作戰研究

DOI:10.6237/NPJ.202104_55(3).0008

面對中共網軍威脅國軍資訊網路安全之探討

海軍少校 劉嘉偉、海軍中校 張家瑍

提　　要：

一、近年隨著網際網路的快速發展，全世界資訊流可以互相共享，高度資訊化國家對資訊基礎建設的依賴亦逐年加重；然而，隨著網路的興起，伴隨而來的是層出不窮的網路資安事件，資訊網路安全儼然成為全球性議題。

二、中共在1991年「波灣戰爭」後，受到極大的震撼與啟發，尤以「信息化」作戰領域，也激發並改變其對傳統戰爭的觀點與看法，更強烈地加深其致力於「軍事事務革新」的決心，連中共國家主席習近平都指示「沒有網絡安全，就沒有國家安全」，顯見共軍重視的程度。

三、中共「網軍」對我國發動的資訊安全攻擊，始終沒有停歇，尤以對國軍的威脅最為明確，除竊取軍事機密外，並對資訊裝備及網路系統進行干擾、破壞、摧毀或控制，連帶也影響以網路為基礎的軍事系統及各項資訊、通信安全設施。面對「網軍」的網路攻擊，國軍應縝密加強資訊網路防護的安全政策與因應作為，提升資訊安全防護強度，進而確保戰力得以正常發揮。

關鍵詞：資訊網路安全、信息化、中共網軍、網路攻擊及網路防護

壹、前言

近年來，美國、歐盟及印度等國家陸續示警，共軍在網路空間的攻擊能力正持續不斷的提升。2019年7月，中共在發布的《新時代的中國國防》報告中談到，已將「網絡安全」與核武、導彈及太空等傳統軍事項目並列，並以相當篇幅論述網路安全面臨的威脅及後續發展規劃[1]。其內容除證實相關國家的警訊外，更符合中共國家主席習近平所提出「沒有網絡安全，就沒有國家安全」的指示[2]。而近年外界持續關注的神祕單位「中國網路戰總部」（屬共軍「61398部隊」）[3]，以及共軍負責網路安全的部門，雖未在白

註1：〈《新時代的中國國防》白皮書〉，中共國防部，2019年7月24日，http://www.mod.gov.cn/big5/regulatory/2019-07/24/content_4846424.htm，檢索日期：2021年2月18日。

註2：〈習近平談網絡安全：沒有網絡安全就沒有國家安全〉，中共新聞網，2018年8月17日，http://cpc.people.com.cn/xuexi/BIG5/n1/2018/0817/c385476-30234135.html，檢索日期：2021年2月18日。

註3：〈中國人民解放軍61398部隊〉，維基百科，2020年12月12日，https://zh.wikipedia.org/wiki/%E4%B8%AD%E5%9C%8B%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E8%BB%8D61398%E9%83%A8%E9%9A%8A，檢索日期：2021年3月12日。

皮書詳述提列，但仍可從軍費分配章節中獲得證實；且自2012年以來，持續增長的國防費用，有一部分用於網路發展，並在軍隊訓練的網路化建設方面亦多有加強[4]。

面對中共「網軍」威脅，為確保國軍資訊網路安全，有必要探討資訊網路防護的政策與因應作為。本文從網路戰緣起概念為基礎，分析中共對網路戰的定義、意義與運用，並針對其網軍發展背景、經過、相關組織及作戰能力實施分析；另一方面，探討我國網路戰建構與發展、中共網路戰對我影響及國軍因應中共網路戰之對策。尤其，國軍在面對中共網路作戰能力日益增強的威脅下，不僅應積極建立網路作戰能量，更應持續周延資安保護機制與強化網路戰略目標防護，才能避免遭敵網路資訊作戰先制攻擊，確保國家安全，這也是撰文的主要目的。

貳、網路戰概述

「網路」先期設計為傳遞訊息的一種方式，在「web1.0」時代，僅提供軍事與學術使用，迄發展至「web2.0」，網路逐漸普及(平民)化後[5]，網路使用方式開始轉向多元化。在電腦世界中最早出現的攻擊方式為惡意軟體，也就是俗稱的「病毒」[6]。當電腦連接網路，惡意軟體透過網路傳播做為一種攻擊方式，即稱之為「網路攻擊」[7]；隨著網路攻擊的頻次越來越頻繁，種類也越來越多變，影響範圍與規模亦越來越廣泛，演變至最終可將其提升為「網路戰爭」層次。

在2008年8月「俄格衝突」中，俄羅斯於軍事行動前，便已先期控制喬治亞(或稱格魯吉亞)的網路系統，使得喬治亞的交通、通訊、媒體及金融互聯網等服務，幾乎全面癱瘓，為其後續軍事行動開創有利態勢[8]；又如2009年1月，法國海軍內部的電腦系統，因一部電腦受到病毒入侵，進而擴散到整個內部網路，系統一度不能啟動，海軍所屬戰鬥機也因無法下載「飛行指令」，全面停飛2日[9]；2014年3月南韓國防部高調宣布正在對北韓實施網路戰，他們以此前成功攻擊伊朗核設施的「超級工廠病毒(Stuxnet)」為藍本，正在研發類似的網路病毒，主要針對北韓核設施造成物理性破壞[10]。這些前例都是「網路戰」足以左右戰爭勝敗及高度影響國家安全的實證。

一、網路戰定義

(一)在《網絡戰：信息空間攻防歷史、

註4：仇佩芬，〈中國新國防白皮書聚焦「網路戰」並列核武項目等級〉，上報，2019年7月25日，http://ww.upmedia.mg/news_info.php?SerialNo=67960，檢索日期：2021年2月18日。

註5：〈Web 2.0〉，維基百科，2021年2月9日，https://zh.wikipedia.org/wiki/Web_2.0，檢索日期：2021年3月12日。

註6：〈電腦病毒〉，維基百科，2021年1月2日，https://zh.wikipedia.org/wiki/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%97%85%E6%AF%92，檢索日期：2021年3月12日。

註7：〈網路攻擊〉，維基百科，2020年9月16日，https://zh.wikipedia.org/wiki/%E7%BD%91%E7%BB%9C%E6%94%BB%E5%87%BB，檢索日期：2021年3月12日。

註8：〈俄羅斯-喬治亞戰爭〉，維基百科，2021年3月3日，https://zh.wikipedia.org/wiki/%E4%BF%84%E7%BD%97%E6%96%AF%EF%BC%8D%E6%A0%BC%E9%B2%81%E5%90%89%E4%BA%9A%E6%88%98%E4%BA%89，檢索日期：2021年3月12日。

