中國大陸資訊戰對國軍資訊安全威脅之研究

空軍少校　楊鎮瑋　空軍中校　張景翔

提　要

21世紀是資訊戰發展的巔峰時期，也是資訊科技投入戰爭運用的時代，中共為了在新形勢下貫徹其軍事戰略，以達成強軍目標，已具備相關專業部隊，運用資訊網路融合各種作戰力量，打贏網路資訊化戰爭。面臨中共的資訊戰威脅，國軍歷年來雖已建置嚴密的資安防護機制，惟網路攻擊手法不斷精進，整體資安環境所面臨挑戰亦不斷提升，本文透過研析中國大陸網軍資訊攻擊手法，以預見資安威脅之發展，俾利及早提供防範作為，以提升國軍整體資訊戰防護能量。

關鍵詞：資訊戰、網路戰、網軍、資安威脅

前　　言

21世紀是資訊戰發展的巔峰時期，也是資訊科技投入戰爭運用的時代，中國大陸從波斯灣戰爭的經驗瞭解到，現代戰爭受到資訊科技的影響，已經呈現出成長的趨勢。中國大陸曾在18大報告指出，要把資訊化作為軍隊現代化建設發展方向，推動資訊化建設加速發展，加強高新技術武器裝備建設。[1]

2017年中國大陸19大報告中，中國大陸國家領導人習近平也說，中國大陸即將由「網路大國」，轉變為「網路強國」。未來戰爭將以技術科技取勝，在先進科技及技術影響下，戰場空間將更加擴大，傳統的軍事力量與核力量地位急劇下降，隨著資訊科技迅速發展而生的新型兵種已從幕後走到台前，逐漸成為軍事鬥爭中的主角。

2015年中國大陸國防白皮書「中國的軍事戰略」中可以看出，為了在新形勢下貫徹中國大陸的軍事戰略，以達成其強軍目標，必須以國家核心安全需求為導向，著眼建設資訊化部隊，運用資訊網路融合各種作戰力量、作戰單元成為整體作戰能力，打贏網路資訊化戰爭，全面深化國防和軍隊改革，逐步構建作戰要素無縫鏈接、作戰平臺自主協同的一體化聯合作戰體系。[2]

資訊戰相關概述

1 新華社，「胡錦濤在中國共產黨第十八次全國代表大會上的報告」，新華網，2012年11月17日，http://www.xinhuanet.com//18cpcnc/2012-11/17/c_113711665_10.htm (檢索日期:2021年8月3日)

2 萬耀鈞，「中共資訊戰作為之研析-以中共網軍為例」，臺北：淡江大學國際事務與戰略碩士論文，2018年，頁1。

一、資訊戰的演進

(一)資訊戰的緣起與定義

美軍在20世紀末提出資訊戰做為一種新型式的作戰概念，這種作戰概念在軍事領域上的運用是創新的發展。資訊戰的突破主要在於資訊科技與資訊網路的建立與整合，使部隊由傳統作戰演變到資訊化作戰，並結合指、管、通、資、情、監、偵系統(C4ISR)的運用形成軍事力量。波灣戰爭後，世界各國開始重視資訊戰的發展與運用。中國大陸在1980年代中期即發展出資訊戰的思維理念，他們與西方國家的理念大致相同，即透過資訊科技與資訊網路的建立，將政治、經濟、軍事和社會等活動資訊緊密結合與系統化。

資訊戰的定義從廣義上來說，是敵對雙方在政治、經濟、軍事、社會、科技等各個領域之間，以資訊手段獲取戰略優勢的鬥爭和對抗。從狹義上來說，資訊戰為利用資訊技術對敵方進行偵察、干擾、偽裝、欺騙、破壞等行為，以及防範敵人對我採取上述行為的反制措施。美軍對資訊戰的定義為：「干擾敵方資訊、資訊流程、資訊系統、電腦網路，並保全我方資訊、資訊流程、資訊系統、電腦網路，藉以達成資訊優勢的行動」。[3]

國軍對資訊戰之定義：「資訊戰係透過指管程序，藉情報戰心理戰、實體破壞、資訊攻擊、電子戰及傳統武力攻擊等手段，對敵方任何資訊與系統，加以遲滯、干擾、癱瘓與摧毀，並獲取敵方資訊，供我軍運用；同時藉由軍事欺敵、安全措施、資訊防護等方法，保護我方資訊與系統之完整、防止洩漏、瓦解或遭受破壞，支援並維持我軍事決策指揮作戰」。[4]

中國大陸稱資訊戰為「信息戰」，其定義為：「綜合運用信息技術和武器，打擊敵人信息系統(偵察與指揮控制系統)，使情況不明，決策錯誤或放棄抵抗；在此同時採取一切措施，保護自己信息系統不受敵人干擾和破壞，得以充分發揮功能；這種戰爭核心是爭奪制信息權，以掌握戰爭之主動權」。高科技與資訊戰爭已經成為未來戰爭的主軸，交戰雙方保護己方資訊、截斷敵方資訊的能力對於戰爭的最後勝負將有決定性的影響。而此種截斷或保護資訊的能力將依賴軍事技術進行，擁有技術優勢的一方，將有很大的機會截斷敵方資訊，從而成為「資訊壟斷者」，而被壟斷的一方，其作戰計畫、節奏將被完全破壞。也就是，誰掌握科技與資訊優勢，誰掌握了戰場的主動權。[5]

總體而言，資訊戰的定義就是：敵對雙方於平時與戰時，採軍事與非軍事作為，運用資訊技術手段為爭奪資訊優勢而進行的對抗行動。這不但是一種決策及指揮的戰爭，也是一種知識與智能的戰爭，其目的係由傳統作戰觀念的「保存自己，消滅敵人」，轉

3 USA Department of Defense, Department of Defense Dictionary of Military and Associated Terms(New York: USA Department of Defense, 2009), pp.212～213.

