軍事國防

中國大陸網路戰作為之研究

空軍上校　黃獻忠、陸軍中校　王健民

提要

現今電腦使用普及，網路已成為資訊傳輸的主要途徑，網路作戰已是一場看不見的砲火戰爭，美國前國防部長潘內達就曾以「未來戰場在網路」論述告訴世人，爭取網路作戰優勢將是未來決勝的重要關鍵。為了建構足夠網路作戰能量，全球至少已有四十六個國家成立相關網路作戰部隊，對網路戰場的攻防無人再有疏忽之意，各國對網路世界紛紛藉由投入經費與擴編人力，俾以鞏固網路安全防線。尤其近年全球一再發生網路駭客入侵事件，對此事件發生所有矛頭均指向中國大陸，也因此多數先進國家在資安領域上均不敢掉以輕心。

中國大陸積極發展信息化軍事作戰能力，最佳因應之道乃全面建構資訊時代戰爭的戰場管理能力，將組織、人(指揮官與參謀群)同步提升至具備資訊時代戰爭的戰場管理能力，始能適應各種潛在威脅與挑戰。面對中國大陸網軍威脅，我們除應積極建立國家層級資訊戰指揮體制外，並應強化資訊暨基礎作戰能力、推動資安認證提升資訊系統安全防護網、具備監偵及反偵蒐全軍節點能力防止指揮管制機能遭破壞、結合C4ISR指管通情系統建置聯合作戰資訊戰反制能量、研發安全保密通道與加密技術確保資料安全等，以確保國軍資訊安全與國防整體戰力。

關鍵詞：電腦病毒、網際網路、駭客、網路戰、網軍

壹、前言

隨著電子科技產業及網路科技的蓬勃發展，使人類生活添增許多的便利，伴隨著網際網路普及，上網幾乎已成為人類生活上不可或缺的行為。【註1】但也成為不肖人士或特定組織藉由網路工具，針對特定個人、公(私)營企業及政府機關之資料或重要設施進行竊取或破壞。【註2】

近年多則新聞媒體報導中國大陸解放軍中有為了網路活動而被訓練出來的駭客與組織存在，美國某網路安全公司於2013年3月甚至公開指出，中國大陸網軍位於上海浦東的61398解放軍駭客部隊【註3】是竊取國家軍事及商業機密的元凶。【註4】同年3月20日國安局發表：中國大陸網路攻擊臺灣的情況非常嚴重，竊取目標除了政府、軍事單位，現在還包括高科技產業機密資料，而且模式也從竊取資料轉為發動攻擊，破壞基礎建設。2014年5月美國FBI通緝起訴61398部隊5軍官間諜罪，這群解放軍中的駭客菁英被稱作「網路藍軍」，他們的任務是保護國家免受網路攻擊，同時致力於防禦和攻擊。中國大陸國防部發言人在一份新華網上的資料中宣稱：「這個團隊是為了提升武力的網路安全而建立的，網路安全是一個國際性的問題，他影響了民間和軍事區域，而中國大陸在網路安全保護方面還是屬於相對弱勢的，也極可能受到網路恐怖攻擊的傷害。」。【註5】

「網路」戰爭將是世界舞臺上新世紀的主角；網路戰乃為資訊戰之重要一環，開放式觀念及主從式架構成了現在網路應用的趨勢。如何保護我國不會受到網路病毒與駭客攻擊的傷害，所以我們在網路戰這個課題上，較如何使用網路戰來攻擊中國大陸更為重要；中國大陸發展「網路戰」不遺餘力，國軍必須採取積極之作為，以有效遂行未來網路資訊作戰。【註6】

貳、中國大陸網軍任務與現況

註1　湯君年。〈網路恐怖主義對國際網路安全之影響〉。國防大學政治作戰學院，碩士論文，2011年6月。

註2　莊芳昇。〈網路蠕蟲主動防禦機制之研究〉。樹德科技大學，碩士論文，2006年6月。

註3　根據美國曼迪安網路安全公司(Mandiant Internet Security Corp.)報告指出「61398部隊」是中國網軍大本營，企圖掌握美國基礎設施並竊取資訊，例如：電 網、供水廠、變電所、汽油及天然氣設施等。61398部隊的正式稱謂是人民解放軍總參三部二局，在官方對中國軍隊的描述中，幾乎找不到它的存在。

註4　「駭客」為無組織之個人網路破壞者，其所施行之網路攻擊多為個人利益或追求成就感而為之；然「駭客」部隊乃是共軍吸納具有資訊網路專才的科技人員，加以有組織之訓練編組，而針對其對手進行攻擊的人員，這些進行非直接戰鬥的資訊作戰人員，是可配合共軍軍事行動的，亦即是解放軍之「網軍」。

註5　2013年2月，《China vs US, cyber superpowers compared》，臺灣電腦網路危機處 暨協調中心。

註6　行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，臺北:五南文化出版，2002年。

中國大陸「網軍」一詞是在西元1999年中國大陸解放軍報上首次出現，中國大陸在西元2015年國防白皮書中，在「軍事力量建設發展」項次中對網路空間特別強調：「網絡空間是經濟社會發展新支柱和國家安全新領域。網絡空間國際戰略競爭日趨激烈，不少國家都在發展網絡空間軍事力量。中國大陸是駭客攻擊最大的受害國之一，網絡基礎設施安全面臨嚴峻威脅，網絡空間對軍事安全影響逐步上升。加快網絡空間力量建設，提高網絡空間態勢感知、網絡防禦、支援國家網絡空間鬥爭和參與國際合作的能力，遏控網絡空間重大危機，保障國家網絡與信息安全，維護國家安全和社會穩定。」【註7】。

一、中國大陸網軍的任務：

就如何達到國防白皮書所強調的目標而言，目前中國大陸「網軍」的任務共區分：

平時：利用駭客技術獲取他國的政治、經濟、軍事情報。

戰時：侵入敵方指揮網路系統，控制敵方的指揮系統，或實施電腦病毒戰、癱瘓敵方網站。運用各種手段施放電腦病毒直接攻擊，控制或摧毀敵方武器系統。同時運用病毒、駭客攻擊敵國要害部門，如金融、交通、電力、航空、廣播、電視、政府等網路系統，製造社會動盪，使敵方顧此失彼，以達到「不戰而屈人之兵」的目的。

