以資安角度談國軍面對網路戰的防範作為

陳炳炫

提　要

一、現階段中共以網路技術入侵我國的野心及能力是顯見且不容忽視的，因此面對中共的網路入侵，國軍的資安防範作爲變得更爲重要。

二、網路攻擊戰的成效可以在不損傷人員及不花費任何預算狀況下，獲致先發制敵的作戰效益，這是各國競相打造「網軍」的主要原因。

三、爲因應21世紀資訊高安全需求的挑戰，資訊安全防護等級應提升爲國家安全層級，由國家規劃最高層級的資訊安全作爲及政策，以確保國防安全的生命線。

四、基於資訊網路戰的日益艱難的環境，加強個人資安檢測及防護知識，爲資安防範作爲中最優先的要求。

五、面對一個新形態的戰爭，我們在觀念上必須從全球性、區域性及國家性三個層面去加以思考，以擺脫傳統思維的束縛。

壹、前　　言

現代戰爭的形態隨著資訊工業革命的興起而有了劇烈變化，這是因資訊技術的革新推動了軍事事務的改革，而徹底改變了軍事衝突的形式，網際網路則更是資訊工業革命中最創新的典範。世界超級強國美國在傳統武器及部隊武力獨佔世界鰲頭，美國空軍空優及海軍制海能力也都領先各國，然而提到全球通信網路部份，連美國五角大廈官員都承認那是美國國防部最弱的一環。就如美軍聯參「資訊首席」指管通資處長陸軍准將勞倫斯(Susan Laurance)表示，美軍可在傳統戰場上輕鬆面對敵人，但是面對虛擬世界的敵人，則是一項新的挑戰。[註一]此一訊息很明白地凸顯出網際網路的戰場，目前仍是混沌不清的，即使強權美國也可能在網際網路交戰中受害，更遑論其它資訊工業不如美國的國家，在面對網際網路的防攻戰時，將會面臨多麼不堪的境地。

中共是我國長久威脅的主要來源，面對中共在21世紀的經濟及軍事力量的崛起，許

註一　Stew Magnuson著，宋家駒譯，＜網路戰：美國國防部憂心其網路漏洞，Cyber War: Network Vulnerabilities Worry Pentagon＞，國防譯粹，第33卷第12期，民國95年12月，頁25。

多的學者主張中共已經是「資訊戰」強權，[註二]在網際網路戰場上將會威脅到美國的霸權地位或可能對鄰國進行侵犯；但也有另一部份學者認爲中共資訊科技相當落後，所謂「網路戰」不過是紙上談兵。[註三]雖然學者對中共的網路戰能力的看法不一，但從美國國防部對國會近兩次2005年及2007年提出的「中國軍力」(The Military Power of the People's Republic of China)年度報告顯示，共軍已預見網際網路作戰將成爲未來衝突中奪取主導權的關鍵方式，故已成立網軍以發展電腦病毒來攻擊敵之資訊系統和網路。[註四]我國國家資通安全會報於2002年起舉辦資安攻防演練，演練結果經深入調查及研判發現，有國內或國外別有用心之駭客團體，有計畫大規模入侵我國及國際社會，當時會報執行長蔡清彥政委即指示：會報之「網路犯罪工作組」偵九隊應全力偵查駭客的身分和犯罪動機，同時責成「技術服務中心」配合偵九隊提供技術支援，以協助政府各單位清除木馬程式及執行電腦系統復原工作。[註五]因此，就我國之資安環境而言，遭受到有心團體的入侵機率相當高，而且中共一直是我國潛在的敵手，因此我們可以合理的判斷，中共入侵我國軍事單位網路的企圖是極爲強烈的。

中共運用網際網路的能力及技術到底如何？我們用幾個案例來看便可以窺得一斑。1998年5月印尼屠殺華人，引起全球華人的憤怒。同年8月印尼國內許多著名網站首頁都遭到竄改，首頁上均出現「你的網站已被來自中國的黑客所駭，印尼的暴徒你們的暴行是會有報應的」等字眼。[註六]1999年5月8日美國誤擊中共駐南斯拉夫大使館事件，次日美國駐華使館的網站即遭到中共駭客改得面目全非，隨後美國白宮(White House)網站亦遭到攻擊，首頁的兩面美國國旗被換成了骷髏旗，更留有簡體中文「中國的黑客們，加油啊！打倒北約，打倒USA!」。總括此次事件，導致包括美國白宮、能源部(Department of Energy)、內政部(Department of the Interior)、美國國家公園服務處(The National Park Service)等，甚至連美國海軍通信中心(U.S. Naval Member of the Allied Control Commission: USNACC)亦難逃被駭的命運。[註七]1999年前總統李登輝先生接受德國之聲專訪時，提出「兩國論」詮釋臺灣與中共之關係，此舉引起中國大陸的駭客族，對我國發動了高達七萬餘次的攻擊。首先我國的監察院、屏東縣政府、臺大圖書館、營建署、NII等單位網站的首頁被大陸駭客入侵，網頁被「世界只有一個中國、也只需要一個中

註二 此謂「資訊戰」其義爲包含六個作戰手段：指管戰、情報偵蒐戰、電子戰、心理戰、網路戰及經濟資訊戰。詳見呂爾浩、魏澤民，＜中國「資訊作戰」的類型分析＞，遠景基金會季刊第7卷第3期，2006年3月，頁192。

註三 呂爾浩、魏澤民，＜中國「資訊作戰」的類型分析＞，頁188。

註四 Sina全球新聞，＜五角大廈發布中國軍力報告 美警告中犯臺後果＞，2007年5月26日，http://news.sina.com/oth/kwongwah/000-103-102-103/2007-05-26/02112071188.html，2007年7月10日。