註9：〈網路戰〉，MBA智庫．百科，2017年10月24日，https://wiki.mbalib.com/zh-tw/%E7%BD%91%E7%BB%9C%E6%88%98，檢索日期：2021年2月23日。

註10：同註9。

案例與未來》(A Multidisciplinary Approach)乙書中定義：「網絡戰是政策(或政治)的延伸，它由國家或非國家行為體主導，可以對國家安全構成嚴重威脅；也可以是出於國家安全目的，為回應可能的威脅，而發起的網路攻擊。」[11]；另依《網路戰爭：下一個國安威脅及因應之道》(Cyber War-The Next Threat To National Security And What To Do About It)書中介紹：「網路戰爭是一種未經授權的滲透，透過進入他國的電腦或網路，或是其他任何影響他國電腦系統的活動，進而對電腦、網路裝置或電腦系統控制的裝置，達成阻礙或損壞的目的。」[12]

(二)中共專書《直面信息化戰爭》中則敘述，針對網路戰的定義，應區分為兩大類，一類是「戰略網路戰」；另一類是「戰場網路戰」。平時戰略網路戰是指雙方在不發生大火力殺傷、破壞的戰爭情況下，一方對另一方的金融、交通、電力、民、軍網路系統等部分，以病毒、邏輯炸戰、駭客等手段實施攻擊；而戰場網路戰，則區分兩種，狹義部分係指攻擊、破壞、干擾敵軍戰場資訊網路和防護我方資訊網路的作戰行動；廣義而言，則指網路中心戰，將軍隊所有偵察系統、通信聯絡、指揮控制及各種武器裝備整合在一起，網路是作戰行動倍增器[13]。

(三)國內學者則認為「網路戰是指利用網際網路做為攻擊的媒介，是資訊戰概念底下的一種攻防型態，一種特殊發揮的形式。其特色在於網路空間完全不受時間、地理區隔、天候的影響，讓傳統疆界變得模糊不清。」[14]

綜觀而論，「網路戰」並不單指兩國之間的軍事行動交戰，而是包含各種形式上的攻擊與行為，舉凡傳統戰爭中的軍事設施、情報竊取、間諜行為，到國家編制內的網軍、政治宣傳、駭客攻擊等均屬之。

二、中共網路戰發展緣起

80年代以來，許多國家紛紛投入大量的人力與物力，把發展高技術列為國家發展戰略的重要組成部分。像美國於1983年提出的「戰略防禦倡議(Strategic Defense Initiative，SDI)」[15]及歐盟在1985年共同研究發展的「尤里卡計畫(European Research Coordination Agency，EURECA)」[16]等，這些計畫的實施，除了對世界高新技術發展產生重大且深遠影響外，也促使中共為因應世界高技術的蓬勃發展，而在1986年3月啟動「高技術研究發展計畫」(簡稱「863計畫」

註11：Paulo Shakarian等著，吳奕俊等譯，《網絡戰：信息空間攻防歷史、案例與未來》(A Multidisciplinary Approach) (北京：金城出版社，2016年9月)，頁001。

註12：Richard A. Clarke理查・克拉克、Robert K. Knake羅伯・柯納克著，王文勇譯，《網路戰爭：下一個國安威脅及因應之道》(Cyber War：The Next Threat To National Security And What To Do About It) (臺北：國防部政務辦公室，2014年9月)，頁229。

註13：王清安，〈中共發展網路戰之研究〉，《國立政治大學戰略與國際事務碩士在職專班碩士論文》(臺北)，頁11。

註14：林穎佑，〈大陸網軍與APT攻擊〉，《展望與探索》(臺北)，第11卷，第3期，2013年3月，頁97。

註15：〈戰略防禦計畫〉，維基百科，2020年9月21日，https://zh.wikipedia.org/wiki/%E6%98%9F%E7%90%83%E5%A4%A7%E6%88%98%E8%AE%A1%E5%88%92，檢索日期：2021年3月12日。

註16：〈尤里卡計畫〉，維基百科，2020年10月8日，https://zh.wikipedia.org/wiki/%E5%B0%A4%E9%87%8C%E5%8D%A1%E8%A8%88%E5%8A%83，檢索日期：2021年3月12日。

)[17]，用以提高自主創新能力，堅持戰略性、前沿性和前瞻性，並以前沿技術研究為發展重點，統籌部署高技術的集成應用和產業化示範，以充分發揮高技術引領未來發展的先導作用，特別是在高性能電腦、第三代移動通信與高速信息網路等領域[18]。

1991年「波灣戰爭」開啟科技戰爭的新紀元[19]，也掀起另一波「軍事事務革新」，尤其資訊科技主宰整個戰場，讓世人意識到資訊時代的來臨，戰爭形態已澈底改變，未來戰爭「信息化」將是世界強國竭力追求的目標。中共方面更是受到極大的震撼與啟發，尤以「信息化」作戰領域為最，同時激發並改變其對傳統戰爭的看法，進而更強烈推動與致力於軍事事務革新的決心，及網路戰發展[20]。

三、我國網路戰緣起

(一)在全球化資訊社會中，各國企業及政府機關為減少人力、物力、財力之投資，追求行政效能以實現便民、利民之目標，無不相繼採用電腦資訊化作業。我國亦同步利用電腦及網際網路提供創新服務或改善業務效率。在便利、快速前提下，如何防止機密外洩、網路犯罪以及不當言論散播等，儼然成為國家安全之重要議題。2000年5月，「國家安全會議」(簡稱「國安會」)研提《建立我國通資訊基礎建設安全機制》建議書；翌年成立行政院「國家資通安全會報」，積極推動我國資通安全基礎建設工作，逐步達成「建立整體資安防護體系、健全資安防護能力」之階段性目標[21]，並由「國安會」負責協調行政院資通安全會報技服中心、科技部與國防部等相關部會，進行網路資訊安全之整體規劃；其中國軍在國防轉型與軍務革新等方面，亦配合其整體規劃逐步推展網路資訊戰力建構，以因應網際網路時代作戰之需求。

(二)近年來，「數位經濟」帶動產業朝跨世代、跨境、跨領域、跨虛實等趨勢發展，促使全球產業格局翻轉，加上隨著數位經濟與「物聯網」(Internet of Things，IoT)時代的來臨[22]，為配合資安及國安政策方向，下一階段國家資通安全發展，需從資通安全角度來確保數位國家安全。爰此，行政院提出以「打造安全可信賴的數位國家」為願景，並以「建構國家資安聯防體系，提升整體資安防護機制，強化資安自主產業發展」為目標，著手推動策略，以因應我國特