對內：模擬各類網路攻擊手段，測試己方各單位(部隊)通資網路安全漏洞、研發網路戰新戰法，並協助研究機構研發網路戰安全防護及測試作業系統安全性。

對外：從事網路實際先期攻擊測試，掌握目標，俾利攻擊發起時可迅速癱瘓敵方網站，獲取資訊影響心理，並結合電子戰，形成網電一體，獲取信息戰優勢。也就是在於能否有效進行電腦網路的攻擊或防禦的網路戰，專門負責資訊戰中的網路心理戰、駭客戰和網路襲擊戰。【註8】

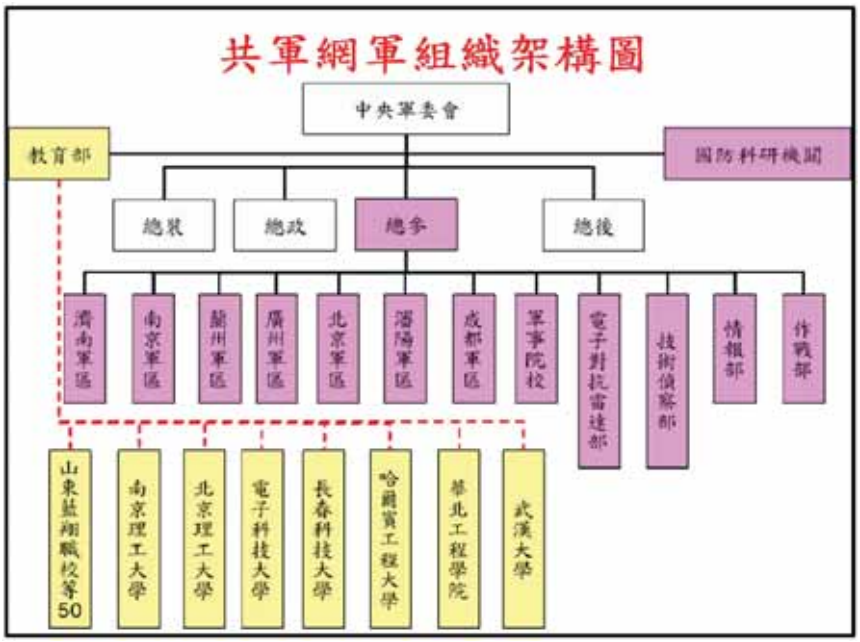
此為中國大陸為了因應超限戰，建軍方向朝向陸、海、空、天、電、網一體化的作戰方式發展，而「網軍」可能是繼陸、海、空及火箭軍之後，成為解放軍的下一個軍種。【註9】

註7　〈中國的軍事戰略白皮書全文〉，《東森新聞報》，2015年5月27日，版4，網址：http://www.ettoday.net/news/20150526/511925.htm，檢索日期：105年4月28日。

註8　黎兆煒，〈共軍發展「網電一體戰」之能力虛實研究〉，《淡江大學國際事務與戰略研究所碩士論文》，101年1月，頁1-3。

註9　楊曉欣，〈中共網軍對我資訊安全威脅之探討〉，《清流月刊》，96年10月號，網址：http://www.sec.gov.tw/cncj/CNCJ0602/cncj0602_09611.html，檢索日期：105年4月18日。

在中國大陸方面，非軍事的駭客組織聯盟計有國際駭客聯盟、歲月聯盟、駭客基地和華夏駭客同盟等，因相互之間競爭，可想而知其撰寫惡意程式來攻擊他人網站或電腦的能力已經越來越強。目前中國大陸已有數萬人可自行撰寫木馬、後門、病毒等程式，而且他們不只是寫單一的病毒，而是寫「病毒產生器」，讓其他人可以輕易地製造病毒，使得病毒的數量一直居高不下。也就是說未來資訊安全將面對的是更棘手的局面及更難纏的病毒。這些人難保不會被中國大陸軍方納為所謂地下網軍，如西元2013年2月美國麥迪安網路安全公司發佈的報告，總結141個主要駭客攻擊的反跟蹤分析，認為中國大陸人民解放軍61398部隊和多次從事進階持續性滲透攻擊的駭客襲擊有密切關連，並披露其實際地理位置是中國大陸解放軍駐紮在上海的一座塔樓，隸屬於解放軍總參謀部三部二局，此報導當然受到中國大陸國防部否認，但可想而知這是中國大陸一貫的手法，先做了被發現堅決否認，最後瞞不住了再用另一個說法圓過去，紙是包不住火的早晚會被戳破。【註10】



資料來源：筆者自行整理；實線表直屬管制單位，虛線表中國大陸將網軍藏在校園內或從事網軍培育。

圖1　解放軍網軍組織架構圖

二、中國大陸網軍的現況：

據國安局2014年11月20日資料顯示中國大陸「網軍」多達18萬人，中國大陸解放軍負責網路戰的單位包括：解放軍總參謀部、7大軍區、國防科研機

註10　〈揭秘中國網路戰部隊〉，《紐約時報中文網》，2013年2月19日，網址：http://cn.nytimes.com/china/20130219/c19hack/，檢索日期：105年4月30日。

關、各級院校等(如圖1)，負責統合相關部會職能，平時主責網路竊密滲透，戰時負責網路攻擊，並且暗中扶植民間駭客組織，從旁協助網路間諜活動，【註11】另還成立「中央網絡安全及信息化領導小組」，以統合相關部會職能，藉由頂層設計、統籌規劃、創新發展等，將中國大陸建設為網路強國。【註12】

解放軍總參謀部為和平時期電腦網路攻擊的核心平台，戰時成立「信息對抗中心」，這個單位由各軍種指揮官及幕僚所組成，負責信息對抗、計畫及整合信息系統，以及引導和整合各個作戰群層次的信息對抗工作提供建議。同時也是綜合策劃、電子對抗、網路戰、信息系統防衛、情報的防護與保密、武器與裝備支援、和綜合支援部門的綜合體。【註13】由此可見中國大陸網軍從軍方、民間、學校三個方面吸收培養人才，並時常進行組織化的於國內與國際間試兵練兵，藉以提升其網攻能力。