註五 行政院國家資通安全會報-技術服務中心資安論壇，＜「成功遏止駭客團體企圖大規模癱瘓我國電腦系統案」新聞稿＞，http://forum.icst.org.tw/phpBB2/viewtopic.php?t=1513&highlight=%B0%EA%A4%BA%B8%EA%A6w，2007年10月3日。

註六 「駭客」是由英文的「hacker」音譯而來，原意是表示「電腦能力很強的人」，但是漸漸地大家都混淆了這兩個字的含意，再加上中文在翻譯時，也乾脆把「hacker」翻成「黑客」(有點邪惡的形象)，於是大家將錯就錯，將凡是在網路上有任何利用技術危害他人的人，就稱爲「黑客」。一般大陸統稱「駭客」爲「黑客」情形較多。

註七 余開亮、張兵，＜駭世黑客，第九章網路無界人有界：黑客的民族情結＞，雲臺書屋，http://www.b111.net/base/yklzb-hshk/009.htm

國」爲主題的不當聲明取代。[註八]2002年2月23日，日本一些懷有復辟軍國主義的右翼分子，企圖否認南京大屠殺，再度引起華人的不滿，因此中共駭客對日本進行網路的攻擊。首先是日本科技廳網頁遭到改寫，網頁首頁上以英文描述「日本是一條咬敗了的狗」；次日日本總務廳網頁無法打開，接著人事院、企劃廳等政府機關都陸續遭到入侵及篡改網頁。日本政府特別針對中共駭客入侵事件組成特別小組進行政府機構網路的防範，但很難堪地，日本科技廳的網頁雖經過加強防護措施後，仍然遭到中共駭客第二次的入侵。[註九]

由以上的實例不難發現中共駭客的實力及技術並不低，加上近年中共採取改革開放政策，相關的網路技術及觀念自國外引進，助長中共在網路戰的實力，這是我們不可忽視的環節。況且連美國最先進的國家都不敢諱言在虛擬的網路戰場上，具備百分之百防堵網路駭客入侵的能力，因此我們寧可相信中共已具備網路入侵的技術，我方絕對不能不加以防範。從中共對我發動網路戰的企圖明顯，且其網路技術能力亦不可小覷等面向下，我國資安作爲就顯得相當重要。然而，近年來我國軍卻屢屢發生機密資料遭駭客竊取或外洩情事，尤其是以作戰演習期間尤甚，此顯示我國軍人員對資安防護作爲出現嚴重的漏洞，故如何防範資安事件再度的發生是我國軍現階段最重要的課題。

貳、電腦病毒在軍事上的運用

隨著網際網路的逐漸普及與將網路視爲軍事用途後，以電腦病毒作爲戰爭武器及如何杜絕病毒危害的防護作爲等等問題，也越來越受到大家的關注。究竟電腦病毒能在軍事作戰上達到什麼程度的效應？又能造成敵對國何種影響？等等問題就成爲軍事專家及戰略學者們關注的焦點。再進入研析這些問題前，首先我們可以回顧一下幾個以網路病毒進行破壞及入侵的案例，來看運用電腦病毒作爲武器的應用及達成軍事上的成果如何。

1998年2月25日美國國防部副部長哈姆雷(John Hamre)在新聞例會上向美國新聞界透露，美國軍事情報網路連續感染木馬病毒，駭客得以利用病毒所開啓的系統漏洞侵入五角大廈的電腦系統中心，據估計有4個海軍系統及7個空軍系統的電腦網頁遭竄改，相關機密文件遭到盜取。[註十]

1998年5月3名不明國籍的十幾歲少年駭客通過即時聊天室的功能，成功侵入印度巴巴原子研究中心(Bhabha Atomic Research Centre, BARC)，截獲了十幾封印度核武科學家的電子郵件，以作爲對印度進行一系列核試驗的報復。據傳他們之所以能夠進入印度原子研究中心，是經由美國軍方的網路迂迴侵入，因爲美國的軍方網路系統與印度原子研究中心是對接的。[註十一]

2003年伊拉克戰爭爆發前不久，美國中央情報局(Central Intelligence Agency)截獲伊拉克將從法國購買新型電腦印表機作爲防空系統的資訊設備，其運送的路線準備通過約旦首都安曼(Amman)，再偷偷轉運回到巴格達(Baghdad)。美國中央情報局獲悉後，立

註八 趨勢科技，＜防毒入門＞，http://www.trend.com.tw/corporate/security/topic_virusprimer.htm, 2007年6月12日。
註九 大紀元，＜到底是誰大?了日本網站＞，http://www.epochtimes.com/b5/1/3/3/n53531.htm, 2007年6月12日。
註十 袁文先、涂俊峰、周德旺，＜數字黑客，信息武器＞，（北京：解放軍出版社，2001年），頁85-86。
註十一 遠流博識網，＜企業風雲—商業世界諜對諜（場景二：虛擬世界）＞，http://www.ylib.com/ymba/eading/default.asp?DocNo=78，2007年7月6日。

即派特工人員前往安曼，並買通機場守衛人員，在該印表機抵達安曼機場後，由美國特工潛入機艙，以一套固化有電腦病毒的同類晶片置換印表機中的晶片，讓伊拉克帶回並安裝到防空系統上。當戰爭爆發後，美軍即透過網際網路以指令「啓動」該防空系統電腦印表機晶片內的病毒程式，病毒通過印表機再侵入防空系統的電腦中，使伊拉克整個防空系統的電腦陷入癱瘓。這是世界上首次將電腦病毒用於實戰，並且取得極佳的作戰效果的案例。[註十]

