中共網路作戰之研究

海軍上校　馬立德

提　　要：

一、近年來從網路遭到入侵的相關報導中，可以了解駭客技術不斷精進，網路各種類型的攻擊與破壞行爲與日俱增，手法也愈來愈多元，不但導致世界各地的電腦網路系統遭到破壞，也造成了經濟上相當程度的損失。

二、廿一世紀是數位化戰場，從解放軍歷年來演習中可以看出演練的重點與企圖，其目的是藉駭客與電腦病毒等手段，實施干擾、破壞、竊取、摧毀等攻擊作爲，進而入侵電腦系統癱瘓我決策能力、降低軍隊效能、影響我指揮機制，因而導致喪失反擊能力。

三、國軍未來建軍方向，應積極發展數位武器與預警防護機制，並落實全民國防，強化網路資訊安全觀念，培訓專業人才，確保國家與軍隊安全。

關鍵詞：駭客、網路戰、網路資訊安全

壹、前言

隨著網路科技發展與時俱進，不論在日常生活或工商市場上，都有成功運用的經驗，各國軍事研究人員發現，若將其運用於軍事方面，將具有無限的潛力〔註一〕。這也是繼物資、能源之後的一種新戰略資源，不僅是決定今後世界經濟、社會、政治、文化發展的關鍵因素，更是影響作戰過程乃至戰爭勝負的第一要素〔註二〕。

自 1985 年起中共就已高度重視網路作戰，歷經多年的研究，雖然外界很難得知其真實的發展情況、科技現況與作戰能力，惟從最近幾次演訓狀況及國內、外軍事專家的研究報告中顯示，解放軍在網路作戰方面已有相當的成就，其戰術戰法也進入實際驗證階段〔註三〕。在未來戰爭裡，破壞力最大的已不再是核武攻擊，兵戎相接傳統戰場也不復見，隨著電腦技術在軍事領域愈來愈廣泛應用，網路作戰可以更多元且迅速的投入戰場，而成爲廿一世紀的新利器〔註四〕。

貳、網路作戰定義與意涵

網路作戰是近年來在軍事科技領域中一個相當新的議題，並掀起軍事事務的革命浪潮，廿一世紀是網路作戰的時代，其重要性就如同廿世紀核子武器的發展一樣，都是代表著一個新時代的出現〔註五〕。然而傳統大規模戰爭將不再出現，未來戰爭型態也朝向高科技、局部性與低度衝突的型式邁進。

一、網路戰定義

由於網路發燒熱正在全球各地蔓延中，而且電腦網路的發展已經超越國家之領土與領海等地域，並且同等經濟、政治和軍事之重要性。然而網路作戰就是運用國際電腦網路所進行的政治、經濟、文化、科技、軍事等戰爭，其各國定義彙整如表一。

有關網路戰之定義，各國均有許多不同層面與角度的詮釋，爲避免造成理論混淆與研究領域失焦，故以我國網路戰定義做爲本研究發展之理論基礎。

二、中共網路作戰發展意涵

(一)波斯灣戰爭促使發展網路作戰

西元 1991 年的波斯灣戰爭，美軍藉著高科技的電子設備，竟能指揮調動自如，除有效掌握戰場變化，又能反制伊拉克的電子及癱瘓網際網路等設備，徹底掌控戰場，而打一場絕對優勢的高科技戰爭〔註八〕。開啓了中共的認知，並改變作戰的思維，使得傳統的戰略思想，進入一個資訊化的戰爭軍事事務革命。

(二)打贏高技術條件下的局部戰爭的戰略指導〔註九〕

解放軍在 1980 年代後期進行大規模的裁軍，強調從量到質的轉變。鄧小平於第十一屆三中全會，提出「以經濟建設爲中心、堅持四項基本原則和堅持改革開放〔註十〕」，並修正毛澤東「人民戰爭」的看法。因此，中共便大刀闊斧地進行多項軍事事務的改革。前國家主席江澤民上台後，承襲鄧小平的軍事改革理念，經由美軍波斯灣戰爭的激化，及日益發展的經濟力量，且因應整體綜合國力發展的需要，因此網路作戰的觀念，更受到深化與重視〔註十一〕。2001 年中共決定重新組建國家資訊化領導小組，制定網路資訊發展規劃，開發利用網路資源等方面做了一系列重要決定和戰略部署，確立了往後 15 年國家網路資訊化的發展戰略方針〔註十二〕。