註17：〈863計畫〉，維基百科，2021年1月17日，https://zh.wikipedia.org/wiki/863%E8%AE%A1%E5%88%92，檢索日期：2021年3月12日。

註18：〈863計畫〉，MBA智庫・百科，2017年1月5日，https://wiki.mbalib.com/zh-tw/863%E8%AE%A1%E5%88%92，檢索日期：2021年2月24日。

註19：〈波斯灣戰爭〉，維基百科，2021年2月20日，https://zh.wikipedia.org/wiki/%E6%B5%B7%E6%B9%BE%E6%88%98%E4%BA%89，檢索日期：2021年3月12日。

註20：沈誠忠，〈中共的信息心理戰之研究〉，淡江大學國際事務與戰略研究所碩士在職專班學位論文，2006年，https://www.airitilibrary.com/Publication/alDetailedMesh1?DocID=U0002-0902200616092700，檢索日期：2021年3月22日。

註21：〈行政院國家資通安全會報-緣起背景〉，行政院網站，https://nicst.ey.gov.tw/Page/C008464A6C38F57C，檢索日期：2020年2月24日。

註22：〈物聯網〉，維基百科，2021年2月24日，https://zh.wikipedia.org/wiki/%E7%89%A9%E8%81%94%E7%BD%91，檢索日期：2021年3月16日。

殊的政經情勢及全球複雜多元的資通訊變革，並做為國家推動資安防護策略與計畫之重要依據[23]。

參、中共網軍建構與發展

在1991年「波灣戰爭」後，中共領導階層深刻體認其三軍武器現代化程度遠遠落後於美、歐、日等先進國家，然而這些國家卻又高度依賴資訊化、科技化，而這個「脆弱環節」便成為共軍「電子珍珠港」(An Electronic Pearl Harbor)侵襲的極佳目標。此外，中共也認為癱瘓敵方金融、交通、電力、電信及軍事核心機制，可以獲得最佳作戰效益[24]。「網路戰」逐漸凸顯的重要性，澈底改變了正在進行機械化與半機械化建設的共軍單一思維，進而提出「新時期戰略方針」，朝現代化建設「三步走」戰略目標，以推進共軍資訊化與機械化複合式發展，實現共軍現代化跨越式的發展，並積極建設網路空間，發展相關理論；更瞭解到「網路戰」除了具備改變傳統作戰概念之潛力外，在未來作戰亦將扮演成功關鍵角色，並可實現其打贏「資訊網路化戰爭」的目標[25]。

一、網軍發展背景

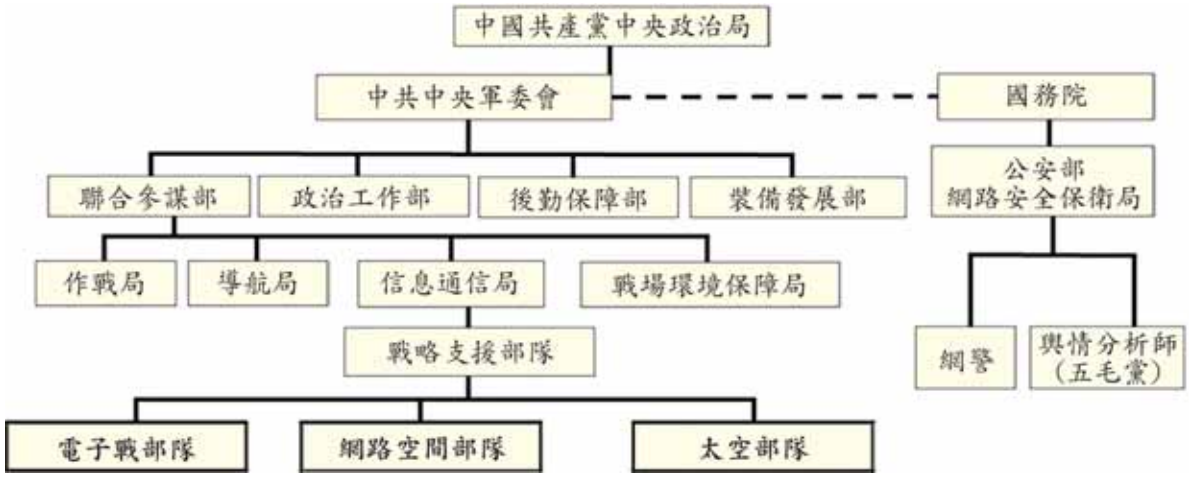
(一)1999年11月，中共《解放軍報》首次提出「網軍」一詞，成為傳統陸、海、空三軍以外的新「軍種」，主要任務為保衛網路主權、從事網路作戰，仿效美國將網軍分為攻擊、防衛、維護三大部門，同年，共軍正式將「訊息戰」、「駭客攻擊」、「網路攻擊」等納入演習範圍[26]。自2002年開始，中共規劃全國性國家戰略層級的資訊戰分工，共軍階層負責電子戰和網路戰，簡稱「網電一體戰」，由總參謀部負責規劃成軍；而網軍部隊則由共軍和國防動員部委民間IT的產、官、學界的信息民兵共同組成[27]。

(二)為深化國防和軍隊改革，2015年12月新組建「戰略支援部隊」；2016年1月撤銷共軍總參謀部及其下屬的技術偵察部、電子對抗部；2017年7月正式成立共軍「戰略支援部隊網絡系統部」(網絡空間部隊)，主要由原總參三、四部和總裝備部等相關部門組合而成，並改番號為「32069部隊」，專責空間信息和計算機網絡系統等工作[28]。

二、組織架構

中共除正式將網絡作戰武力部隊納入正規作戰行列外，並在民兵部隊及人民武警部隊中，各自成立專職電腦網絡作戰的網軍部隊。由此可見，中共電腦網絡作戰的基本架構區分為共軍網軍、民兵網軍及人民武警網

註23：同註21。
註24：同註13，頁41。
註25：金登富，〈中共網路戰略思維之概念性探討〉，《國防大學戰略研究所戰略與國際事務碩士班碩士論文集》(臺北)，頁60。
註26：〈中共網軍襲臺的案例與效應〉，國防部政戰資訊服務網，2017年2月6日，https://gpwd.mnd.gov.tw/Publish.aspx?cnid=513&p=4440，檢索日期：2021年2月26日。
註27：同註13，頁49。
註28：〈中共戰略支援部隊網絡系統部〉，維基百科，2020年12月12日，https://zh.wikipedia.org/wiki/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E6%88%98%E7%95%A5%E6%94%AF%E6%8F%B4%E9%83%A8%E9%98%9F%E7%BD%91%E7%BB%9C%E7%B3%BB%E7%BB%9F%E9%83%A8，檢索日期：2021年1月13日。