4 國防部，國軍資訊發展策略(台北：國防部通資局，2000年)，頁10。

5 李顯堯、周碧松，信息戰爭(北京：解放軍出版社，2000年)，頁145。

變成「保存自己，控制敵人」。[6]

(二)資訊戰範疇

資訊戰不是要殺傷敵人，而是以使敵方屈服為主要目的。所以資訊戰的範疇不僅侷限在武裝衝突，其所涵蓋的範圍可遍布整個社會現象，這個社會現象包括了政治、經濟、心理、科技、宗教、社會、軍事與意識形態等各類領域，資訊戰本質上不受時空限制，其活動範疇為：[7]

1.資訊攻擊(attacking Information)：包括情報戰、心理戰、軍事欺敵、資訊攻擊、電子攻擊、以及實體破壞等。

2.資訊保護(defending Information)：包括心理建設、指管防護、電子防護、安全措施、資訊網路安全、及資訊防護等。

3.資訊管理應用(exploiting Information)：就消極而言就是透過指、管、通、資、情、監、偵系統(C4ISR)迅速獲得一切情資並加以運用，使其成為軍事指揮決策依據；就積極而言，是指在敵方之指揮決策網路體系中發生阻礙、破壞作用。

二、資訊戰特性與運用

資訊及網路安全的維護，隨著資訊科技快速發展，已成為各國新興議題。近年來國軍資訊戰的發展策略，即整合國軍資訊基礎設施，建立三軍通用資訊戰數據鏈路，並結合民間資源，擴大資訊運用；另強化資訊網路安全防護能力，建置主動式資安防禦系統，具備主動預警及防禦作為，確保戰場資訊優勢，發揮最大效益，獲致最後勝利。

(一)資訊戰特性

運用資訊手段，對敵人核心資訊節點、系統及資料庫實施滲透入侵及破壞，以竊取情資或癱瘓運作，擾亂其政策及命令之傳遞，破壞敵方關鍵基礎設施，使人民造成恐慌，進而影響政府的運作機制，此為資訊戰主要特性；同時，要能確保我方資訊網路，不受敵人攻擊。[8]

鑑於網路空間無遠弗屆的特性，人們已可輕易運用資訊技術在網際網路和社群媒體上發揮自身專業能力，不論是個人或團體，均可透由網路對國家外交、經濟與軍事等相關層面造成影響，其影響程度已越來越重大。[9]

(二)資訊戰的運用

美軍在波灣戰爭中，運用資訊戰打擊及癱瘓伊拉克軍隊的指管系統，為資訊戰應用的經典案例之一，伊軍從開戰的第一天起就處於混亂無序，甚至癱瘓的狀態，一直到戰爭結束也未能恢復，在此可看出資訊戰對現代戰爭的影響性。國軍在資訊戰的運用方面，以支援作戰為主要任務，確保部隊指管系統安全正常運作，以「確保國軍網路環境安全」與「厚植國軍網路戰能力」為目標，

6 楊明芬，「中共資訊戰對台灣資訊安全之影響：以網際網路為例分析」，嘉義：國立中正大學戰略暨國際事務研究所碩士論文，2012年，頁22～23。
7 陳友武，「未來電子戰在武器系統發展之展望」，中山科學研究院論文講座，2000年，頁129。
8 林宜昌，「資訊戰對國防衛作戰重要性之研究」，海軍學術雙月刊，第53卷，第6期(2019年12月)，頁117。
9 章昌文，「網路治國的多面向本質」，國防譯粹，第2卷，第43期(2016年2月)，頁14。

透由建立早期預警機制，掌握敵人作戰意圖，防護國軍指管系統安全，阻滯及限制敵攻擊行動，並伺機對敵進行攻擊及癱瘓，有關運用如后：

1.確保國軍網路環境安全

建構安全國軍網路環境，在網路遭受敵攻擊或破壞時，仍可維持正常運作，並正確傳遞指管命令；另加強相關資安防禦機制，防護國軍核心系統運作，確保網路安全提高戰時存活率，其具體措施如下：

(1)建立早期預警機制，針對各類已知及未知網路威脅及攻擊手法建立網路攻防知識庫，並透過跨部會及國際交流機制獲取新的預警情資，早期因應並防範各類網路攻擊威脅。

(2)加強防禦縱深，運用多層次資安防護及備援系統，強化資安防禦機制，確保國軍重要指管系統安全運作。

(3)提升緊急應變處置及復原能力，針對重大資訊網路攻擊事件能迅速反應，並降低災損、限縮受影響範圍及具備立即復原能力，同時確保情傳及指管系統任務運作不中斷。

(4)建立區域聯防機制，與各單位、部會及國際盟友透過網路平臺及研討會分享情資交流合作，共同維護網路系統安全。

2.厚植國軍網路戰能力

平時實施戰場情蒐，運用網路手段針對中國大陸核心系統與目標執行漏洞刺探及偵察，於戰時癱瘓敵關鍵指管及武器系統，擾亂其政治、經濟、軍事、社會秩序，影響及遲滯其政府運作及作戰決策下達，並持續對核心網路系統實施破壞，以削弱敵作戰反應及決策能力，其具體作為如后：