2006年3月日本一位通信上士擅自使用個人電腦存取業務相關資料，因爲電腦遭受中毒，又使用點對點(peer to peer)的Winny傳輸檔案軟體，導致資料外洩。這些外洩的資料是由日本海上自衛隊佐世保基地「朝雪」號通信上士所保管，包括自衛艦的無線呼號、暗號表、亂數表、船艦電話號碼、衛星電話號碼、戰鬥訓練計畫表與情報等級「祕」、「極祕」的文件，隊員名冊與個人情報也都一併流出，若再加上訓練情報等，獲得資料的有心分子將能經由解析這些文件內容，推算出日本海上防衛的作戰能力，造成日本國家海上安全的危機。另外，外洩資料中還有極爲重要且由日本自行研發的海圖軟體，據報載該套軟體可以很快的完成作戰行動圖，包括經緯度、水深、海底地形和橫斷面等一清二楚，而且連島嶼名稱、日出、日落時刻和太陽方位等都能輕易入手。[註十一]

由以上幾個案例，可以發現發起網路攻擊戰的一方，幾乎在不損傷人員及花費預算狀況下，就能獲致極大的成功，發揮極其重要的效益，這就是網路戰最引人入勝之處，也是各國競相打造所謂「網軍」的原因。如美國位於南卡羅萊納州薩姆特(Sumter)附近的空軍基地工作的609中隊，是世界第一支以保護網路及資訊攻擊的作戰部隊，它的出現也預告資訊戰的來臨；[註十二]2002年美國總統布希簽署「國家安全第16號總統令」，要求美國國防部主導並組織中央情報局、聯邦調查局(Federal Bureau of Investigation, FBI)、國家安全局(National Security Agency, NSA)等政府部門制定網路戰戰略，以便在必要時攻擊和破壞敵方的網路信息系統；[註十三]美國空軍也已建立一支專門負責實施信息網路進攻的航空隊—第8航空隊(The Mighty Eighth)；[註十四]五角大樓1995年招募駭客成立資訊戰「紅色小組」，以及美軍特種部隊也可利用專門設備執行計算機網路攻擊任務等等。[註十五]以上是美軍對網路戰的投入，讓美國擁有世界上規模最大、裝備最先進的「網軍」。另外如日本、印度、俄羅斯、德國、以色列及中共也都紛紛投下巨資，打造自己的「網軍」。由於網路戰具備高技術性和高開放性等特性，各國「網軍」的人員結構、戰備訓練與普通部隊有著明顯的差異，因此

註十 中國經濟網，＜美戰略司令部承認擁有世界上最強大“駭客部隊”＞，http://big5.ce.cn/xwzx/gjss/gdxw/200702/28/t20070228_10528157.shtml，2007年，7月5日。

註十一 張志裕，iThome online，＜檔案交換軟體讓日本防衛廳情報外洩＞，http://www.ithome.com.tw /itadm/article.php?c=35872，2007年7月5日。

註十二 奇摩知識網，＜世界第一支資訊戰部隊＞，http://tw.knowledge.yahoo.com/question/?qid=1405101601580，2007年7月5日。

註十三 中國國防報，＜制網權”：關乎未來戰爭勝負的新制權＞，2007年02月08日，http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/mil/2007-02/08/content_5714949.htm，2007年7月4日。

註十四 臺灣科技資訊網，＜中國挑戰美國網路霸王地位＞，http://taiwan.cnet.com/enterprise/topic/0,2000062938,20119249,00.htm，2007年7月5日。

註十五 自由電子報，＜組建網路大軍謀奪第五空間＞，http://www.libertytimes.com.tw/2006/new/nov/5 /today-int5.htm，2007年7月5日。

各國通行的做法是吸收該國內的駭客爲網軍的主要成員。在戰爭或者網路戰中，駭客由於具有高超的網路及電腦技術，往往成爲網軍攻擊的新力軍。因此網軍的成立關鍵就是在於是否能掌握一批精良的駭客，其實美國和印度早就已經公開招募駭客入伍，這對於駭客侵入他人網路的犯罪行徑視若無睹的包容，也是民主國家宣稱具有國際道義的一種諷刺吧。

參、軍事作戰的資安問題

所謂資訊安全，尤其是應用在軍事網路戰的資訊安全指的是有效的防止資訊遭竊取、竄改、毀損、滅失或遺漏。簡言之，就是確保資訊的機密性、完整性及可用性，這即是資訊安全的三要素。機密性表示保護資訊不被非法存取或揭露；完整性表示能確保資訊在任何階段沒有不適當的修改或損毀；可用性則表示經授權的使用者能適時的存取所需資訊。[註六]要達到資訊安全的範圍，則必須對保護及維護資料的安全進行全方位的考量，包含資料的使用、資料的傳遞、資訊的處理及儲存等，這些作爲在20世紀90年代網路應用更爲廣泛後，也隨之變得更重要。

各國對網路設施工程的積極建設，扮演推動該國經濟全球化、軍事革新運動、改變人民的生活方式與社會結構的重要角色。其中有關軍事方面，網際網路已革命性地改變了戰爭的基本形態。當一個國家政治、經濟、軍事及整個社會對網際網路的依賴性越來越大時，而又無力進行網路系統的安全防護下，國家、軍隊及社會就會於處在一種極不安定的狀態。尤其當網際網路進入21世紀後，隨著網路技術不斷的翻新，新的網路攻擊技術也隨之不斷出現，使得網路戰的技術及機會大爲提高，這是21世紀資訊安全的新挑戰。爲接受21世紀的資訊安全挑戰，現行資訊安全防護的開展工作，大都直接由國家和軍隊接手。相同地，網路的攻擊技術亦由國家及軍隊加以主導及開發，這使得網際網路安全的威脅逐漸擴大。因此，現行網際網路的安全等級已提升爲國家安全層級，亦成爲國防安全的生命線。[註九]

