10.6326/NDJ.2015.30(6).1

共軍網路作戰對我資電作戰之影響

The Impacts of the PLA Cyber Warfare on the ROC's Information and Electronic Warfare

呂兆祥 (Chao-Hsiang Lu)
教育部國民及學前教育署中校教官

摘　　要

本研究旨在探討共軍網路戰略與能力發展現況，藉分析共軍網路戰略與能力發展的官方及學者之論述與談話等相關文獻，以文獻分析法進行研究。

共軍在國防預算充分支持下，正逐年實現軍力現代化目標，網路作戰更以尋找可資竊取資料之特定電腦網路的弱點爲重心，一旦臺海衝突爆發，中共網軍將癱瘓我指管、後勤網路，影響國軍資訊系統正常運作並遲滯國軍應變能力，並可於危機或衝突期間搭配軍事攻擊，強化其作戰效能。

國軍在共軍網路作戰能力日益增強威脅下，應善用有限國防資源，建立網路作戰能量並強化網路戰略目標防護與建立資安防護機制，提升三軍聯戰效能，使其戰爭成本與風險增加，降低其武力犯臺意圖，達成「防衛固守、有效嚇阻」戰略，確保國家安全。

關鍵詞：網路空間、網路作戰、防衛作戰、國家安全

Abstract

This study explores the current cyber warfare strategy and capacity of the People's Republic of China (the PRC). It analyzes the PRC's military build-up through official discourse and academic literature, and takes Document Analysis as a research method.

Given ample support of annual defensive budget, the People's Liberation Army (the PLA) has gradually realized its objective of military modernization, with cyber warfare being an instrument to look for the weakness of the opponent's computer network. Should a military conflict erupt across the Taiwan Strait, the PRC cyber army may be able to paralyze the command and logistics network of the Republic of China (the ROC), to affect the normal functioning of the information system of its armed forces, and to weaken the latter's response capability. The cyber army can even enhance the warfare effectiveness by working with military attacks during crises or conflicts.

Under the growing threat of the PRC cyber warfare, it is suggested that the ROC should

make good use of its limited defense resources to build a cyber warfare capacity, strengthen the defense of strategic targets, and establish information security mechanisms, so that the effectiveness of combined operations among the army, navy and air force can be enhanced. It is through increasing the costs and risks of military invasion that the PRC's willingness to attack Taiwan can be largely lowered, the ROC strategy of "tenacious defense and effective deterrence" realized, and the ROC national security achieved.

Keywords: Cyberspace, Cyber Warfare, Defense Operations, National Security

壹、前　　言

網路攻擊事件已從個別、單純的炫耀，演變成有組織、以經濟或政治等特定利益為目的的入侵行為。[1] 近來網路犯罪組織趨於高度專業分工，加以網路攻擊不受時空條件限制，已使國家安全之概念及範圍產生實質變化。依據美國參議院「情報委員會」分析全球威脅評估報告指出，美國目前面臨重要的威脅即為網路空間帶來的挑戰。[2] 共軍近年來利用網路科技，大量招募專業技術人員組成「網軍」，[3] 由近期的相關報導指出其已具有執行網路攻擊和防禦的能力。[4] 而我國又是中共網路攻擊的主要對象之一，顯示我國資安環境相當嚴峻（如圖1）。[5]

我國國安局2013年4月在立法院報告內容指出，中共網軍正式編制約十餘萬人，對該局之網路惡意攻擊行為每日平均209次。其次就我國遭受攻擊對象分析，已由政府機關、駐外館處轉向民間智庫、電信業者、委外廠商等，並轉變思維攻擊我較疏於防護之網路節點或車輛交通號誌儀控設備、寬頻路由器、工業微電腦控制器、網路儲存系統等崁入式系統設備。[6] 顯示共軍對我之網路攻擊行為，已不再侷限於軍事目標，正快速滲入我民生系統。而我重要資通訊設施一旦遭受破壞，勢將影響經濟、民生及整體政府運作；而各類關鍵基礎設施(Critical

1〈FBI公佈新力遭攻擊細節指朝鮮是網路攻擊源頭〉，《鉅亨網》，2015年1月9日，<http://fund.cnyes.com/news.aspx?choose=newscontent&sn=20150109115921245405212>（檢索日期：2015年3月20日）；鍾詠翔，〈駭客攻擊日內瓦銀行個資遭洩〉，《聯合新聞網》，2015年1月11日，<http://udn.com/news/story/6811/635102>（檢索日期：2015年3月20日）

2 James R. Clapper,"Worldwide Threat Assessment of the US Intelligence Community," March 12, 2013, p. 1, Office of The Director of National Intelligence.

3 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。

4 連雋偉，〈陸駭客竊密　美國年損逾9兆〉，《中時電子報》，2014年5月20日，<http://www.chinatimes.com/newspapers/20140520000379-260102>（檢索日期：2014年9月30日）；〈美報告再指責中國大陸軍方網路間諜活動〉，《BBC中文網》，2014年6月10日，<http://www.bbc.com/zhongwen/trad/world/2014/06/140610_usa_china_cybersecurity>（檢索日期：2014年9月30日）

5 湯佳玲，〈中國18萬網軍威脅我將分級聯防〉，《自由時報》，2015年1月13日，版A8。

6 國家安全局，〈我國如何因應網軍與駭客攻擊並強化資訊安全措施報告〉，《立法院公報》，第102卷第29期，2013年4月29日，頁6。

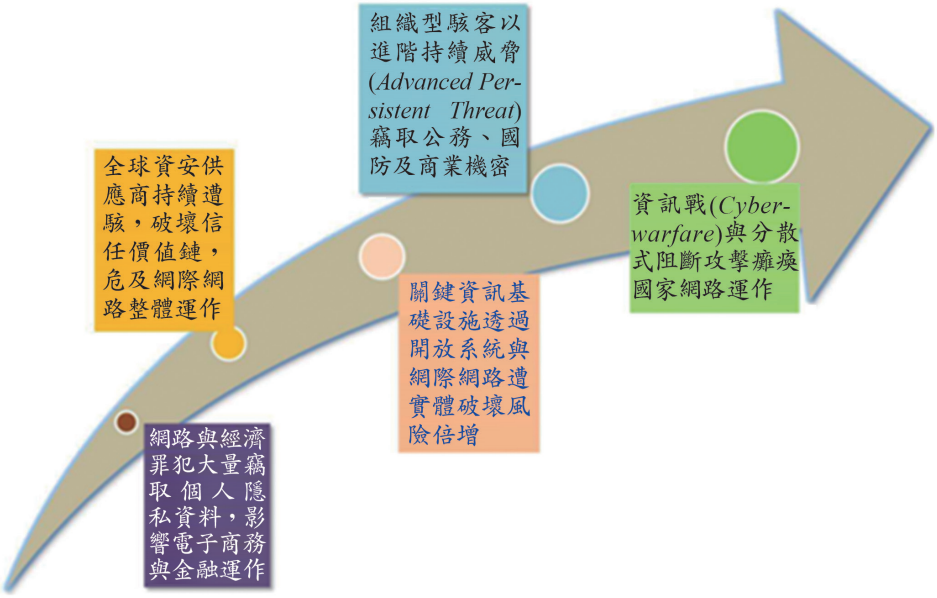

圖1　資安威脅示意圖

資料來源：行政院國家資通安全會報，〈國家資通訊安全發展方案〉，《政府機關資訊通報》，第315期，2013年12月25日，頁2。

Infrastructure, CI)的監督控制與資料獲取系統(Supervisor Control And Data Acquisition, SCADA)，通常較無堅實的資安防護設計，平時即為網路駭客重要攻擊目標。關鍵基礎設施是國家為維持民生、經濟與政府的運作；提供人民日常生活的基本功能與服務，諸如通信、金融、電力、供水、電子化政府等營運的基石；若這些基礎建設的運轉中斷，將對公共服務、民眾生活及國家安全導致危害。[7]未來臺海若發生軍事衝突，其恐將透過網路攻擊以癱瘓我國軍事、民生之關鍵基礎設施運作。

綜上，可以發現網路雖帶來生活便利性，但亦可作為駭客惡意攻擊的媒介。因此，從軍事面向了解共軍網路攻擊方式與能力，進而加以防範，以維護國家安全，實為我國人必須有效應對的議題。

貳、共軍現階段網路作戰發展

孫子曰：「凡戰者，以正和，以奇勝。」網路作戰雖仍未歸類為正規作戰，然就第一次波灣戰爭以來之重大軍事衝突，網路作戰所占比重日益增加，在共軍網路作戰能力日益提升的現況下，將對我國家安全造成重大威脅。本文除說明網路發展對戰爭的影響與共軍網路戰略的發展，亦將分析共軍網路作戰能力現況。

一、網路發展對戰爭的影響

曾復生認為「網路戰」是一體兩面的戰略，一旦運用網路部隊進攻別國的網路，導致網路癱瘓，而本國的網路作用也將急劇下降，所以國際間的網路必須靠合作，才能提

7 樊國楨、韓宜蓁，〈美國關鍵基礎設施防護法案與資訊安全管理技術控制標準化〉，《國防雜誌》，第30卷第4期，2015年7月，頁99。

升網路的便利性與使用價值。面對各國網軍較勁升溫的新形勢，未來的戰爭中電腦本身就是一種武器與戰場，前線無所不在，奪取戰場控制權將不只是導彈、飛彈和士兵，還包括電腦網路與數位通訊機制。[8]

吳嘉龍指出，隨著資訊科技快速進步，電腦與網際網路的運用日益普遍，資訊戰不僅成為國際間廣泛討論的熱點，更被許多軍事戰略學者認為是未來戰爭的主流，甚至認定為「第五戰場」。以軍事強權美國為例，美國在2003年便制定「確保網路安全的國家戰略」，將戰略目標置於預防國家重要基礎建設遭受網路攻擊，降低遭受網路攻擊的弱點，同時亦投入大量預算，積極建置網路及資訊作戰專業部隊，對可能攻擊美國資訊基礎建設或竊取重要資料的潛在敵國，進行攻勢的反制行動。[9] 美國政府將「關鍵基礎建設」定義為：「對美國極具關鍵作用的實體或虛擬資產、系統與網路，[10] 其認定之重要關鍵基礎建設項目如表1。

簡華慶認為現代及未來戰爭，越來越倚重資訊及網路，如同武器載臺對於目標的計算、訊息的傳遞、衛星的定位、戰場透明的程度等等，若無資訊處理及傳輸，上述功能都無法實現，就連現在處處所談到的C^4ISR系統，若無資訊處理及傳輸，就如同一堆廢鐵，是無法發揮戰力的，未來戰爭型態，借助資訊的力量只有增加不會減少。[11]

大陸學者認為戰爭經歷農業時代、工業時代和資訊時代三個階段，在每個歷史階段中，都有相對應的戰爭型態。以資訊為中心，是資訊化戰爭所有作戰樣式的普遍特徵。因此，它對資訊作戰、火力戰、特種戰等各種樣式的作戰都具有普遍指導意義。資訊化戰爭是軍事、政治、經濟、外交、科技等多種因素的一體戰，其中軍事領域的對

表1　美國政府的關鍵基礎建設

農業與食品系統	水壩	資訊科技系統
銀行與金融系統	國防工業基礎	核能反應、材料、廢棄物系統
化工產業	緊急救護系統	運輸系統
商業設施	能源供應系統	水資源系統
通訊系統	政府運轉體系	
關鍵工業設施	公共醫療系統	

