資訊安全對國軍影響之探討

海軍上校　黎健文

提　　要：

一、隨著現代武器系統的數位化與網路化，除了必須面對實體的敵人，亦必須面對網路上無遠弗屆的敵人，做好資安工作就是做好戰場經營，這是身為科技時代的國軍官兵應有的認知與覺悟。

二、維護國軍資訊網路安全為全軍共同資安目標，國軍資訊安全政策要求各級應依組織層級發展適合單位任務的資安政策，以管控資安風險，形成健全、有效率的資訊安全組織。

三、資訊安全對國軍的重要性，不亞於台海的制空權與制海權。在新世紀的戰爭中，必須加強資訊安全教育，要求官兵正視國軍資安問題，營造一個零風險的資安環境，以有效防範敵人網路攻擊，確保國軍資訊網路安全。

關鍵詞：網軍、網路作戰、資訊安全、資安政策

壹、前言

近期「維基解密」網站（Wikileaks揭　露數十萬筆情報文件，引起國際注目，網路的興起對未來國軍機密資訊的防護已形成莫大的挑戰，再加上平均1.5秒就有一個惡意程式出現〔註一〕，國軍如未能落實資安防護，便可能成為遭攻擊的目標。以色列一名士兵在社群網站「臉書」（Facebook狀更新　態上透露部隊發動突擊的時間與地點等細節後，以軍考慮此一洩密行為可能導致軍事行動失敗，立即取消突襲巴基斯坦領土的行動，除了處分該名士兵外，亦同時宣布以後將全面禁止以色列軍人使用「臉書」等類似社群網站〔註二〕；另民人以FOXY分享軟體在網路上搜尋到包含陸軍特勤隊反劫持計畫、叢林戰人員編組與裝備名冊等多筆陸軍檔案文件　案，顯示儘管三令五申祭出重罰，國軍資安觀念仍相當薄弱〔註三〕。

檢討國軍資安管理，除系統問題外，最易出　況的根源仍然在於「人」的疏忽，　次資安事件發生多屬未按現行標準程序、人為輕忽及未落實一級輔導一級所致。故各單位應加強宣導教育，落實資安管控及稽核制度，並妥採適切之風險處理作為，以消弭資安風險，要求官兵正視國軍資安問題，營造一個零風險的資安環境，

貳、各國網路作戰發展現況

網路的威脅遍及各層級，從無知用　、惡意的挖土機（切斷電源）、好玩的駭客、專業的駭客、有組織的犯罪活動，甚至國　、國際、他國政府贊助的活動都有。入侵者可能是搜尋可盜用的身分或從事工業間諜活動的資訊，以主電腦操控一群受到殭屍網路病毒感染的電腦，企圖接管政府電腦，或是試圖藉此在未來衝突中，擁有可能的軍事優勢〔註四〕。

2009年3月加拿大資訊作戰觀察（Information Warfare Monitor）研究機構公布一份名為「追蹤間諜網路」（Tracking GhostNet）　研究報告，調發現103個國家中有1295台被入侵電腦是與在中國的間諜網路（GhostNet）伺服器相連〔註五〕。2010年4月資訊作戰觀察與影子伺服基金會（Shadow Server Foundation）兩研究單位聯合公布另一份「雲中陰影」（Shadows in the Cloud）　報告中指出，網路間諜行動的駭客利用各種雲端運算系統、社交網路、或是免費的代管服務以掌控被駭電腦，而主要的控制伺服器則位於中國，以建立全球「殭屍電腦」（Botnets）網路〔註六〕。一場由中國駭客所掀起的網路惡戰，讓各國開始擔心基礎設施遭到駭客惡意攻擊。因此，世界各國紛紛被迫建立網路安全機制，陸續成立網路作戰中心，甚至開始對駭客進行招兵買馬，未來可能會演變成一場不可避免的「網路新冷戰」（Cyber Cold War）。中共網路作戰係由「軍委」層級主導，係屬戰略階層作戰運用，自八o年代初起始，現已具網軍規模，中共已將網路戰，列入「節點」打擊作戰之一環，其破壞程度不容小覷。所以資訊安全對國軍的重要性，已經不亞於台海的制空權與制海權，國軍必須更積極強化資訊安全防護基礎建設及強化資安防護應變能力，才能有效防範敵資訊網路攻擊，確保我資訊網路安全。

一、中共

中共首次正式資訊戰演練於1997年10月進行，作戰想定是以某軍區集團軍遭病毒攻擊，該集團軍使用防毒軟體進行防護，以避免戰情系統癱瘓。1999年，中共「網軍」一詞首見於解放軍報，網軍初期規模大概為「營級」，之後規模不斷擴充，包括有攻擊、防衛與維護三大部門，對外國進行資訊滲透、改造與破壞等工作。2002年1月1日組成「科研實驗部隊」，其中將共軍全軍規範為七大類，即陸軍、海軍、空軍、第二砲兵、科研實驗部隊、預備役部隊、武警部隊等，分別研擬訓練大綱體系。另因應軍事科技革命而組建一批新的科技型部隊，亦即所稱之「科研實驗部隊」。該部隊包括因應「資訊戰」而新成立的「電子戰部隊」、「網軍」和「心理戰部隊」，以及為搶奪立體空間「制高點」的「天軍」。中共在2005年開始將「電腦網路作戰」的攻勢作為列為演習的項目，二砲部隊於2006年還成立電子戰藍軍部隊，以攻防演練的方式大幅增進共軍網路攻擊能力〔註七〕。在2002年至2007年間，解放軍七大軍區所轄之電抗團（營），採任務編組方式或納編民間資訊、官、學界、省屬縣市及鎮之民兵共同組成，配合各項軍演實施網路作戰，陸續設置了電子戰分隊、網路戰分隊、黑客（駭客）分隊、信息救護分隊及在各個業　設立國防訊息組織分隊(如表一)，極大地擴充了網軍的規模〔註八〕。