資訊安全問題的發展趨勢，是隨著網路病毒技術的演進而變化，因此資訊安全的防護作爲也隨之改變，但原則上大約可以分爲三個階段。第一階段在1980年代，因應大多數的病毒是由駭客惡作劇及爲標榜個人電腦知識的淵博之意圖下發展，故此階段病毒目的是以破壞電腦主機的檔案及擾亂程式的正常運作。相對的此階段防護作爲是以資料檔案的防護爲目的，因此發展各種密碼演算法作爲防護資料的手段是該階段的重點工作。第二階段在1980年末起，新種病毒不再以刪除電腦主機之檔案爲目標，而改以大規模的感染區域內之電腦主機，造成網路內所有電腦癱瘓爲其目的，此新種病毒一般稱之爲「蠕蟲」或「病蟲」。[註十]例如1988年11月3日由美國羅伯特．莫里斯設計的電腦「蠕蟲」，在一個上午的時間就使包括美國國防部「遠景規劃署」、蘭德公司(Rand)研究中心和哈佛大學等之軍、民用約6000餘台電腦陷入癱瘓。[註二]相對此階段的防護工作重點除加強第一階段加密技術外，還開發了許多

註六 臺灣電腦網路危機處理暨協調中心，＜建立與實作一個成功的資訊安全政策＞，http://www.cert.org.tw/document/column/show.php?key=74，2007年7月10日。

註九 張黎主編，＜信息化戰爭中的防御與防護＞，（北京：解放軍出版社，2004年10月），頁149-150。

註十 中華電信防毒防駭網站，＜看不見的殺手—談蠕蟲及蠕蟲的預警模式＞，http://hisecure.hinet.net/Tech-docs/A1.pdf，2007年7月6日。

註二 臺大資訊中心網站，＜電腦病毒的起源(節錄自牛頓雜誌)＞，http://www.csie.ntu.edu.tw/~wcchen/asm98/asm/proj/b85202030/a1.html，2007年7月6日。

針對網路環境資訊安全與防護新技術，如安全漏洞掃描器、安全路由器設置、防火牆、入侵檢測系統，各種防網路攻擊技術、網路監控系統等等，來防範「蠕蟲」癱瘓網路的作爲。然而這些技術還是停留在被動防禦的層次。第三階段的資安防護成形於1990年代起，最主要是針對第二階段被動的防護層次提升至主動防禦的層次，並從戰略角度論述與解決網路的防禦問題，亦即針對病毒檢測、掃毒反應及系統恢復的網路防禦模型提出主動式的防禦概念並納入常規作業的一環。

網路戰的攻擊是指以電腦技術透過網路進行偵察、獲取、干擾、破壞對方指揮系統、武器系統及人事、組織與後勤等重要資料，進行欺騙、滲透及心理戰的戰術，達到影響他國的政、經、軍、心等各層面的結構，製造戰爭前哨的優勢及攻擊契機。網路戰攻擊方式眾多，較爲先進的作法如美國現正研發通過衛星將病毒直接輸入至敵對國的網路系統等。但不管以任何形式執行網路的攻擊，都不外乎可歸類爲電腦駭客戰及電腦病毒戰等兩類。

一、電腦駭客戰

電腦駭客戰是指駭客以各種手段侵入對方電腦網路系統，對敵方電腦網路系統進行破壞的作戰攻擊方式。從網路防禦角度來看駭客，它是一個揮之不去的惡夢；以網路進攻的角度來講，駭客軟體則是網路戰的戰略新武器。借助駭客的軟體工具，即使未具高超專業技術能力的使用者，都可能成功對目標發動襲擊並令其癱瘓。若集合多名駭客，同樣可以借由這些駭客軟體於不同地點「集中火力」對目標發動攻擊，更可提高入侵的成功機率及縮短攻擊成功的時間。另外駭客常使用的攻擊手法，就是將這些病毒程式偷偷的安裝到敵人網域中，然後將其電腦當作跳板平臺，對其它敵方網站發起攻擊，這是「借刀殺人」的技倆，也是駭客常使用的方法之一。藉由跳板以行駭除可達到竊取資料及破壞電腦的目的，還可以避免露出行蹤，完全隱藏自己的來源，以持續對目標實施入侵及滲透。1997年6月美國國家安全局曾舉行一次代號爲「合格接收者」的秘密演習，參與者包含五角大廈資訊戰「紅色小組」，以及雇傭的35名駭客。演習的任務想定就是由35名駭客負責闖入美國本土及美軍駐太平洋司令部使用的電腦網路。演習結果令美國國防部深感震驚，擔任駭客的攻擊小組就在短短的4天之內成功闖入美軍駐太平洋司令部(U.S. Pacific Command)以及華盛頓(Washington)、芝加哥(Chicago)、聖路易斯(St. Louise)和科羅拉多州(Colorado)部分地區的軍用電腦網路，並控制了全國的電力網系統。而且這些攻擊者都能全身而退，避開守勢小組的追蹤。此演習案例顯示只要通過電腦、數據機和電話線，使用一些在網路上垂手可得的駭客軟體，就能輕易對網路進行大規模的破壞活動，有鑒於此，美軍認爲在未來電腦網路進攻戰中，電腦駭客戰將是其基本戰法之一。[註三]

二、電腦病毒戰

電腦病毒戰顧名思義就是利用電腦病毒作爲武器，對敵方網路的訊息進行破壞，以造成電腦主機癱瘓或壅塞，阻斷資訊的流通，或是篡改資訊來製造不實訊息，使敵國下達不正確的作戰命令，爲己國提供戰爭致勝的先天條件。電腦病毒的目標並不僅侷限於電腦主機，所有由主機所控制的資訊裝備都可能成爲電腦病毒攻擊的目標。如指揮控