資料來源：樊國楨、韓宜蓁，〈美國關鍵基礎設施防護法案與資訊安全管理技術控制標準化〉，《國防雜誌》，第30卷第4期，2015年7月，頁108。

8 曾復生，〈美「中」網路間諜戰最新情勢研析〉，《國家政策研究基金會》，2014年6月9日，<http://www.npf.org.tw/post/2/13698>（檢索日期：2014年9月30日）

9 吳嘉龍，〈網路科技發展與資訊安全管理研究探討〉，《危機管理學刊》，第10卷第2期，2013年9月，頁83。

10 U.S. Department of Homeland Security, *National Information Protection Plan* (Washington: Department of Homeland Security, 2006), p. 103, <www.chs.gov/xprevprot/programs/editorial_0827.shtm>（檢索日期：2014年9月30日）

11 簡華慶，〈網路資訊戰所扮演角色及因應策略之研究〉，《國防雜誌》，第27卷第1期，2012年10月，頁137。

抗，主要表現為以資訊為中心的對抗行動，亦即資訊中心戰（如圖2）。[12]

從以上有關網路發展與戰爭關聯性之內容分析，網路已成為各國現代化軍隊從事部隊指揮與管制、情報與後勤，以及發展與部署武器科技的重要媒介，顯示網路發展將對戰爭過程與結果產生重大影響。

二、共軍網路作戰戰略

王高成認為共軍由於受到美國自1991年波灣戰爭以來歷次戰爭的影響，近年也提倡「遠戰速勝、首戰決勝」的作戰概念，積極運用遠程精準的打擊火力，以及資訊與電子戰的戰力，以求在戰爭初始，即對敵人施以

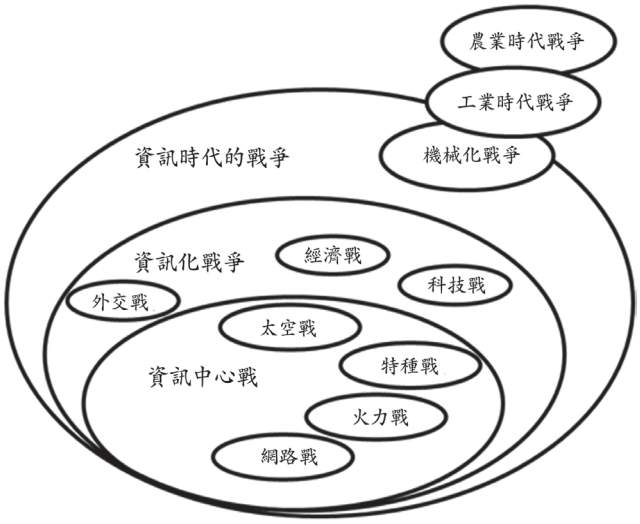

圖2　資訊戰與戰爭型態關係

資料來源：張占軍，《論信息中心戰》（北京：國防大學出版社，2007年），頁9。

致命的打擊，迅速取得勝利的戰果。共軍正發展不對稱作戰，一方面以嚇阻或阻滯美軍對臺海衝突的介入，其手段係以軟硬殺武器對美軍「指揮體系、資訊體系、先進武器系統、後勤體系、關鍵連結體系」加以摧毀或癱瘓。[13]

蔡明彥指出，共軍認為電腦網路攻擊是在軍事上「以弱擊強」最有效的方法，發動電腦網路攻擊，可成功地干擾敵國的軍事運作，主要以敵國C^4ISR的資訊網路系統視為優先攻擊的目標，目的在干擾敵國部隊的通訊與指管設施，以癱瘓敵人戰場識別系統、資訊處理系統與指揮控制系統，瓦解敵人整體的指揮與作戰能力。[14]

我國102年國防報告書指出共軍致力網軍攻防技術發展，力爭2020年基本實現「資訊化」[15]建設取得重大進展，並運用組織編裝調整、加強各軍（兵）種聯訓與籌建高新武器，構建戰略（術）單位情監偵平臺，依其「軍事現代化進程、戰略思維發展、兵力結構與部署、武器研製」研判，現已具備「監偵立體化、打擊多樣化、威懾多元化」能力。[16]其中打擊多樣化與威懾多元化能力即包含網路作戰能力。

中共2012年國防白皮書有關網路戰略內容：「立足打贏資訊化條件下局部戰爭，加強軍兵種力量聯合運用，提高基於資訊系

12 伍仁和，《信息化戰爭》（北京：軍事科學出版社，2004年），頁29；張占軍，《論信息中心戰》（北京：國防大學出版社，2007年），頁9-10。

13 王高成，〈中共不對稱作戰戰略與臺灣安全〉，《全球政治評論》，第6期，2004年4月，頁26。

14 蔡明彥，〈美國東亞軍事優勢地位的挑戰：中國「反介入」與美國「反反介入」的角力〉，《全球政治評論》，第21期，2008年1月，頁71。

15 共軍將Information譯為信息，國軍譯為資訊，就譯名而言，兩者係屬通用語，故本文統一使用資訊一詞，然在引用部分仍以原文顯示。

16 國防報告書編纂委員會，《中華民國102年國防報告書》（臺北：國防部，2013年），頁56。

統的體系作戰能力，創新發展人民戰爭戰略戰術。」顯現共軍認為資訊優勢為軍事鬥爭之基礎，並藉由創建網路戰民兵，擴大其網路作戰基礎。[17] 另部分中共學者認為共軍在借鑑外軍發展網路戰的研究過程中，發現「網電一體戰」為解決網路戰、電子戰各自為戰，削弱敵網路及電磁空間運用，及確保己方網路及電磁空間優勢，以遂行一體化聯合作戰的最佳方法。[18]

從以上有關共軍網路戰略相關研究顯示，其網路戰略思維與發展概可區分為不對稱作戰、網路癱瘓戰與威懾戰，終極目標係以網電一體戰癱瘓我民生供給與軍事作戰系統為手段，以達成威懾我軍民抗敵意志，實踐其不戰而屈人之兵的戰略目標。

三、共軍網路作戰能力

孫子曰：「知彼知己，勝乃不殆；知天知地，勝乃可全。」在共軍網路作戰能力日益提升的嚴重威脅下，我國資安防護能力能否適切因應，將直接影響我國家安全。「102年國防報告書」指出共軍已在四總部、七大軍區、國防科研機關、國防動員、資訊及民兵等部門，組成網路攻擊、防禦的基本戰力；自2010年起進行新款間諜軟體研改作業，於網際網路空間伺機竊密，其軟體功能朝「自動化」作業模式發展，具變更資料加密模組、隱匿傳輸通道、反制網路安全人員追蹤等能量。[19]

伍爾澤認為共軍有16個技術偵查（信號情報）單位與機構，和至少7支電子戰與電子反制部隊。共軍七大軍區均編制電子反制團加以支援，另二砲部隊轄下亦編制專責網路滲透、網路諜報與電子戰的支援部隊。[20]

吳胤曠認為共軍已具資訊戰力，建立如共軍電子科技學院、總參謀部第三分部與資訊戰模擬中心等機構，且當前共軍四大總部、七大軍區均設有網軍部隊。共軍網路作戰大本營為共軍61398、61486部隊，後者又被稱為「推桿熊貓」(Putter Panda)駭客小組，前述兩者皆隸屬上海共軍總參謀部三部（技術偵察部）；而中共資訊大學作為訓練基地，也是共軍發動網路作戰部門之一。[21]

陳立函指出，從近期遭到中共駭客的攻擊事件的密度分析，共軍對外的網路入侵攻擊以及情報蒐集仍不斷在發生，且已可針對特定對象或單位進行攻擊，令受害者和防禦者疲於奔命，顯現共軍網路攻擊能力正日益進步。[22]

17 中共國防部，〈國防白皮書：中國武裝力量的多樣化運用〉，2013年4月16日，《中共國防部》，<http://www.mod.gov.cn/affair/2013-04/16/content_4442839_4.htm>（檢索日期：2014年10月13日）

18 王克海、王兵、曹正榮，《一體化聯合作戰研究》（北京：解放軍出版社，2005年），頁92-93。

19 國防報告書編纂委員會，《中華民國102年國防報告書》，頁54。

20 Larry M Wortzel著，章昌文譯，〈評論中共軍事現代化及其網路活動〉(China's Military Modernization and Cyber Activities: Testimony of Dr. Larry M. Wortzel before The House Armed Services Committee)，《國防譯粹》，第41卷第10期，2014年10月，頁11；*Directory of PRC Military Personalities* (Washington, D.C.: Defense Intelligence Agency, March 2013).

21 吳胤曠，〈全球隱密監控與國家間反應：以「梯陣」、「稜鏡」間諜網絡為例〉，《國防雜誌》，第29卷第5期，2014年9月，頁135。

22 陳立函，〈近年網路攻擊與中國駭客活動〉，《前瞻科技與管理》，特刊，2010年11月，頁143。

綜合上述研究內容，可發現共軍網路作戰能力將持續朝向提升攻擊能力發展，顯見其發展網路作戰能力的主要目的，在以其作為軍事衝突的輔助手段，故其網路戰略與能力發展現況與對我資電作戰之影響，乃本文聚焦重點。

參、共軍網路戰略發展現況

共軍自1990年以來即積極推動軍事現代化，美國國會「美中安全委員會」更明確指出，網路戰已正式納入共軍的軍事準則，[23] 顯示網路已成為其作戰任務中不可或缺的一環，反映出共軍已較不重視傳統人民戰爭的戰略思維，轉向著重運用網路連結的資訊系統，進行定位、追蹤及標定敵軍，同時攻擊敵資訊系統，阻止敵擁有與運用相同的資訊能力。

一、不對稱作戰

網路作戰的重要用途之一即是情蒐活動。[24] 據中共學者指出，網軍平時的主要任務是蒐集與分析潛在敵人的電腦網路，並找出其弱點、重大裝備及部署配置。[25] 電腦偵察對共軍甚為重要，因為據其評估，若面臨軍力優越於己的敵國，對方一旦有周延的準備，將有能力擊敗共軍。因此，共軍必須在衝突初期即採取決定性行動。電腦偵察可藉由提供敵部隊配置的重要資訊，及衝突期間敵電腦網路可資利用的弱點，以提供共軍不對稱作戰運用的方式與重點。[26]

共軍「不對稱作戰」的戰略思維，強調處於作戰劣勢的一方以靈活變化，謀求優勢地位，以求得較高效益，特別注重謀略的運用，並將重點集中在戰略重心及影響雙方對抗的關鍵點。[27]「不對稱戰略」除不對稱作戰手段外，也包括不對稱作戰力量的建立、發展與運用。[28] 因此，共軍所發展的不對稱戰略思維，相當強調「網路戰」的重要性。乃期望在網路化的戰場中，攻擊敵戰略重心或破壞無線網路、鏈路關鍵節點，利用攻擊網路空間的「延伸效應」，削弱敵人軍事力量，達到終戰的目的。有鑑於此，近年來共軍作戰準備的重點，便以「打贏資訊化條件局部戰爭」為目標，顯示共軍已將資訊技術視為提升共軍戰力、打贏現代化戰爭的主要工具。[29]