(三)發揮損害小、效率高、快打、速決，首戰即是決戰之特色〔註十三〕

爲避免外來國家對於中國內政問題干涉，若對台用武的時間拖得太久，可能會造成美國或者是國際上同情台灣的國家有反應和聲援的機會。所以網路戰就顯現出它「損小、效高、快打、速決、首戰即是決戰」的特點〔註十四〕，因此，具有明顯的決戰性質，再配合高科技武器的使用，創造先發制人的優勢，並可集中戰力打擊敵人脆弱的「穴道」，破壞其內部結構的完整與系統運行的連續性，進而癱瘓或失去抵抗的能力〔註十五〕。

(四)網路作戰可避免流血景況減低殺戮或遺留民怨〔註十六〕

台灣百姓人員素質與生活水平、自由民主，在亞洲國家均有一定的水準，倘若受到外力的迫害和武力侵犯時，反而更能凝聚力量，團結一致的對抗外侮〔註十七〕。而台灣地形多山適合游擊戰，城市街道密集適合城鎮戰，且可實施兩棲登陸作戰的地點又不多，因此若以戰機轟炸、海空封鎖或導彈射擊等方式攻擊，除了耗費時間，並易造成台灣百姓身家性命財產的重大損失。若是以更嚴厲、更高壓的手段入侵台灣，則重蹈覆轍二二八事件的錯誤思維，則增加往後統治的困難度。所以運用網路作戰，可由內部破壞、局部重點的攻擊，使我民心士氣大爲混亂爲目標，減少不必要傷亡，造成我方自亂陣腳的局面〔註十八〕。

參、中共網路戰發展

西元 1991 年美軍運用高科技優勢，在波斯灣戰爭中大獲全勝，促使中共加速研發網路戰的決心，致力積極發展各項作戰計畫與訓練、考核大綱等之研究。

一、網路戰現況

1990 年至今，中共電腦、網路通訊科技產業上有了快速的發展，奠定國防資訊基礎建設。在作戰概念方面，以電腦病毒作爲不對稱之戰略手段，其特色具有「攻擊容易、無實際軍事衝突、破壞小、成本低、時效高、效果大且國際負面影響小

之優勢」，其發展如表二。

二、網路戰組織編制

(一)有關解放軍網路戰組織編制，在各類學術或文獻研究並不常見，僅部分書刊雜誌或報章媒體的片段報導。到底組織編制規模有多少，其實無法探知，推測可能深怕遭受各國抨擊，所以至今均保留尚未正式公開，除非在實際應用的戰場上或公開介紹網軍在網路作戰上的攻防運用，否則難以查證〔註十九〕。

(二)西元 1992 至 1995 年，解放軍因師學美軍在波灣戰爭中，對伊拉克所實施的網路作戰，便開啓了新穎的軍事思維。在組織變革上，1997 年中共成立國家信息化領導小組，召開全國信息化工作會議，1998 年國務院成立「信息產業部」，對全國各相關部門進行分工至 2002 年，中共完成國家戰略級的網路戰分工規劃。惟網路戰之部隊，統由解放軍七大軍區所轄之電抗團（營），係採以任務編組之方式，或納編民間 IT 產、官、學界、省屬縣市及鄉鎮之民兵共同組成，配合各項軍演實施網路作戰。其組織編組模式如下〔註二十〕：

1.電子戰分隊：以連爲單位。從電子行業抽調人員，負責僞冒〔註二一〕、電子干擾〔註二二〕、反干擾、欺騙、反欺騙及攻擊敵人電子系統。

2.網絡戰分隊：以連爲單位。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。

3.黑客（駭客）分隊：以排爲單位。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爲目標，藉假情報、假資訊、病毒等進行節、點式破壞、竄改、銷毀等攻擊。

4.訊息救護分隊：以連爲單位。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。

5.網路民兵組織：由北京、清華、交通及復旦等著名大專院校資訊科系和研究所，成立民兵分隊，其組織規模概等同於營級之編制，下轄不同專業之連、排、班，其運用上，可適時抽調相關工程人員實施彈性的編組。如北京中國科學院紅旗軟件技術有限公司，內建有北京信息民兵編組，下轄有數個連、排級等組織，賦以訊息救護專業，搶救維修軟、硬體系統等〔註二三〕。