狹義的網軍，係指解放軍的正式編制，美方學界評估為營級規模，成員包括民間大學及訓練中心所訓練的民間網路專家；廣義的網軍，則由解放軍、公安網路安全單位及網路管制單位整合而成，規模約數萬人〔註九〕。中共除了正式編組的網軍外，網軍預備役部隊亦是「網路戰」的重要部分，目前中共有150萬預備役部隊熱衷於打「網路人民戰爭」。在部分地區，共軍已經把預備役部隊編成小型「網路戰」部隊。組織上包括網路戰營、電子戰營、情報心理戰營以及技術分隊等等，可以進行電子對抗、網路攻擊和防護、雷達偵察等演練。國安局長蔡得勝表示，2008年中國網軍對我政府單位網站進行高達3100多起的攻擊〔註十〕，目前中共至少有3萬網軍　天在對台灣滲透2010年1月初美國媒體引用FBI的一份機密報告中指出，中國大陸已經組建一支超過18萬人的網路部隊，其中3萬為網路特工，15萬為民間駭客。2010年4月中央軍委更發表了《關於加強了新形勢下軍隊資訊安全保障工作的意見》，意見　容強調，「加強資訊安全保障工作是資訊時代國防和軍隊現代化建設的客觀要求，提高資訊安全保障能力是做好軍事鬥爭準備的現實需要，構建資訊安全保障體系是資訊化建設的緊迫任務」，進一　增強共軍資訊安全意識〔註十一〕。2010年7月19日解放軍總參謀部成立「信息（資訊）保障基地」，除因應外軍的網路攻擊外，另對全軍資訊化建設進行集中統管，目標是2020年建立全球第一支資訊化武裝的部隊。

二、北韓

北韓人民軍從 1986 年起，開始在金日成軍事綜合大學培養電腦專業人員，學制為五年。近二十年來，這所大學每年提供北韓人民軍一百名高級電腦人才，他們集中接受電腦、情報傳送體系、暗號開發、駭客技術等專業技能的學習和訓練。目前這支專業駭客部隊維持在五百人左右，年度預算為七百多萬美元。這支網路駭客部隊必須不斷進行人員淘汰、不斷更新電腦知識，以求跟得上瞬息萬變的網路世界。隨著北韓駭客部隊能力增強，一般認為，北韓已經有發動網路戰爭的能力。北韓現在擁有建造和部署網路武器和電磁脈衝裝置的技術能力，能夠在有限的範圍內摧毀敵方的電子設備和電腦。2008 年北韓實施一種含有惡意代碼的電腦程式網路武器試驗，在某些事件或在某個預設的時間點就會自動執行，能導致電腦當機、資料數據被刪除等電腦災害的邏輯炸彈試驗。2009 年 3 月 5 日，北韓駭客對南韓陸軍第三軍司令部發動網路襲擊，盜取了國立環境科學院化學物質安全管理中心的安全密碼，再利用密碼盜取了環境科學院構建的「化學物質事故應對情報體系」相關情報，這些資訊有助於北韓發展化學武器，在戰時對南韓發動襲擊。2009 年 11 月南韓《5027 作戰計畫》被網路駭客所竊取，南韓軍方在報告中指出，北韓駭客可以癱瘓美軍太平洋司令部的指揮系統。美國在對資訊戰的威脅評比等級中，也將北韓列為第 8 位，可見美國與南韓都對於北韓網路部隊的威脅，感到高度憂慮。

三、南韓

2009 年 7 月 7 日，美國白宮、國防部、財政部與南韓總統府青瓦台、國防部、國家情報院等政府機構網站，不斷遭受阻斷式網路攻擊。據統計，美國與南韓方面共有約 25 個網站遭到攻擊、南韓 12,000 部個人電腦和國外 8,000 部個人電腦成為「傀儡電腦」，並淪為攻擊其他目標網站的平台。南韓國家情報院表示，這些網路攻擊的幕後黑手應該是北韓與支持北韓的勢力所為。據 2009 年 12 月中旬發行的《朝鮮月刊》報導，韓國國家情報院發現，由於美韓聯合司令部某位軍官在使用存有軍事機密的 USB 隨身碟時，因為操作疏忽，不小心連接到外部網路，卻沒有及時拔掉 USB 隨身碟，因而導致美韓聯合司令部針對朝鮮半島發生全面戰爭時，制定的具體作戰計畫《5027 作戰計畫》的部分二級機密內容，被使用中國大陸網路伺服器的駭客所竊取。南韓軍方推測，這可能又是北韓專業駭客部隊所為；國家情報院和機務司令部還因此針對美韓聯合司令部的業務電腦，實施了大規模的網路安全檢。雖然南韓在 1999 年就提出了未來資訊建設的總體構想，但是 600 多個政府部門機構中，平均一個政府機構只有 7 名資訊安全專家，負責維護網路安全，甚至還有近七成的政府部門根本就沒有網路安全專家。然經了近來一連串的北韓駭客網路襲擊後，目前，南韓已經擁有了約 10 萬接受過專業訓練的龐大的人才隊伍，而且年國防經費的 5% 被用來研發和改進實施網路戰的核心技術。2010 年 1 月份成立「資訊安全司令部」，同年 7 月起正式運作。南韓國防部表示，新成立的「網路司令部」隸屬國防情報本部，由少將級軍官指揮的 200 人左右的獨立部隊，除了維護南韓國家的網路資訊安全外，還將具備擾亂他國網路系統的攻擊能力〔註十二〕。

