內移動式的寬頻基地台密布，且陸軍部隊又將比海、空軍更容易接收訊息，其意味著網路文宣攻勢，將對我國軍內部造成威脅。

二、建議策進之道

由前述研析，中共網路攻擊威脅已為傳統武力威脅以外的重要手段，僅提供以下建議作為相關單位決策參考。

(一)擴編電腦緊急應變小組

無法掌握網路攻擊態樣，即無法做好網路安全防禦。為能處理網路安全緊急事故，國軍各軍種資安部門均設有「電腦緊急應變小組」(Computer Emergency Response Team, CERT)。然而，隨著網路攻擊型態朝向複合式發展，僅靠「電腦緊急應變小組」，將無法面對未來網路安全的威脅。根據2015年《國防雜誌》刊載《共軍網路作戰對我資電作戰之影響》研究指出，中共網路戰能力，已對我資電作戰產生嚴重威脅。我國應建置資安監控中心，保護網路本身及防護各端點，以強化作業系統及資訊設備的網路安全防禦縱深。[44]因此，面對中共的網路攻擊，國軍擴編「電腦緊急應變小組」，其成員應納編具有法律、政戰、網路安全技術人員及資電作戰戰略等專長人員，以利掌握中共網路攻擊的戰術、技術與程序。同時，建議相關單位成立網路戰略情報分析中心，整合民間網路科技能力強化研發防禦軟體，並建立軟體修補機制。

(二)擴大網路人才召募對象

網路高手來自民間。軍、民、學界合作，才能讓網路人才學以致用。根據2018年2月《青年日報》報導，臺中市為培養程式設計人才，提升產業智慧升級，由該市教育局籌組產、官、學合作的「程式設計產學聯盟」，於2018年甄選出50名高三學生，試辦高中職程式設計就業專班，順利結訓並通過技能檢定及面試者，將獲到「修平科大」產學專班升學，並享有到廠商就業保障。[45]故國軍資電人才召募，應擴大召收對象。首先建議國防部授權

41 程嘉文、林庭瑤，〈中共戰機攜飛彈繞臺闖我防空識別區〉《聯合新聞網》，https://udn.com/news/story/12009/3096961，檢索日期2018年6月6日。

42 Strava號稱「運動員的社群網路應用程式」，所提供「熱圖」顯示用戶透過智慧手機，還有可穿戴電子產品記錄下騎單車、跑步，游泳與滑降滑雪時所行經的所有路線。

43 謝宗憲，〈國防部：營內依規使用通信資訊器材〉《青年日報》(臺北)，2018年1月30日，版4。

44 呂兆祥，〈共軍網路作戰對我資電作戰之影響〉《國防雜誌》(桃園)，第30卷第6期，國防部國防大學，2015年6月，頁21、22。

45 於下頁。

由各作戰區與縣市教育局合作，針對教育部審定過的高三學生提供入伍方案，並優先進入我陸軍旅級資電部隊。此外，網路安全教育，應區分講習的對象，管理階層的軍官，建議比照公務人員終身學習證照，鼓勵軍官參與民間網路安全講習；士官、兵，則重點培育網路安全防護課程證照考取。

(三)採構新型網路偵察裝備

隨著複合式戰爭型態的發展，網路空間的輿論戰已成為未來奪取網路空間制高點的新領域。面對假新聞的危害，國軍除強化溝通管道，建立公開透明的機制外，建議增購新型網路偵察裝備。根據2016年Nicole Perlorth表示，幾乎所有國家都購買商業間諜軟體(Spying Tools)，以便掌握手機短訊、來電和位置。如以色列的NSO Group與Cellebrite及德國的Finfisher。[46]因此，面對中共不斷提升的網路攻勢，我國網路安全戰略不可再過於保守。建議政府及相關單位，儘速購置網路監控軟體，以便掌握中共對我的用戶攻擊。

結　　語

中共網路攻擊能力，在中央軍委統一指揮下，其網路攻擊編組將包括解放軍體系、國安體系及民間網路駭客。在軍民合作網路戰略推動，網路科技的發展將使網路攻擊獲得所需的裝備，其網路攻擊對外的作戰影響，已從網路偵察、竊取，到具有癱瘓他國關鍵網路基礎設施的能力。同時，還具有運用網路大數據分析，操控他國輿論及顛覆他國政權的能力。此外，隨著中共積極研發AI創新產業，其網路戰已朝向智能化作戰發展，其攻擊目標已可掌握他國人民重要情資。最令人驚訝的是，中共2015年底公開成立的「戰略支援部隊」，在其軍、民合作下，其網路人才的獲得，已使網路攻擊能力得到實質上的提升。然而，網路攻擊能力，可否達到操控他國網路數據，如美國國安局與以色列2011年共同研發的網路病毒(震網, Stuxnet)癱瘓伊朗核設施，值得後續觀察。此外，我國「資通電軍指揮部」雖已於2017年成立，但卻也面臨人才缺乏的問題。為此，相關單位應擴編電腦緊急應變小組、擴大網路人才召募對象、採構新型網路偵察裝備，以強化國軍網路安全防護能力。

45　張廷誠，〈中市育才程式設計產學班開訓〉《青年日報》(臺北)，2018年2月1日，版18。

46　Nicole Perlorth, "Governments Turn to Commercial Spyware to Intimidate Dissidents,"https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html,檢索日期2018年6月8日。