三、網路戰入侵攻擊模式

(一)收編駭客

解放軍有關網路作戰之架構，因無固定的組織編組，係採任務編組之方式彈性調整，所以有關駭客等成員，仍以吸收學校、社會熱中於程式設計的人士或從事網際科技公、民當機構等各階層爲主。其入侵模式，係以通訊軟體，透過網路非法進入他人系統，截獲或篡改電腦數據，藉以危害資訊安全〔註二四〕。而通常以他國大型企業，政府部門或軍事機構等爲入侵爲目標如表三。

(二)入侵事件

2007 年 4 月 9 日國防大學某上校教官，因擔任漢光 23 號演習攻擊軍演習計畫指導組人員，惟違反公務電腦使用規定，將機敏公務資料習攜回家辦理，連接民用網路後，遭植入木馬程式，因而導致漢光 23 號演習攻擊軍、軍種簡報與演習

操演動次等相關資料外洩〔註二五〕。該名教官雖學、經歷豐富，教學認真，惟嚴重違反資安規定，導致機敏資料外洩，因而遭受嚴厲之處份，對仕途發展造成相當程度之影響，歷年網路入侵事件詳如表四。

(三)入侵方式

隨著全球化網際網路的風行，以及國軍全面資訊化，資安與國防安全已密不可分，近年來中共積極研發網路作戰能力，發動駭客攻擊，對國軍仰賴日深的電腦網路運用，造成極大威脅，以下彙整入侵可能的方式〔註二六〕，如表五。

(四)常見網路戰使用之電腦病毒

電腦病毒屬於惡性程式，是專門用來破壞或干擾電腦作業。通常隱藏於電腦中，不易發現，並依其程式性質，能夠自我複製、自動入侵及篡改其他程式，影響電腦正常運行，損害其功能〔註二七〕。目前解放軍除積極研究電腦網絡之防衛技術外，另外也自行研製數種「電腦病毒」、邏輯炸彈和特洛伊木馬程式」等惡性程式，如附表六。

四、網路戰之特、弱點

網路遍佈全球，不僅改變人類的生活，也使未來戰場產生新的變化，並促使另一種新的作戰模式的出現〔註二八〕。網路戰是一種新型態的戰爭形式，也是最抽象、無固定形式的戰爭。其特、弱點如后〔註二九〕：

(一)特點

1.網路作戰範圍廣泛

(1)可從任何時間、地點或方式，遂行網路作戰。

(2)攻擊目標範圍廣，其範圍不再局限軍用設施，可包含民間基礎建設或軍民通用性等設施。

2.易造成對方恐慌與極大壓力

(1)受到攻擊的單位，可能無法判定攻擊者是誰、來自何方，亦無法評估其真相與實力。

(2)無法精確掌握攻擊效程，並對下一次的攻擊做有效的偵測及防護。

3.作戰時間可連續無限制性可收猝然與突襲之效果

(1)可於短時間內或一次微不起眼的小型攻擊中，癱瘓敵方各種指揮機構，造成目標國整個政治、社會、經濟、軍事等系統全面或局部性之傷害。

(2)無法讓敵方有預警和準備的機會，可憑藉網路光纖傳輸，以收奇襲效果。

(3)網路作戰並無明顯之交火作爲或區分，且具有低強度的特徵，可使得網路衝突事件層出不窮，並持續不斷。

(二)弱點

1.網路基礎建設仍落後先進國家

中共目前無法全面普及網路基礎建設，仍需努力師法先進國家網路建設之水準，並自行開發網路技術〔註三十〕。中共人口過於集中，且幾乎都集中於沿海以及大城市，如此將使得網路基礎設施難以設置相關的電力與通信設備也難以到達，有關網路科技教育成本投資高、光纖纜路費用昂貴，若全面鋪設更是不符成本效

益。因此區域發展無法均衡，雖然近年中共極力呼喊資（能）源「西部大開發」的口號，但能否解決這種因爲區域發展不平衡所帶來的失衡，仍待觀察〔註三一〕。

2.國際社會對中國威脅論重視〔註三二〕

中共在經濟及軍事的實力日益強大，每年以兩位數成長國防預算，大肆擴張軍備，並致力於推動軍隊現代化，提升各種武力投射能力，勢必引起各方矚目，造成美及東亞周邊國家強烈的不安與關切〔註三三〕。