四、日本

日本其重要作戰指導思想是通過掌握「制網權」達到癱瘓敵人作戰系統的目的。日本在構建網路作戰系統中強調「攻守兼備」，撥付大筆經費投入網路硬體及「網戰部隊」建設，分別建立了「防衛資訊通信平台」和「電腦系統通用平台」，實現了自衛隊各機關、部隊網路系統的相互交流和資源共用；成立由 5000 人組成的「網路空間防衛隊」，研製開發的網路作戰「進攻武器」和網路防禦系統，目前已經具備了較強的網路進攻作戰實力。同時，日本注重與美國聯合發展，在引進先進技術的基礎上不斷完善自身建設，不斷提升「網戰」能力。2009 年，日本防衛省決定新建專門應對電腦攻擊的「電腦空間防衛隊」。2010 年，日本防衛省開始進行相關準備，爭取在 2011 年組建電腦防衛隊。防衛隊主要負責蒐集最新的電腦病毒資訊，研究避免病毒感染對策，並加強對防衛省和自衛隊情報系統的監管。

五、印度

印度基於對網路技術的精通和利用網路能達到何種戰爭效果的瞭解，堅持自主研發、軍民合作的原則，投入大量人力物力，力求在網路技術、晶片技術以及作業系統方面自成體系。除完善防禦體系外，印軍面將網路戰攻擊寫入作戰條例，明確指出要建立能癱瘓敵方指揮與控制系統以及武器系統的網路體系。2008 年印度軍方曾提出建立萬人網路部隊的構想，目前已在陸軍總部、各軍區以及重要軍事部門分別設立網路安全機構；另一方面通過吸納民間高手入伍和對軍校學員進行「駭客」技術培訓等方式，課程著重於獲取情報和反網路偵察上，逐步完成未來網路戰的人才儲備。

六、英國

英國首先於 2001 年組建了一支隸屬軍情六處（MI6）、由數百名電腦精英組成的「駭客」部隊。2009 年 6 月 25 日公布國家網路安全戰略〔註十三〕，英國政府並考量保護政府機關及民眾免於網路安全威脅下，宣布成立網路安全辦公室（Office of Cyber Security），工作人員來自軍情五處（MI5）、軍情六處（MI6）和其他政府機構；2008 年針對網路攻擊的防禦設立「網路安全行動中心」（Cyber Security Operations Centre），該行動中心隸屬政府通信總部（GCHQ），兩個網路安全新部門，分別負責協調政府各部門網路安全和協調政府與民間機構主要電腦系統安全保護工作，並於 2010 年 3 月正式運作。由於現在包括通訊、水力、鐵公路，甚至核電廠等基礎設施，都已成為網路戰的攻擊目標。英國安全事務大臣韋斯特日前表示，英國將招募年輕駭客做為核心戰力，建立一支擁有反擊能力的強大網軍。同時，英國內閣辦公室發出聲明表示，英國政府將網路安全訂為二十一世紀政府的安全防護重點，並認為透過設置這個新的機關協助維護國家安全，是達成這個目標的重要步驟。英國政府承認網路安全對於政府在安全防護上的挑戰，因此，內閣辦公室強調，網路安全防護策略之整合是重要的，其將透過企業、國際合作夥伴及民眾的力量，藉由專業知識及能力的提升以及更為完善的策略，降低安全風險及發掘安全防護機會，發揮英國在網路安全防範之優勢〔註十四〕。

七、美國

美國國防部網路安全係由華府的「全球網路作戰聯合特遣部隊」（Joint Task Force for Global Network Operations）主導，此部隊隸屬美國戰略司令部。美空軍成立「網域全球打擊網路作戰指揮部」（Cyberspace, Global Strike and Network Operations Command），具備遂行攻擊任務的能力，毋須投擲炸彈即可阻止敵軍事行動或政府運作。美國在 2005 年 4 月在國防部戰略指揮部（USSTRATCOM）中，

成立了「網路戰聯合司令部」（Joint Functional Component Command for Network Warfare, JFCC-NW），負責具體為美國進行攻擊性的網路戰。美國戰略司令部係美國戰略部隊之統一作戰司令部，負責管制軍隊太空作戰、資訊戰、戰略預警和情報評估、規劃全球戰略作戰，並全權負責電腦網路作戰。美國戰略司令部下轄太空與全球打擊、情監偵、網路作戰、整合飛彈防禦，以及打擊大規模毀滅性武器等數個聯合作戰指揮部。