圖一：2017年中共網軍編組圖

資料來源：參考；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11，由作者彙整製表。

軍等三大組成，其業務分工散布於中央軍事委員會聯合參謀部、訓練管理部、國防動員部、戰略規劃辦公室、機關事務管理總局、國際軍事合作辦公室，及共軍戰略支援部隊等7個部門及5大戰區(東、南、西、北、中部戰區)、國防科研機關與各級院校等單位，任務包括平時網路竊密、戰時網路攻擊及滲透等諜報活動；另國防動員亦將信息民兵納入編組，整體軍事機關網軍架構基本成形，預判其整體正式編制人力超過10萬人[29]。組織架構簡要概述如後：

(一)共軍網軍

1.1950年12月，中共軍事委員會總情報部成立，負責管理情報、技術、聯絡三個部門；1953年2月，軍事委員會總情報部撤銷，下屬各部門隨後在1954年劃歸共軍總參謀部建制，原技術部改為共軍總參謀部技術偵察部，後來設番號為共軍「61195部隊」[30]。1977年4月，共軍總參謀部電子對抗、雷達部正式成立；1982年8月，再併入總參通信部(對外保留總參四部名稱)；1985年8月，再恢復成為總參直屬部，稱「電子對抗雷達部」[31]。

2.到2015年秋，中共啟動深化國防和軍隊改革，對共軍和武警部隊組織架構進行調整；同年12月成立了「戰略支援部隊」[32]，並由國家領導人習近平親授軍旗及致訓詞，更凸顯出對此部隊之重視程度。該部隊原由網軍－網路黑客隊伍、天軍－軍事航天部隊(以各類偵察、導航衛星為主)及電子戰部隊(以干擾和誤導敵方雷達和通訊為主)等三大部分組成；2016年1月，撤銷總參謀部技術

註29：同註13，頁75。

註30：同註27。

註31：同註27。

註32：〈解放軍組織大改造：設立陸軍司令部、火箭軍、戰略支援部隊〉，風傳媒，2016年1月1日，https://www.storm.mg/article/77300?page=2，檢索日期：2021年3月20日。

表一：民兵網軍編組與任務一覽表

編組區分	任務概況
電子戰分隊	以連為單位，從電子行業抽調人員，負責偽冒、電子干擾、反干擾、欺騙、反欺騙及攻擊敵人電子系統等。
網絡戰分隊	以連為單位，從相關高等院校和科研單位抽調專業人員組成。負責設置防火牆，保護己方網絡安全，製造電子垃圾阻塞對方。
黑客(駭客)分隊	以排為單位，由資訊科系或具有相關專長興趣等人才，施以特別訓練，專以入侵敵人網絡穴道為目標，藉由假情報、假資訊及病毒等，進行節點式破壞、竄改、銷毀等攻擊。
訊息救護分隊	以連為單位，從相關行業中抽調專業人員訓練編組，負責網絡系統硬軟體維修和復原工作，以發揮戰時網路作戰正常功能。

資料來源：參考；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11，由作者彙整製表。

偵察部、電子對抗部等單位；2017年7月，共軍「戰略支援部隊」再成立「網絡系統部」(網絡空間部隊)[33]。經調整後之戰略支援部隊組成計三部分，其一是網絡空間部隊，負責網路攻擊與防禦；其二是電子戰部隊，負責對敵指管通網情監偵系統進行欺敵、干擾；第三是太空部隊，負責監偵及衛星任務(編組，如圖一)[34]。

(二)民兵網軍

1. 中共於2003年3月完成信息民兵編組，其基層為省屬縣市和鄉鎮的信息民兵分隊，在性質部分視單位特性區分電子戰分隊、網路戰分隊、黑客(駭客)分隊及信息救護分隊等(如表一)。

2. 民兵網軍亦有由北京、清華、交通及復旦大學等頂尖院校資訊系和研究所成立之民兵分隊，其組織規模概等於營級編制，下轄不同專業連、排、班，且在其彈性運用上，可適時實施相關工程人員的抽調編組。例如北京中國科學院「紅旗軟件技術有限公司」，便有北京信息民兵編組，其下轄數個連、排級等組織，賦予訊息救護專業，搶救維修軟、硬體系統等[35]。

(三)人民武警網軍

為掌握全國網路安全，中共公安部所屬公共信息網路安全監察局(簡稱網監局)，在各省、市、自治區公安廳(局)下設立網監處，負責轄區內網路信息安全監察和違法查處工作。依2014年非官方正式統計，公安部負責網路保密、偵防的網路警察和網路安全人員已多達23萬餘人；另各相關單位網路科研機關人員亦有4萬餘人。自2015年起，中共警方也招募志願人員成立「網警志願者」，俗稱第6支的「王牌群眾力量」，該部隊約3,000員，遍布中國大陸境內各行各業[36]。

三、中共網軍網路作戰能力

中共為加強網路戰略嚇阻要域，確保國家利益拓展，持續不斷強化組建資訊化部隊

註33：王朋飛，〈專家稱戰略支援部隊獨立成軍理念領先於美軍〉，新浪軍事，2016年1月8日，http://mil.news.sina.com.cn/china/2016-01-08/doc-ifxnkkuy7732953.shtml，檢索日期：2021年1月21日。

註34：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》，第54卷，第3期，2020年6月1日，頁86。

註35：廖文中，〈中國網軍：國安、公安與解放軍〉，《全球防衛雜誌》，第271期，2007年3月，頁58-60。

註36：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13。

，以推動其戰略轉型，2015年12月將天軍、網軍及電子戰部隊整合為「戰略支援部隊」，便是希望達到集中兵力的目的，以提升網路攻擊能力。其網路攻、防能力概述如下：

(一)攻擊能力

中共已發展出「高級數據武器」，並有能力加以運用，武器本身還包括「自我漸變」(Self-Morphing)惡意程式碼應用、電子電路摧毀能力、惡意程式碼自我加解密及無線網路外部破壞等能力[37]。據資料顯示，中共網路戰首先攻擊目標置重點於敵國後勤補給系統，透過其對敵國後勤物資數量、投送地點的掌握，分析作戰部隊的關鍵訊息，並以阻斷式服務攻擊，致使敵國後勤系統對外阻塞[38]。由此可見，中共網路戰能力已越來越先進，不僅藉由電腦病毒使敵國系統癱瘓外，更提升其偵蒐、分析、破壞及阻絕能力。