3.駭客及病毒製作技術普遍不高

解放軍網路戰技術在駭客及病毒製作的水準並不高明。通常是基於政治的因素或是惡作劇的心態，而來攻擊台灣或其他國家的網站。均僅止於騷擾性質，並不能對系統與資料造成真正的危害〔註三四〕。

五、中共網路作戰對我之影響

(一)防護目標廣不再局限於軍事設施致備多力分

目前我國各項軍事科技及設施，有部分與民間科技共享或通用。例如電力系統、作業軟（硬）體、中華電信軍租網路設備等，由於軍事科技及設施並未獨立，所使用的軟（硬）體皆爲一般的資訊設備，易遭敵方攻擊或破壞，若發動全面性攻擊，恐癱瘓國家整體秩序與運作能力。

(二)易造成我民心士氣分化與心理恐慌

台灣社會的資訊化程度高，網路設施亦發達，然而網際網路的應用，更涉及政治、經濟、科技、軍事、文化及日常生活等各個領域，並成爲台灣社會的一個重要組成。所以在任何一個環節，若遭受到網路戰損害或攻擊，都會造成連鎖效應。由於網路戰的手段日益翻新，從以往替換政府機關網頁，到入侵電子金融市場，造成敵方股市混亂、金融失序等，這都是網路戰發展的特點，除可使我社會金融失序，造成我民心士氣分化，產生震撼與威懾效應，屈從於敵方的意志，達不戰而屈人之兵的要求，進而達成戰爭的政治目的。

(三)網路戰攻擊手段多樣無法精確掌控攻擊效程

網路戰的攻擊目標往多渠道、多形式成長，其領域如政治宣傳戰、經濟資訊戰、指管戰、情報戰、電子戰等等，所針對的目標已非限定於軍事場域。其入侵手段，可來自軍事機構、或某一非政府組織甚至莫名的駭客，對我方機要資訊網路實施入侵、攻擊、破壞等。如此情況複雜、真僞難辨，難以掌控攻擊效程，顛覆我對於傳統慣用戰（術）法的認知。

肆、國軍因應中共網路戰之作爲

爲降低解放軍網路作戰對我產生的衝擊，所以必須對解放軍軍事戰略、軍事科技的演變，提出因應之道。我國國防報告書從 2002 年將原本的「戰略持久、戰術速決」的用兵原則，爲因應科技時代的變遷，遂行整體戰的概念，轉變爲「資電先導、遏制超限、聯合制空、制海，確保地面安全，擊滅犯敵」，做爲我國建軍備戰的指導。反映出面對科技的進步，必須調整國防戰略。其提升國軍網路作戰之具體作法如下：

一、建立適切戰略指導蓄積資訊防衛能力

從我國網路戰戰略指導來看，目前國軍通信電子資訊的整體規劃與發展，係依防衛固守、有效嚇阻之戰略構想及聯合作戰需求，達成爭取資訊優勢、鞏固國防與制敵機先之目的。面對中共網路戰發展趨勢，台灣研發網路戰能否達致有效嚇阻的戰略目標？台灣網路戰發展適切的戰略指導又爲何？此點應是探討台灣資訊戰發展首應釐清的課題。目前台灣採取守勢防衛政策，不能也無法發動軍事主動攻擊，但是台灣能否蓄積本身的資訊防衛能力，如研發點穴致命的打擊能力，可以在關鍵時刻先制奇襲，或掌控中共的資訊網路，讓中共不致輕易發動攻擊，應是首要任務。

二、建立多重備援指管通情系統

從波灣戰爭的經驗我們學習到當切斷指揮者與軍隊的指管通情系統，則指揮官如失耳目，與部隊無法通聯，軍隊也無所是從。解放軍對台軍事威脅，從原本的大量武力封鎖、癱瘓台灣政經軍心爲指導原則，轉變爲精準打擊癱瘓我國的指管通情能力，藉以縮小影響範圍。使得我國在指揮管制系統上必須要做好緊急應變措施，當指管通情系統一旦遭受破壞，必須有立即性的備用系統，有效支援系統正常運作。