註三 中國政法大學博士學位論文，＜網路犯罪若干問題研究＞，頁77。

制中心、電腦管理中心、雷達系統、各種傳感器等。另由電腦控制的各種武器系統，如飛機、艦艇、坦克及導彈等自動駕駛、火控、制導系統等也都是電腦病毒攻擊的目標。

網路的防護是指以電腦技術爲主軸，以網路傳輸管道爲載體，在敵我雙方互不見面的條件下抵制網路不良企圖訊息的入侵。因此，如何保衛自己的網路和防護資訊資源就越來越成爲各國軍隊關注的重要議題。本文提出數點防範之道如後：

㈠設置防火牆並定期檢測系統

入侵防護的主要手段在於將網路外部的不當封包阻擋在外，一般較爲常用的方式即在內部及外部網路的接口安裝防火牆，在內部網路中再安裝入侵檢測系統，以形成一道防守的壁壘。通常防火牆可以實施較爲廣泛的安全策略來控制訊息流進內部網路，以防止不可預料的入侵破壞，同時也可以限制內部網路的使用者對外不當的訪問及動作。所以防火牆若能管理配置得當，將可抵擋大部份網路攻擊行爲。但防火牆是一種靜態的安全防護技術，對於病毒不斷翻新及每日都有新病毒的產出的現狀，防火牆的防護是缺乏主動的反應能力。

㈡隨時更新系統補丁程式及建立管理策略

電腦病毒是一段可以執行的程序，具有潛伏性、複製性、傳染性及破壞性等特點，它所造成的危害並不比硬體遭到破壞的損失小。但其實電腦病毒也是能夠防治及消除的。一般採取的措施可以安裝防毒的軟體，定時的掃瞄及更新病毒碼，以補丁程式修補網路漏洞等都是基本的病毒防護方法。但最主要的防範措施仍應該以「七分管理、三分技術」爲原則，亦即建立嚴格的網路運作管理機制，執行有效的管制和操作規範，從管理面及制度面進行人員教育以提高安全意識等，才是最佳的防護作爲。

㈢加強密碼防護和資料隱藏

密碼技術是一種非常有效的電腦資料的保護手段。密碼的功能可以通過加密及適當的密碼管理協議，提供身份識別與確認，來保護數據完整性和網路通信的不可抵賴性等多方面的網路特性。目前採用密碼防護常碰到的困難在於使用者對密碼設定原則的輕忽，使用者基於便利的因素，常常設定簡短且易於猜測的密碼，如此將無法抵禦一般的密碼猜測攻擊，很容易就會因密碼被解析而遭到主機的主權易位的狀況。因此改進密碼的設定原則或策略，如採用隨機變數作爲密碼認証的智能卡、或以請求/應答方式作爲密碼認証的一次口令機制等，都是比傳統的輸入單一密碼認證方式要來得安全可靠。另外密碼的保管及管理也是防護重點之一，其重要性並不比密碼的設定來得低，值得管理者用心規劃。

資料隱藏技術指的是將資訊秘密地隱藏在公開的設息中傳遞，而不被人發現的方法。將一個秘密的通信僞裝成一個普通的信件，以實現安全通信也是一種資訊防護的作爲。密碼技術保護的是通信的內容，而資料隱藏則是將通信的存在「隱形」，如果第三者根本察覺不出某個通信的存在，那麼該通信就是安全的。所以網路訊息僞裝將在網路戰訊息對抗中發揮很大的作用，有時甚至比密碼防護更爲有效及更能達到安全的目的。

㈣隨時進行網路監控

在眾多的資安事件中，有大半部分的問題是來自於網路內部的問題，而且所造成損害也遠比來自外部網路的入侵要來得嚴重。網路監控系統的主要功能就是要監控網路內部所有主機的行爲，包含主機間的封包流量，不正常的服務要求等等，以此來發現

內部網路的攻擊行爲和內部網路節點間的非法行爲。當然網路監控還有另一個重要的功能就是能對檢測到的危害進行回應，比如說停止提供服務，發出警訊通知資安維護人員等。因此建立監控系統能有效地阻止來自網路內部和外部的攻擊，提高整個網路縱深防禦能力。

㈤確實演練災難復原程序

當系統受到攻擊而導致癱瘓時，及時的恢復系統的運作，是降低損失的最佳方案。要達到快速的復原能力及保證系統正確地再運作，就必須建立在平時的災難復原的紮實演練。另外要作好災難復原的前提就是要有完整的備份資料。資料備份的工作必須視爲一項定期重要工作，同時必須注意備份設備的穩定性、容量及傳輸的速度，甚至考慮備份資料的儲放地點必須遠離主機較遠的地方(如100公里外)，如此才能確保有正確的復原資料及流暢的復原程序。

㈥執行網路攻擊的誘騙手段

網路攻擊誘騙的主要用意是通過各種方法來欺瞞網路攻擊者，以達到保護網路眞實目標的目的。要執行誘騙的方法可通過僞造假訊息和設置圈套等方式，構造誘騙空間，以迷惑攻擊者的目標及增加對攻擊者的工作量，來達到安全防護的目標。同樣地，通過這樣故意暴露假目標，並執行多重IP地址的轉換，製造大量假資料流量之訊息，以及建立欺騙性的網路動態配置和信息欺騙技術，也是一種反間諜的手法，更是反守爲攻的積極作爲。