(二)防禦能力

1.中共國家防火牆即「防火長城」(Great Firewall，GFW)，大陸民眾俗稱「牆」、「網路長城」、「功夫網」等，為中共政府用於過濾跨網際網路訊息的審查系統。例如中共政府將其查獲的特定網點阻斷，造成大家所熟知的連線錯誤現象，此防火牆不是中共特有的一個專門單位，而是由分散部門的各伺服器和路由器等裝置，加上相關公司的應用程式所構成，是一個跨軍民合作的大型資訊管制系統。

2.世界其他一些國家也存在網路審查，不過其審查物件、規模、執行主體等均與中共審查機制有著相當大的不同，例如他國僅止於金融洗錢、國際詐騙等犯罪行為，或審查兒童色情等相關內容。而「防火長城」作用是監控所有經過國際閘道器的通訊，對認為不符合中共官方要求的傳輸內容，進行干擾、阻斷、封鎖。由於中共網路審查廣泛，其國內含有「不合適」內容的網站，都會受到政府直接的行政干預，進而被要求自我審查、監管，乃至封鎖關閉。故「防火長城」主要作用為分析和過濾中國大陸境外網路的資訊互相存取[39]。

由此可見，中共對內網路的審查制度是相當獨立威權，而中共近年對外網路政策亦產生「由守轉攻」的變化。在2015年，中共已研發出一種俗稱「大砲」(Great Cannon)的網路戰攻擊武器。當外國資訊流向中共網站後，該「大砲」系統藉由攔截大量網路流量，並注入惡意代碼，再行發回給該打擊目標。簡言之，中共除網路攻擊外，還曾對翻牆技術討論網站進行攻擊[40]；另在網路安全防禦部分，中共也在資訊系統上強化其功能，其攻防能力均日益增長，實力不容小覷。

肆、國軍資訊網路安全探討

因為網路世界沒有「百分之百」的防禦，資安更沒有絕對的安全。面對中共網路戰

註37：〈中共網路發展情勢研析〉，亞太和平研究基金會-研究成果-安全情勢，2016年12月30日，https://www.faps.org.tw/article-ap-2108-5814，檢索日期：2021年1月21日。

註38：〈網路空間的國家安全挑戰：虛擬與現實交織的博弈〉，《世界知識》(臺北)，第1673期，2016年3月，頁23。

註39：〈防火長城〉，維基百科，2021年2月13日，https://zh.wikipedia.org/wiki/%E9%98%B2%E7%81%AB%E9%95%BF%E5%9F%8E，檢索日期：2021年2月18日。

註40：同註37。

表二：我國三大網軍特性概述一覽表

項次	區分	部隊	預估人數(員)	主要任務
1	正規軍	老虎小組	30	網路監控與研發
2	非正規軍	國安局	1, 500	網路情蒐與作戰
		軍情局	不詳	

資料來源：參考；〈中華民國國家安全局〉，維基百科，2021年2月21日，https://zh.wikipedia.org/wiki/%E4%B8%AD%E8%8F%AF%E6%B0%91%E5%9C%8B%E5%9C%8B%E5%AE%B6%E5%AE%89%E5%85%A8%E5%B1%80，檢索日期：2021年2月26日；〈網戰升級 中國大陸與臺灣網軍天天交戰〉，超越新聞網，2014年8月16日，https://beyondnews852.com/20140816/8315/，檢索日期：2021年2月26日，由作者彙整製表。

的不斷擴充發展，國軍亦面臨嚴峻的網路攻擊威脅。因此，唯有瞭解其特點及威脅，並儘早研擬防護因應作為，並從建構相關研發機構提升網路戰作戰能量、建立電腦病毒資料庫、網路戰專業人才培訓與長留久用及修訂完善反制軍事假信息法規等四大面向提出參考建議，方能憑藉堅固的資安防護網，保護國家、民生基礎設施機密不致洩露，並確保國防軍事安全。以下就國軍網路戰建構與發展、對我之影響及因應對策三部分，逐項分述如後：

一、國軍網路戰建構與發展

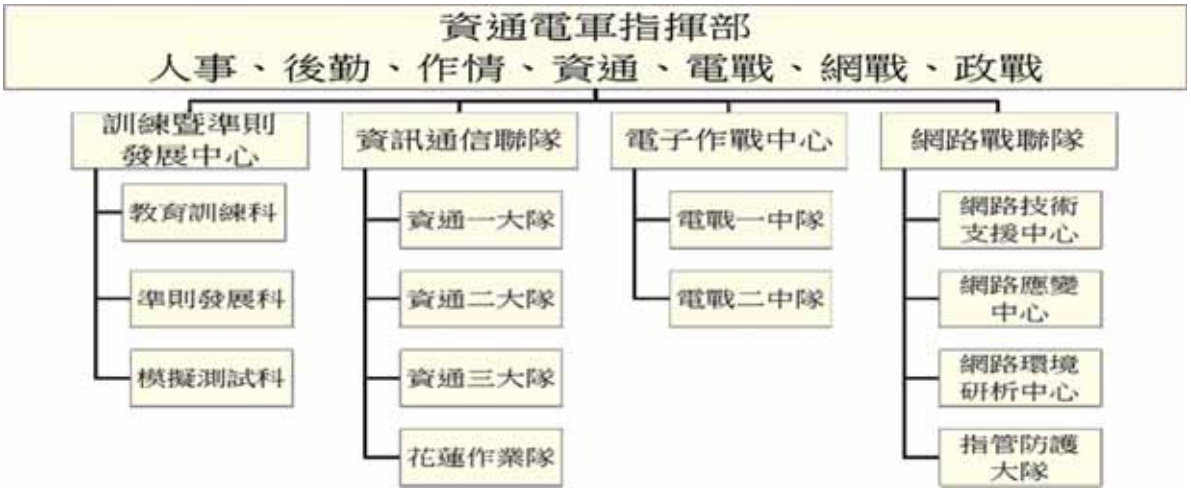
(一)2001年4月23日，時任國防部長伍世文先生於立法院備詢時，即證實國軍已正式成立第一支網路作戰隊伍「老虎小組」[41]；另媒體亦披露，國軍「對外網路作戰」包括三大系統，即「老虎小組」部隊、「國安局」和「軍情局」三支網軍。其中「老虎小組」兩大任務，一是24小時監視中國大陸各網站，二是秘密蒐集與研發電腦病毒，以攻擊中共網路系統；另外兩支網軍則偏重於情報蒐集。國家情報單位為增強網路戰生存能力，相信也會將不少網軍隱藏於境外，以便依時機及指令適時啟動網路攻勢，獲致期望戰果。依國內媒體分析，我國對外網路作戰中，「老虎小組」重作戰，屬於編制內「正規軍」；「國安局」和「軍情局」重情蒐，略屬「非正規軍」，並以對外招募的民間駭客高手為多(網軍特性概述，如表二)[42]。