(1)目標偵察：針對中國大陸高價值目標進行刺探及偵察，透過各種網路偵蒐手法掌握目標物風險漏洞並伺機突襲，展現具有震懾之網路作戰能力。

(2)精準打擊：藉傳播假訊息，擾亂中國大陸政策及軍事命令下達，使其誤判情勢；另運用網路攻擊手法對其重要指管及武器系統實施精準打擊，以削弱共軍作戰反應及決策能力。

(3)有效反制：針對駭客發動大規模網路攻擊事件，運用國家整體資訊力量，進行有效反制，確保網路安全無慮。[10]

中國大陸資訊戰發展及運用

一、中國大陸網軍發展經過

中國大陸「網軍」乙詞，最早於1999年《解放軍報》刊登專文就指出，「網軍」很有可能成為繼陸、海、空軍之後的一個新的軍種；同年成立「解放軍理工大學」，專注於培育網路人才，專研信息戰相關理論、技術及積極訓練「網軍」，可謂開始萌芽階段。[11]2001年，中國大陸依「863計畫」完成駭客部隊編組，這是中國大陸最早的一支網軍部隊；另外，為發展「資訊的獲取與網路

10 林宜昌，資訊戰對國防衛作戰重要性之研究，頁118～119。

11 余佳玲、方淑惠，中共科技先驗－從核子時代到資訊時代的國家安全與戰略競爭(台北：五南文化廣場，2006年)，頁245。

監控」，啟動「973計畫」。[12]

2003至2005年，成立「國防信息民兵隊」，結合民間網路高手駭客，培育具高資訊技術能力的優秀人才。中國大陸建立資訊戰力的具體作為，已朝「全民皆兵、平戰結合、軍民兩用」目標發展。[13]2002至2005年期間，中國大陸有6個軍區設立「特種技術偵察部隊」，遂行守勢和攻勢網路作戰。至此，中國大陸已進入到真正具有規模的網路戰部隊，中國大陸網軍已能發展電腦病毒，並攻擊敵人之電腦及系統網路。

近年來中國大陸大量招募專業技術人員組成「網軍」，並運用資訊科技執行網路攻防戰，人才來自學界及業界。[14]2015年底，中國大陸啟動軍改，新組建「戰略支援部隊」，專職從事網路戰攻擊與防護。該部隊成立後，使得網軍部隊得以更集中管理。中國大陸已朝資訊化作戰指揮邁進，並積極培養技術專業作戰人才。中國大陸並意識到網路戰將成為未來的作戰型態，因此資訊能力將攸關資訊作戰的勝負關鍵，將積極培育資訊人才，強化網路戰效能，並將網路戰提升至國家安全戰略層級統一管制運用。

二、中國大陸網軍組成

(一)軍方組織

中國大陸於1999年成立網軍，主要任務為執行各種網路偵蒐、網路攻擊，以竊取各國國防機密。2003年其在「國防動員委員會」下成立「信息動員辦公室」，負責戰時資訊戰所有人力、物力的總動員，並納入民間組織，整合民間資訊力量，從事網路入侵、破壞等工作，同時融合電子防護以達持續作戰之目的。[15]

自2006年以來，中國大陸網軍61398部隊已造成美國多家企業商業機密遭竊取，估計損失約3,000億美元；另自2007年以來，西方國家及其國防承包商的網路系統多次遭受到中國大陸另一支網軍61486部隊的網路攻擊。[16]

2014年，據報導指出，中國大陸另有一支61419網軍部隊，設在山東青島，隸屬總參謀部，專門對日本執行網路偵察、滲透及攻擊。[17]2015年，另一項報導指出，中國大陸另有一支在成都軍區的78020部隊，該部隊已對許多東南亞國家之政府、軍事、媒體和能源公司的網路系統進行滲透。[18]另據美國資安公司的分析報告指出，另外兩支網軍部隊，代號61398及61486的部隊長期對美國等西方國家進行商業和軍事機密竊取。解放軍已擁有多個網軍部隊，職責為執行情資蒐集、分析

12 沈芳祥，新世代解放軍(台北：黎明文化，2003年)，頁240～241。
13 余佳玲、方淑惠：中共科技先驗－從核子時代到資訊時代的國家安全與戰略競爭，頁244。
14 陳育正，「美國網路安全防護經驗-對我國網路安全情勢之啟示」，國防雜誌，第30卷，第3期(2015年5月)，頁78。
15 謝茂淞，亢龍有悔-中共反介入戰略之研究(台北：高手專業出版社，2010年)，頁109。
16 王文勇，「網路防衛戰略方案」，國防譯粹，第40卷，第9期(2013年9月)，頁53。
17 楊家鑫，「青島網軍曝光專司攻擊日本」，中國時報，2014年8月23日，版16。
18 大陸中心，「美給臉色再揭陸網軍竊資」，蘋果日報，2015年9月29日，版7。

及網路攻防戰。

中國大陸網軍主要接受總參謀部的指揮，其組織依任務區分為技術偵察部(總參三部)負責維護網路安全及防制網路間諜，電子對抗部(總參四部)，負責電子情報蒐集、分析、資訊與電子戰之研究、反雷達干擾以及電腦網路攻擊之反擊。

我國《中華民國104年國防報告書》首度證實中國大陸已於各總部、各軍區及國防科研機關等軍事部門部署網軍，具備網路戰攻防能力。這些網軍的主要任務為進行網路滲透及網路攻擊。