試想中國大陸有組織的網軍單位就如此龐大，如發起大規模網路攻擊，癱瘓我國電腦系統、竊取我機密資料、攻擊民眾生活基礎設施、大規模停電、醫院記錄造假或水庫大壩被操控造成特大洪水等方式，造成國人恐慌，不僅初期國人會誤以為遭受網路恐怖分子攻擊，以達到其階段性的任務引起國內慌亂，進而拓展進行下一個階段的攻擊任務，或全面發起網路作戰。

參、中國大陸網路戰作為與未來發展

美國總統歐巴馬在美國的國情咨文裡提到嚴加防範駭客對本土的攻擊，美國白宮的作戰司令部受到駭客入侵，惡意程式攻擊追查來源是中國大陸上海浦東大同路208號十二層樓高的駭客部隊61398部隊。中國大陸組建「網軍」部隊新兵種，並且重點培訓具高科技作業能力的優秀人才，列為培植人才的「863專案」。不只有軍方人員，學術機關及民間企業也在解放軍總參謀部第二部的資助下，執行對國外政府機關的網路滲透作戰。61398部隊所屬的總參謀三部，即為總參謀部第三部，負責監聽與處理國外通訊傳播訊號任務，先後攻擊了美國白宮、五角大廈、太空總署NASA及美國太平洋司令部。

註11　〈中共建構網軍專責防禦攻擊〉，《國防部軍事新聞網》，2007年9月28日，網址：http://news.gpwb.gov.tw/news.php?css=2&rtype=2&nid=26216），檢索日期105年04月12日。

註12　謝莉慧，〈國安局證實中共「網軍」多達18萬人〉，《頭殼newtalk電子報》，2014年11月20日，網址：https://tw.news.yahoo.com/%E5%9C%8B%E5%AE%89%E5%B1%80%E8%AD%89%E5%AF%A6-%E4%B8%AD%E5%85%B1-%E7%B6%B2%E8%BB%8D-%E5%A4%9A%E9%81%9418%E8%90%AC%E4%BA%BA-063307540.html，檢索日期：105年4月3日。

註13　R0y Kamphausen/David Lai/Andrew Scobell，〈超越臺海—臺灣問題外的解放軍任務〉，《國防大學譯印》，100年6月翻印，頁235。

一、中國大陸網路戰作為：中國大陸前軍委主席江澤民於1999年7月下令組建了「解放軍信息工程大學」，顯然有意將此學院做為「網軍」培訓搖籃，這是全世界第一所資訊戰專業軍事學校，稱它做「駭客大學」亦不為過。【註14】「網路戰」從駭客「人不分男女老幼」、「地不分東南西北」的特性可得知，解放軍作為中國大陸發展「網路戰」主力，因而中國大陸本身也易成為「網路戰」目標，自然投注最多人力、物力軍隊建設及演訓，有下述作為：

(一)電腦病毒攻擊：所謂電腦「病毒」即是一種人為破壞性程式，它的型態有：

1.「定時炸彈」型：此種病毒會先潛伏在對方網路，等到特定時間才會開啟破壞作用，例如中國大陸可對某國的網路植入此種病毒，該病毒會在解放軍入侵前一刻才對敵國C4I系統發動攻擊，癱瘓對方作戰指揮體系，以配合正規作戰，不過此種攻擊型態還是有可能被發現而加以防止。

2.複製超載型式：此種病毒侵入後會大量不間斷的自我複製，致使主機超載而無法工作，美國多個大型網站曾於2000年2月受到此種病毒攻擊而停頓，而此種網路攻擊型態雖然是破壞性較小，但也是最難以防禦的，因為網路主機永遠不可能拒絕接受外來資料，此種手段可以輕易突破最高級的防禦措施，暫時癱瘓對方主機。

3.間諜入侵型式：此種病毒進入對方主機後，會按程式設計並竊取特定文件，而自動轉發至特定地點或公共WI-FI網路，此類手法亦可用來攻擊金融機構主機，將竊取主機內的資料(帳戶)，大規模的入侵將造成被入侵國經濟混亂。

4.邏輯潛伏型式(Logic bomb)：邏輯炸彈型態類似「定時炸彈」，同樣藉由潛伏在對方主機中等待時機突擊，只不過邏輯炸彈攻擊能力更強，可以在發作時完全控制對方主機而為所欲為，例如中國大陸可以將此一病毒潛伏於某國戰管系統中，邏輯炸彈型可以在需要時控制戰管系統，對戰管系統下達錯誤指令，造成對方發生誤擊敵機(艦)等混亂事件；邏輯炸彈型亦可潛伏在敵國民用交通管制系統如航空管制或捷運控管電腦中，誤導資訊令其發生大量重大交通意外，造成被入侵國社會秩序完全失控。

(二)電腦破解滲透：滲透和入侵一向是駭客最愛，因為可神不知鬼不覺竊取資料、控制、監看、獲得對方主機活動，其方式包括：

1.應用密碼破解技術，突破防火牆和電子安全措施，而後可自由竊取機密訊

註14　沈偉光、解璋、馬亞西，《信息化軍隊-未來戰爭的主角》，北京:新華出版社，2003年。

息。

2. 使用硬體滲透，在電腦設備上預先裝置接收晶片，待被入侵主機運作，機密便會自動洩密。
3. 控制對方主機網路，此種滲透難度較高，不過一旦控制對方電腦設備，形同於網路遠端指揮的武器、措施拱手送人。