能力的建立是不對稱作戰中很重要的關鍵因素，故發展「殺手鐧」武器，[30] 攻擊電腦網路關鍵節點或重要基礎設施，為建立不

23 Michael Chertoff著，鄧炘傑譯，〈網路公共領域的戰略意義〉(The Strategic Significance of the Internet Commons)，《陸軍學術雙月刊》，第51卷第542期，2015年8月，頁143。

24 戴清民，《網電一體戰引論》，頁33。

25 郭勝偉，《信息化戰爭與網電部隊》（北京：國防大學出版社，2008年），頁218。

26 戴清民，《網電一體戰引論》，頁33、115。

27 李宇林，〈中西「不對稱作戰」概念之比較研究〉，發表於2008年「國防事務專案研究暨戰略學術研討會」（桃園：國防大學，2008年10月），頁67-69。

28 謝之鵬、謝游麟，〈國軍發展不對稱軍事思想與作為之研析—孫子兵法觀點〉，發表於2012年「戰略與國防：不對稱作戰議題」學術研討會（桃園：國防大學戰爭學院，2012年5月24日），頁79-81。

29 U.S. DOD. *Annual Report to Congress on the Military Power of the PRC 2006* (Washington, DC: U.S. DOD,2006), p. 36.

30 林中斌，《核霸：透視跨世紀中共戰略武力》（臺北：臺灣學生書局，1999年），頁1-9。

對稱作戰打擊能力的必要條件之一，且資訊網路為不對稱作戰提供更多手段與方法。[31] 其中包含以現有劣勢裝備「以小搏大」，及冀求科技強軍後「以強擊弱」作戰力量的建立、發展與運用，破壞敵國重要基礎設施及軍隊資訊網路系統，使敵政經混亂、武器作戰效能降低，將可進一步達到戰略威懾遏制戰爭的作用。[32] 其網路戰略目標，包含政治、基礎設施以及戰略設施三種類型如表2。[33]

二、網路威懾戰

共軍的威懾戰略包括威懾與反威懾，威懾是壓制措施，反威懾是對抗與防護措施。共軍自認其威懾戰略主要是確保國家安全與領土完整，故威懾與反威懾都是一種自衛的戰略。威懾戰略之目的既是迫使對手不去追求，或者放棄對目標的追求，藉由向敵方展示可靠的實力與運用實力進行報復的決心，達成威懾的戰略目標。[34] 共軍的網路威懾戰戰略思維，除建立基於不對稱作戰思維的實力，另網路空間的「開放式架構」，[35] 亦是提供網路威懾戰成功的條件。

康經彪認為資訊時代的戰爭主要是以網路戰為核心的戰爭。交戰雙方通過對網路資訊的爭奪（生產、蒐集、傳遞、保存、加工、處理或銷售資訊），不斷地製造出無形的威懾力量，如理論威懾、戰備競賽、潛力抗衡、輿論爭奪、情報戰、心理戰、電子戰等。[36]

金登富認為共軍的網路戰略乃希望藉由平時雙方充分運用網路空間的效應，以達到

表2　網路戰略目標

政治	中央政府機關與辦公中心—例如行政中心，命令輸出單位。
	國內警政與維持治安能力—例如指揮部、情蒐中心、支援資料庫。
	國際及國內宣傳系統—例如主要傳媒、政治作戰組織、文化中心、政府網頁、國際通訊網路。
基礎設施	資訊基礎設施—電信、電力系統、微波傳輸中心、C4ISR中心。
	能源供應來源—如發電廠、核能設施、電力傳輸線路。
	交通設施—如機場、公路網路、港口以及管理交通的電腦與電子系統。
	財政中心與金融網路—如銀行、股市。
	民生供應中心—例如主要食物與飲水分配系統和管理中心。
軍事設施	國家戰略防衛—作戰指揮中心、緊急危機處理中心、防衛性指揮與管制中心。
	戰略性攻擊計畫系統—例如傳統武器發射傳輸系統、毀滅性武器的發射與研究發展中心。

資料來源：曹邦全，《中共信息戰之研究》（高雄：國立中山大學大陸研究所碩士論文，2001年），頁19-20。

31 戚世權、梅軍、陳克林、單琳鋒、朱玉萍、劉慶國，《論制信息權》（北京：軍事科學出版社，2001年），頁255-257。
32 戴清民編，《信息作戰概論（修訂版）》（北京：解放軍出版社，2001年），頁170-172。
33 曹邦全，《中共信息戰之研究》（高雄：國立中山大學大陸研究所碩士論文，2001年），頁19-20。
34 王鳴鳴，《外交政策分析：理論與方法》（北京：中國社會科學出版社，2008年），頁71-80。
35 金登富，《中共網路戰略思維之概念性探討》（桃園：國防大學戰略研究所碩士論文，2014年），頁68-87。
36 康經彪，〈中共「未來戰爭」研究之威懾作用：兼論國軍因應之道〉，《黃埔學報》，第54期，2008年，頁125。

相互威懾的效果；交戰時單向維持網路空間的優勢，則可達到震懾與迅速制敵的目標。因網路戰係以網路空間為戰場，使網路空間成為作戰重心，強調打擊作戰重心的不對稱作戰，與相互競逐網路空間優勢，遂衍生出「網路威懾戰」之戰略思維。[37]

共軍的網路威懾戰，不僅只針對電腦及網路實施病毒攻擊。其威懾手段主要有二：其一是將國家實力轉化為資訊，以達成遏制侵略者的威懾戰略。[38] 其次為軍事上的積極防禦，強調以積極的攻擊削弱敵國的進攻，化被動為主動，適時以突發性攻擊進行反擊，並發展網路威懾力量，以抵銷和遏制強國的威懾。[39] 平時藉由展現國家總體能力及軍事力量，或威脅攻擊敵網路空間，以達到遏制戰爭維護和平的目的；戰時則透過網路竊取、病毒攻擊等軟殺傷，結合火力硬摧毀，破壞敵民生基礎設施、關鍵節點，迫使敵屈服。[40]

共軍在參考美軍在波灣戰爭中對媒體的運用後，認為運用網路等媒體宣傳武器性能、以虛擬技術擴大戰果畫面輔以兵力佯動逼敵就範、以網路戰及電子戰攻擊敵聯合作戰指揮系統擴大威懾效果，為運用網路威懾戰的戰法，可形成電磁、網路、心理空間結合的威懾效果。[41] 因此，共軍的網路威懾戰，將適時透過廣電、網路等媒體展示「實力」。而中共運用「中國國際廣播電臺」(China Radio International, CRI)於1998年成立網路電臺利用多國文字散布資訊，並迅速擴增其境外電臺及網路電視頻道，即為網路威懾戰的手段之一，[42] 藉由媒體宣傳國力，提高其國際地位，以增加中共在區域的影響力。

三、網路癱瘓戰

任何系統都具有一定功能，而系統的功能又與結構、要素和周遭環境關係密切，三者中任何一個發生改變，都將使系統功能產生變化。共軍認為癱瘓戰就是針對敵各作戰系統內的要素、結構進行破壞，或是利用外在環境因素對敵造成不良影響，進而造成敵作戰系統部分或全部功能喪失，以致無法正常運作。日本軍事專家亦指出「癱瘓戰是憑藉資訊技術催生的各種戰爭手段，以摧毀敵方抵抗能力與意志，使其作戰機器癱瘓的戰爭樣式。」[43]

網路作戰對照其所反制的武器系統，成本相對低廉，[44] 且網路作戰可迅速達到效果。更重要的是，網路作戰具隱密特質，電腦攻擊可能有一段時間無法偵知，即便敵方擁有安全軟體，亦僅對已知的病毒有效，電腦攻擊較其他類型作戰更容易遂行，幾乎無

37 金登富，《前揭文》，頁106。
38 沈偉光，《第三次世界大戰—全面信息戰》（北京：新華出版社，2000年），頁109-185。
39 沈偉光，《2010信息災害：發展中國家生存戰略》（北京：新華出版社，2005年），頁41-42。
40 總參謀部通信部編著，《信息作戰學》（北京：解放軍出版社，2002年），頁526-527。
41 戴清民編，《信息作戰概論（修訂版）》，頁222。
42 金登富，《中共網路戰略思維之概念性探討》，頁122。
43 中國國防報，〈日本啟動軍事轉型提出「癱瘓戰」理論〉，《中華網》，2005年5月24日，<http://big5.china.com/gate/big5/military.china.com/zh_cn/critical/25/20050524/12340309.html>（檢索日期：2015年3月30日）
44 徐小岩編，《信息作戰學》（北京：解放軍出版社，2002年），頁157-158。

地點限制。由於將通信、金融與運輸中心等民用網路列為潛在攻擊的目標，若同時攻擊軍用與民用網路，將可直接影響敵戰略決策與全般戰略情勢，並完全削弱與癱瘓敵方政治、軍事、經濟、文化之戰爭潛能。[45]

謝游麟認為共軍癱瘓戰主要在打擊敵軍的中樞或關鍵節點，尤其是敵軍要害或是薄弱的關節目標。其本質並不在於殲滅敵主力或是占領要地，而是為了要癱瘓敵人的作戰體系，使敵快速瓦解或潰敗，塑造己方有利的戰略態勢，其目的是要以最小損失來獲致最大戰果。[46]

其癱瘓戰略主要是採取「電子戰、網路戰、火力戰、縱深兵力突擊和特種作戰」等多種攻擊手段（或可歸納為電子癱瘓、火力癱瘓及兵力癱瘓），重點打擊敵作戰體系中的要害目標和關鍵環節，造成敵作戰系統功能部分或完全喪失。[47] 其中在網路作戰部分係藉由全面監偵掌控動態、網路攻擊心理威懾、精準打擊實體破壞及電磁干擾癱瘓指管等手段，打擊我指揮中樞，癱瘓我戰略與戰術指管機能。[48]

中共部分學者認為癱瘓戰是「使敵作戰系統功能部分喪失或完全喪失的作戰」；或「使用高技術武器裝備，集中打擊對方作戰系統內的重要關節點，破壞系統內部結構，使系統運行失調，整體功能不能發揮，進而導致整個系統陷於癱瘓的重要作戰方式」；及「打擊敵軍整個作戰系統的主要關節要點，癱瘓敵軍整個作戰能力，並無須全殲敵軍主力，即可達戰勝目的之作戰方式。」[49] 由此可知共軍網路癱瘓戰略是藉由網路作戰同時攻擊敵軍事與民生核心資訊系統，大幅降低或癱瘓敵軍事資訊系統指管能力，使敵因喪失資訊能力而無法發揮協同作戰能力。

四、網電一體戰

網電一體戰為共軍網路戰最重要的戰略思維之一。主要在建立力量，以摧毀敵網路中心戰體系，奪取戰場網路空間使用權，確保能於戰時，有效運用電磁頻譜與電腦及網路，遂行共軍一體化聯合作戰體系為目的。[50] 這是共軍對1991年之後美軍所進行的幾場戰爭，於各式作戰手冊、細則等重要文件中所提出對網路戰的研究結果。[51] 其認為結合電子戰與網路戰所形成的網電一體戰理論，不僅是一種作戰思想，更是一種能有效整合電子戰與網路戰的作戰形式與手段。[52]