2015年底，中國大陸為適應現代化戰爭需求，實施軍改，新增戰略支援部隊，針對網路戰能量整合原總參謀部技術偵察部(總參三部)及原總參謀部電子對抗部(總參四部)；[19]另在聯合參謀部內部設立「信息通信局」整合原總參謀部訊息化部(總參五部)，負責網路攻防戰，調集共軍全國菁英，專門研究各式攻擊手法用於網路滲透及攻擊，預估中國大陸網軍正規軍約7萬人(如圖1)。

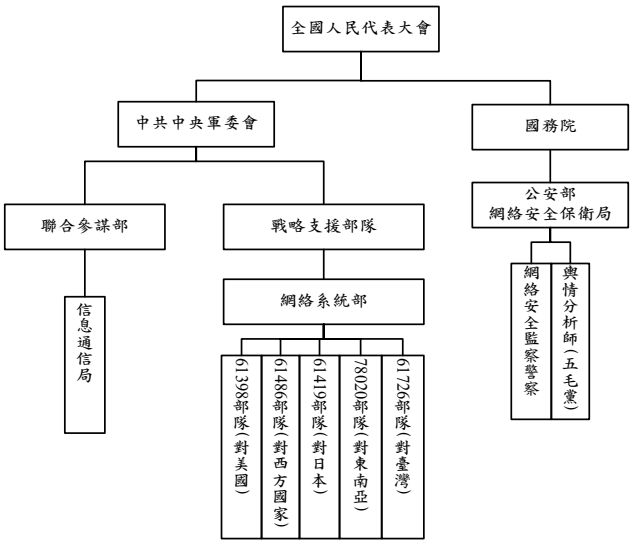

圖1　中共網軍組織圖

資料來源：本研究自行整理。

(二)非軍方組織

中國大陸公安部所屬「公安部網絡安全保衛局」為掌控全國網路安全，於各省、市、自治區的公安廳局下設立的「網監處」，負責區域內網路訊息監督及網路違法犯罪案件查處工作。據2004年非正式統計，中國大陸負責網路安全防護及偵察的相關網路警察，已多達23萬人。另外，各相關網路科研機關人員還有4萬人，總計27萬人員。[20]

中國大陸為落實對國內網路的監控，由政府雇用網路評論員俗稱的五毛黨，他們於各網路論壇宣揚共產黨的重大政策，並對於反對共產黨的評論內容進行過濾與制止或企圖利用子虛烏有的假新聞或似是而非的評論針對特定目標發動攻擊，其每發一則評論便可以獲得一定的報酬。[21]2013年10月，中國大陸首次舉辦輿情分析師培訓，這些人員多半分布在黨政宣傳部門與各大入口網站從事網路監控工作，預估從事輿情分析師人員約200萬人。另據研究指出，中國大陸已招集15萬名民間駭客，從事網路偵蒐並運用各種網路攻擊手法竊取各國國防機密。

19 中央通訊社，「戰略支援部隊作用中共黨媒：致勝關鍵」，中央通訊社，2016年1月24日，https://www.cna.com.tw/news/acn/201601240213.aspx(檢索日期:2021年2月22日)

20 謝璿，「中共網路維穩打手年刪50萬筆貼文」，青年日報，2016年1月18日，版6。

21 謝茂淞，亢龍有悔-中共反介入戰略之研究，頁111。

另外，中國大陸近年來積極規劃及建設網路基礎設施，並廣招民間人才，延攬技術精湛之駭客，將其納入網軍中，並依其專長及視任務需求予以編組，入侵各國網路及資訊系統，伺機截取機敏資料，這些隱藏而無法估計的網路駭客人員，中國大陸俗稱黑客。

綜合上述各項資料，預估中國大陸網軍正規軍約7萬人，若加上民間招集等網路駭客15萬，預估中國大陸網軍將達22萬之多(如表1)。

三、中國大陸網軍作戰能力

(一)攻擊能力

1.滲透攻擊

中國大陸網軍攻擊能力已是有組織具計畫性的針對式攻擊，而非過去單純的情資竊取，透過癱瘓、破壞來完成戰略目標。當前中國大陸「網軍」大量使用「社交工程」手法(如圖2)，針對機敏機關及重要政軍人士，透過偽裝或標題聳動的電子郵件夾帶惡意木馬程式來引誘使用者點取，滲透受害者的電

表1　中共網軍人數統計表

組織	部隊	預估人數	備註
軍方組織	戰略支援部隊、聯合參謀部	7萬人	網路戰攻擊為主
非軍方組織	約僱駭客	15萬人	
	公安部	27萬人	網路戰防護為主
	輿情分析師	200萬人	

資料來源：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14。

圖2　社交工程攻擊手法

資料來源：陳嘉玫，「網路安全的社交工程」，科學發展，第461期(2011年5月)，頁19。

腦，進而突破單位資通安全防禦機制，獲取組織內部網路系統最高權限後，大肆干擾、破壞或癱瘓網路系統等。

此外，中國大陸網軍還慣用「進階持續性滲透攻擊」(Advanced Persistent Threat, APT)(如圖3)，其攻擊方式是由目標的外圍進行滲透、潛伏並伺機攻擊，而非直接朝最終目標進行攻擊。中國大陸為全面掌握政治、外交、國防等動態，除對我政府機關、駐外館處及軍事單位發動網路戰攻擊外，並逐漸轉換思維攻擊較疏於資安防護之單位，如政府委外廠商之網路設施或資訊系統進而取得政府機敏資訊。