(三)自主系統研發：中國大陸自2000年起，為區別美國微軟及IBM等主力大廠之電腦作業系統，自力開發出一套更安全的電腦作業系統麒麟(Kylin)，並於近年逐漸用於政府和軍事戰位電腦系統，希望能防堵美方和情報機關入侵發動網路戰的企圖；如此亦說明中國大陸政府對於與美國進行網路戰所做的準備，它「強化」中國大陸重要伺服器，而美國的網路戰能力向來著重針對採用較不安全的作業系統如微軟系統，因此麒麟降低了美國對中國大陸的攻擊能力。正如中國大陸電腦駭客大舉攻擊美國電腦系統之際，「中」、美和俄羅斯的網路戰能力相當，加強電腦和資訊網路的保護是較顯著的方式。

(四)針對重點打擊：網路戰主要的打擊目標可分為軍事與非軍事目標。而軍事目標有：C4ISR系統指揮下軍種及偵察預警設備，一旦C4ISR落入敵方駭客手中或遭癱瘓，三軍形同喪失指揮系統和耳目，非軍事目標有：

1. 政府網站——竊取重要個資：中國大陸軍事理論認為以電腦病毒或滲透的方式竊取敵國國防機密，而非軍事目標的政府機構亦同樣有價值，因為在所謂全面推行「電子化政府」後，大部分的政府將會資訊化資料，入侵者便有機會從網路上竊取諸如首長個人資料、犯罪資料、民眾稅務戶政資料和軍民兩用科技等政府機密。
2. 輸運系統——破壞交通管控：引發人為災害和社會秩序動亂邏輯炸彈最佳攻擊目標之即為交通運輸管控系統，在現代化國家大眾交通運輸工具(如飛機、火車和捷運)系統多半重度倚賴電腦系統操作及管派，交通運輸系統是整個現代化國家經濟社會命脈，此系統出問題後果將十分嚴重，在遭到邏輯炸彈攻擊後，電腦將被邏輯炸彈接管，而造成大量陸空交通意外，造成被入侵國交通完全停擺和社會秩序大亂。
3. 經貿機構——引發金融動亂：中國大陸稱此種戰術為「金融戰」，駭客可以入侵國際金融交易網路，入侵之後在一瞬間鉅量「買賣」敵國貨幣，令其經濟一夕間「泡沫化」，東南亞金融危機給了中國大陸軍事理論界一個很好示範，駭客只是在網路中灌輸不實數字而已，然而事實上根本沒有「買賣」可言。

4. 輿情管控——內部輿論封控：中國大陸政府習慣封鎖所有的消息，並且驅逐國外記者。所有中國各級媒體均採用CCTV與新華社的通稿，不准私下進行任何報導，於是全世界的人都無法獲得突發事件的任何最新消息，事件的詮釋權就落到中國大陸官方的手裡。若在中國大陸境內，輕則行政拘留與罰款，重則交予國安部門判刑下獄。若訊息發生在國外，中國大陸官方政府則會發動輿論戰，駁斥境外的報導為捕風捉影的惡意中傷，因為當時國外的記者早就被趕出事件發生的現場。

二、中國大陸網路戰未來發展方向：

中國大陸於2006年5月8日發布《2006至2020年國家信息化發展戰略》，【註15】具體指出中國大陸未來15年資訊化發展的策略目標，「為普及資訊基礎設施，顯著增強資訊技術自主創新能力，大幅提高資訊安全保障水準，全面優化資訊產業結構，獲取新型工業、經濟和社會的資訊化發展，提高資訊技術應用能力，完善資訊化發展制度、環境與政策體系，邁向堅實資訊化社會」。【註16】該文件不僅具體規劃出中國大陸資訊化發展藍圖，掌握自主知識產權的關鍵技術，並總結出中國大陸資訊發展狀況。因此中國大陸國防建設及軍隊信息化獲得重要進展，解放軍得以建構與發展極為廣泛的軍事信息系統工程，提高主戰武器與系統的信息化與數據化，並深化軍事信息基礎建設，建立信息安全管理體制和工作機制，增強信息保障能力。儘管如此，解放軍為因應網路戰威脅，於2010年6月嚴令全軍禁止製作個人網頁、網路社交、設立部落格、網路聊天和約會，即使休假也不允許，並於2010年7月19日成立「信息(資訊)保障基地」(隸屬總參謀部)，以因應網路威脅。【註17】面對中國大陸積極發展信息化軍事作戰能力，最佳因應之道乃全面建構資訊時代戰爭的戰場管理能力，將組織、人(指揮官與參謀群)同步提升至具備資訊時代戰爭的戰場管理能力，始能適應各種潛在威脅與挑戰。【註18】

現在全球人類除了電腦可以上網外，人手一機的智慧型手機更是駭客攻擊

註15 〈2006-2020年國家資訊化發展戰略〉，《中國網》，2006年5月8日，網址：http://www.china.com.cn/chinese/PI-c/1203246.htm，檢索日期：105年4月29日。

註16 李比奇(Martin C.Libicki)、包克文(Kevin L. Pollpeter)，《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。

註17 周宏仁主編、徐愈副主編，《中國信息化形勢分析與預測》，北京:社會科會文獻出版社，2010年。

註18 國防部史政編譯局譯，費學禮(Richard D. Fisher Jr.)，《中共軍事發展-區域與全球勢 佈局》(China’s Military Modernization- Building for Regional and Global Reach)，臺北：國防部史政編譯局，2011年。

目標，也悄悄的轉移到可以獲得更多重要資訊及商機的新目標；在暢行無阻的網路國界中，重要關鍵資訊基礎建設保護更突顯它的重要性。社群網站上揭露個人資訊，各種網路攻擊手段、社交工程、後門程式隨時都可能感染安裝在我們所使用的資訊設備上，根本防不勝防；組織型網路犯罪與詐騙行為顯著上升；基此，行動裝置(如手機、平版電腦)市場蓬勃發展逐漸成為網路犯罪者的更大目標。【註19】

互聯網發展賦予了國家主權、安全、發展利益新的內涵，中國大陸要維護自身利益就不能忽視互聯網產品和服務的主導權、控制權和全球話語權。首屆世界互聯網大會於2014年11月19日在浙江烏鎮開幕，大會以「互聯互通，共享共治」為主題，是中國大陸舉辦的規模最大、層次最高的互聯網大會，可視為中國大陸政府為國際互聯網搭建的新平台。