網電一體戰中「網」為網路戰，「電」

45 戴清民，《網電一體戰引論》（北京：解放軍出版社，2002年），頁32；徐小岩，《信息作戰學》，頁166-167。

46 謝游麟，〈中共「癱瘓戰」思維與戰力發展研析〉，《國防雜誌》，第24卷第2期，2009年4月，頁81。

47 范承斌，《高技術條件下戰役癱瘓戰之研究》（北京：國防大學出版社，2003年），頁50。

48 國防報告書編纂委員會，《中華民國97年國防報告書》（臺北：國防部，2008年），頁176。

49 范承斌，《前揭書》，頁5-6。

50 Mulvenon James著，顏永銘譯，〈解放軍電腦網路戰：背景、原則、組織與能力〉，美國陸軍戰爭學院編，國防大學譯著，《超越臺海—臺灣問題外的解放軍任務》(*Beyond the Strait: PLA Missions other than Taiwan*)（桃園：國防大學，2010年），頁225-235。

51 廖文中，〈中國組建國家網軍：全球資訊戰〉，顧尚智、李夢麟主編，《2007年解放軍研究論壇彙編》（桃園：國防大學，2007年），頁263。

52 戴清民，《直面信息戰》（北京：國防大學出版社，2002年），頁259-274。

為電子戰，為奪取戰場網路控制權的重要戰略理論。[53] 網路戰以奪取網路控制權為主，電子戰則以爭取電磁頻譜控制權為主。網路戰乃於網際網路及戰場網路上同時進行的兩條戰線，網際網路戰線以敵基礎設施網路系統為攻擊目標，目的為削弱敵電腦系統效能，戰場網路戰線，則攻擊敵戰場有線、無線電網路，以削弱敵作戰能力。[54] 最有效的攻擊方式之一，是以病毒預置或感染目標電腦，平時可潛伏於遭感染電腦，並不動聲色的造成大規模傳染事件，執行網路刺探，以竊取重要情資，並待適當時機癱瘓敵電腦網路系統。共軍深知網電一體戰必須對網路作戰能力、指揮體系建置與編組等加以高度重視。[55] 如：對敵指揮控制中樞實施病毒攻擊，應以各種電子手段，將病毒輸入敵資訊網路的接收處理系統，癱瘓指管中樞。故現代戰場應由「電子戰」與「網路戰」來共同捍衛資訊權的重任，相互提高作戰效益創造勝利條件。[56] 並主張研發新式電子武器，包括高功率微波武器、等離子體武器、高能激光武器、電磁脈衝武器與動能武器等系統，用來干擾並摧毀敵人的C^4ISR系統。因此「網電一體戰」所要建構的能力為：C^4ISR一體化聯合作戰系統與網路空間攻擊的能力。另外，戴清民也指出對敵資訊網路系統打擊手段又分為電磁干擾制壓、電腦網路攻擊、綜合火力摧毀、新概念武器破壞、特種兵力破壞襲擾。[57] 因此建立軟殺傷、硬摧毀能力，成為共軍發展「網電一體戰」另一個重要的環節。

肆、共軍網路作戰能力

網路作戰(Cyberwarfare)已成為共軍最具破壞性的威脅，近年來共軍的網軍與民間駭客極可能已對世界各地目標展開廣泛有效的間諜活動，這些攻擊的範圍與效能突顯出戰時共軍可能將網路攻擊列為優先順序並加以運用。以下將進一步對共軍網軍部隊編制與教育訓練及作戰模式敘述如下：

一、共軍網軍的編成與教育訓練

中共網路空間的建設是以863計畫為起點，並以發展衛星、光纖、通信、電子、電腦相關技術為主，積極推動電腦網路基礎建設及電子商務「黃金計畫」的發展。[58] 中共鑑於波灣戰爭及國際間網路安全所引發相關爭議問題，進而大力扶植自主的電腦網路基礎技術產業。由此可知，中共對網路空間的建設，並非源於對資訊網路戰的先知，而是為了提升經濟及科技水準以吸引外資。中共中央軍委則震懾於波灣戰爭模式的改變，和國際間網路所引發的諸般問題影響，遂加速網路空間基礎建設的發展。其在發展資訊網路技術的同時，亦發現藉由網路入侵技術，

53 戴清民等編著，《信息作戰概論（修訂版）》（北京：解放軍出版社，2001年），頁21-25。

54 戴清民，《求道無形之境》（北京：解放軍出版社，2009年），頁90-94。

55 梅軍、樊祥，〈未來網電一體戰〉，《解放軍報》，2000年9月6日，版7。

56〈綜觀網路戰爭〉，《解放軍報》，2004年10月26日，版1。

57 戴清民，《直面信息戰》，頁285。

58 Feigenbaum A. Evan著，余佳玲、方淑慧譯，《中共科技先驅：從核子時代到資訊時代的國家安全與戰略競爭》(*China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to information Age*)（臺北：國防部部長辦公室，2006年），頁227-229。

可獲得重要的情報科技，得以跟進或模仿他國的軍事科技，乃向世界主要國家看齊，積極發展網路入侵、攻擊、防禦等相關程式技術。[59]

㈠網軍部隊編制

共軍超越傳統電子戰領域，發展出「網電一體戰」，針對資訊戰的發展，中共於1997年成立由國家主席所親自領導的「國家資訊安全工作領導小組」，整合軍、情、公安與資訊產業等各相關部門，進行網路安全保障與攻防能力的整體建置，其中由共軍總參負責對敵軍事與政治單位網路情蒐與攻擊任務，同時組建資訊民兵負責資訊安全保障。另在北京、蘭州、濟南與南京軍區均籌建有「資訊戰研究中心」，並投入大量人物力進行資訊作戰整備，包括加強人員訓練，以各軍事院校的資訊基礎教育為重點，配合新引進的光纖、數位通訊、衛星等裝備，培育專業人才，成立一支能進行高效能網際網路攻防戰的專責部隊「網軍」。[60] 主要正規編制如下：

1.共軍「總參二部」（軍事情報部）

科學裝備局負責發展電腦病毒、電磁脈衝等技術與試驗，研製戰術性「非殺傷性武器」。[61]

2.總參謀部第三部

負責「國防資訊化保障任務」，執行戰場網路情報蒐集，其位在武漢地區的第六局負責對我國技術情報（包括對臺衛星與高空偵照、電波截聽及從行動電話、網路數據）的情蒐及統整與研析。[62]

3.資訊戰基地

共軍自1999年5月發生駐南斯拉夫大使館遭到北約轟炸事件後，迄今已分別在山西大同、福建廈門、上海、四川宜昌及陝西西安建立5大資訊戰基地，各設有後備電子戰部隊。各基地負責不同發展重點，如上海基地著重無線電通訊網路、密碼設定及破譯；另在東北的吉林省則設有假想敵電子戰部隊，其目標包括：施放資訊水雷、實施資訊偵察、變更網路資訊、投下資訊炸彈、傾倒資訊垃圾、散播心戰宣傳、複製資訊、組建資訊防護措施與建立網路間諜站。[63]

4.資訊兵團

各軍區設置戰區聯合作戰指揮部，並成立「資訊對抗中心」，負責電子對抗及網路資訊體系的防護，另設置若干資訊兵團，其下並組建資訊戰營。

5.資訊戰武器及戰略專責研究機構

⑴解放軍電子科技學院。

⑵共軍軍事科學院及國防大學

負責研發各種資訊戰的作戰指導與準則，並積極培育訓練各項執行任務的軍官和士兵。

59 李華球，〈沒有煙硝的戰爭—中共解放軍網軍資訊作戰的初步觀察〉，顧尚智、李夢麟主編，《2007年解放軍研究論壇彙編》（桃園：國防大學，2007年），頁240-241。

60 李文忠、張國城、陳文政、陳宗逸、蘇紫雲，〈民間版「國防白皮書」〉，《臺灣新社會智庫》，2009年5月11日，<http://www.taiwansig.tw/index.php?option=com_content&task=view&id=1383&Itemid=117>（檢索日期：2015年3月30日）

61 陳以明，〈中共在網路戰及其網軍發展研析〉，《安全局科技情資》，第16期，2008年，頁56-57。

62 羅添斌，〈中國對臺網攻大本營藏身武漢大學〉，2015年3月9日，《自由時報》，版A2。

63〈美軍方研究報告「中共培訓資訊戰部隊，駭客擔綱」〉，2001年5月25日，《中國時報》，版11。

⑶資訊戰模擬中心

各軍團還全面規劃相關訓練課程，使指揮層級軍官了解資訊戰發展，課程內容包括：資訊戰理論、通訊網路技術、電子反制、數位化部隊、資訊戰略戰術及電腦病毒攻擊等。

共軍「非接觸先敵攻擊」參演部隊曾加入北京軍區第38集團軍數位化合成營。[64] 共軍自1985年起，就開始發展「網電一體戰」的能量。現已組建一支超過10萬人的網路部隊，而其目標是在2020年建立全球第一支「資訊化武裝部隊」。共軍將網路戰發展成整合軍事、情報、研發等部門，已由理論走向實務，企圖直接攻擊美國通訊網路基礎建設，掌握發動攻擊入口，進一步癱瘓後勤，攻擊供應鏈，包括運輸、物流、金融業者等。[65]

㈡網軍教育訓練

1.人民解放軍理工大學

共軍1999年整併通信工程學院、工程兵工程學院、空軍氣象學院以及總參附屬的63個相關研究所，重新組建「人民解放軍理工大學」，並於該校成立「全軍網路技術研究中心」。從全國調集400餘名數學、理工、電子、電機、電腦、雷達、天線等專業科目的專家、教授任教，全力研發資訊戰的關鍵技術。學員生自民間大學和軍中招收，國防部同時設立獎學金，自北京、清華及交通大學等名校挑選天才型學生，提供資助並於畢業後到軍隊工作。2002年時已有200多名學生接受所謂培才獎助。該校計畫每年引進和選留60名博士生充實師資，要求在10年後達到40歲以下教授群全都具備博士學位目標。[66]

另該校主要研究項目，是戰爭型態由機械化轉向資訊化過程中的各種變化，包含軍隊編制、武器裝備、戰略戰術，教育訓練和後勤補給等。該校的成立對其軍隊轉型和未來面對高度資訊化的軍事力量、戰爭條件、戰略決策、戰術研究、準則分析、裝備發展等新作戰空間形成兼具教育訓練，準則發展、實作驗證等多重作用的智庫和基地。[67]

2.中共國防科技資訊中心[68]

負責資訊技術、軟體科學研究及支援服務。

3.中共資訊安全研究室[69]

於1989年成立，由中共科學院主管，附屬於中國科學院信息工程研究所，從事電腦病毒、駭客攻擊及反制的「軟件組織的對抗」。

4.共軍資訊戰研究中心

共軍各軍區設立性質不同的研究中心：

⑴濟南軍區：在鄭州組建資訊戰模擬研究中心。

64〈我軍6月下旬將舉行首次新型作戰力量聯合演練　數字化合成營首次公開亮相〉，《新華網》，2013年5月28日，<http://news.xinhuanet.com/mil/2013-05/28/c_124777402.htm>（檢索日期：2015年3月30日）