除了「網路戰聯合司令部」外，美各軍種也分別組建自己的網路戰部隊。美國陸軍成立「陸軍電腦緊急反應隊」（Army Computer Emergency Response Team, ACERT），負責陸軍各基地的電腦網路防衛（Computer Network Defense, CND）行動，必要時也可發起網路攻擊，侵入他國的軍事網路。海軍主要的「資訊戰」計畫稱為「海軍資訊戰活動」（The Naval Information Warfare Activity, NIWA），與「艦隊資訊戰中心」（Fleet Information Warfare Center, FIWC）共同研擬與規劃海軍資訊戰的相關事宜。「艦隊資訊戰中心」還在諾福克（Norfolk）成立了「海軍電腦事件反應隊」（Navy Computer Incident Response Team, NAVCIRT）。「海軍網路防衛作戰指揮部」（Navy Cyber Defense Operations Command），位於維吉尼亞州的諾福克（Norfolk）該指揮部約有 170 名成員逐行「24 小時監測」。監測包括海軍與陸戰隊的　部網路和戰術網路，計有位於 6 國的 300 個基地 76 萬 1,000 名用　。目前的美海軍網路防衛作戰指揮部，其前身是「艦隊資訊戰中心」FIWC）於 1995 年成立的處級單位，2003 年成立獨立的指揮部，即「海軍資電立即反應小組」（Navy Computer Instant Response Team），美海軍網路防衛作戰指揮部負責網路防衛和網路管理，由位於諾福克的指揮部人員與所有業務的系統經管人員密切合作執行這兩項工作。美國空軍則直接在第八航空隊（8th Air Force）的基礎上，在 2006 年轉化為「空軍網路戰指揮部」（Air Force Cyber Command, AFCC），以擴大整備因應網域戰爭。該指揮部位於路易斯安那州的巴克斯岱爾（Barksdale）空軍基地，將籌設成為美空軍第一個主要從事網路作戰的司令部，專職部隊訓練與配備，並透過網域與航太作戰充分整合，以逐行持續性全球網路作戰。「空軍網路戰指揮部」共有 2 萬 5 千人在此工作，負責防衛網路、基礎建設系統保安和監察工作。國防部長蓋茲 2009 年 6 月 23 日正式下令組建網路司令部，以統一協調保障美軍網路安全和開展網路戰等與電腦網路有關的軍事行動，美軍的網路戰部隊將於 2030 年全面組建完畢〔註十五〕。

參、駭客手法與未來趨勢

網路上超過百萬個教導製作病毒及駭客程式之網站，不同於傳統武器須投入大量資金、時間研發，倘若未能落實執行資安防護措施，認識駭客攻擊手法，便可能成為遭攻擊的目標。當網頁服務的規模與複雜性增加時，暴露於外的風險也逐漸增加〔註十六〕　。開放 Web 軟體安全計畫（OWASP）公布 2010 年世界十大網頁安全風險〔註十七〕，世界各國網路作戰單位為符合現時網站攻擊的趨勢，也針對最新的攻擊手法列入研究，美國聯邦貿易委員會（Federal Trade Commission）及美國國防資訊系統局（Defense Information Systems Agency）等官方機構強烈建議甚至明列於作業標準中以做為相關單位之執行依據，透過新版本的文件，我們可觀察到駭客針對網站攻擊趨勢的變遷已從常見的安全性弱點（僅考量發生的可能性）提升到安全風險（考量發生的影響程度）。多數人認為在全球資訊網或網際網路上才能展開電腦網路攻擊，但事實上，藉由動態手段實體破壞電腦系統或網路，亦屬於電腦網路攻擊〔註十八〕。針對敵資訊戰能力增長，入侵技術不斷變化(如表二)，研析對國軍資安可能風險，發展資安關鍵技術，以因應不斷變化之資安威脅。平時應針對敵方可能遂行之資訊網路攻擊方式，演練各項因應作為，並研發安全防護技術與設備，建立密碼邏輯、系統防護管制與應變等標準規範，嚴密資訊作業安全紀律。戰時則經由國軍通資網路，掌控全軍資訊、通信、指管系統之資料傳輸，確保國軍指管機制與神經中樞運轉之安全無虞。

一、OWASP 2010 Top 10 攻擊手法與防護作為

(一)資料隱碼攻擊（Injection）

常見的有 SQL Injection、Command Injection 等注入攻擊手法，發生的主因是網頁程式中未檢驗使用者的輸入，讓攻擊者可以藉由輸入指令的方式來對後端的資料庫等系統進行詢或其他操作。

防護作為：

1.嚴密的檢所有輸入，對於字串的輸入加以過濾，並限制長度。

2.加強資料庫帳號與網站的權限管理，做好軟體開發控管。

(二)跨網站攻擊 Cross Site Scripting（XSS）

互動式網頁程式中未檢驗使用者的輸入，讓攻擊者可以藉由輸入網頁語法來達到攻擊目的。

防護作為：

1.檢頁面輸入數，不信任使用者輸入的資料。

2.加入編碼並使用白名單機制過濾。

(三)權限奪取與控制（Broken Authentication and Session Management）

網站中自行開發的身分驗證與連線管理等功能具有安全性上的缺失，讓攻擊者可以冒用特定或全部使用者的身分與權限進行操作，造成更大的危害。

防護作為：

1.登入及修改資訊頁面使用 SSL 加密並設定完善的 Timeout 機制。

2.驗證密碼強度及密碼更換機制。

(四)不安全的物件參考　(Insecure Direct Object Reference)