(二)2017年7月1日，國軍「資通電軍指揮部」正式編成(以下簡稱，「資通電軍」)，屬國防部參謀本部直屬單位，其成員多來自原資電作戰指揮部、電訊發展室以及陸、海、空三軍的資電部隊編組而成，主要任務為電子作戰、資訊作戰、網路作戰及維護管理(資通電軍組織，如圖二)[43]。平時統合國軍網路、電子及資通平臺等三大領域，執行網路空間安全維護、電磁頻譜偵蒐及指管系統建立與維運，維護國軍各式資通電系統及防衛國防資訊網路，以支援國軍資通安全緊急應變及國家層級網際防禦，確保各項指管系統暢通。戰時除依令執行國軍資通安全防

註41：程文理，〈資訊戰概論 Part.1兩岸資訊戰現況〉，國防新聞網，2016年6月26日，http://www.ewmib.com/news.php?news_id=124&cate_id=9，檢索日期：2021年3月22日。

註42：〈網戰升級 中國大陸與臺灣網軍天天交戰〉，超越新聞網，2014年8月16日，https://beyondnews852.com/20140816/8315/，檢索日期：2021年2月19日。

註43：〈國防部參謀本部資通電軍指揮部〉，維基百科，2021年2月15日，https://zh.wikipedia.org/wiki/%E5%9C%8B%E9%98%B2%E9%83%A8%E5%8F%83%E8%AC%80%E6%9C%AC%E9%83%A8%E8%B3%87%E9%80%9A%E9%9B%BB%E8%BB%8D%E6%8C%87%E6%8F%AE%E9%83%A8，檢索日期：2021年2月21日。



圖二：資通電軍組織圖

資料來源：參考〈國防部參謀本部資通電軍指揮部〉，維基百科，2021年2月15日，https://zh.wikipedia.org/wiki/%E5%9C%8B%E9%98%B2%E9%83%A8%E5%8F%83%E8%AC%80%E6%9C%AC%E9%83%A8%E8%B3%87%E9%80%9A%E9%9B%BB%E8%BB%8D%E6%8C%87%E6%8F%AE%E9%83%A8，檢索日期：2021年2月21日；呂昭隆，〈資通電軍 擬納入情報機關〉，中時電子報，2019年9月30日，https://www.chinatimes.com/newspapers/20190930000445-260118?chdtv，檢索日期：2021年3月21日，由作者彙整製表。

護任務外，並確保國軍指管網路、資訊安全及情監偵系統有效運作，以及協防國家關鍵資訊基礎設施，捍衛國家安全[44]。

二、中共網路戰對我之影響

(一)資安威脅部分

1. 我國每月均遭受至少數千萬次以上的網路攻擊，僅國防部所屬各單位每月就承受近2,000萬餘次。到了2014年，更大幅增為7億2,686萬次數，後續年度雖有逐年遞減，但亦均保持破億次數的網攻事件[45]。探究其原因，應為中共網軍正改變其網路攻擊型態，並由原先大量進攻模式，調整成網路精準打擊，如此意味著一旦攻擊成功，後果將更形嚴重[46]。

2. 雖然資安攻擊事件往往難以追溯確認其發動來源，但仍可透由資安鑑識與行為模式辨識來判定，許多攻擊事件可能多來自於中國大陸網軍所發起。尤其，網路科技快速進步，採取新技術來隱匿行為，將讓網路攻擊更加難以被察覺，例如透過搜尋引擎或部落格，使資訊安全部門誤認為一般網路平台而忽略其行動；另亦有許多攻擊是繞道經由其他國家所發動，使其來源更難以被追踪確認[47]。

3. 我國部分軍事科技及設施常與民間科技共享或通用，如電力系統、作業軟(硬)體、軍租網路設備等，且軍事科技及設施均未獨立，所使用軟(硬)體皆為一般資訊設備，

註44：國防報告書編纂委員會，《2017年國防報告書》(國防部：軍備局第401廠，2017年12月)，頁61。
註45：蘇紫雲 曾怡碩主編，《2018國防科技趨勢評估報告》(臺北，財團法人國防安全研究院)，2018年12月，頁93。
註46：同註45，頁94。
註47：同註46。

同樣可能遭敵發動全面性攻擊或破壞，屆時恐將癱瘓國家整體秩序與資安網路運作能力，國軍更應有所警覺。

(二)網路輿論心理戰部分

1.傳統「輿論戰」與「心理戰」都能套用到網路世界。謠言、耳語及假消息經特定的網路造勢、洗版、分化及推波助瀾下，即形成如網路同溫層效應般不斷的延伸擴大。除假消息外，利用社群媒體散布仇恨言論，達到動員暴力行為目的，也讓網路虛擬言論造成實體世界的性命傷害[48]，像是2021年1月6日，前美國總統唐納・川普(Donald Trump)支持者，因受到陣營內流傳的假消息、陰謀論及不斷滋生的暴力與仇恨言論鼓動下，爆發攻擊國會事件，造成流血暴力衝突[49]，同樣值得國軍重視，並注意防範。

2.在2016年12月，中共空軍在微博上張貼一張「轟-6K」的飛行照片，並透過討論區宣傳背景即為我國玉山山脈；又如2019年5月香港媒體報導，我國的戰鬥機飛行員在與中共戰機相遇時，意外地發射了一枚「自衛性武器(熱誘餌彈)」等案例[50]。此二次事件，雖經國防部立即澄清，然這未經證實的「假新聞」，卻在國內主流媒體的討論區與社群媒體，諸如PTT、臉書、Line、What App等平臺，引發熱烈討論，嚴重影響民眾對國防施政與建軍備戰的信賴[51]。顯見，共軍正無所不用其極地對我國進行多渠道、多面向及多層次的網路攻擊。