65 吳胤曦，〈前揭文〉，頁135。

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

67 廖文中，〈中國網軍：國安、公安與解放軍〉，頁2。

68 陳以明，〈前揭文〉，頁56-57。

69 陳以明，〈前揭文〉，頁57。

⑵濟南軍區：在濟南組建資訊戰保密研究中心。

⑶北京軍區：在北京組建資訊戰作戰研究中心。

⑷南京軍區：在南京組建資訊戰情報研究中心。

⑸蘭州軍區：在西安組建資訊戰裝備發展中心。

其中北京軍區的資訊戰作戰研究中心與國家安全部所屬特種資訊研究中心（前身為特異功能研究中心）合作，將各地產業機構、機關院校中具有編碼、破譯等數學天資優異人士，送到該所鑑定，並運用曾在資訊網路利用電腦系統進行「駭客」活動（如竄改資料、經濟犯罪、金融犯罪）的犯人，經過判刑後送至該所一邊服刑、一邊在研究中心執行若干秘密任務。[70]

駭客是指運用資訊軟體，利用電腦或網路安全漏洞或破解安全措施進行非法侵入，擷取或篡改資料，危害資訊安全的行為者。駭客從遠端秘密的侵入，受害者難以察覺。駭客攻擊之相關資訊如表3，駭客對資訊系統攻擊的目的為癱瘓資訊系統或獲得所需的資料，其攻擊型態與方式多樣。[71]

二、共軍網路作戰模式

共軍認為電腦網路攻擊是在軍事上「以弱擊強」最有效的方法，其發動攻擊的方式包括：駭客攻擊、病毒攻擊、資訊污染、資訊干擾與資訊偵察等。[72] 共軍進行網路戰的目標，主要包括：摧毀敵軍的指揮系統、縮短戰爭運作時程、以及加強軍事運作效能。

㈠共軍網路戰特性

依據共軍網路戰略發展現況，再從近年來的局部戰爭中網路作戰的運用，推論其網路戰具有以下主要特性：

1.長期性始終連綿不斷的全面戰爭。

2. 全方位有形與無形戰線的總體戰爭。

3.綜合型生死存亡攸關的特殊戰爭。

並進一步可歸納出網路戰11項的基本特徵（如表4）。

㈡共軍網路作戰方式

在電腦網路領域的攻擊手法，主要以病毒、邏輯炸彈、晶片等手段，削弱、破

表3　駭客攻擊資訊系統目標與方式

資訊系統元件	攻擊目的	攻擊型態
實體元件	使電腦硬體失效或發生錯誤。	預置硬體炸彈瓦解、電力系統。
傳送元件	截收數據或瓦解通信。	竊聽、欺騙或干擾、電腦入侵。
軟體	使軟體功能失效或破壞或建立對其之控制。	預置軟體邏輯炸彈、運用軟體害蟲、病毒或電腦入侵。
資料	摧毀、竊取或破壞電腦資料。	病毒、電腦入侵。

資料來源：Zalmay M.Khalilzad, John P. White，國防部史政編譯局譯，戰爭中資訊的角色變化(The Changing Role of Information in Warfare)（臺北：國防部史政編譯局，2003年）：頁226。

70 廖文中，〈中國網軍：國安、公安與解放軍〉，頁4。

71 曹邦全，《中共信息戰之研究》（高雄：國立中山大學大陸研究所碩士論文，2001年），頁84。

72 蔡明彥，〈前揭文〉，頁71。

表4　網路戰特徵

終極武器	電子干擾器、電腦病毒、定向能武器、電磁脈衝彈等。
武器效應	資訊刪除或極小精準的破壞。
作戰時段	全天候、全時辰。
作戰下令至執行的時間	實時(real time)。
決勝負的時間	瞬間。
戰爭的空間	陸、海、空、天（太空）、磁五維。
前後方之分別	無。
決勝負地點	敵我方內部爲主。
戰況能見度	我方：單向透明、敵方：隱蔽性高。
參戰人員	無性別年齡限制。
出兵密度	低。

資料來源：陸委會，〈信息戰及超限戰的涵義、特徵〉，《陸委會大陸資訊及研究中心》，1999年9月28日，<http://www.mac.gov.tw/ct.asp?xItem=48917&ctNode=5842&mp=4>。

壞敵電腦網路系統使用效能，並以保護己方電腦網路運行為目的，性質上則區分電腦網路偵察、進攻、防禦等任務。[73]「麥卡菲」(McAfee)電腦安全公司自2009年起發現全球石油、能源、和石化公司員工極易遭受魚叉式網路的釣魚電子郵件攻擊，導致油、氣田投標與公司營運之私有資訊遭竊，報告更直指網路攻擊行動來自共軍位於上海的61398部隊。[74]並指出攻擊行為雖「不甚複雜」，但卻協調良好、目標明確、且「極為成功」。[75]顯見共軍網路攻擊不僅只於戰時實施亦可攻擊非軍事目標，且戰法已從低階的網頁置換，提升至社交工程攻擊、零時差攻擊、郵件精準攻擊、網頁漏洞攻擊、資料庫隱碼攻擊及針對網路節點執行網路癱瘓等網路戰作為。

依國際資安廠商分析駭客採用的攻擊手法分析，可以將網路攻擊的方式，依其實施階段歸類區分為：偵察、零時差攻擊、入侵潛伏、植入後門程式、遠端控制、資料過濾外傳、撤離及預留隱藏的活棋等8種類型：[76]

1. 偵察

駭客鎖定特定對象，先利用社交工程取得相關資料，進而發覺可以入侵或利用的弱點。

73 總參謀部通信部編著，《信息作戰學》（北京：解放軍出版社，2002年），頁158。

74 Office of the U.S. National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (Washington, D.C.: Office of the U.S. National Counterintelligence Executive, 2011), p. 5.

75 Brian Prince,“McAfee: Night Dragon Cyber-Attack Unsophisticated but Effective.”*eWeek.com*, February 10, 2011, <http://www.eweek.com/c/a/Security/McAfee-Night-Dragon-Cyber-Attack-Unsophisticated-But-Effective-303870/.>（檢索日期：2015年3月30日）

76 陳嘉宏，〈新型態戰爭及資安防護策略探討〉，《新新季刊》，第42卷第1期，2014年1月，頁229-230。

2.找出可利用的漏洞（釣魚郵件或零時差）

利用發送互動式的網路釣魚郵件，針對被鎖定對象寄送相關的惡意郵件，夾帶惡意Word或PDF文件，利用還未修補的漏洞，取得在電腦植入惡意程式的第一個機會。

3.入侵潛伏

駭客入侵、滲透進企業後，通常會先潛伏一段時間，並偵測目標物是否為誘捕密罐(Honey pot)。為了確保攻擊成功，該惡意程式入侵後，會自我隱藏以避免被安全軟體發現。

4.植入後門程式

植入後門或惡意程式取得管理者的帳號、密碼和權限，針對橫向沒受攻擊的網路系統，利用漏洞植入後門程式後，也會取得其他重要人士的帳號密碼。

5.C & C可遠端控制工具

安裝遠端遙控下指令(Command & Control)工具，用來偷密碼、存取電子郵件、修正運行程式，還可以將機敏資料或智慧財產權，利用Tunnel或是木馬程式將內網資料往外送。

6.資料過濾外傳

當駭客鎖定攻擊對象、過濾找到所需的機敏資料外，會利用FTP和加密方式傳送機密資料至連線中繼站等行為；若有無法辨識的檔案格式，駭客也可能採用自己的加密方式外傳。

7.撤離

將機敏資料往外傳後，駭客會先確認任務完成後才會進行撤離，同時會隱藏自己在系統中存在的蹤跡，不讓人有跡可尋，也會利用洋蔥式的路由和加密方式傳送機敏資料，隱形自己存在。

8.預留隱藏的活棋

為了未來有需要時還可以操控該臺受駭電腦，駭客撤離前會在受駭系統留下沉睡的惡意程式(Sleeping Malware)，或將之設定為僵屍網路(BOTNET)其中一員，以便有需要時隨時可用。

林肯(E. Lincoln Bonner)認為網路作戰的重點在於平日以網路偵察蒐集技術情報以獲取優勢，並於戰時運用情蒐成果，對敵弱點、重點與關鍵節點施以阻絕作為，以擴大交戰雙方網路優勢差異。以俄羅斯與喬治亞戰爭結果為例，說明俄羅斯的網路攻擊集中且經過精心準備，顯示其對喬治亞的網路優勢與阻絕行動，乃早在衝突前就展開的網路偵察及網際空間情報整備之產物。其對喬治亞所進行的網路阻絕活動包括網站篡改及分散式阻斷服務(distributed denial of service, DDoS)攻擊，另殭屍網路攻擊(botnet as-sault)的範疇與集中度都相當精準，只專注攻擊11個目標，且自始自終持續攻擊相同的網站。大部分的網路攻擊都是專門針對喬治亞的特定目標，其中至少有一次網路篡改行動是在戰爭爆發的2年前就已準備就緒。[77] 顯示戰時使用的網路攻擊方式包括網站篡改及分散式阻斷服務(distributed denial of service, DDoS)與殭屍網路攻擊(botnet as-sault)等方式。

1.網站篡改

對敵主要官方、通信、金融與新聞

77 E. Lincoln Bonner著，高一中譯，〈網權在21世紀聯合作戰的角色〉(Cyber Power in 21st-Century Joint Warfare)，《國防譯粹》，第42卷第2期，2015年2月，頁21。

媒體網站進行網站篡改，可使敵國人民與官員無法獲得正確訊息，藉以散布混亂狀況，打擊敵國軍民抗敵意志，並遲滯國際因應行動。

2.分散式阻斷服務

藉由傳遞大量資訊，使敵國網路資訊流量與流速的需求激增，亦可阻塞正常資訊的傳遞速度，最終造成系統癱瘓。

3.殭屍網路攻擊

於戰前傳遞病毒至特定資訊系統潛伏，並於開戰直前啟動，以癱瘓敵重要網路系統。

㈢網軍作戰演訓

共軍瀋陽、北京及成都軍區分於1997、1999及2000年實施電腦病毒攻擊、電腦對抗演練及網際網路演訓，中共國務院自2002年起在資訊產業部（2008年6月29日改制為工業和資訊化部）底下成立「網路戰士」秘密組織，化名為民間電腦駭客組織。並提升部分網路戰士為駭客，由共軍與國家安全部實施更高層級的訓練和任務；另一部分則轉入軟體設計，從事突破敵防火牆以進行放毒、竄改和網內盜竊資料的訓練，最終成為「密碼破解員」，專門執行對美、日、臺灣等地要害部門的電腦入侵任務。具備國外生存能力者，則由中共設法安排出國，作為派駐國外進行網路戰的節點，定期或不定期返國經驗交流，必要時由中共投入資金組成公司型態的海外「駭客」據點。[78]

2004年共軍在成都軍區進行一體化聯合作戰訓練會議，由時任共軍總參謀長助理的范長龍主持，集合中央和成都軍區內相關院校、機關、軍隊的專家和部隊長進行有關「一體化聯合作戰和一體化訓練的新理論研究」為題的研討會。總結軍隊一體化訓練就是「資訊融合的整體訓練」、「作戰體系的聯合訓練」、「作戰要素的整合訓練」，而貫穿全程作戰經絡的就是資訊戰能力。同年11月濟南軍區動員轄屬各級部隊投入資訊化軍隊聯合訓練的各項演練，並於2006年11月8日進行「前衛206B」實兵軍事演習。演習兵力以電子戰部隊為主，結合陸軍航空兵、新型砲兵部隊和集團軍特戰兵力共8千餘人，在膠東半島萊州灣實施資訊戰實兵演練。[79]