目前，全世界網民數量達到30億，普及率達到40%，世界真正變成了地球村。互聯網是把雙刃劍，用不好，它是潘多拉的魔盒；用得好，它是阿里巴巴的寶庫。中國大陸已然是互聯網大國，但要由大到強要有自己的技術，有強勢的技術。網際網路發展至今，關鍵核心的技術基本都掌握在西方國家手中。例如，連接網際網路的13台根服務器，美國就佔了10台，而作為互聯網用戶最多的中國大陸1台也沒有；這意味著不掌握核心的強勢的技術，就容易受制於人。【註20】要有良好的網路基礎設施，形成實力雄厚的網路經濟。網路經濟是與農業經濟、服務經濟及工業經濟緊密聯繫並相互促進的。因此，要發展壯大網路經濟，就必須加快發展後三者的網路化。

肆、對我防衛作戰可能之影響

中國大陸一篇研究臺灣發展網路戰的專論中，指出臺灣在網路戰方面有五大弱點：【註21】

- ■臺灣社會網路化程度高及網路發達，但在所有的政經、科技和軍事事務均過於依賴網路。
- ■地理位置狹小、無迴旋空間，抗打擊能力薄弱。
- ■軍事信息系統主要仰賴進口、對外依存度過高。

註19　東鳥，《網路戰爭:互聯網改變世界簡史》，北京:九洲出版社，2009年。
註20　立法院，《我國如何因應網軍與駭客攻擊並強化資訊安全措施》，《立法院公報》，第102卷第29期。
註21　張小平，〈台灣想要打信息戰嗎？〉，原載於「軍事文摘」，網址：轉引自人民網http://www.peopledaily.com.cn），檢索日期：105年5月1日。

■C3I信息系統處理能力有限，缺乏有效支撐。

■海、空戰力不足，遠程打擊能力有限，無法對大陸內部指管通情要害實施有效攻擊。

中國大陸準備與當今強國美國相抗衡之時，若我能深切省思並有效運用地緣優勢結合不同國際戰略思維，在美、「中」矛盾關係中，評估中國大陸是否已具備實力掌握網電作戰能力，找出平衡點與我有利因素，並將其靈活運用，為我國未來生存發展、國家安全、建軍整備與防衛作戰上，提供因應之道。

一、對解放軍之威脅認知：

近年來，中國大陸解放軍依國家領導人要求，加強質量建設，在正規化與現代化均獲得相當程度的進展。【註22】值得注意的是，在中國大陸現階段的軍事理論，高技術局部戰爭理論為指導方針，而以網路戰(美軍稱做Information Warfare，IW；國軍稱為資訊戰)為導向的軍事革命，其著眼在於中美未來有可能發生衝突，猶在軍力態勢不佳情況下，充分運用電腦網路資訊，以癱瘓美國軍方及民間資訊網路系統才有獲勝之可能，這種趨勢將發展成當安全環境不利或軍力處於劣勢時，會成為下一波軍事革命發起的動力。【註23】

中國大陸軍事專家認為，未來一個國家最有效、最強大的戰鬥力是網路，戰爭的基礎、決策及戰略轉變的基礎亦是網路信息。因此現今戰爭型態係以高技術戰爭下所發展出網路戰為主要意涵的作戰模式。【註24】

共軍各級電戰部隊近年運用模擬臺海實戰電子環境，致力研發電子戰戰術戰法，並於共軍各軍、兵種部隊演訓時進行實質攻防，從中發掘電子戰弱點研擬反制對策，期於作戰全程掌握「制電磁權」。【註25】當前中國大陸解放軍網路戰可能對我造成的威脅如下：

(一)作戰配套成形：中國大陸各兵種、科研中心，近年來積極研究網路戰建構模式，推行落實於九七年部隊實兵演練與驗證中。由「軍區網路作戰與訓練指導要則」建立作戰程序，組織「軍區計算機網絡防護與攻擊技術研究小組」，及提出網路對抗戰法。另依其現階段電子戰軟、硬殺裝備性能研判，可遂行電磁參數偵蒐，及對國軍監偵與指管系統進行阻斷與干擾能力，顯示解放軍對網路戰相應之軍備、建制與作戰準則，現正逐漸配套形成中。

註22　翟文中、蘇紫雲，新戰爭基因（RMA軍事事務革命），（臺北：時英出版社，2001年5月），頁83。

註23　Hans Binnendijk，and Ronald N. Montaperto eds.，Strategic Trends in China（Washington，D.C.：Government PrintingOffice，1998），頁15。

註24　趙路生主編，《高科技對軍事的影響》，北京：兵器工業出版社，1997年8月，頁109。

註25　國防部國防報告書編纂委員會，《中華民國104年國防報告書》，臺北：國防部，民104年10月，頁56。

(二)兵棋模擬實戰：解放軍近期各大軍區與軍種演習，年度例行性協同和聯合演訓，都不同以往「大規模實兵對抗」，而是轉趨進駐軍區聯訓基地、電腦模擬兵棋推演。1999年10月份「北京軍區」即曾進行歷年來規模最大的網上戰役對抗演練，有此顯示解放軍已能夠成功運用戰役訓練自動化系統進行大規模戰役演習，亦反映「網上練兵」已成為科技練兵的核心與關鍵特色，且亦趨向解放軍「新一代訓練大綱」少動兵、少花錢之特點。【註26】

(三)網攻能力提升：解放軍目前網路化發展情況及近期在沿海各軍區演習的特點，已凸顯其犯臺的針對性，由於其已具網路戰攻擊能力，未來犯臺可能以「躍島」方式對我國防設施進行信息遮斷、壓制，組建特工部隊來臺或收買同路人，對臺灣內部進行騷擾、破壞，跨出傳統軍事框架運用國際網路部署「入島宣傳工作」與不利我之國際文宣等作為，以其目前能力應是游刃有餘。【註27】