肆、未來的軍事網路安全的挑戰

網路系統在未來資訊工業及技術不斷的提升，其安全性亦會隨之提高，但這並不意味著未來的網域就安全無虞，沒有任何的脆弱性。如同微軟公司發展的視窗作業系統風靡全世界，也成爲全世界最多人採用的作業系統，但至今微軟公司仍持續地爲其作業系統發表修補程式，顯然再怎麼完美的系統，總是還有其缺陷存在。更何況網路攻擊的手法還是會再更新、提升，新的病毒會再變形而產生新的威脅。換言之，未來的網路環境並不會比現在更安全，因此防護的工作將會比現在更困難。預判未來的軍事網路安全的挑戰計有：

一、以「癱瘓戰」作爲軍事網路中心戰的主軸

「網絡中心戰」的觀念及建立都是由美國率先提出，[註三]美國因提出「網絡中心戰」而使其軍事的資訊化的程度和資訊化的作戰能力，獲得空前的提升，進一步拉開與各國的資訊能力差距。各國在體認這種網路戰趨勢之後，也紛紛學習美國並構建各自的網路中心戰組織，以大力地推展軍隊的訊息化，加快網路訊息系統的建設，提升軍隊訊息作戰能力。由於「網絡中心戰」的戰場相當倚重四通八達的網路系統，因此網路中心戰的攻防重點就是以癱瘓網路爲主，故未來的網路發展趨勢將以「癱瘓戰」爲主軸，如何攻擊使其網絡癱瘓及如何防護就成爲各國軍隊資訊化建設和提高資訊作戰能力的核心內容及要求。

二、以全面性脆弱的基礎設施爲目標

越是開發的國家，其國內基礎設施安全就越難以保證，最主要的原因是國內基礎設

註三 2001年7月，美國防部向國會提交了長達1000頁的“網絡中心戰”報告，首次提出並論證網絡中心戰這種新的作戰方式。美軍認爲，資訊時代的軍隊是一個互連互通的網路化實體，軍隊的網路化能生成新的戰鬥力，是戰鬥力新的增長點。詳見新華網，＜從自然中心戰到網絡中心戰＞，http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/newmedia/2007-02/15/content_5737412.htm，2007年7月10日。

施的資訊化工程及各基礎設施之間的緊密依賴關係。如2003年8月14日美國主幹電網問題導致從美國紐約到底特律(Detroit)、加拿大的多倫多(Toronto)至渥太華(Ottawa)之間，在短短的9秒鐘之內因停電而陷入停擺的癱瘓狀態，造成100多座電廠先後停止運轉，美加等七個主要機場一度關閉，至少影響5,000萬人的作息，初步估計經濟損失更高達40～60億美元不等，[註四]這正是基礎設施脆弱性的一個例證。未來的網路戰雖以軍事作戰爲主軸，但網絡攻擊的目標並不限於軍事設施。凡能藉由破壞敵國國內的硬體工程或民生設施，以達到損害其經濟層面、降低其人民反抗意志及減少交戰時敵人之反擊能力，都會是戰爭進行前網路戰攻擊的目標。經由這種國內民生基礎設施的損壞，可以形成骨牌效應的威嚇效應，重挫敵國的整體國力，增加己方實兵交鋒時的優勝環境。另外，現在攻擊的來源並不僅有敵對國家的資訊部隊所發動，有些威脅來源可能是恐怖分子，更有可能僅是某些爲政治訴求而發起攻擊的團體或好奇心驅使的個人駭客。這些入侵的來源都是不可預測的威脅，更可能以全面性脆弱的基礎設施爲目標，因此防護的等級提高由國家層級的主導，實在有其必要性。

三、以無線技術突破攻擊障礙

網路的通信管道通常爲有線的光纖、電纜線，但是無線及衛星通信也是其重要管道之一，未來以無線及衛星作爲通信途徑的範圍及機率將更爲提升，原因是在戰爭時部隊原本就以無線和衛星作爲通信的主要管道。由於資訊化的普及，這些無線通信設備也都與有線網路連結在一起，成爲網路中心戰規劃中的一體。又因這些軍事作戰時所使用的無線和衛星通信設備大都爲商用產品，因此未來的網路環境將直接暴露在這些無線及衛星攻擊的威脅之下。網路戰的對手和恐怖組織，應會專門收集全球網路所用的無線及衛星通信管道的頻譜特性，訊息流參數等特性，使用電子戰武器，干擾、截獲、破解或終止全球資訊網的訊息流，使區域內的作戰單位與全球資訊網隔絕，這是未來朝向無線技術攻擊的趨勢。

四、實施多層次、重疊性的攻擊策略

現行網路空間的攻擊已朝更激烈及更高層次的面向進行，面對如此網路攻擊的趨勢，其防護作爲也相對加強其嚴密性及管理層次，以應付層出不窮及日新月異多變的網路攻擊手法。這使得網路的應用在安全考量及規劃下，變得極爲不便甚至直接限制網路的使用，完全否定及摒棄網路帶來的優勢及對世界的改變事實。這無異是走回頭路，未來勢必被資訊社會或國家所邊緣化，成爲資訊社會下的孤兒。爲避免如此現象，縱深防禦的理念將成爲網路防護的主導策略。縱深防禦策略的基本思想是實施多層次和可重疊的防禦，亦即把網路空間劃分爲不同敏感級的區域或層次，對不同層次採用不同的保護措施。針對這樣的防護策略，未來的攻擊方式也將以多層次及重疊性的攻擊策略爲主，以「集中火力」對關鍵網路實施先發攻擊，減少對次要目標花費大多時間及資源，更避免行蹤遭防護人追蹤暴露攻擊地，以取得戰爭執行前哨戰時的優勢。