行政院前副院長張善政指出，從2009年1月至2014年10月「進階持續性滲透攻擊」(APT)分析，中國大陸網軍為吸引使用者開啟含惡意軟體之信件，配合節慶、政經事件製造釣魚郵件，進行社交工程攻擊，並對總統府等政府單位執行網路戰攻擊。[22]2015年，前國安局長李翔宙曾在立院證實，中國大陸

22 鍾麗華，「張善政：中國將台灣當網攻試驗場「自己的資安自己做」」，自由時報，2015年1月23日，版A9。

圖3　進階持續性滲透攻擊方式

資料來源：iT邦幫忙，「[Day27]攻擊行為－進階持續性滲透攻擊APT」，iT邦幫忙，https://ithelp.ithome.com.tw/articles/10188821(檢索日期：2021年5月4日)。

網軍及駭客已長期鎖定國安局，國安局遭網路攻擊事件每年平均達377萬次。同年，前立委蕭美琴在立法院外交國防委員會爆料指出，2015年3月24日，民進黨中央的網站遭到中國大陸網軍的惡意攻擊，僅5分鐘，就遭到10萬次以上的惡意攻擊，此攻擊手法就是DDOS(Distributed Denial of Services)「阻斷服務攻擊」，就是在遭植入惡意程式的電腦中對目標發動大規模攻擊，讓服務中斷。[23]中國大陸網軍作戰能力已具備阻斷及癱瘓敵方運用資訊網路的能力，並減低對手反應的時間，已對我形成重大威脅。

2.電腦病毒

據美國學者費學禮指出，中國大陸已經發展相關電腦病毒具有摧毀電子電路和資料自動加解密以及破壞無線網路的能力；另中國大陸正研發網路攻擊工具針對「聯合戰術偵報分發(傳送)系統」(Joint Tactical Information Distribution System, JTIDS)數據鏈路系統的指管節點與網路實施反制措施，以利中國大陸網軍發動全面的網路戰攻擊。據報導指出，中國大陸在2015年已研發出一種俗稱「大砲」的網路戰攻擊武器，當外國資訊流向中國大陸網站後，該系統即進行攔截並植入惡意程式，再發送回原目標進行打擊。

美國資安公司邁克菲(McAfee)於2010年對「極光行動」(Operation Aurora)的調查報告指出，美國約30多家公司遭受到網路攻擊，其攻擊手法是利用社交工程方式誘使人員連結到含有惡意程式的網站，並透由惡意程式入侵公司網路進行破壞，經追蹤電腦病毒來源，是來自臺灣的伺服器，其是遭中國大陸網軍植入病毒所造成。

中國大陸發展網路戰，正積極研究新式網路攻擊手法，以提升網路戰能力，確保網路戰優勢，並有計畫地鎖定政府部門、軍事、情報及國安單位進行網路攻擊以癱瘓其運作。[24]

(二)防禦能力

中國大陸為阻擋外界入侵其網路，已採取措施建立相關網路防禦工事。其投入逾10億美元建設網路監控金盾工程「防火長城」，防火長城的主要功用是監控網路上的傳輸內容，對認為不符合中國大陸官方規範的內容，進行干擾、阻斷、遮蔽。

由於中國大陸對網路審查嚴謹及廣泛，國內含有敏感及批評政府等不合規範的網

23 王炯華，「民進黨官網遭駭李翔宙證實是DDOS攻擊」，蘋果日報，2015年3月27日，版7。
24 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16。

站，會受到政府直接的干預，被要求自我審查、自我監管，乃至關閉。另外，中國大陸為掌握官員上網情形，已由北京市平谷區紀委開發出電子監察系統。該電子監察系統透過瀏覽之關鍵字及事項即可找到違規人員的網路IP位址，並馬上對違規的單位及員工進行網路封鎖。[25]

2016年中國大陸為嚴格管控網路新聞資訊，由國務院制定網路新聞資訊管理新規定。據新規定指出，中國大陸網路資訊的監管部門，變更為「網信辦」，作為建立信用檔案和約談制度。同年，中國大陸國家主席習近平視導「新華社」時，要求媒體牢牢堅持「黨性原則」，並要求加強網路監控、升級長城防火牆及大砲等網路安全工作，並落實禁止外企及中外合資公司從事網路訊息服務。

中國大陸目前對網路的控制主要可分為兩個面向，第一是對內控管異議份子的言論，及對外封鎖對黨不利的負面消息，以達到意識形態的控制；第二是防堵美國等西方國家對中國大陸進行網路滲透及攻擊，使其即便遭受攻擊也能藉由防火牆追蹤攻擊來源。

中國大陸領導階層因忌憚開放的網路空間，威脅到共產黨的統治權，已開始將媒體從業人員有系統性的納入「中央」統戰部培訓體系，名單則由中國大陸負責網路安全相關部門決定。中國大陸為了進一步影響全世界，未來可能持續藉由掌控網路言論及自由力道來達成。

我因應中國大陸資訊戰威脅之策略

一、中國大陸資訊戰對我之影響

中國大陸網軍已是一支具有實戰經驗的部隊。中國大陸為確保網路戰優勢，正積極發展網路攻防技術。中國大陸發展網路戰，已從以往單純情資竊取，進展到專精各式網路戰攻擊手法，提升其網路戰能力。中國大陸資訊戰發動方式，係透由網路情蒐及植入惡意程式入侵我政府機關、軍事單位、企業集團及重要民間機構之資訊系統，並利用其事前偵獲之弱點執行網路攻擊，以獲取我國重要情資及破壞系統網路；其攻擊能力如下：