(四)關鍵智能運用：解放軍近來投入發展「信息高速公路」基礎建設及致力網路戰研究，從開發陸、海、空、火箭軍專業練模擬器至合成戰術、戰役層級之模擬架構，未來解放軍將以推動「指揮決策智能化」、「業務處理自動化」及「系統管理工具化」為主要目標，並鼓勵學習高科技信息知識藉使此熱潮持續高漲，另尋求C4ISR所需關鍵技術之突破，以開發具戰略層次智能網路；透過太空工具，使其在掌握「網路信息優勢」上，增益其戰略層次智能及網路之研發與運用，冀望達到「決勝千里之外」之作戰目標。

二、對我可能採取的手段：在資訊時代裡，科技是一切的原動力，因此人們常會將注意力集中在如何加密和防火牆設置等這些技術上，而忽略了訓練、動機程序和人為操作上的問題，臺灣擁有為數龐大的高科技人才，目前兩岸的高科技競爭已發展到國防軍事方面的激戰，如能妥善規劃網路教育，結合政府、民間組織或科技人才加入「國防役」的行列，不僅使其學以致用，更能充實我國防科技戰力，亦可建立新一代的軍事革新。

(一)重點指管優先摧毀：針對我網路資訊系統點多線長，分佈面廣，難以組織嚴密防禦等弱點，通過點穴、斬首、斷脈與電磁脈衝等方法，對我網路資訊系統關節點和鏈路實施軟、硬打擊，先期摧毀、癱瘓我作戰指、管、通、情、

註26 〈解放軍罕見四萬人大演習引關注〉，《文匯網》，2013年9月11日，網址：http://news.wenweipo.com/2013/09/11/IN1309110022.htm，檢索日期：105年5月2日。

註27 伍凡，〈中共網路戰急劇擴張危害和平〉，《大紀元》，2013年3月1日，網址：http://www.epochtimes.com/b5/13/2/28/n3811069.htm，檢索日期：105年5月1日。

體系及政經、工、商業電腦、網路系統，使我政府各機構無法正常運作與指揮，再利用我各級部隊混亂間隙，乘機實施快速打擊，達到瓦解我政、經、心、軍戰力之目的。

(二)欺騙迷惑隱匿企圖：為掩護其作戰企圖，中國大陸積極運用聲東擊西、隱真示假、虛張聲勢等欺騙行動和各種網路技術手段及媒體，製造假集結地域、假航渡(空)編隊、假登陸場、假主攻方向、假空降地域等多層次、多種類的全方位佯動佈局，以達欺騙、迷惑我軍。

(三)精準威懾摧毀心防：此法用於戰役全程，特別是在我遭受精準打擊，防禦體系遭受到嚴重破壞後，中國大陸將充分發揮網路媒體的作用，輔以內部網攻駭客等方式對我威懾，進行洗腦式「宣傳」，使之感到其強大的實力和可怕性，以徹底動搖我軍民意志，摧毀心理防線，以達不戰而屈人之兵目的。

伍、結論

網路運用範疇廣泛，可藉由電腦病毒或駭客等手段，實施干擾、竊取、摧毀等多樣式攻擊作為，進而破壞資訊基礎結構，製造假資訊、癱瘓指揮決策能力，導致喪失反擊能力，若不有效防範將成為我國防資訊安全的一大隱憂。中國大陸正透過各種途徑積極發展網路戰力，為有效充分掌握「制資訊權」，並減低國家安全威脅，我應強化國家資訊基礎建設、嚴密通資安全、持續教育訓練、提升技術研發等方向賡續發展。

從本文前述說明中，吾人可確定中國大陸資訊戰對我真正的威脅，在於無平戰時緩衝，亦無備戰動員期，更無軍民對象差異。惟依其「首戰即決戰」特性，資訊戰發起日，亦即國家安全受到重大衝擊，政治緊張、市場經濟失序、社會民心不安以及軍事行動受阻等，都可能同時發生。因此，對於中國大陸積極研究資訊戰，我們必須深切瞭解它對國家安全的重大影響，並以國家戰略層次來思考以為因應。應有之策進建議作為臚陳如后：

一、在國家政策方面：

(一)建制國家安全防護之機構：國家網路資訊戰以獲取國與國之間網訊優勢為目的，包括情報戰、外交戰、商業戰與心理戰等，運用工具國家的通訊社、電視台、廣播電台、報刊、通信網路、外交活動與各種偵察、竊聽活動等。中國大陸以宣傳起家熟諳運用、掌握輿論之道，不排除將對我進行網路「登島宣傳工作」，近期「新華社」所控股「中華網站」搶先登記網址，意圖混淆我國家定位的問題，並結合謀略與宣傳等文攻武嚇對我進行心理恫嚇。【註28

]我應儘早建制國家級安全防護機構，由行政院委請「資訊策進會」構建監控網路非法侵犯的查報機制，如偵測或統計災害管制、分析資訊攻擊事件、發佈諮詢報告及通知修護單位緊急復原等，以具備電腦網路危機處理能力，並對「負面文宣」作適時澄清，以避免中國大陸「心理威懾」打擊我股市、金融機構與民生經濟，而動搖分化我民心士氣。

(二)深植全民網路資訊戰教育：1999年7月「特殊國與國關係」發表後，連續發生中國大陸利用網站冒用中央社名義發佈虛構臺海空戰消息，及中國大陸網路駭客侵入監察院等政府機關網站，顯示中國大陸對臺文攻武嚇之餘，已經展開其網路戰的威懾，透過網路散佈虛構、不實消息，打擊臺灣人心安定。各級學校應加強網路戰攻防教育，相關大專院校應與資訊企業合作，積極投資擴大研究，並不定期舉辦資訊學術研討，以促進網路資訊戰研究發展。

(三)落實資訊建設與技術研發：網路戰能力植基於國家資訊基礎建設，現今世界先進國家，莫不制定長程計畫積極推行。我國於95年2月22日正式成立「國家通訊傳播委員會」，負責國家資訊基礎建設(NII)的推動，期使我國能成為世界最先進的資訊化國家，提升國家競爭力；並置重點於國防資訊基礎建設(DII)，期以奠定網戰良好基礎。【註29】有關資訊技術的發展由行政院主導，召集國內資訊工業相關廠商，對於未來五至十年內資訊工業的發展趨勢進行評估，同時結合工研院、資策會、中科院等單位，對於資訊戰的關鍵技術持續進行研發，俾使國家網路戰在軟硬體上保有相對優勢。