三、加強訓練網管人員網路安全維護能力

國軍各級網路之安全維護，除了建立良好的制度規範、良好的系統之外，重點仍在於各級網路管理人管理網路的技能與觀念。因此，應由網路安全權責單位定期訓練及提供最新技術資訊給各級網路管理人員，期能使各級網路管理人皆有足夠之能力與正確的觀念維護網路安全，並能在遭受攻擊時發現並記錄入侵行爲，即時回報。簡單的說，要訓練各級網路管理人員皆有「確實掌握網路現況、提高網路可信度、適當調整網路架構、預防網路事故發生、即時修復網路故障」之能力〔註三五〕。

四、連結聯合作戰網絡，強化部隊資訊戰力

面對網路戰的發展趨勢，網際網路順暢與否？電腦設備夠不夠？保密機制是否縝密？作戰指揮、武器能否有效連結？是否具備心戰、情報、宣傳、組織戰力等，均應列入考慮重點。爲了符合未來網路資訊作戰需求，國防預算應增列相關研發經費，以深化理論研究與實務工作。對網路戰攻防技術之研究，除國防部相關機關之外，亦是各大學院校與研究機構共同努力的方向。網路作戰可達到不戰而屈人之兵之利〔註三六〕。有鑑於此，吾人應正確認識網路戰對國家安全之影響。但從另一個角度看來，台灣若能發揮不對稱的優勢與潛力，利用台灣的人才優勢，網路戰正可以開創以小搏大的轉機與契機！

五、以全民國防理念推動全民網路戰教育

爲推動全民國防教育，增進全民國防知識及全民防衛國家意識，健全國防發展，確保國家安全，特制定全民國防教育法。行政院訂每年的9月3日爲全民國防教育日，不論是學校教育、政府機關（構）在職教育、社會教育、國防文物保護、宣導及教育都包括在內。由於網路戰影響層面廣泛，面對非軍事網路戰防不勝防，反制之道在於政府、產業、媒體、官員與民眾都要具備網路戰相關知識，透過全民

國防教育法的推動，了解解放軍網路戰的手段與影響，方能降低解放軍網路戰奇襲效應，並於必要時配合政府發揮反制效果。

六、落實保防及網路安全教育

當網路安全防禦達到一定程度之後，駭客其實已經很難實施攻擊，尤其是架設嚴密的防火牆，定期修補系統安全漏洞之後，入侵者如果單純想從遠端利用系統漏洞佔領主機，幾乎是不可能的。這時駭客可以利用的方式，就是竊取使用者密碼。各單位人員如果保密警覺不夠，很容易就被入侵者利用取得重要資訊，藉以入侵攻擊。因此，教育國軍官兵妥善使用網路是網路安全最重要的環節，如要求或強迫採較複雜的密碼、定時更改密碼、帳戶不外借、電子信件須經加密、簽名之後送出、儘可能使用有加密的協定傳送資料、不隨便執行來歷不明的程式及對內部網路不正常的事件有所警覺等。

七、加強資訊人員保密訓練與安全查核

國軍各單位應透過訓練或其他方式，以提升對電腦與網路系統管理作業安全之警覺性與責任感。對於新進人員，更應該適時灌輸正確的資訊作業程序，嚴格的實施考核，以免因一時的疏忽，造成資訊作業上的疏漏，危害軍機安全。除了作業人員安全訓練外，人員安全查核也是相當重要的，再嚴密的防禦措施也難防有技巧的內賊，國內多數已破獲重大的網路犯罪皆爲知道密碼的內賊，而非外部駭客入侵。爲防制肇生電腦洩違密事件，國軍各單位應要求各級保防部門賡續配合資訊部門執行電腦作業人員安全查核，加強蒐報危害單位資訊安全預警情資等作爲，以有效管制電腦及網路洩密違規案件〔註三七〕。

八、研究網路攻擊方式並成立假想敵小組

網路攻擊方式日新月異，可在網路安全指導單位之下，由國防部電展室專責成立研究小組，以瞭解各種系統最新被公開的漏洞、新發現的病毒，並提供最新修補方案。不定期從事假想敵攻擊演練，嘗試突破國內各軍事或民間網路安全防禦系統，以監督各級網路，如有發現弱點，立即要求改進〔註三八〕。