伍、國軍人員應有的資安防護作為

一、加強個人資安檢測及防護知識

高安全規格的防火牆動輒需要新臺幣數十萬元，就是一般的防毒軟體也都要數千

[註四] 謝惠子，臺灣經濟研究院，＜92年10月能源報導：美加大停電事件始末剪輯＞，http://www.tier.org.tw/energymonthly/outdatecontent.asp?ReportIssue=9210&Page=5，2007年7月10日。

元，一般個人的預算是無法購置如此昂貴的防護工具，因此個人資訊防護資源一般來講是相當有限的。然而更可怕地並不是個人不能添購高昂的防護軟、硬體，而是個人缺乏一般的網路知識及資安概念，這使得個人的電腦更處在一個極端危險的境況。事實上即使有完善的防護機制，由於個人的資安知識的貧瘠，也會輕易遭受病毒的危害而不自知；反之，具有專業的資訊知識及資安的直覺，縱使沒有高昂的防護軟硬體，也一樣可以悠遊於網海之中，而不會招惹病毒的覬覦，更不會讓個人電腦變成「木馬場」。

在眾多國軍發生的資安事件中，可以發現發生資料外洩的主事者幾乎都是階級較高、年齡較大的軍官，此一獨特現象顯示年紀稍長的世代對資訊技能普遍存在一定的陌生程度，這恰巧呼應一般天才型的駭客都是17、18歲的小伙子，對電腦操作相當熟稔，對網路具有無比的狂熱，且又具極佳的體能可持續長時間專注網路攻擊的說法。因此，培養個人基本的網路概念，諸如不對問題網站進行好奇的點選，不安裝非法的軟體，不下載來路不明的程式等等，都是個人資訊防護及基本認知的重要關鍵。另外對主機是否中毒要有一些判斷直覺並熟悉基本的檢測方法及指令，諸如在安全模式下進行病毒掃瞄，可以避免開機時自動載入一些非法程式，使得防毒軟體無法偵測或刪除執行中的非法軟體；或借用他人電腦下載最新病毒定義檔並執行更新，可避免個人主機因受病毒感染而下載非法的病毒碼；讓新的病毒定義檔從開機啓動階段即發揮作用，可加強掃毒的效應。另外按Ctrl +Alt+Del開啓「工作管理員」監視電腦狀態，注意CPU使用率是否偏高，偏高表示有太多的非法程式正在運行中，即可能發生中毒的癥兆；在「命令提示字元」鍵入netstat-n指令，即可檢視是否有多餘的、陌生的對外連線，諸如上述等等基本的網路安全基本概念，都是防護個人主機不受危害或自保的不二法門。

二、遵守「公務不家辦」的原則

將機敏公務資料帶回家中辦理而發生洩密事件層出不窮，甚至已佔導致資安事件發生原因的首位，故遵守「公務不家辦」的原則爲杜絕資安事件的最重要的要旨。公務資料屢在家中遭駭客竊取的原因莫過於家中的網路環境有太多的風險。風險一是家中沒有如單位具有功能強大及設定完備的防火牆安全機制的防護；風險二是在放置在家中的檔案資料遭到偷竊的機率較高；風險三是家中的網路沒有如國軍規劃實體隔離的安全網路體制。這些風險使得資料外洩的機率大增，也使得國家安全及個人前途陷入危機，故單位及個人都應該徹底遵守「公務不家辦」原則，以防範相關情資外洩或遭到竊取的情事發生。

三、養成資料加密及隱藏習慣

加密可以使資料隱藏，使訊息的非法使用者不能了解訊息的眞正內容。資料擁有者如果能在使用該資料檔案後進行加密，不管在爾後的傳輸或儲存時，均提供最基本的防護保障。即使資料遭到竊取時，也不至於立即洩露訊息的內容，從而達到保護數據的目的。目前由軍備局中山科學研究院所設計的檔案加解密軟體(filesecurit)即是一套相當便利的工具，可以提供使用者對任何檔案進行加密，是個人應該於平日時常加以利用的防護工具。惟仍須注意對檔案加密之密碼設定應符合嚴謹複雜之規範，如以無意義字母組合及摻雜特殊字元、變化字母大小寫等原則之要求，較能確保防護資料之功能。

四、使用適當的防護工具

防範病毒入侵的防護最直接的方式就是安裝防毒軟體。但防毒軟體的防護效果並非

百之百，新病毒或尚未被發現的病毒碼，均不是防毒軟體得以檢索及根除的，故防毒軟體仍有其不足之處。但這並不表示防毒軟體不適用，一般說來防毒軟體可以防範百分之八十病毒的感染。爲了加強防護效果，我們可以儘可能採用多重的保護措施及使用多樣的防護工具，例如除安裝防毒軟體外，另外亦可加裝「系統還原」工具。「系統還原」軟體的原理是先將電腦某一時間點的作業系統作猶如ghost軟體一般的儲存，並置放在系統啓動區內。當電腦作業系統重新開機時，無論前次作業更動了任何系統中資料，均會在重新開機後回復到「系統還原」所儲存的那一個時間點作業系統的環境，故萬一電腦遭到病毒攻擊或被植入木馬程式時，只要重新開機後即可立刻清除這些惡意的病毒行爲，達到保護電腦作業系統的目的。同時「系統還原」還因此回復特性可以達到防止系統當機、資料遺失、系統癱瘓、檔案誤刪、檔案毀損、甚至硬碟死當等的問題。雖然還原軟體會造成系統操作上的一些不方便，諸如新增軟硬體工具或更新病毒碼時均須重新儲存及定義新的作業系統還原時間點，但比起遭到病毒的危害，這些不便利就顯得微不足道。