(一)具情資偵蒐能力，所有網路攻擊於發動前都必須做到事前蒐集被攻擊目標的相關情資才有可能達到目的，運用各式網路手段針對我重要指管、武器系統等目標執行漏洞刺探及偵察，竊取我機密情資。

(二)具系統網路破壞能力，透過各式攻擊手法入侵網路系統並植入病毒，直接攻擊、破壞我政、經、軍等資訊系統。

(三)具電磁脈衝癱瘓能力，利用電磁脈衝彈干擾及癱瘓我指管通情及武器系統，影響我系統正常運作發揮效能。

目前中國大陸網軍已具備對我重要指管

25 中央通訊社，「上班點擊千次色情網大陸官員被舉報」，台灣英文新聞，2015年9月15日，https://www.taiwannews.com.tw/ch/news/2804890(檢索日期:2021年2月24日)。

26 林宜昌，資訊戰對國軍防衛作戰重要性之研究，頁122。

常見攻擊	DDoS攻擊 (分散式阻斷服務攻擊)	SQL Injection (資料庫隱碼攻擊)	APT (進階持續性滲透攻擊)
利用弱點	網路頻寬不足與系統效能負荷過大	網站程式撰寫弱點。	各種方式。
攻擊手法	利用各國伺服器跳板或中木馬電腦同時連線網站意圖癱瘓系統	運用網站程式撰寫弱點，進行惡意語法注入，取得網站控制權。	持續且潛伏運用新型攻擊手法。
攻擊前兆	電腦遭植入木馬程式。	事先進行系統弱點掃描動作。	無聲無息，僅能綜合判斷。
防禦步驟	1.監測網路流量有無高於平常值(5Mbit/s)、連線數量有無高於平常值(如監測設定為10,000筆)。 2.監控入侵偵測系統有無系統掃描情形。 3.發現以上行為，進行綜合分析判斷。 4.進行網路過濾，篩選可疑IP進行封鎖，必要時進行網段封，直到流量恢復正常。	1.監控入侵偵測系統發現有掃描行為進行自動化行為阻擋。 2.監控網頁防置換軟體有無跳出警訊。 3.將疊積掃描行為IP納入防火牆黑名單。	1.監控入侵防禦系統、APT防禦資安設備、高階網頁型防火牆，綜合分析攻擊型式。 2.主動瞭解該攻擊入侵目標，參考相關國際資安網頁消息。 3.資安防禦設備發現該行為模式，將行為封包阻斷，並納入防火牆黑名單。
窒礙問題	若遇國際大規模攻擊，將難以阻擋。	須增加監控人員、時常進行軟體版本升級。	須增加監控人員、培養專才人員多角判斷。

圖4　中共網軍攻擊手法及防禦步驟

資料來源：林宜昌，「資訊戰對國軍防衛作戰重要性之研究」，海軍學術雙月刊，第53卷，第6期(2019年12月)，頁122。

系統，執行偵蒐、破壞與癱瘓等攻擊能力，其主要攻擊方式分別有分散式阻斷服務攻擊、資料庫隱碼攻擊及進階持續性滲透攻擊等種類(如圖4)，[26]說明如下：

(一)DDoS攻擊(分散式阻斷服務攻擊)：此種攻擊是阻止遭攻擊目標繼續提供服務給使用者，利用跨國伺服器跳板或遭植入木馬程式之電腦同時連線網站，藉傳送大量封包阻塞網路頻寬進而使系統效能負荷過大，意圖癱瘓系統。

(二)SQL Injection(資料庫隱碼攻擊)：先期針對系統網站執行弱點偵掃，並運用程式碼撰寫弱點，植入惡意語法，取得系統控制權。

(三)APT(進階持續性滲透攻擊)：利用多重攻擊手法，潛伏單位網路，針對關鍵目標實施刺探情蒐，並逐步掌握目標動態，駭客鎖定目標後，便處心積慮蒐集各種可以使用的弱點和漏洞，包含各種社交工程手法與偵測所使用之資通系統漏洞、供應鏈等各種資安攻擊入侵手法等，藉以達到成功入侵組織內部的目的，伺機發動攻擊，竊取其鎖定的資料或進行破壞。

中國大陸意識到未來作戰型態，已成立網軍部隊，積極培養資訊技術專業等作戰人才，以充實網路作戰能力。面對中國大陸網軍的攻擊威脅，我應採取各網系實體隔離及專網專用原則，並於各網系間加強防禦縱深，部署多層次資安防護設備，定期實施系統風險漏洞檢測及各項資安稽核機制，強化執行各項資安管控措施，方能有效防範中國大陸網軍攻擊行為。

二、我國資訊戰之發展現況

自2000年11月20日中國大陸宣布準備將網路戰做為新世代戰爭利器的同時，我國在2001年的4月23日宣布成立第一支網路作戰的隊伍「老虎小組」，[27]主要的任務有二：(一)24小時監控大陸各網站，(二)祕密蒐集與研發新的電腦病毒及攻擊大陸網路系統。2007年政府同時也宣布除老虎小組外，我國還有「國安局」及「軍情局」兩大網軍。

2017年7月1日我國國防部正式成立第四軍種資通電軍指揮部，擔負國軍資訊作戰的重責大任，過去國軍的資訊戰能量是分散在

27 程文理，「資訊戰概論」，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2月24日)