九、結合民間資源奠定網路安全關鍵技術

網路戰之技術能量除由國軍自力研發外，應結合全國資訊安全防護領域之研究單位，就資訊安全方面之研究資源進行整合，再針對各單位之研究特性，選定不同研究領域或重點項目，以充分發揮分工合作之效益，期由對某些網路安全之關鍵技術獲得，逐漸累積研究成果，以奠定國軍網路安全防護科技自行研發之基礎。

十、增加專業軍事資訊人才

我國整體資訊環境進步，民間企業更是人才濟濟，相較於民間機關，國軍資訊人才的培育必須再加精進。首先必須建立資訊戰鬥部隊編裝，並修訂軍職專長，針對重點人員訓練。培養軍事人員的專業資訊素養，無法一蹴可幾，故須依據長、中、短期需求，律定資訊專長的培訓計畫，落實作業人員的分級教育訓練。建立專業的教育訓練軍事院校，針對資訊戰人才進行培訓。其次部隊資訊戰力的提升，除透過軍中的教育訓練，並可透過民間交流的方式提升整體素質，增進資訊作

業人員的本質學能。或透過在職進修的方式，利用公餘時間，鼓勵官兵考取相關資訊專業證照，不僅提升官兵素質，同時也帶動整體學習風氣，加強學習意願。

伍、結語

台海上空表面的寧靜，所呈現的是和平的假象，事實上，網路戰是斷斷續續地在進行中，因爲沒有血腥的殺戮，也沒有驚悚的報導，所以也造成了人們對危險的麻痺。眾所週知，台灣的安全威脅，主要還是來自於海峽對岸，雖然我們未明顯察覺，然網路戰已悄悄地替代了傳統戰爭，成爲兩岸對峙角力的新形態。資訊安全是現今國防安全概念中重要的一環，也是科技時代作戰的主要特色。然「國防」一詞乃泛指爲捍衛國家領土主權完整和安全，防備外來侵略和顛覆，而進行與軍事有關的政治、經濟、文化等方面的建設與戰鬥。網路科技的領域，已經成爲國家領土的一部分，是不容忽視與侵犯的，因此現代全民國防的概念，應要特重於信息安全層面。另外，據稱中共現今所掌握的精密技術，均足以對我方進行截聽、監視、偵察等危及我國國防安全的行爲，所以我國應詳細研究有關政治、經濟、金融、心理、基礎民生建設及軍事等方面的脆弱性，以全方位角度，強化我全民心防，使全民在平時就能有危機意識，並在政府所宣導的文件中，能明瞭中共運用網路戰攻台的可能手段，避免出現被中共從心防弱點突破，而引發的崩盤效應。

中共每年持續增加國防預算，而我國的國防預算卻不增反減，且因志願役兵力大幅增加，造成國防預算無法妥善分配運用，確實是一個隱憂，尤其是要投入網路戰這一未知的領域，更是要有充沛的研發經費才能有所作爲。因此政府應在合理的範圍內增加國防預算，尤其是網路戰等層面的預算，更應優先分配與執行。另外在實際執行層面上，則需事先做好妥善的資源分配計畫，除了自行研發外，也要和各大有關民間企業加強合作開發，落實軍事科技委外計畫，秉持著「把錢花在刀口上」的謹慎精神，使得我國在有限的國防資源發揮出最大的效用。