三、國軍因應中共網路戰之對策與因應作為

網路作戰已是一場無煙硝的戰爭，2021年3月中旬，於美國阿拉斯加州舉行的美、「中」「2+2」高層會談中，美國務卿安東尼・布林肯(Antony Blinken)將中共網軍對美攻擊列為重要議題[52]，由於中共將我國視為網攻的練兵場，臺灣形同是網路作戰前沿。現階段除以網軍情蒐及竊取軍、工、商業等機密資料外，並意圖掌握我國關鍵節點，建立攻擊清單，做為後續作戰階段之網路攻擊目標。為因應中共網軍威脅與日俱增，我國雖成立第四軍種「資通電軍」，亦結合政府及民間企業相關資源，大幅提升網路系統及技術，然在面對中共網路戰方面的不斷擴張發展，仍須針對不足之處加以精進。爰提因應建議如后：

(一)建構研發專責機構提升網路戰能量

要有好的人才及裝備，才可使網路作戰發揮最大效能。完整的網路作戰系統包括「硬體」、「軟體」及「通信」三大部分，如有任一部分出現問題漏洞，整個系統安全性將遭受重大威脅。依現行「資通電軍」組織

註48：同註45，頁96。

註49：蔡婠嫣，〈「美國總統與暴民合謀」 美聯社：川普煽動政變未遂，躲在白宮見證親手造成的混亂〉，風傳媒，2021年1月7日，https://www.storm.mg/article/3366810?page=1，檢索日期：2021年3月20日。

註50：〈國軍監控共機發射熱焰彈？國防部：假訊息〉，大紀元時報，2019年5月1日，https://www.epochtimes.com.tw/n280275/%E5%9C%8B%E8%BB%8D%E7%9B%A3%E6%8E%A7%E5%85%B1%E6%A9%9F%E7%99%BC%E5%B0%84%E7%86%B1%E7%84%B0%E5%BD%88-%E5%9C%8B%E9%98%B2%E9%83%A8-%E5%81%87%E8%A8%8A%E6%81%AF.html，檢索日期：2021年3月3日。

註51：同註26。

註52：呂昭隆，〈臺美軍方交流 切磋網路戰爭〉，《中國時報》，2021年3月22日，版A1。

，已具備訓練暨準則發展中心，負責教育訓練、準則發展及網路作戰戰術戰法研發等任務，然因其編制規模相比其他各軍種，尚具備擴充發展之潛能，且任務仍有依需要，納編各部隊人員予以合署支援執行；惟因現有部隊除須執行日常例行任務外，尚須分心於前述工作，且部分成員來自各軍種，恐無法完全整合運用，形成每個單位雖有專業專精人員，恐仍無法滿足現況需求。因此，建議可參考美國網路部隊，成立裝備研發與籌獲等機構，以爭取最大研發經費及能量，讓基層資訊通信與電子戰部隊更能專注於網路作戰任務與訓練執行，方能真正發揮其建制效能。

(二)整合建立電腦病毒資料庫

電腦病毒資料庫主要功能為記錄電腦病毒名稱、分類、傳播途徑、發作行為與查殺方法等內容，且提供使用者查看與手動操作時使用。電腦病毒資料庫記錄大數據病毒名稱，並進行分類，只要在病毒資料庫檢索器內輸入病毒名稱，就能得到病毒詳細資料，有利後續反制應對[53]。國防部應積極與行政院「國家資通安全會報」研討共同成立一個專門病毒資料庫，網羅蒐集各式各樣可能影響政、經、軍、心的重大性病毒，並結合國內各大學術機構研究成果，針對各種病毒特性與功能做一個完整詳細的分類與管理。系統建立後，國軍即可在最短的反應時間內，找出具威脅性的病毒類型，並予以解除，應可避免電腦病毒於網域內造成持續性的擴散影響。

(三)專業人才培訓與長留久用

1.「資通電軍」屬國軍高度專業化部隊，其任務特性及屬性亦與一般部隊有所差異。相形之下，人力來源除受限於資訊、資安專長外，也易遭國內廠商如台積電、華碩、宏碁等高科技產業所吸收，使現階段相關單位規模普遍較小，也造成專業人員軍職生涯發展受限，如因調職、升遷因素而離開原體系，恐不利專業人才培訓與長留久用[54]。對此，除持恆強化人才招募與現員留營作為外，國防部亦針對具資安專長的軍事訓練役役男，調整於新訓中心接受基本軍事訓練後，至資通電軍受訓，透過與軍中不同等級人才切磋交流，提升資安技能，也培養團隊默契。結訓後，有意願者可留在軍中發展，如於民間產業發展者，亦可成為資安後備動員戰力，一旦動員徵召，即能加入網路作戰行列[55]。

2.以美軍為例，其陸軍早已與多家中學簽署協議，共同為學生合辦專業網路資訊安全培訓課程，並組織各類網路競賽，遴選培養未來網路戰士；又如美國「空軍協會」(The Air Force Association)每年舉辦的「網路愛國者」(Internet Patriot)競賽，亦吸引全國近2萬名高、初中甚至小學生參

註53：〈電腦病毒資料庫〉，維基百科，2020年9月15日，https://zh.wikipedia.org/wiki/%E7%94%B5%E8%84%91%E7%97%85%E6%AF%92%E8%B5%84%E6%96%99%E5%BA%93，檢索日期：2021年2月27日。

註54：〈揭仲：從中共戰略支援部隊，思考蔡政府的資通電軍〉，端傳媒，2016年7月5日， https://theinitium.com/article/20160705 -opinion-jiezhong-informationandcommunicationsecurity/，檢索日期：2021年3月13日。

註55：呂昭隆，〈網路戰士 國軍秘密武器〉，《中國時報》，2021年3月22日，版A2。

賽，如程度到達一定水準，軍方就主動登門造訪，邀請其參加實習項目[56]，以提升人才培育管道並向下紮根。因此，建議可參考美軍作法，除致力留用現役網路人才外，並充分尊重其專業能力，提供軍中發展利基，或針對網路專長人才，新增、調整或授予相關官科軍職專長，並深入各級院校，運用所提供之網絡安全知識和技能課程培訓，樹立軍方重視網路專業優質人才之形象。

3.除透過軍事教育訓練外，亦可透過民間企業交流、大學策略聯盟或公餘在職進修等方式，增進人員本質學能，鼓勵官兵考取相關資訊專業證照，不僅提升官兵素質，同時透過整體學習氛圍，為未來網路戰奠定基礎。如「資通電軍」於成立初期，即與臺大、清大、交大及臺科大等建教合作，以提升官兵的資安技術和管理能力，並鼓勵官兵和軍校生透過參加各種網路競賽，例如「神盾盃」等，提升相關的資安攻防能力[57]。2021年2月中旬，國軍派出隊伍參加美國主辦的「國際虛擬網路安全競賽」(International Virtual Cyber Security Competition)，與美國等14個全球資通科技領域發展先進國家隊伍較量，在54支隊伍裡突破重圍，取得第一、第四、第六及第七名的佳績，此即是透過參加國際級競賽的經驗，汲取國外網安人才培訓模式、網路攻防訓場發展及各國網路戰發展能量等鮮明、成功的案例[58]。