表2　我國網軍概述表

區分	部隊	預估人數	備註
正規軍	老虎小組	30	網路監控與研發
非正規軍	國安局	1500	網路情蒐與作戰
	軍情局	不詳	

資料來源：萬耀鈞，「中共資訊戰作為之研析-以中共網軍為例」，淡江大學國際事務與戰略碩士在職專班碩士論文，2018年1月，頁51。

資電作戰指揮部、電訊發展室以及其他軍種部隊在內的各個不同軍種與單位。鑒於以往為各軍種單兵作戰，國軍資訊戰能量分散無法集中運用，在面臨越來越複雜的網路威脅環境，已不足以發揮有效戰力，因此不僅需要一套完善的情資系統，更需要統合國軍資訊戰能量，並提高其戰略層級與高度，才能夠真正有效因應這些來自數位網路的威脅。資通電軍指揮部成員多來自國防部資電作戰指揮部、電訊發展室以及陸、海、空三軍的資電部隊編制而成，其成立之目的除打造成為一支具有處理網路威脅、緊急應變及作戰實力的軍隊外，更必須要做到：以通訊安全為基礎，以網路攻防為核心，以電磁發展為前瞻的部隊，組織編制下轄資訊通信聯隊、網路戰聯隊、電子戰中心等單位。

除此之外國內政府的網路攻防能量，也是我網路戰能力的一環，就現行的政府網路攻防力量由行政院帶領，設有負責網路安全與防護工作的行政院資安小組；警政署刑事警察局、法務部調查局負責整合產、官、學、民間專業人士，建構「民間網路防護力量」。

行政院於105年8月1日成立資通安全處，由行政院層級統整政府資安治理機制，以專責、專業及專人的方式推動國家資通安全工作，並配合資通安全業務主管機關移轉，技服中心督導機關遂由行政院資通安全處接手，除此之外也設立了關鍵資訊基礎設施安全管理組，將所謂的關鍵基礎八大設施(能源、水資源、通訊傳播、交通、金融、醫療、中央與地方機關、高科技園區)，列入了資安項目，並分主管機關業管，其目的也是為了在面對網路攻擊的時候，明確分工，防止中國大陸及其它國家對我政府網路攻擊事件發生。

國軍的網路戰戰略思維受制於傳統守勢作戰戰略觀點，以網路防禦為重點，雖有網路攻擊能力，但極其有限，與其他西方先進國家相較，更缺乏完善的聯合、統一指揮機制，[28]故在遂行「反制作戰」時，受制於體制與系統，難以掌握先機，更因過度著眼處處防備，造成備多力分困境，未能統合各軍種能力，無法淋漓盡致發揮網路戰能力。雖然我們效法美軍2010年5月21日成立的「網路戰司令部(Cyber Command, CYBERCOM)」的精神，成立所謂的「資通電軍」軍種，其目的也是希望整合國軍現有資電作戰與民間能量，補強國軍資訊作戰能力，進而使國防相關的資產與基礎設施免於組織性駭客與恐怖分子的網路侵襲。

三、我因應中國大陸資訊戰之作為

28 程文理，資訊戰概論，http://www.ewmib.com/news.php?news_id=124&cate_id=9(檢索日期:2021年2月24日)

隨著資訊科技的進步與發展，網路空間已成為新的戰場，網路作戰已成新型作戰型態，其對軍事嚇阻、戰力投射及戰略威脅，具有相當程度的影響力，面對中國大陸資訊戰威脅，國軍須重視我資訊戰能力，建立實質嚇阻力量及有效反擊能力，以確保國軍網路及指管系統運行安全，支援作戰任務，並有能力反制敵攻擊作為，相關應處作為說明如后：

(一)落實「實體隔離」政策

國軍網路屬封閉性網路，可有效降低外來威脅及風險，為避免駭客透過網際網路入侵國軍網路，應嚴格落實軍、民網路「實體隔離」政策，並精進「資安防護管理機制」，運用防護管控作為，杜絕各種可能之駭侵行為。

(二)定時實施資安稽核作業

依年度排程定期針對所屬單位進行資安稽核作業，協助提升單位資安防護之完整性及有效性，從「策略面」、「管理面」及「技術面」3個構面進行稽核，稽核項目包括：「機關首長對資安業務之支持度」、「資訊委外安全管理」、「所屬機關監督管理」、「資安事件通報及處理」及「資通系統開發及維護安全」等項目，[29]並藉年度重大演訓規劃之網路攻防演練，驗證「指管系統」及「關鍵資訊基礎設施」防護強度，以為後續資安整備之參據。

(三)網路戰實兵演練驗證防護作為

藉網路戰實兵攻防演練，運用弱點偵掃、社交工程及滲透攻擊等方式，實際驗測國軍各單位之通資系統與網路防護能力，演練單位依既有之資安防禦機制，針對攻擊事件執行應變處置及防護作為，藉以驗證其處置程序及防禦機制是否周延，並針對遭驗證成功者，持續檢討、精進及驗證，以強化我整體資安防禦作為。

(四)完備資安應變處置

為確保通資系統於遭敵網路攻擊致癱瘓時，我重要指管系統要能持續發揮效能，使作戰任務不受影響，各單位平時應依資料重要等級，定期規劃各系統備份週期，並建立異地備援及備份機制，使重要系統於受損後，立即啟動備援系統，迅速接替任務運作，縮短受影響時效，確保作戰任務不中斷，並配合行政院執行資通安全事件應變、處置及相關演練作業，俾適時調整回報、處置與復原等機制與程序。