　　攻擊者透過修改應用程式提供的　案讀取功能參數，任意存取並未對外公開的重要　案與目　，屬於一種未驗證輸入的攻擊手法。

防護作為：

1.避免將私密物件直接暴露給使用者，驗證所有物件是否為正確物件。

2.使用 Index/Hash 檔方法，而非直接讀取　案。

(五)跨網站冒名請求 Cross Site Request Forgery（CSRF）
屬跨站本攻擊（XSS）的一種，常搭配 XSS 弱點發動攻擊。當使用者已經登入系統情況下，常可透過某些連結或指令碼進行系統操作，或修改系統設定。
防護作為：
1.確保網站　沒有任何可供 XSS 攻擊的弱點。
2.在輸入欄位加上亂數生的驗證編碼，在高權限的頁面，重新驗證使用者。
(六)網站安全組態設定缺失 (Security Misconfiguration)
檔管理面的問題；可能使用者未修改預設帳密，或是沒有作必要的安全性更新，或未針對重要的　案或目　進行保護等，都屬網站安全組態設定缺失弱點。
防護作為：
1.不需要的帳號、頁面、服務、連接埠均關閉。
2.系統密碼禁止使用安裝時之預設密碼，檢伺服器均經過防火牆等設備保護。
(七)未適當限制的 URL 存取（Failure to Restrict URL Access）
某些網站並未有效定義權限的控管，導致攻擊者可透過修改 URL 路徑或參數，來存取包含有機敏資訊或管理權限的頁面。目前還是有大量的網站將後台管理系統暴露在網際網路上並開放使用者任意存取，形成潛在的網站安全風險。
防護作為：
1.使用防火牆阻擋，密碼授權加密。
2.網站架構最佳化。
(八)未驗證的網頁重新導向（Unvalidated Redirects and Forwards）
某些網頁程式提供網頁重新導向功能，讓使用者可透過該程式連接到其他網站；但攻擊者可利用這種特性，將惡意或釣魚網站暗藏在網頁重新導向的參數中發送給使用者，讓使用者疏於防範，連接至攻擊者指定的惡意或釣魚網站。
防護作為：
1.非必要時避免使用 Redirect 及 Forward。
2.驗證導向位置及存取資源是合法的。
(九)不安全的加密儲存（Insecure Cryptographic Storage）
攻擊者通常較少直接針對加密進行破解，而是透過其他攻擊方式去存取到後端的機敏資料，若機敏資訊在儲存時並未經過加密處理，將讓攻擊者直接獲得許多有用的機敏資料。
防護作為：
1.使用現有公認安全的加密演算法，減少使用已有弱點的演算法。
2.安全的保存私鑰。
(十)不安全的傳輸防護（Insufficient Transport Layer Protection）
當使用者在傳輸機敏資訊時，若網站未提供安全的傳輸通道，將允許攻擊者進行連線竊聽，竊取使用者傳輸的機敏資訊。
防護作為：
1.盡可能的使用加密連線。
2.確認加密憑證是有效並符合 domain。
3.後端連線也使用加密通道傳輸。
二、資安未來趨勢分析
OWASP Top10(如表三)常被視為網站安全參考標的之一，透過參考 OWASP Top10 可更了解目前所遭遇的網站風險，進而透過技術與管理層面，降低問題與風險的發生。新版的風險評比方式，是依威脅、攻擊方式、脆弱度到偵測性、技術與營運的衝擊等網站安全項目作量化評比。我們透過這份新版本的文件，可以觀察到駭客針對網站攻擊趨勢的變遷已從常見的安全性弱點（僅考量發生的可能性）提升到安全風險（考量發生的影響程度），歸納出以下趨勢：
(一)資安技術面與管理面需並重
資訊安全除了技術面的安全威脅外，管理面的安全威脅造成的影響一樣不容忽視；技術面的問題除了透過技術解決與修補方案外，還可透過資安管理制度的建立，來做通盤的審視，避免在各個獨立的技術環節中生的間隙；而資安管理制度的建立，除了必須對資安技術具有一定程度的了解，更要以資訊使用者能便利安全的使用資訊系統及管理者能確實有效的管理網路行為的角度，規劃建置一套良好的資訊環境，提供服務，才能妥善地規劃出適合組織的資安管理制度。
(二)「社交工程」（Social Engin-eering）快速興起
社交工程，就是利用人性的弱點，進而達到詐騙、入侵的目的。而最大的漏洞，就是在「人」這個字上面。「社交工程」是利用網路為媒介或工具，針對人性弱點所進行的詐騙手法，是一種利用人際關係間的互動特性所進行的攻擊法，以影響力或　服力來欺騙他人，藉以獲得有利入侵的資訊，這是近來造成企業或個人極大威脅和損失的駭客攻擊手法，攻擊時避開較不容易破解的防火牆，是非常難以防範的攻擊模式。近來社群網站興起，攻擊者將可快速地利用社群網站並影響到大量的使用者，衍生出許多使用者隱私與安全性上的問題。
(三)大批量及複合式攻擊成為主流
大批量攻擊成為網站攻擊的主流，這與 Google 的超強搜尋能力顯然有正相關，許多安全性弱點，都可以搭配 Google 搜尋到相關攻擊資訊與攻擊標的，可讓攻擊者快速地將攻擊模式複製到其他攻擊標的，造成大規模攻

擊效果，甚至還可以搭配其他安全性弱點或網站服務，來擴大攻擊的效果。

(四)未驗證輸入（Unvalidated Input）仍是最大風險

許多網頁程式上的安全性弱點都與未驗證使用者的輸入有關；如果在程式開發過程中，就導入安全程式的寫作觀念，並針對使用者輸入的　容進行過濾與處理，將可阻大半的網站安全風險〔註十九〕。

肆、資安事件分析與管理

管理學中提出一個「破窗理論」（Broken Window Theory）〔註二十〕，假若有一幢建築物的窗　破損而未獲得及時修復，就會有更多的窗　被人打破，而且這幢建築物很快就會成為犯罪的　床。「破窗理論」是一種集體行為，要防止不良集體行為的發生，當出現「破窗」就必須趕快處理。資訊安全也是同樣的道理，一旦發生資安事件，各單位都會立即受到影響；因為只要有一處資安漏洞，就會危及全軍。隨著對資訊科技的依賴越來越深，資訊安全的威脅也就越來越大，若是稍有疏失，輕則造成資料遺失，重則釀成重大災害，現今資訊安全重點強調的是由上而下的整體架構，重視的是管理而非技術，因此，我們應以一種全新的觀點來建立對於資訊安全的認知，唯有建立良好且完整的資訊安全管理機制，才能確實降低組織所面臨的各種資訊安全問題。資訊安全的定義，雖然不同學者各有不同之看法，然而主要均著眼於如何確保資訊安全性之作法，特別是越來越重視資訊安全之管理層面；美國電腦聯邦調局（FBI）對於電腦犯罪及安全所做研究調也顯示，大多數之危安事件均是由於人員的疏失或是蓄意破壞所造成的，其中企業或組織　部的員工所造成的危安事件更占了大部分，由此可知即使企業或組織使用再好的資訊技術，也無法防範人員所造成的威脅或意外事件，因此如何強化組織內部管理已成為現階段非常重要之議題。歸納資訊安全事件所發生之原因，不外人為及自然因素所造成的，一般說來　，資安事件發生原因可歸納表四〔註二一〕所示。