五、區別公務與私務的使用

曾經有人提過要防範網路駭客及病毒最好的策略就是不要使用網路，這種說法雖是事實，然而卻是本末倒置的作法，就好像因懼怕發生車禍就不要使用車子的原理一樣，是不符合道理的。網際網路的優點遠勝於其危險性，以不使用網路或降低使用率都不是最佳的解決之道。其實按安全層級的觀念來使用網路，才是最好的策略，亦即屬於公務的資料應以隔離獨立於網際網路外的電腦主機作業，並配屬專屬的隨身碟，所有資料在退出獨立電腦主機前，必須對所有檔案加密，如此可防遺失或於網路上使用時遭竊的情況發生。另外配合還原軟體於使用網際網路後，進行個人的資料處理前，先重新開機以將電腦主機回復至初始安裝狀態，將中毒的環境及機會盡量排除，以建立最安全的電腦使用環境，雖然作業方式頗爲煩瑣，然而多一層防護，才能多一份資訊安全的保障，也才能建立更安心的資訊作業環境。

陸、結　　論

網際網路的發展已宣示21世紀進入新的資訊時代，社會結構、組織、經濟、文化及軍事因這股資訊工業而面臨革命性的改革及變化，這第三波資訊文明的演進使得人類的生活達到以往社會所沒有的先進及舒適程度。[註五]然而船能載舟卻也能覆舟，運用資訊科技所創造的知識及即時性，讓經濟活動及各國的交流達到前所未有的熱絡及便利，創造了更多的商機及交往，但同時也因資訊科技的便利性及無遠弗屆的特性，讓有心分子有了可乘之機對網路世界進行破壞及犯罪的行爲，造成各國在經濟、社會福利及軍事上的重大損失及傷害，因此各國在第三波資訊文明發展時勢必面臨更大的挑戰。

由資訊科技引發的軍事變革及運用資訊技術所進行的軍事行動，是這些所面臨挑戰中最激烈也是各國最積極關注的重點。軍隊在網絡上進行攻防，發展有如生物病毒般具有感染、隱密性佳、破壞力強、具欺騙及能自我防衛的智慧型病毒，希望一旦在不可避免的軍事衝突中，能先搶得資訊優勢，掌控戰場透明度，以達到不戰而屈人之兵之最大目標。未來隨著資訊科技的發展，可以預判

註五 第三波文明指的是資訊時代，第一波文明及第二波文明分別指的是農業時代及工業時代。

電腦病毒的發展將同步提升，應不致於發生停滯的現象，且趨勢應會形成電腦病毒大量充斥於網路上、病毒將更具智慧性及殺傷力、攻擊面向亦朝多層次目標等，使得網路軍事作戰更爲複雜，攻守更爲艱鉅。但不可避免地，網路戰已經是21世紀的新興戰場，而病毒則爲這場新興戰場的重要殺手鐧武器。

爲因應21世紀資訊高安全需求的挑戰，資訊安全防護等級應提升爲國家安全層級，由國家規劃最高層級的資訊安全作爲及政策，以確保國防安全的生命線。然而，儘管由國家來主導資訊戰的作爲，但此並不意味著未來的網域就安全無虞，反而因國家對網路技術提升及有計畫的運作，使得未來的網路環境更複雜及危險，因而防護的工作將會比現在更困難，預判未來的軍事網路戰安全應以「癱瘓戰」爲主軸，以國家全面性脆弱的基礎設施爲攻擊目標，配合無線技術實施多層次及多重疊性的攻擊策略，以取得傳統武力戰爭形成前的網路攻防的優勢。

基於資訊網路戰日益艱難的環境，首先加強個人資安檢測及防護知識，要列爲比使用高等級的防火牆更爲優先的要求，諸如不對問題網站進行好奇的點選，不安裝非法的軟體，不下載來路不明的程式等等，都是個人資訊防護及基本認知的重要關鍵，也是個人防護中最重要的基本條件。另外根據統計將機敏公務資料帶回家中辦理而發生洩密事件，已佔資安事件發生原因的首位，故遵守「公務不家辦」的原則應爲杜絕資安事件最基本的規範。其次，養成隨時對資料加密或加以隱藏的習慣，均可提供最基本的防護保障，即使資料遭到竊取時，也不至於立即洩露訊息的內容，從而達到保護數據的目的。最後使用適當的防護工具及區別公務與私務的使用，來加強個人的資料防護等，都是相當有用且應該隨時保持的方法。

面對一個新形態的戰爭，我們在觀念上必須從全球性、區域性及國家性三個層面去加以思考，以擺脫傳統思維的束縛。有鑑於此，我國國防部策頒「國軍資訊作業安全管理獎勵及懲處標準表」、「國軍電腦輸出入裝置暨移動式媒體管制作法」、「國軍筆記型電腦使用管制作業規定」等相關管制規定，以重視及推動通資安全相關工作。另外國防部又責成陸軍司令部於95年舉辦了兩梯次「國軍通資安全督檢示範觀摩」，藉由教學與觀摩合一、檢討與策進並重方式，以期有效落實國軍的通資安全工作，爲建構一個無危害之虞的資安環境奠定更爲堅實的基礎。其目的就是要在此無比複雜、不具固定形體、沒有明確界線、所有權曖昧不清的網際網路環境中，取得更安全無虞的資訊作業環境，以避免國內軍事或財經任何一個政策領域，遭到難以估計的衝擊和損害。身爲國軍幹部，我們更應該力行各項資安保密規定，加強個人資訊專業技能，進而影響整個單位以建立一個安全網路環境。

收件：96年08月20日
修正：96年10月15日
接受：96年10月22日

作者簡介

空軍上校陳炳炫，中正理工學院航空系78年班、中工理工學院兵器研究所碩士81年班、國防大學理工學院國防科技研究所博士93年班；曾任助教、系統分析官、程式設計官、研究教官、助理教授；現任職於國防大學戰爭學院戰略研究所助理教授。