(五)強化人員資安意識

回顧國軍這幾年來的資安違規事件，大部分是因人為疏失所造成，故資安防護基本應處作為，為逐級建立資訊安全觀念，為避免中國大陸網軍利用社交工程手法攻擊造成機敏資料外洩，各單位應持續提升人員之資安意識，宣導使用者注意郵件來源之正確性，勿開啟不明來源郵件之附檔或連結，勿使用公務郵件帳號註冊外部服務，並應定期更新作業系統弱點修補程式以及防毒軟體病毒碼。

(六)強化委外廠商資安督管機制

29 行政院，「108年國家資通安全情勢報告」，2020年6月，頁12～13。

維護廠商提供機關之資通設備，因未落實適當檢查與管制，導致存有惡意程式，利用機關網路進行中繼站連線，或委外廠商遭感染勒索軟體，透過遠端存取擴散至機關等事件。為避免國軍單位委外供應鏈遭受攻擊之情形，應針對委外廠商之資安及監督管理機制加強要求，定期對資通系統進行系統更新、源碼檢測及弱點偵掃，並配合系統開發廠商之漏洞修補程式，即時進行修補。

(七)培育專業網路戰人才

資訊技術需靠不斷學習及持續精進，方能面對未來新型網路威脅變化及挑戰，故人才培育方面應建立制度化的培訓機制，針對資訊人員分級訓練，藉由開設專業技術班隊或編列預算，將人員派送政府或民間專業機構學習相關網路進階駭客攻防技術課程並取得相關專業證照，並積極建立優質專技人才資料庫，此對國軍網路戰能力的向上提升具正面且長遠發展意義，以此建立網路戰穩固之戰力。

(八)建置相關研發機構

要使網路作戰發揮最大的效能，首先就必須先具備好的人才及裝備，一個網路作戰系統通常包括三部分：硬體、軟體及通信，只要任何一個部分出現漏洞，就可能威脅到整個系統的安全。建議我資通電軍指揮部單位，如要與中國大陸的戰略支援部隊相抗衡，可效法美國的網路部隊，成立相關的研發機構，這樣方能爭取最大相關研發經費及能量，使現有部隊能專注於執行任務，發揮建制效能。[30]

(九)結合民間資安能量

我國為強化國防科技能量，使民間科技人才適時支援軍事作戰，根據《全民防衛動員準備法》及《科技人才支援軍事勤務辦法》資訊人才為科技動員對象之一，國防部可因應實際需要挑選合適之科技人才，予以編組、演訓，納入科技動員人力資料庫，掌握相關科技物資與人才資源，一旦需要動員相關的資安人才提供協助，可以精準掌握並立即徵用動員，強化軍民合作，達到整體資安聯防之效。[31]

(十)定期檢討國軍資通能量

透過國防部定期召開之網、通安全會報研討年度重大資通工作成效，並針對國軍所面臨之資通安全威脅現況，研擬相關資安防護建議，同時要求各單位落實政策要求，強化資通核心安全，建立有效的資安防護網，期望藉由會報之研討，持續加強國軍資安防護意識，提升國軍資安防護能量。

結　　論

網路作戰結合現代各式戰術戰法，是現代戰爭中決勝的利器。未來戰爭是力求戰力整合的時代，且近年來網路作戰引發人們心理畏戰且懼怕的高度發展。中國大陸各研究機構不斷研發資訊戰的理論、戰法與戰具，並透過部隊演訓予以驗證。

30 萬耀鈞，中共資訊戰作為之研析-以中共網軍為例，頁67～68。
31 科技部，科技人才支援軍事勤務辦法。

就我國現今的資訊科技技術而言，運用在資訊戰作為上，是擁有足夠展開資訊攻擊與防衛行動之能力，尤其是針對電腦網路作戰方面。由此可知，資訊網路作戰是我方較佔優勢的武力，亦可能是贏得戰爭的關鍵，在中國大陸的高科技條件下的局部戰爭規劃中，與其每日擔心中國大陸的導彈指向、軍機的防空識別區越界等事件，還不如學習中國大陸的網軍部隊如何能在決勝於千里之外的對岸，使用網路病毒、滲透、操控及癱瘓等攻擊手段，對敵對國家及政府的基礎設施實施網路大規模的作戰能力，來得比較經濟且有效些。[32]

資安威脅日益嚴峻，國軍歷年來雖已建置嚴密的資安防護機制，惟網路駭客(含網軍及其周圍組織)手法及惡意程式不斷精進，整體資安環境所面臨挑戰亦不斷提升，除加強全軍資安教育，提升資安危機意識外，並持續掌握新型網路威脅型態，綿密各項資安管控機制，以提升國軍整體資安防護能量。

國軍可藉由年度定期之資安稽核、技術檢測及攻防演練，期能兼具深度與廣度檢視國軍資安防禦之完備度與韌性；另透過研析新興資安議題與資安攻擊手法，以預見資安威脅之發展與趨勢，同時洞悉未來資訊科技應用之資安風險，俾利及早提供防範作為，爭取我作戰時空優勢，並運用多重攔截及網路阻斷方式，遲滯敵作戰節奏，為國軍爭取反制作為。

作者簡介

楊鎮瑋少校，空軍航空技術學院二技95年班、國防大學管理學院資管碩士101年班。曾任資網官、資參官、分隊長。現任國防大學空軍指參學院少校學員。

張景翔中校，大葉大學資管碩士，曾任連長、作戰長、隊長、教官。現任國防大學空軍指參學院中校教官。

UH-60M型救護直升機(照片提供：葉秀斌)

32 萬耀鈞，中共資訊戰作為之研析-以中共網軍為例，頁63。