註釋：

註一：劉宴慈，<中共網路中心戰能力之研究>，《國防雜誌》，第 23 卷，第 6 期，民國 97 年 12 月，頁 100。

註二：林勤經，<中共發展信息作戰軍事運用之探討>，「中共對信息戰之研發與影響研討會」，2000 年 2 月 19 日，頁 1。

註三：〈國軍因應中共信息戰發展應有作爲〉，《青年日報》，民國 97 年 4 月 23 日，版 2。

註四：同註三。

註五：國防部史政編譯局譯，《使用非致命性武器的未來戰爭》，（台北：國防部史編局，2001 年），頁 169。

註六：沈偉光，《二十一世紀的戰爭型態與安全觀》，（北京：中國評論月刊，1998 年 2 月）。

註七：國防部頒，《國軍軍語辭典》，（國防部，93 年 3 月 15 日），頁 9-3。

註八：蕭朝琴，<中共發展高技術資訊戰爭對台安全之威脅>，《共黨問題研究》，

第 25 卷，第 6 期，民國 88 年 6 月，頁 56。
註九：平松茂雄著，楊鴻儒編譯，《中國的軍事力》，（台北：凱侖出版社，民國 88 年 9 月），頁 182。
註十：曾錦城，《下一場戰爭－中共現代化與軍事威脅》，（台北：時英出版社，1999 年 7 月），頁 10。
註十一：平松茂雄著，楊鴻儒編譯，《江澤民與中國軍》（台北：凱侖出版社，民國 88 年 8 月 10 日），頁 20。
註十二：人民網，〈胡錦濤：推進軍事訓練向信息化轉變〉，2006 年 6 月 27 日，http://politics.people.com.cn/BIG5/1024/4537204.html。
註十三：曾章瑞，〈中共研究信息戰對我國的影響及因應之道〉，《中共對信息戰之研發與影響研討會論文集》，2000 年 2 月 19　日，頁 3。
註十四：同註八。
註十五：朱小莉 、趙小卓，《美俄新軍事革命》，（北京：軍事科學出版社，1996 年 9 月），頁 97。
註十六：葛立德、黃文政，《21 世紀信息戰》，（北京：未來出版社，1999 年 10 月），頁 190。
註十七：轉引自林中斌，《核霸》，（屏東市：新民書局，1995），頁 10 。
註十八：曹邦全，《中共信息戰之研究》，（國立中山大學研究所碩士論文，2001），頁 101。
註十九：廖文中，<中國網軍：國安、公安與解放軍>，《全球防衛雜誌》，第 271 期，民國 96 年 11 月，頁 3。
註二十：同註十九。
註二一：將欺騙性的情報如假指揮命令等，加入敵正常通信流程中，以造成混淆的通信欺騙。
註二二：指電磁能爲意輻射、再輻射或反射，目的在破壞敵人對電子裝置、裝備或系統之運用。
註二三：廖文中，<中國網軍：國安、公安與解放軍>，《全球防衛雜誌》，第 271 期，民國 96 年 11 月，頁 3-4。
註二四：孫格勤、張林宏，《討戰中國》，（北京：台海出版社，1999 年 10 月），頁 251。
註二五：許紹軒，〈中國網軍入侵漢光演習資料外洩〉，http://www.epochtimes.com/b5/7/4/9/n1672357.htm
註二六：廖宏祥，<中共資訊戰攻擊能力與可能行動>，《聯合報》，2000 年 8 月 23。
註二七：周碧松，《信息戰爭二十一世紀軍事展望叢書》，（北京：解放軍出版社，1998 年 6 月），頁 155。
註二八：葛立德、周碧松，《21 世紀信息戰》，（西安：未來出版社，1999 年 10 月），頁 128。

註二九：周碧松，《信息戰爭》，（北京：解放軍出版社，1998 年 11 月），頁 151-153。
註三十：行政院大陸委員會編印，《從 Internet 看大陸資訊之蒐集與應用》，（台北：行政院大陸委員會，民國 85 年），頁 22。
註三一：曹邦全，《中共信息戰之研究》，（國立中山大學研究所碩士論文，2001），頁 93-94。
註三二：白禮博(Richard Bernstein)、孟儒(Ross H.Munro)、許綬南譯，《即將到來的中美衝突》，（台北：城邦出版社，1997 年 9 月 1 日），頁 3。
註三三：國防部史政編譯局譯，《四年期國防總檢(1997)》，（台北：國防部史政編譯局，民國 86 年 10 月），頁 30。
註三四：同註二七，第 94 頁。
註三五：陳旻萃，〈Second Life 創造 V-Business 新時代〉，http://blog.tmu.edutw/cbi/004168.html
註三六：喬良、王湘穗，《超限戰－對全球化時代戰爭與戰法的想定》，（北京：解放軍文藝出版社，1999 年）。
註三七：張大順，<資訊作戰之研析論網路攻防>，「國防大學第一屆國家安全軍事戰略學術研討會論文集」，2000 年 11 月 30 日。
註三八：謝君誠譯，《突破資訊戰的枷鎖》，《國防譯粹月刊》，第 24 卷，第 2 期，頁 68-71。