「前衛206B」資訊戰實兵軍事演習是共軍自2000年起到2006年，經歷多次研究和實證，在不同軍、兵種間進行稍具規模的實兵演習，期間不同階段、軍種、兵種、輸具、戰具與屬性的戰力，透過電子戰部隊的「網軍」資訊力予以整合，顯示其網路戰已不再是單一軍兵種的獨立作戰。[80] 另由共軍「使命行動—2013」演習實況觀察，其電子戰攻擊及防護能力雖不如美軍，但未來發展的空間卻極大，且已在C^4ISR系統方面獲得革命性進步，並具備很多此前只有美軍才擁有的資訊戰能力。[81]

78 廖文中，〈中國網軍：國安、公安與解放軍〉，頁4-5。

79 張玉清、徐壯志，〈濟南軍區“前衛－206B”軍事演習進入作戰階段〉，《新華網》，2006年11月14日，<http://big5.news.cn/gate/big5/news.xinhuanet.com/mil/2006-11/14/content_5330020.htm>（檢索日期：2015年4月10日）

80 廖文中，〈網路斬首戰及公安網軍〉，《全球防衛雜誌》，272期，2007年11月8日，頁2。

81 李可為，〈外媒稱中國軍演「近十年世界罕見」〉，《文匯網》，2013年9月20日，<http://news.wenweipo.com/2013/09/20/IN1309200028.htm>（檢索日期：2015年9月28日）

伍、對我資電作戰之影響

具體而言，網路作戰賦予共軍三項能力：首先，使共軍具備竊取特定電腦網路弱點之資料能力；其次，可供其標定後勤、通信及商用網路，藉以限制敵行動或延緩其反應時間；第三，可於危機或衝突期間搭配軍事攻擊，強化其軍事作戰效能。[82]

國軍通資電作戰係依「科技先導、資電優勢」的建軍構想，以整合通資基礎建設、發揮國軍聯合電子戰力、強化國軍聯合作戰指管系統能力、提升資訊確保能量與創新國軍資訊服務等手段，建立與運用資電戰力，以支援軍事作戰行動。[83] 因此，上述資電作戰主要手段之執行將直接影響國軍能否獲得資電優勢，亦將影響我防衛作戰之成敗，以下依上述國軍資電作戰手段進一步分析共軍網路作戰能力對我資電作戰之影響。

一、整合通資基礎建設

以建置國軍資訊傳輸主幹網路，提供國軍戰情、指管等系統資訊傳遞，以提升國軍網路作戰效益及戰場存活率。然共軍網路作戰模式之一，即為戰前截斷並損害敵基礎設施網路。[84] 若國軍資訊主幹網路遭敵網路攻擊，將嚴重影響國軍聯戰效能。

二、發揮國軍聯合電子戰力

整體規劃與整合國軍無線電通信頻率資源，強化通資系統作業環境，並結合軍種與聯戰網路，以滿足三軍聯合作戰需求。然若過度依賴資訊作業且未建立備援系統，將使全軍遭受嚴重資安威脅。

三、強化國軍聯合作戰指管系統能力

為有效發揮統合戰力，國軍將以現有C^4ISR系統為架構，持續建構國軍網狀化作戰能力，以使情資、指管及武器載臺能同步實施戰場情資交換，提升戰場透明度，發揮聯戰效益。惟過度依賴網路空間增強聯戰效能的同時，本身亦將成為網路攻擊的受害者，一旦網路空間遭敵控制，非但無法增進聯戰效能，更將癱瘓全軍戰力。

四、提升資訊確保能量

國軍結合國家資通安全防護體系，強化網路安全整備，並透過資安講習、資安通報、資安突檢及緊急應變演練等各項強化作為，以提升整體資安強度。惟近年來共軍常以電子郵件偽冒長官、同僚及部屬身分遂行社交工程，誘使收件人開啟惡意郵件，致使電腦遭植入病毒，進而攻擊特定對象，盜取資料，嚴重威脅國軍資訊安全。

另國軍為建立網路戰的反制能量，已成立資電作戰部隊，配合通資安全技術研發及中科院網安計畫，建立監控病毒與防制技術能量。然共軍網路作戰兵力已達十萬餘人，國軍僅3千餘人且以網路防護為主，數量懸殊且戰略過於消極，戰時恐難確保資電優勢。

五、創新國軍資訊服務

配合國家電子化政府政策，整合運用資訊科技與通信網路，可使使用者於任一時間、地點與電腦上網作業，提升工作效能，奠定國防部知識管理與決策指導之基礎。然水能載舟亦能覆舟，綿密的資訊系統與網路空間，雖能提升工作效能，卻也增加遭受網

82 Ashley J.Tellis著，李永悌譯，《戰略亞洲2012-13中共軍事發展》(*STRATEGIC ASIA 2012-13 CHINA'S MILITARY CHALLENGE*)（臺北：國防部，2014年），頁187。

83 國防報告書編纂委員會，《中華民國102年國防報告書》，頁111-112。

84 Larry M Wortzel著，章昌文譯，〈前揭文〉，頁12。

路攻擊的風險與機率。

以2008年俄羅斯介入喬治亞內戰為借鏡，[85] 可知共軍網路作戰除戰時運用外，亦可於平時非法入侵我電腦資訊系統及使用惡意軟體，包括運用邏輯炸彈、後門、木馬程式及其他電腦病毒。[86] 惡意軟體可透過各式手段安裝於電腦系統，包括直接入侵電腦系統、利用「網路誘捕系統」(honeypots)及「魚叉式網路釣魚」(spear phishing)（電子郵件冒名頂替）等。[87] 亦會將錯誤的資訊置入我資訊系統以收欺敵之效。[88] 面對複雜的資電作戰環境，網路空間已成為現代戰爭之重要戰場，共軍網路軍事發展及駭客攻擊能力已成為當前國防安全威脅。共軍持續入侵我相關網站，並透過遠端滲透、病毒（惡意程式碼）感染、竊取或監控等侵入行動。一旦衝突爆發，將癱瘓我指管、後勤網路，影響國軍資訊系統正常運作並遲滯國軍應變能力。[89]

陸、我防衛作戰因應作為

網路空間已成為作戰領域之一，[90] 面對共軍網路作戰能力的潛在威脅，依據102年1月修正之「行政院國家資通安全會報設置要點」，我國資通訊安全政策及通報應變機制（如圖3）等重大計畫與事務之協調及督導，統由該會報負責。（如圖4）

由上述內容可知我國面對網路安全威脅，在國家安全階層已成立相關組織統籌綜合國力與訂定相關應變程序以為因應，惟以2008年俄羅斯介入喬治亞內戰為例，網路作戰最重要亦是最不易察覺的階段就是戰前網路偵查與情蒐階段，故我防護重點應置於防制共軍網路偵查之各項作為，以下將依據上述內容，並參考國防部資安相關作為及美國學者理查克拉克(Richard A. Clarke)之網路防禦戰略，[91] 於軍事安全階層提出我資電作戰相對因應之道。

一、加強網路戰略目標防護

依據我國行政院訂頒「國家關鍵基礎設施安全防護指導綱要」，[92] 配合關鍵基礎設施業管部門排定之防護優先次序，確認我國網路戰略防護目標，配合研修防護計畫與實施演練，並加強網路光纖主幹線第一層網際網路服務提供者的資訊安全作為並設置檢查點，確保關鍵基礎設施安全。

二、建置備援資訊系統

為有效維護國軍聯戰效能，應於平時

85 E. Lincoln Bonner著，高一中譯，〈前揭文〉，頁15。

86 郭勝偉，《前揭書》，頁255。

87 郭勝偉，《前揭書》，頁312。

88 戴清民，《前揭書》，頁197。

89 國防報告書編纂委員會，《中華民國102年國防報告書》，頁59。

90 DOD, DOD Strategy for Operating in Cyberspace(Washington, D.C.: GPO, July 2011), p. 5.

91 國防部，〈我國如何因應網軍與駭客攻擊並強化資訊安全措施報告〉，《立法院公報》，第102卷第29期，2013年4月29日，頁4-5；Richard A. Clarke著，王文勇譯，《網路戰爭下一個國安威脅及因應之道》(*CYBER WAR THX NEXT THREAT TO NATLONAL SECURITY AND WHAT TO DO ABOUT IT*)（臺北：國防部，2014年），頁178。

92 行政院國土安全辦公室，〈國家關鍵基礎設施安全防護指導綱要〉，《行政院國土安全辦公室》，2014年12月29日，<http://www.rrb.gov.tw/05810.aspx?id=142>。

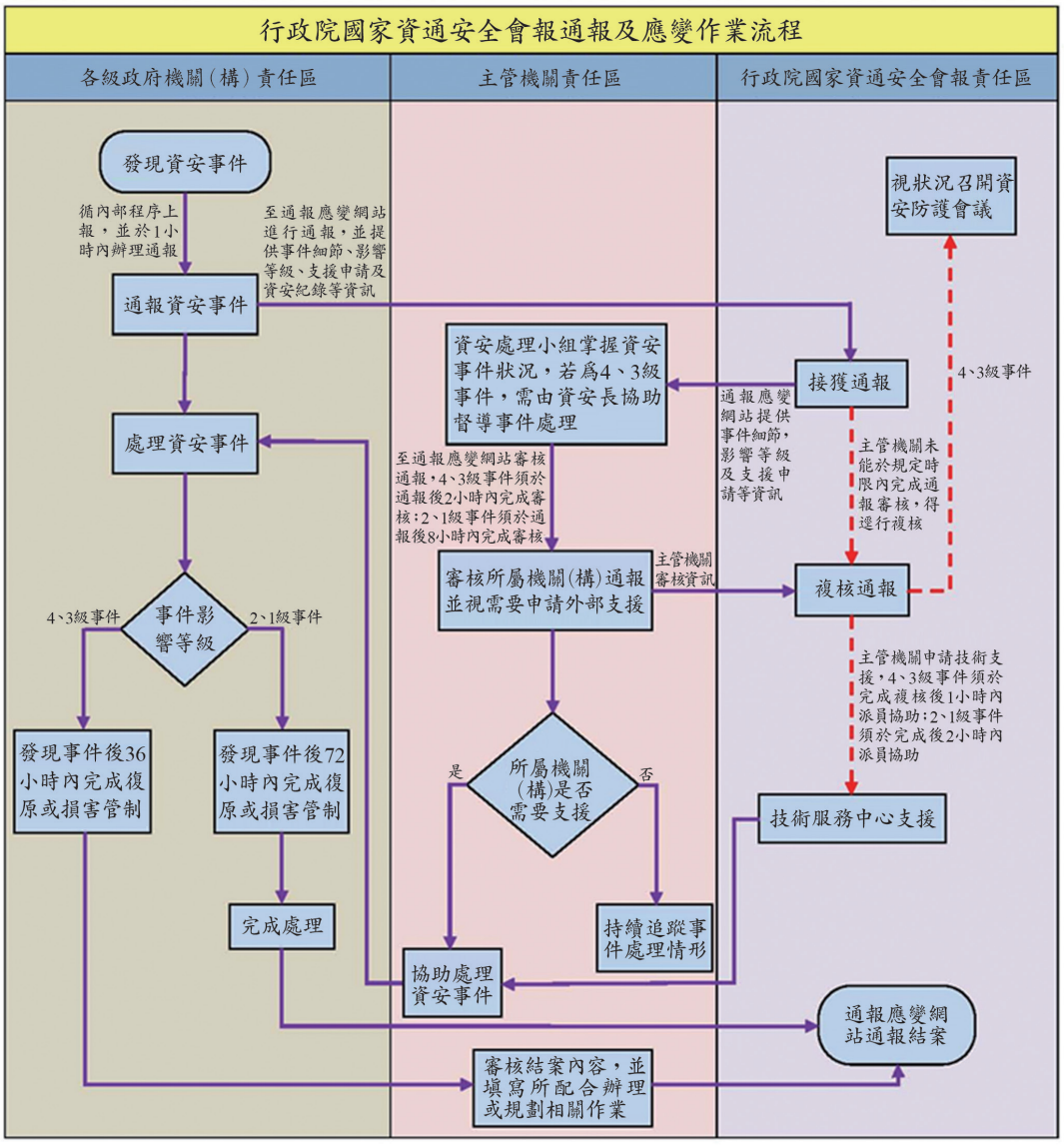

圖3　資安事件通報及應變作業流程

資料來源：行政院國家資通安全會報，〈國家資通訊安全通報應變作業綱要〉，《行政院國家資通安全會報》，2014年6月23日，<http://www. nicst.ey.gov.tw>。