(四)完備反制軍事假信息法規

1.國軍現階段反制中共「假訊息」，以「逢假必打」、「逢虛必說清」為原則，並編成「反制假訊息快速處理小組」，依照「鞏固心防」、「新聞應處」、「文宣反制」等3個面向，藉由《青年日報》、各軍報刊等平面媒體與「漢聲電台」、網路社群等管道，即時駁斥澄清不實新聞[59]，然而在司法層面，仍有待立法機構協助通過相關法條修正與訂定，強化司法行動的打擊力度，杜絕不實新聞流竄。如同前述有關「2019年共軍演訓被F-16戰機插入中共軍機編隊」、「F-16V採購案數量與經費不正確」、「2020年4月9日遼寧號逼臺」等假消息、新聞，雖然國防部均努力澄清，但訴諸司法都不罰、被駁回或未獲起訴，在在對國軍形象士氣都是重大打擊，不可不謹慎以對[60]。

2.針對「意圖散布於眾，明知而捏造或傳述有關軍事作戰、演習、訓練、武器裝備研製或採購之謠言或不實訊息，致生危害於公安者；或以廣播電視、電子通訊、網際網路或其他傳播工具犯前項之罪者」等《刑法》修正草案內容，國防部業於2019年4月辦理修訂，惟囿於衍生媒體採訪、監督權遭壓

註56：〈美軍如何網羅網絡戰人才〉，每日頭條，2016年11月18日，https://kknews.cc/zh-tw/military/bxk6z66.html，檢索日期：2021年3月13日。

註57：同註52。「神盾盃網路奪旗競賽」(CTF)係由國防部主導，中科院主辦的網路攻防競賽。

註58：〈嚴部長接見國際網安競賽選手 肯定傑出表現〉，軍事新聞通訊社，2021年2月5日，https://mna.gpwb.gov.tw/news/detail/?UserKey=86cd8e0e-fd91-4456-b8d4-2b5928f5df1a，檢索日期：2021年3月22日。

註59：〈反制中共假訊息！國防部設快速處理小組　依3面向即時因應〉，風傳媒，2019年5月2日，https://www.storm.mg/article/1240242，檢索日期：2021年3月17日。

註60：〈修刑法打軍事假訊息惹議 國軍：兼顧言論、新聞自由審慎訂定〉，《自由時報》，2020年4月16日，https://news.ltn.com.tw/news/politics/breakingnews/3135531，檢索日期：2021年3月12日。

縮等疑慮，迄未完成修法。另國防部依敵情威脅，配合各部會檢討反制假信息等相關「依法行政」應處措施，辦理《陸海空軍刑法》有關「軍人造謠罪」內容修正，基於確保言論自由及新聞自由之前題，為免除後續爭議，亦可參考外國立法條例及學者意見，持續與法務部審慎研討訂定修法內容，讓國軍有實質法條依據，藉以遏止假消息流傳散播，亦屬當前重要工作[61]。

伍、結語

我國面臨網路犯罪與駭客入侵癱瘓政府機關網站的案件日益增加，面對近年來網路犯罪及攻擊猖獗，包括透過垃圾郵件、網路釣魚、社交工程、網路詐騙及資訊戰爭等作為，並導致關鍵基礎設施資訊系統中斷、國防資訊洩密、網頁置換及遭受非法入侵的事例屢見不鮮，也常見各種利用網際網路造謠、煽動的網路謠言與聚集活動，造成社會或民眾普遍不安。從現在盛行的網路攻擊手法顯現，國人對於新型態網路犯罪和網路攻擊，及其對國家安全及關鍵基礎設施的威脅，切不可掉以輕心[62]。特別從近年來的網路攻擊事件可以窺知，網路攻擊模式已由原先的單一手法衍生成複合式的攻擊，尤其以進階且持續性的滲透攻擊為最，其具備長期潛伏且不易被偵測的特性，已成為駭客竊取各國機敏資料的主要手段。

現代戰爭隨著資訊科技不斷更新與發展，網路戰不僅是軍事衝突的前哨戰，更成為平時國家基礎建設的城牆、戰時軍事武力致勝的關鍵。未來臺海衝突的趨勢，恐不再只侷限於制空、制海、反登陸及國土防衛等態樣，而是複合式的整體作戰，並由網路與電子作戰貫穿全程。一旦兩岸情勢發生變化，中共勢必積極藉由網路和電磁頻譜技術，發動前置攻擊，先期掌握情資，並癱瘓我方軍事C4ISR系統，以獲取戰場優勢。國軍為有效扼制中共網軍威脅，的確應全面整合有限國防資源，建構多層次安全防護機制，俾得在未來的數位化戰場及網狀化作戰中，能發揮關鍵資訊網路戰力，進而達成網路作戰目標，確保國家及國人的安全。 ⚓

作者簡介：

劉嘉偉少校，海軍軍官學校95年班、國防大學海軍指揮參謀學院109年班。曾任海軍反潛航空大隊海上任務支援中心情報官、大湖軍艦副艦長、海鋒第三中隊中隊長、海軍勤務大隊副大隊長，現服務於海軍艦隊指揮部。

張家瑜中校，海軍軍官學校87年班、美海軍指揮參謀學院100年班、國立臺灣海洋大學海洋法律碩士104年班、國防大學戰爭學院108年班。曾任基隆級艦作戰長、261戰隊支援隊作戰長，現服務於國防大學海軍指揮參謀學院，並為美國戰略暨國際研究中心(CSIS)訪問研究員。

註61：〈對抗軍事假訊息 國防部盼加重刑責〉，中時新聞網，2020年4月5日，https://www.msn.com/zh-tw/news/national/%E5%B0%8D%E6%8A%97%E8%BB%8D%E4%BA%8B%E5%81%87%E8%A8%8A%E6%81%AF-%E5%9C%8B%E9%98%B2%E9%83%A8%E7%9B%BC%E5%8A%A0%E9%87%8D%E5%88%91%E8%B2%AC/ar-BB12EbuH，檢索日期：2021年3月19日。

註62：〈探討網路漏洞產生資通安全之研析〉，立法院網站，2017年3月1日，https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=85429，檢索日期：2021年3月14日。