據統計顯示，在眾多的意外事件中，屬於自然因素的資訊安全事件比率，僅占 15%，人為因素的比率卻高達 85%，在此 85%中，組織　部人員所造成之事件就占了 80%〔註二二〕，因為這不是使用再好的資訊技術所能解決的事件；其問題的核心，在於沒有做好單位　部安全管控，故如何有效防範　部人員所造成的資訊危安事件，實是今日資訊安全的重點議題；然而不論是天災或人禍，若造成資料外洩或毀損的資訊安全事件，均會為組織帶來一股衝擊，其解決之道就是建立組織　部之資訊安全管理制度。所謂「資安事件」，係指該事件已造成國防資訊或資訊資「機敏性」、「完整性」、「可用性」的破壞，資安事件一旦肇生，均需針對傷害程度，檢討處；而「資安違規」係指違反資訊安全相關規定，惟尚未對相關國防資訊或資訊資的「機敏性」、「完整性」、「可用性」造成危害，違規者需依據「資訊安全獎懲基準規定」予以處罰，並且要參加資安再教育。所以對資訊科技的運用不要掉以輕心，因為由「資安違規」衍生為「資安事件」機率是相對較高的，一旦發生資安事件，只要有一處資安漏洞，就可能會危及全軍。

伍、資訊安全政策

資訊安全政策包括與安全作業相關的策略、規範與標準；還包含了降低風險、減少弱點、嚇阻攻擊、國際合作互動、資安事件反應、系統還原和復原的政策與活動能力；也含有電腦網路作業、資訊確保、法律執行、外交、軍事與情報任務。凡此種種，只要和全球資訊基礎建設的安全及穩定相關的議題，皆屬於資訊安全政策的範疇。全軍共同性之資安目標為維護國軍資訊系統網路安全，現正以資安管理制度專案的方式來推動「國軍資訊安全政策」，各級應依組織層級發展適合單位任務之資安政策，持續推動「風險評鑑、文件管理、　部稽核、管理審、教育訓練」等各項資訊安全管理活動，以管控資安風險，形成健全、有效率的資訊安全組織，進而建構一個更堅實的防護基礎，確保資訊安全。

一、我國的資訊安全政策

行政院「國家資通安全會報」，主要負責「強化政府資通安全防護能量、防衛國家資通設施、建立資通安全預警機制、主動偵防降低實質危害因素、推動資通安全技術研發、提升執法機關偵防能力」等國家資安相關工作。行政院國家資通安全會報為我國負責資通安全的最高行政單位，由行政院主管科技之政務委員兼任總召集人，負責推動我國資通安全基礎建設工作。目前已完成建構國家資通安全整體防護體系及建立資安環境與制度等國家資通安全重大工作，刻正針對國　資通安全環境的脆弱性持續加強實施資安作業〔註二三〕。

我國資通安全目標為：

(一)防止資通安全遭受攻擊及導致國家重要基礎建設受損。

(二)減少國家資通安全的弱點，以降低風險。

(三)遭受攻擊時，縮小損失範圍及回復時間。

為達上述目標，必須建立國家資通安全事件通報及危機應變體系及健全國家資通安全防護能力，強化資安認知與訓練及確保國家資通安全促進國際合作。

二、國軍資訊安全政策

國軍資安事件究其原因除資安管理除系統問題外，最易出　況的根源仍然在於「人」的疏忽。檢討　次資安事件發生多屬未按現行標準程序、人為輕忽及未落實一級輔導一級所致，故各單位應加強宣導教育，落實資安管控及稽核制度，並妥採適切之風險處理作為，以消弭資安風險。尤其是通資科技發展快速，駭客入侵手法不斷地翻新，因此國防部順應各單位任務需求與環境特性，解決實務執行窒礙與疏漏，並遵循行政院「資安管理機制」及「CNS27001 國家標準」，修頒「國軍資安政策」，其重點就是要落實資安風險管理及提升資安環境，輔導各單位建立資安風險評鑑的能力，掌握自身的弱點與可能面對的威脅，並採取適當的管理作為做好資安風險管理。導入資安風險管理實施評估與鑑識，明訂危機處理規範與原則，同時律定安全責任機制、側重閘口防禦縱深、強化端點警覺與集中人力資源管控等多項要求。

國軍資訊安全政策，是提供全軍資訊安全管理的一般性指導原則，各單位必須依照組織的層級，發展適合單位任務需求及環境特性之「資安政策」，這也就是 ISMS 資安管理制度所稱的一階文件；並且須規劃、設計配套錄「管理辦法」、「作業程序」與「紀　表單」等二、三、四階文件，這些都須以國軍資安政策之指導原則為基礎而制定，任何不適用本政策指導原則之資訊作業環境，都應該視為特例，這些資安政策及相關配套措施都必須專案報部核定，並且經過資安風險評鑑等程序，確認是可以接受之殘餘風險後，單位才可以依據實施。

「ISMS 資安管理制度」是依據 CNS27001 國家標準制定而成的〔註二四〕，必須依照標準推行建立相關資安管理制度，並以四階文件架構規範文件的製作及管理作為的執行。四階文件就是「資安政策」、「管理辦法」、