訓練增加無資訊系統搭配之作戰科目，並納入演訓規劃，另於異地備援地點建立主要資訊作業系統資料同步儲存與復原中心，平時透過高速網路或專線將資料非同步完成傳送備份；同時建立同步運作的系統，當主機遭受網路攻擊喪失效能時，可即時由備援中心接手運作，以因應戰時喪失電磁權之作戰環境。

三、建立網路作戰能量

美軍為因應網路作戰威脅，於2009年成立網路指揮部，[93] 不僅負責防護軍事網路免於遭受有心人士滲透、竊密，以及破壞，更

93 Richard A. Clarke著，王文勇譯，《前揭書》，頁10。

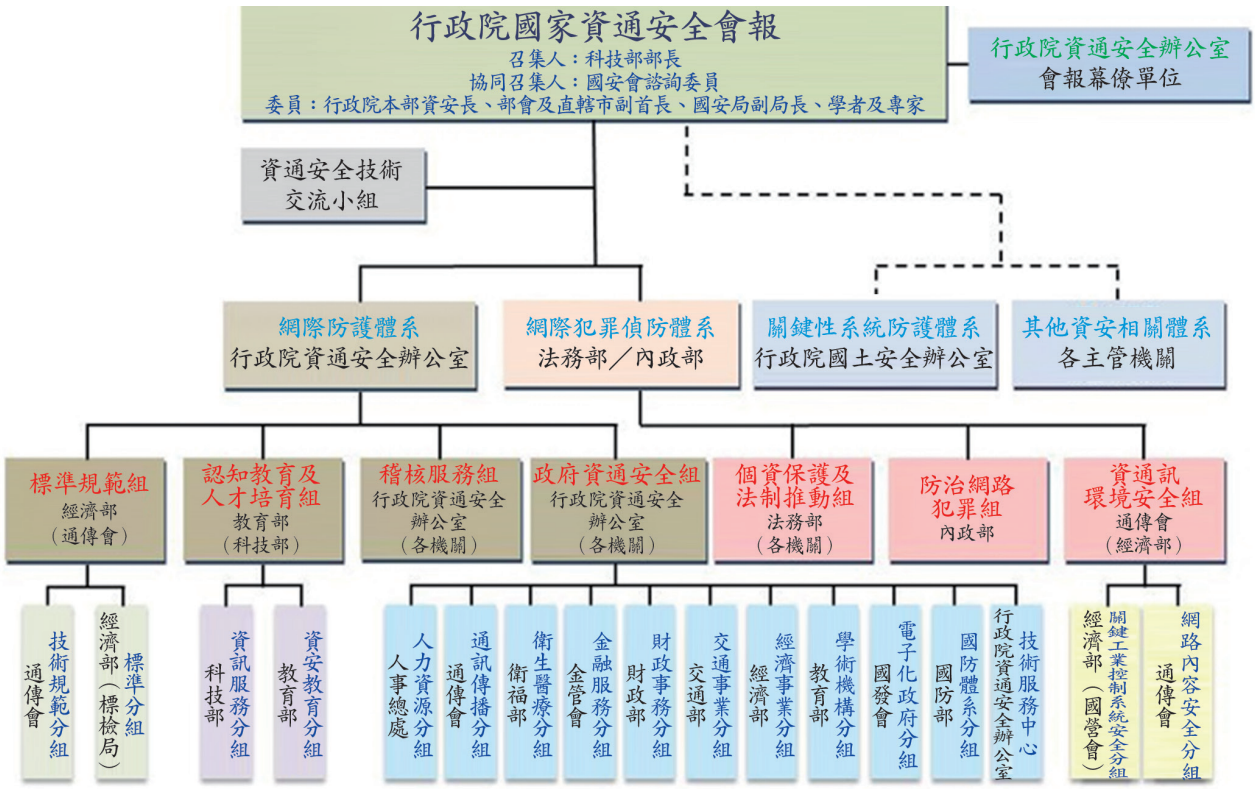

圖4　行政院國家資通安全會報組織架構

資料來源：行政院國家資通安全會報，〈國家資通訊安全發展方案〉，《政府機關資訊通報》，第315期，2013年12月25日，頁8。

是被賦予發展進攻型式之網路武器，作為其進行嚇阻戰略的強而有力之後盾，[94] 我國主要網路作戰部隊為國防部2004年編成之資電作戰指揮部，[95] 作戰任務主要以網路戰與電子戰為主，成軍雖較美軍為早，然其前身為國防部統一通信指揮部，其編組與作戰能力仍以通信網路建立、操作與維護為主。建議應依當前敵情威脅，適時調整組織架構與任務比重，統籌全軍網路作戰能量，並參考美軍與共軍作法，招募民間網路作戰專才，施以初階訓練後依據任務屬性逕行分流，並將網路作戰納入年度實兵演訓規劃，以強化網路作戰能量。

四、強化網路資安環境

建置資安監控中心，訂定相關資安防護策略，除保護網路本身及防護各端點外，還要在連接國軍各種網路的所有電腦中安裝防火牆、防毒軟體，以阻止惡意軟體或病毒的侵入，並監控所有網路以察覺未經授權的新連線，並自動關閉未經許可的裝置，以強化作業系統及資訊設備的資安防禦縱深。

五、提升資安防護作業習性

94 Ellen Nakashima, "Gates Establishes Cyber-Defense Command, The Washington Post, June 24, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062303492.html>（檢索日期：2015年4月21日）

95 邱志強，〈資電作戰指揮部正式成軍〉，2004年4月1日，《青年日報》，版3。

除將現行上傳至光纖電纜主幹線傳輸之整批資料加密外，另所有電腦中的所有檔案及在資料儲存伺服器中的資料，均應予以加密，並要求國軍網路的所有使用者在登錄時，須經過至少兩道驗證程序以證實登錄者的身分。

六、建立資安防護機制

訂定資訊系統安全等級的分類標準，將重要的資訊系統或資料從網際網路隔離單獨運作，加強資通安全軟硬體環境建置，並研擬一套符合國民性的嚴格檢查及研究計畫與防護技術，以確保重要武器、指管、後勤使用的軟體及硬體不會被滲入後門程式或邏輯炸彈。

七、持恆資安教育訓練

為普及資訊安全教育，在基礎、分科、進修及深造等各級教育，規劃資安課程，應於各軍事院校專業系所，排定資訊安全專業課程，俾使國軍各級幹部均具備基本資訊安全素養，另應成立網路作戰研究中心，以奠定網路作戰教育訓練基礎。

柒、結　　論

近年來共軍在國防預算充分支持下，正逐年實現軍力現代化目標，其「網路戰略」概可區分為不對稱作戰、網路癱瘓與威懾，並以網電一體戰癱瘓我民生供給與軍事作戰系統為手段，以威懾我軍民抗敵意志，達成其不戰而屈人之兵的戰略目標；另網路作戰中共軍以找出可資竊取資料之特定電腦網路的弱點為重心，可供其標定特定網路目標，藉以限制國軍行動或延緩其反應時間。最終可於危機或衝突期間搭配軍事攻擊，強化其作戰效能。

共軍網路戰略與能力發展之現況，已對我資電作戰產生重大威脅，嚴重危害我「整合通資基礎建設、發揮國軍聯合電子戰力、強化國軍聯合作戰指管系統能力、提升資訊確保能量與創新國軍資訊服務」等資電戰略之執行。

本研究發現共軍為實現其「立足打贏資訊化條件下局部戰爭」之網路戰略，將持續提高資訊系統於聯合作戰運用的比重，以精進其軍兵種聯合作戰能力。顯現共軍認為資訊優勢為軍事鬥爭之基礎，並藉由創新發展人民戰爭戰略，創建網路戰民兵，擴大其網路作戰基礎。而我國在現有資通訊安全政策屬防禦策略的現況下，將對我資電作戰產生嚴重威脅，實不可不慎。

以美軍為例，美國國防體系在網路安全威脅當中，扮演著非常重要角色。其網路司令部不僅負責防護軍事網路安全，更被賦予發展進攻型式之網路武器，作為其進行嚇阻戰略的強而有力之後盾。對照我國軍事戰略構想「防衛固守、有效嚇阻」，實質上軍隊運作必須謹守「網路資安防護」之思維。然網路攻擊已成為我國家安全的重大挑戰，面對共軍每年持續增加的軍事投資，顯示國軍此項戰略思維仍過於保守，若能運用網路空間之隱匿、快速之特性，結合民間專業人才，建置專業網路作戰部隊，發展國軍網路攻擊能力，方可遂行「有效嚇阻」戰略。

（收件：104年8月14日，接受：104年10月19日）

參考文獻

中文部分

專書

王克海、王兵、曹正榮，2005。《一體化聯合作戰研究》。北京：解放軍出版社。

王鳴鳴，2008。《外交政策分析：理論與方法》。北京：中國社會科學出版社。

伍仁和，2004。《信息化戰爭》。北京：軍事科學出版社。

沈偉光，2000。《第三次世界大戰—全面信息戰》。北京：新華出版社。

沈偉光，2005。《2010信息災害：發展中國家生存戰略》。北京：新華出版社。

林中斌，1999。《核霸：透視跨世紀中共戰略武力》。臺北：臺灣學生書局。

范承斌，2003。《高技術條件下戰役癱瘓戰之研究》。北京：國防大學出版社。

徐小岩，2002。《信息作戰學》。北京：解放軍出版社。

國防報告書編纂委員會，2008。《中華民國97年國防報告書》。臺北：國防部。

國防報告書編纂委員會，2013。《中華民國102年國防報告書》。臺北：國防部。

張占軍，2007。《論信息中心戰》。北京：國防大學出版社。

戚世權、梅軍、陳克林、單琳鋒、朱玉萍、劉慶國，2001。《論制信息權》。北京：軍事科學出版社。

郭勝偉，2008。《信息化戰爭與網電部隊》。北京：國防大學出版社。

戴清民，2001。《信息作戰概論（修訂版）》。北京：解放軍出版社。

戴清民，2002。《直面信息戰》。北京：國防大學出版社。

戴清民，2002。《網電一體戰引論》。北京：解放軍出版社。

戴清民，2009。《求道無形之境》。北京：解放軍出版社。

總參謀部通信部編著，2002。《信息作戰學》。北京：解放軍出版社。

專書譯著

Clarke, Richard A.著，王文勇譯，2014。《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。