二、在國防政策方面：

(一)成立網路戰專責研發機構：成立網路戰專責研發機構，在對網戰相關的攻擊與防禦手段進行研究，如邏輯炸彈、電腦病毒、電磁脈衝與電子戰等裝備，進行理論驗證與實兵對抗，瞭解各項裝備的優缺點與侷限性，方能在未來的網路戰中掌握優勢。另結合運用國內民間資訊、及通信科技與資訊基礎工業，針對中國大陸網路戰能力弱點，研究反制剋制之道，以達到先發制人優勢力量。

(二)組織再造擬發揮加乘戰力：網路時代的戰爭，勝負非由數量的多寡決定，端係交戰兵力整合。國軍因應精粹案組織架構的精簡，對於網路資訊的需求更勝於往，為了有效運用組織與指揮鏈的充分溝通授權，進而達到量小、質

註28　施子中，〈中共積極準備信息作戰之研析〉，臺灣綜合研究院戰略與國際研究所，1999年12月，頁69。

註29　王振坤譯，《戰略性資訊作戰的崛起/Roger C.Molander etc》，臺北：國防部史政編譯局譯印，民國89年5月，頁81。

精、戰力強的網路作戰部隊。否則，勢難進行迅速而確切的反應；因此，國軍應持續地進行組織再造與兵力整建，方能適應這詭譎多變的環境。【註30】

(三)以資訊科技彌補地緣戰略：在未來戰爭中，任何一方若具較佳的戰鬥空間預警能力，即能適時的投入壓倒性兵力擊敗敵人獲得勝利。在地緣戰略上，臺灣毗鄰中國大陸，所獲知的戰情預警時間因縱深不足而無法及時獲得，如中國大陸一旦率先發起第一波攻擊時，國軍勢必因預警時間短促而遭受到嚴重的傷亡。故此，如能建置一套完善的戰情預警資訊化系統，除可有效整合國軍指、管、通、情、監偵(C4ISR)系統外，另將可與作戰及情報自動化整合於共通一致之平台系統，發揮三軍統合作戰之指揮機制，用以彌補台灣缺乏「戰略縱深」的遺憾。

(四)建全網路戰多元嚇阻能力：當前國防政策係以「有效嚇阻、防衛固守」做基調，在我國並無大規模毀滅性武器做為嚇阻戰力的情況下，唯有運用軍事與民用網路的能力方可癱瘓中國大陸網戰攻擊，在如此情況下，若能充分掌握網路資訊，將可對其發起軍事行動形成某種程度嚇阻。為了因應未來戰爭需要，國軍在未來採購政策上應能以系統整合的軟體程式做為考量重點。並配合「網路戰實驗室」之設立，收集各種病毒種類與分類，研發各種資訊武器，以建全國軍網路作戰的能力。

(五)全向推展厚植網路高科技：網路科技屬軍民通用科技，國內民間與學術單位資訊科技潛力雄厚，鑒於國軍面臨人員精簡、役期縮短、厚植高科技基礎於民間等客觀條件，應配合行政院政策，實施國軍網路資訊業務整體委外服務，並有效整合民間業者、公民營研究機構、政府機關等單位，透過諮詢顧問、委外合作等方式，落實國防資訊建設，以達到國軍建軍備戰之總體目標。【註31】

三、國軍網路安全因應作為：

網路攻擊屬主動性資訊作戰，係運用諸如電腦病毒等高科技，針對敵之指揮管制系統等基礎建設，遂行指管網路攻擊、心理戰、經濟戰等資訊攻擊。網路防護為防禦性或反制的手段。包括安全措施、資訊網路安全及資訊防護等。【註32】

註30　蔣永芳、王振坤譯，《戰爭中資訊的角色變化（上冊）/ Zalmay M. Khalilzad, John P. White》，臺北：國防部史政編譯局譯印，民國89年12月，頁145。

註31　林勤經，〈兩岸資訊戰戰力之比較〉，台灣綜合研究院戰略與國際研究所，2000年2月，頁9。

註32　周茂林譯，阿瑞(Guy Ben-Ari)、趙(Pierre A.Chao)編，《因應複雜的世界-發展明日國防與網狀化系統》

國防部長高廣圻在104年「通資電工作檢討會」中提出「因應敵情威脅，落實整體規劃」、「強化戰訓工作，確保資電優勢」、「培育優質人力，強化資電戰力」、「嚴謹指管整合，發揮聯戰效能」、「執行鏈路建置，確符作戰實需」、「恪遵資安規定，確維通資安全」及「結合公民營資源，支援災防整備」等7項指示，並強調國軍應按部隊任務屬性、裝備能量及往年演訓累積的經驗，在複雜電磁環境下，靈活訓練模式與精進測考強度，以肆應不斷變化的戰場實況，並提高通資系統運作能力、發揮網路與電戰效能，強化國軍通資電系統防護與反制能力，確保作戰指管暢通，維持臺海防衛作戰資電優勢。【註33】

國防部為有效整合現有公、民營資源，建立更精實的國防通資電系統，並從國家安全戰略與軍事戰略到戰略資訊戰各層面的重要關鍵資訊基礎建設進行風險評估與分析。【註34】為落實國軍網路安全亦應重視下列管制措施：

(一)嚴密人員進出管制：資訊管制區內建構適當的進出管制保護措施，以確保僅被授權的人員始得進入，不讓有心人士找出電腦設施的所在位置為原則。另要求所屬確依「國軍資通保密裝備管制作業規定(草案)」，落實保密裝備(含附屬物)每日清點及移(監)交會銜，相關領用與出(入)庫均須指派專人負責逐一清點並翔實紀錄備查，如有違失，依規定嚴懲。