錄作業程序」與「紀　表單」，在「國軍資安政策」中也律定各層級的單位所應編製的原則。另外這套制度的精神強調的是結合「風險管理」的作為來確保資訊安全，所謂「資安風險」是指：「威脅利用弱點對資造成衝擊的可能性」，這裡面有威脅、弱點、資、衝擊程度及發生機率這五大風險因子，各單位須從資訊資清做起，並對須保護的資實施風險評鑑，以此建立單位資訊安全所應防護管控之對應政策，並製定單位官兵所應遵循的規範與原則，以落實在足以降低資安風險的各個面向作為當中，建立單位適用的環境。

維護國軍資訊系統網路安全為全軍共同性之資安目標，要確保資訊的安全性，應該由管理面著手，並以科技協助建立資訊安全管理制度，國軍刻正以資安管理制度專案的方式來推動「國軍資訊安全政策」，各級應依組織層級發展適合單位任務之資安政策，持續推動「風險評鑑、文件管理、　部稽核、管理審、教育訓練」等各項資訊安全管理活動，以管控資安風險，形成健全、有效率的資訊安全組織，進而建構一個更堅實的防護基礎，確保資訊安全，打造更安全、更有保障的資訊環境〔註二五〕。

陸、國軍資安防護具體作法

資訊安全政策是資訊安全管理的基礎，而單位主官的支持度，決定資安政策的成敗。維護國軍資訊系統網路安全為全軍共同性之資安目標，要確保資訊的安全性，應該由管理面著手，並以科技協助建立資訊安全管理制度。提升國軍資安防護機制、降低資安違規事件具體作法如后：

一、加強充實資訊新知，提升資安防護概念

據統計目前網路上已經超過一百萬個教導製造電腦病毒及訓練成為電腦駭客的網站。所以人人都能隨時隨地發動資安攻擊，而電腦病毒也已超過百萬種。如果不能時時更新資安防護措施，並認識新種的電腦病毒及駭客手法，便可能成為駭客下一個覬覦的對象。

二、培養良好保密習性，強化人員資安警覺

資訊安全漏洞，大部分是來自於人為的破壞與疏忽，所以最有效的資安防護政策，還是要個人養成良好的保密習性、貫徹實體隔離政策、不將機密資訊儲存於電腦中、關閉不必要的分享設定、不下載非法軟體，及使用加解密軟體，更重要的是，不要將機密資訊帶離作業區或公務家辦，才能將資安風險降至最低。

三、貫徹資安稽核察，建立網路巡機制

網路定期實施網路巡邏、分析警示與異常網路流量，才能有效控管資料外洩及資訊攻擊的風險。培養資管人員、設立專職資安人力，是未來各單位及犯罪防制的目標；各級應重視資訊部門，推廣資安教育，建立網路巡及監控，才能確保資訊能量，適時防堵資訊攻擊。

四、加強人員教育訓練、持恆宣導資安規定

各單位應針對新進人員持續實施資安宣導及相關教育訓練，勿使用非法軟體或好奇任意下載不明程式，各級資安長及資安官確實督導執行，強化各員資安觀念，利用各項集會時機加強宣　導資安政策及規定、根植各員資安防護及即時回報觀念，防範危安於未然，即時通報以處置。

五、建立主動監偵架構、即時管控整體防護

因應資訊網路攻擊對通資系統之影響，強化國軍資安監控中心運作機制，以「分散防護、集中管理」，建立「區域聯防、集中監控」之國軍整體防護架構，實施網路分級管理機制，防範非法及惡意軟體入侵軍網；建立主動監偵、即時管控的資安防護架構，同時確保資訊系統使用人員身分認證及授權，阻網路非法行為方式，防止木馬或病毒植入。現階段營區至資安防護管理中心間已建立整體防護機制，惟更需朝「加強跨單位間資安連結」及「落實區域聯防」等策略，以提升整體資安防護能量，確保國軍網路正常運作。

六、落實門禁管制察，嚴禁私帶資訊設備

持續要求強化各單位門禁安全察作業，要求各項資訊設備及媒體攜出入營區確實填具「資訊設備（媒體）攜出入三聯單」，以有效管制資媒出入營區流向，即時稽資訊設備、媒體所在部位。並加強衛哨勤務　訓練，避免官兵或民人私自攜出（入）資訊設備或媒體，凡發現不當應立即制止，杜軍中資訊外流。

七、強化資訊資管理，精進　部防護作為

各單位應對資訊設備定期實施檢，並透過各項軟體工具及早發掘潛在損壞危機，若有使用年久已屆汰除之設備，應特別注意設備妥善　況，避免設備因非預期之損壞，造成重要資料損失。落實單位資訊設備及媒體稽核作業針對移動式儲存媒體確實執行帳籍清及核對，並管制媒體借出/歸還作業，嚴密資訊媒體使用/存管部位，避免肇生資安事件。

八、　案加密切勿輕忽，硬碟銷毀必須落實

機密資料一旦放上網路，即使是網路警察或法院，都很難讓其停止傳播散布或真正銷毀。國軍官兵應該養成將檔案依類別或重要性分類，並儲存在不同的磁碟分割中，針對重要性較高的　案與磁碟分割給予加密防護的習慣。儘管對資料有嚴密的保護措施，但容易疏忽的是維修與報廢流程，這也是機密資料保護最容易被忽視的一環。一般單位往往缺乏完善的維修與報廢流程，正確的作法是報修時，應將電腦　部的資料加密、清除或將硬碟拔除送修，若真要報廢硬碟，應該先將舊硬碟格式化，再進行拆除外殼的物理性破壞手續，及針對所有物件確實清點，以避免有漏網之魚，才能盡量減少資料外洩的機會。