M.Khalilzad, Zalmay, White, John P.著，國防部史政編譯局譯，2003。《戰爭中資訊的角色變化》(*The Changing Role of Information in Warfare*)。臺北：國防部史政編譯局。

Tellis, Ashley J.著，李永悌譯，2014。《戰略亞洲2012～13中共軍事發展》(*Strategic Asia 2012-13 China's Military Challenge*)。臺北：國防部。

Richard, Spinello著，李倫譯，2007。《鐵籠，還是烏托邦：網絡空間的道德與法律》(*Cyber Ethics: Morality and Law in Cyberspace*)。北京：北京大學出版社。

Evan, Feigenbaum A.著，余佳玲、方淑慧譯，2006。《中共科技先驅：從核子時代到資訊時代的國家安全與戰略競爭》(*China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to information Age*)。臺北：國防

部部長辦公室。

Mulvenon, James著，顏永銘譯，2010。〈解放軍電腦網路戰：背景、原則、組織與能力〉，美國陸軍戰爭學院編，國防大學譯著，《超越臺海—臺灣問題外的解放軍任務》(*Beyond the Strait: PLA Missions other than Taiwan*)。桃園：國防大學。頁225-235。

專書論文

李華球，2007。〈沒有煙硝的戰爭—中共解放軍網軍資訊作戰的初步觀察〉，顧尚智、李夢麟主編，《2007年解放軍研究論壇彙編》。桃園：國防大學。頁237-262。

廖文中，2007。〈中國組建國家網軍：全球資訊戰〉，顧尚智、李夢麟主編，《2007年解放軍研究論壇彙編》。桃園：國防大學。頁263-311。

期刊譯著

Bonner, E. Lincoln著，高一中譯，2015/2。〈網權在21世紀聯合作戰的角色〉(Cyber Power in 21st-Century Joint Warfare)，《國防譯粹》，第42卷第2期，頁14-27。

Wortzel, Larry M著，章昌文譯，2014/10。〈評論中共軍事現代化及其網路活動〉(China's Military Modernization and Cyber Activities: Testimony of Dr. Larry M. Wortzel before The House Armed Services Committee)，《國防譯粹》，第41卷第10期，頁4-19。

Chertoff, Michael著，鄧炘傑譯。2015/8。〈網路公共領域的戰略意義〉(The Strategic Significance of the Internet Commons)，《陸軍學術雙月刊》，第51卷第542期，頁136-146。

期刊論文

王高成，2004/4。〈中共不對稱作戰戰略與臺灣安全〉，《全球政治評論》，第6期，頁19-34。

吳胤璽，2014/9。〈全球隱密監控與國家間反應：以「梯陣」、「稜鏡」間諜網絡為例〉，《國防雜誌》，第29卷第5期，頁113-144。

吳嘉龍，2014/9。〈網路科技發展與資訊安全管理研究探討〉，《危機管理學刊》，第10卷第2期，頁79-86。

康經彪，2008。〈中共「未來戰爭」研究之威懾作用：兼論國軍因應之道〉，《黃埔學報》，第54期，頁119-138。

陳以明，2008。〈中共在網路戰及其網軍發展研析〉，《安全局科技情資》，第16期，頁56-57。

陳立函，2010/11。〈近年網路攻擊與中國駭客活動〉，《前瞻科技與管理》，特刊，頁137-147。

陳育正，2015/5。〈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，頁73-87。

陳嘉宏，2014/1。〈新型態戰爭及資安防護策略探討〉，《新新季刊》，第42卷第1期，頁226-232。

樊國楨、韓宜蓁，2015/7。〈美國關鍵基礎設施防護法案與資訊安全管理技術控制標準化〉，《國防雜誌》，第30卷第4期，頁97-122。

蔡明彥，2008/1。〈美國東亞軍事優勢地位的挑戰：中國「反介入」與美國「反反

介入」的角力〉，《全球政治評論》，第21期，頁61-82。

謝游麟，2009/4。〈中共「癱瘓戰」思維與戰力發展研析〉，《國防雜誌》，第24卷第2期，頁80-95。

簡華慶，2012/10。〈網路資訊戰所扮演角色及因應策略之研究〉，《國防雜誌》，第27卷第1期，頁122-138。

學位論文

金登富，2014。《中共網路戰略思維之概念性探討》。桃園：國防大學戰略研究所碩士論文。

曹邦全，2001。《中共信息戰之研究》。高雄：國立中山大學大陸研究所碩士論文。

研討會論文

李宇林，2008/10。〈中西「不對稱作戰」概念之比較研究〉，「國防事務專案研究暨戰略學術研討會」。桃園：國防大學。頁67-69。

謝之鵬、謝游麟，2012/5/24。〈國軍發展不對稱軍事思想與作為之研析—孫子兵法觀點〉，「戰略與國防：不對稱作戰議題學術研討會」。桃園：國防大學戰爭學院。頁79-81。

官方文件

行政院國家資通安全會報，2013/12/25。〈國家資通訊安全發展方案〉，《政府機關資訊通報》，第315期，頁1-47。

國防部，2013/4/29。〈我國如何因應網軍與駭客攻擊並強化資訊安全措施報告〉，《立法院公報》，第102卷第29期，頁2-5。

國家安全局，2013/4/29。〈我國如何因應網軍與駭客攻擊並強化資訊安全措施報告〉，《立法院公報》，第102卷第29期，頁5-8。

報紙

中國時報，2001/5/25。〈美軍方研究報告「中共培訓資訊戰部隊，駭客擔綱」〉，《中國時報》，版11。

邱志強，2004/4/1。〈資電作戰指揮部正式成軍〉，《青年日報》，版3。

梅軍、樊祥，2000/9/6。〈未來網電一體戰〉，《解放軍報》，版7。

湯佳玲，2015/1/13。〈中國18萬網軍威脅我將分級聯防〉，《自由時報》，版A8。

解放軍報，2004/10/26。〈綜觀網路戰爭〉，《解放軍報》，版1。

廖文中，2007/11/8。〈網路斬首戰及公安網軍〉，《全球防衛雜誌》，272期，頁2。

廖文中，2007/11/9。〈中國網軍：國安、公安與解放軍〉，《全球防衛雜誌》，271期，頁2-9。

羅添斌，2015/3/9。〈中國對臺網攻大本營藏身武漢大學〉，《自由時報》，版A2。

網際網路

BBC中文網，2014/6/10。〈美報告再指責中國大陸軍方網路間諜活動〉，《BBC中文網》，<http://www.bbc.com/zhongwen/trad/world/2014/06/140610_usa_china_cybersecurity>。

中共國防部，2013/4/16。〈國防白皮書：中國武裝力量的多樣化運用〉，《中共國防部》，＜http://www.mod.gov.cn/

affair/2013-04/16/content_4442839_4.htm>。

中國國防報，2005/5/24。〈日本啟動軍事轉型提出「癱瘓戰」理論〉，《中華網》，<http://big5.china.com/gate/big5/military.china.com/zh_cn/critical/25/20050524/12340309.html>。

行政院國家資通安全會報，2014/6/23。〈國家資通訊安全通報應變作業綱要〉，《行政院國家資通安全會報》，<http://www. nicst.ey.gov.tw>。

李文忠、張國城、陳文政、陳宗逸、蘇紫雲，2009/5/11。〈民間版「國防白皮書」〉，《臺灣新社會智庫》，<http://www.taiwansig.tw/index.php?option=com_content&task=view&id=1383&Itemid=117>。

李可為，2013/9/20〈外媒稱中國軍演「近十年世界罕見」〉，《文匯網》，<http://news.wenweipo.com/2013/09/20/IN1309200028.htm>。

張玉清、徐壯志，2006/11/14。〈濟南軍區“前衛—206B”軍事演習進入作戰階段〉，《新華網》，<http://big5.news.cn/gate/big5/news.xinhuanet.com/mil/2006-11/14/content_5330020.htm>。

連雋偉，2014/5/20。〈陸駭客竊密　美國年損逾9兆〉，《中時電子報》，<http://www.chinatimes.com/newspapers/20140520000379-260102>。

陸委會，1999/9/28。〈信息戰及超限戰的涵義、特徵〉，《陸委會大陸資訊及研究中心》，<http://www.mac.gov.tw/ct.asp?xItem=48917&ctNode=5842&mp=4>。

曾復生，2014/6/9。〈美「中」網路間諜戰最新情勢研析〉，《國家政策研究基金會》，<http://www.npf.org.tw/post/2/13698>。

新華網，2013/5/23。〈我軍6月下旬將舉行首次新型作戰力量聯合演練　數字化合成營首次公開亮相〉，《新華網》，<http://news.xinhuanet.com/mil/2013-05/28/c_124777402.htm>。

新華網，2013/5/28。〈我軍6月下旬將舉行首次新型作戰力量聯合演練　數字化合成營首次公開亮相〉，《新華網》，<http://news.xinhuanet.com/mil/2013-05/28/c_124777402.htm>。

楊國文，2007/10/11。〈全新硬碟被植木馬個人資料瞬間傳北京〉，《大紀元新聞網》，<tw.epochtimes.com>。

鉅亨網，2015/1/9。〈FBI公佈新力遭攻擊細節指朝鮮是網路攻擊源頭〉，《鉅亨網》，<http://fund.cnyes.com/news.aspx?choose=newscontent&sn=20150109115921245405212>。

鍾詠翔，2015/1/11。〈駭客攻擊日內瓦銀行個資遭洩〉，《聯合新聞網》，<http://udn.com/news/story/6811/635102>。

外文部分

專書

Defense Intelligence Agency, 2013. *Directory of PRC Military Personalities*. Washington, D.C.: Defense Intelligence Agency.

U.S. DOD, 2006. *Annual Report to Congress on the Military Power of the PRC 2006*. Washington, D.C.: U.S. DOD.

U.S. DOD, 2011. *DOD Strategy for Operating in Cyberspace*. Washington, D.C.: GPO.

官方文件

Clapper, James R., Worldwide Threat Assessment of the US Intelligence Community. Washington, D.C.: Office of The Director of National Intelligence.

Office of the U.S. National Counterintelligence Executive, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011. Washington, D.C.: Office of the U.S. National Counterintelligence Executive.

網際網路

Prince, Brian, 2011/2/10. "McAfee: Night Dragon Cyber-Attack Unsophisticated But Effective." eWeek.com, <http://www.eweek.com/c/a/Security/McAfee-Night-Dragon-Cyber-Attack-Unsophisticated-But-Effective-303870/>.

U.S. Department of Homeland Security, 2006/8/27. *National Information Protection Plan*, Washington: Department of Homeland Security, <www.chs.gov/xprevprot/programs/editiorial_0827.shtm>.

Nakashima, Ellen, 2009/6/24. Gates Establishes Cyber-Defense Command, *The Washington Post*, <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/23/AR2009062303492.html>.