(二)有效人員裝備管控：內部資訊人員為掌握機敏資料的關鍵人物，因此單位內部的系統管理人員平時社交生活狀況應特別注意。內部控管保密資料的機制如未能有效執行與落實，容易淪為有心人士介入的弱點，引發嚴重後果。基此，資訊資產帳籍管理人員應參照國軍財產、國軍物品、軍品及軍用器材等相關作業規定，實施資訊資產清點，清點檢查紀錄及資訊財產清點差異統計表應由單位主官(管)批核後備查。

(三)委外網路安全審查(維護系統時直接接觸主機)：部份機關的資料輸入與系統維護是委外處理的，在委外過程中要考慮那些資料適合委外，那些資料不適合，與以清楚權限劃分。其次，若要委外應要考慮如何做，讓資料不易外洩，例如一些資料可用代碼、代號方式儲存等。，另有關資訊保密裝備送修時，依規定對送修裝備翔實審閱送修憑單及清點，與會同保防(政戰)部門辦

(Organizing for a Complex World - Developing Tomorrow's Defense and Net-Centric systems)，臺北：國防部史政編譯局，2010年。

註33 〈高部長：群策群力爭取資電優勢〉，《青年日報》，2015年11月25日。網址：http://news.gpwb.gov.tw/mobile/news.aspx?ydn=026dTHGgTRNpmRFEgxcbfcCSN9Fhd8KFbqLRgMWauV%2BKIwibOU%2FEPVpJ2bjfKfcoYeUf24RFlVBV%2FIdeDFdx6cT%2B2NpkKFYIhpJxXyfqBCE%3D，檢索日期：105年04月22日。

註34 立法院，《我國如何因應網軍與駭客攻擊並強化資訊安全措施》，《立法院公報》，第102卷第29期。

理，進出營區亦應填寫三聯單並奉權責長官核定。

(四)嚴防勾串內神外通：資訊教育應以強化電腦運用、提升資訊系統管理運用能力為目標，而資訊倫理的教育及隨身碟的管控，更是單位內資訊安全的控管重點；尤其現今病毒發展速度之快，許多看似安全卻充滿危機的動作，常被一般人所忽視，單位內對儲存媒體的控管應多加重視，才能有效防堵任何可能發生問題的漏洞。

(五)確遵資訊安全政策：貫徹「專網專用、實體隔離」及「嚴禁於民網電腦上處理公務」政策要求，嚴禁國軍網路、機敏網路、戰情網路與網際網路搭接混用或誤插情事，此為網路安全最重要也是最基本的概念；民網應集中、公開設置為原則，如有軍、民網資料交換需求，必須設置檢疫區，嚴禁處理公務之網路連接外部網路系統，確保專網專用的實質效益。

(六)落實網路防護機制：由於電腦網路具有開放性、互連性等特徵，易受到電腦病毒、駭客和其他非法攻擊。為確保網路安全，使駭客無法透過網際網路進行攻擊，軍用網路須與網際網路完全隔離。其次，在軍用網路上傳輸和處理軍事機密資料必須採多功能、多層級等加密措施。再其次，針對可能危害網路安全事件進行掃瞄，並分析網路中各個封包內容，對入侵資訊發出警告、跟蹤攻擊源、採取隔離網路連接及記錄攻擊過程等措施。

(七)強化網路稽核工作：針對電腦病毒戰的攻擊，除應以「防火牆」機制，事先劃分若干個封閉「隔離箱」，迅速對症下藥及清除病毒外，應將整個電腦系統即分塊隔離，避免整個系統染上病毒。另針對軍網電腦內舊有檔案(如非統一配發軟體、非公務資料等)，導致病毒違規案件數驟增情事，宜要求管理人員落實資料清整作業，不定期執行軍網網路稽核，避免遭集控式防毒系統判斷為風險檔案，另未經授權軟體亦應一併清除不得使用。

人類文明已進入第三波的網路資訊科技時代，國家目前已遭遇比傳統作戰時更艱鉅的網路安全威脅。而現代戰爭的概念已遠不是兩軍用坦克、飛機、軍艦、甚至導彈核彈等作有形較量，而是包括網絡信息戰在內的無形博弈。這種由中共高層主導、軍方實施的系統的網絡攻擊絕非一般個人駭客侵入，而是一種國家戰爭行為，它超越了目前兩岸關係中的經濟摩擦、外交爭執、工業間諜等層面，實際上是一種准軍事攻擊和宣戰信號。

然，海峽兩岸國家定位的問題一直無法達成共識，長久爭執下去，終有擦槍走火的一天，國家安全的確保，有賴全民對這塊土地認真的經營。中國大陸每年編列的國防經費不斷以倍數以上成長，對我威脅與日遽增，尤其於網路作戰，中國大陸

已將網路戰併同精密制導武器及自動化作戰指揮系統，列為現代化戰爭的三大支柱，可見其對網路戰的迫切需求與重視。

反觀我們國家各部會首長仍舊是說的比做的多，政府機制運作步調永遠慢半拍，未來中國大陸若對臺發動網路戰攻擊，將無前、後方之分，除了軍事層面外，所有政府、民間及商業資訊系統也將成為攻擊目標。所謂「勝兵先勝而後求戰，敗兵先戰而後求勝」，我們應針對敵情威脅，確定我網路資訊戰需求，從健全組織、落實戰訓、人才培育、裝備研發、整合體系等方向及早完成準備，建立一支具備現代化能力的網路戰部隊，以優勢網戰開創對我有利的態勢，同時建立全民認知網路戰對國家安全的重要性，確保國家之生存與發展。

作者簡介

空軍上校　黃獻忠

學歷：空軍官校77年班、情報參謀軍官班、空軍參謀學院93年班、國防大學戰爭學院100年班。經歷：飛行官、作參官、訓參官、情參官、分隊長、作戰長、副隊長、基勤大隊長、國防大學戰爭學院戰略教官、中正預校教育長、空軍官校總務處長，現職：空軍教育暨準則發展指揮部上校參謀長。

空軍中校　王健民

學歷：陸軍官校89年班、陸軍學院99年班、戰研所100年班，國防管理學院決策所96年班碩士。

經歷：排長，連長，參謀主任，大隊長，現職：國防大學陸軍學院防衛作戰組中校教官。