九、違規人員速懲速罰，資安事件獎懲分明

「患生之所忽，禍起於細微」，檢討資安事件之肇生，主為個人輕忽大意，及電腦維修紀律要求不嚴所致，是以各級對所屬單位　部資安管理，應秉持「嚴格考、落實稽核」之原則，要求確遵資安獎懲相關規範，不容有任何模糊空間或便宜行事。各單位凡發生資安事件均應斷然處置，速懲速罰，管制追肇因，以嚴肅資安紀律，隱匿未報者加重處分，毋枉毋縱、賞罰分明，無論違規或系統誤判　況，須依規定於接獲通知30內分鐘　完成初報，並於3內　將相關檢討報告（含策進作為）依行政程序呈報司令部，資安突檢小組不定期至違規單位實施複檢，俾管制各項資安違規處　況，掌握資安違規事件處置進度，消弭各項危安潛在因子，俾達國軍零資安事件目標。

柒、結語

資安防護並非一蹴可及，唯有透過完善的資安政策，加上週全的安全防護計畫，再搭配上熟練的應變程序，才能掌握突發事件，並完善處理。違犯資安規定，除應快速通報外，仍須仔細檢討肇因，修補自身防護的漏洞與弱點，同時再次檢視原訂之安全防護計畫與緊急應變程序是否需要進行相對應修正，以避免類案再生，才能有

效強化國軍資訊安全防護能量〔註二六〕。再完善的資安政策與再嚴謹的資安管控，若國軍不能建立資訊安全共識，並提高資安警覺，縱使有再高階的防火牆、防毒軟體及複雜的鎖鑰，都抵不住官兵的一個小失誤與蓄意洩漏。唯有大家依據資訊安全政策指導，安裝各項資安軟體與養成保密設定的習性，並嚴加保守個人的帳號與密碼，且不定時更新，才能由　而外地強化資訊安全的維護，以有效防範敵之資訊網路攻擊，確保國軍資訊網路安全。

註一：〈威脅與威脅技術的未來　情勢將如何演變〉，趨勢科技報告，2009 年 12 月。

註二：〈小兵 facebook 洩軍機　以軍禁軍人上社交網站〉，2010 年 3 月 4 日，http://iservice.libertytimes.com.tw/livenews/news.php?no=337899&type=%E5%9C%8B%E9%9A%9B)。

註三：〈資安觀念薄弱　FOXY 成搜尋　又見國軍訓練　案〉2010 年 3 月 1 日，http://www.libertytimes.com.tw/2010/news/mar/1/today-p4.htm.

註四：Otto Kreisher,〈Risk to One is Risk to All〉, Seapower, Dec./2007.

註五：〈Tracking GhostNet：Investigating a Cyber Espionage Network〉, Information Warfare Monitor, March,2009, P6, http://www.tracking-ghost.net.

註六：〈Shadows in the Cloud：Investigating Cyber Espionage 2.0〉, JOINT REPORT：Information Warfare Monitor, Shadowserver Foundation, April 6,2010, http://shadows-in-the-cloud.net.

註七：鄭大誠，〈中共網軍的發展與評估〉，http://tw.myblog.yahoo.com/jw!orhcsd.lhwiczmpxnmtwd_6tdq..../article?mid=319&prev=3208next=308

註八：馬立德，〈中共網路作戰之研究〉，《海軍學術雙月刊》，第 43 卷，第 6 期，頁 56。

註九：樂義，〈防止網攻　解放軍設資訊保障基地〉，　《 中國時報 》，民國 99 年 7 月 27 日，第 13 版。

註十：〈 中國箝制網路自由　無所不用其極 〉，《自由時報》，　民國 99 年 2 月 19 日。

註十一：〈中央軍委要求加強了新形勢下軍隊資訊安全保障工作〉，華夏經緯網，民國 99 年 4 月 6 日。http://hk.huaxia.com/thjq/jsxw/d1/2010/04/1824158.html

註十二：呂炯昌，《尖端科技》，第 311 期，民國　99　年 7 月，頁 86-90。

註十三：Cyber Security Strategy of the United Kingdom, UK Cabinet Office,Jane/2009, PP.7-12。

註十四：〈網路新冷戰　資訊攻防引發東西對立〉，中華民國空軍全球資訊網，民國　99　年 6 月 3 日。http://air.mnd.gov.tw/publish.aspx?cnid=1732&p=41505=level=1。

註十五：Otto Kreisher,〈Risk to One is Risk to All〉, Seapower, Dec./2007。

註十六：http://www.owasp.org/index.php/Taiwan。

註十七：http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project。

註十八：里·阿米斯德/編，《資訊作戰-以柔克剛的戰爭》，國防部譯印，頁 149。

註十九：資安人雜誌 67 期，民國 99 年 1-2 月號。

註二十：〈破窗理論〉《Broken Windows: The police and neighborhood safety》，http://www.manhattan-institute.org/pdf/_atlantic_monthly-broken_windows.pdf

註二一：左豪官，〈資訊安全事件分析與管理作為〉，《資通安全專論》，財團法人國家實驗研究院科技政策與資訊研究中心，T98015，2009 年 12 月 2 日。

註二二：李順仁，《資訊安全》，文魁圖書，民國 96 年 10 年 31 日。

註二三：行政院國家資通安全會報。http://www.nicst.nat.gov.tw/index.php

註二四：中華民國國家標準 CNS27001，經濟部標準檢驗局，民國 96 年 10 月 24 日。

註二五：國軍資安政策修頒宣導專輯─國防部總政治作戰局政戰服務網，http://gpwd.mnd.gov.tw/onweb.jsp?pageno=2&webno=3333333023。

註二六：劉建良，〈如何做好資安事件通報應變〉，　政部政風室政風宣導，第 9 期，民國 98 年 7 月。