資訊安全

現代網路科技發展與資通安全管理研究探討

教授　吳嘉龍

提要

網路具有即時性及無國界的優點，也因此帶給現今繁忙的社會無比便利，現代科技運用網路進行資訊查詢、網路連線通訊或交易，但是面對惡意程式攻擊網路防護防不勝防，使網路攻擊有機可乘。也隨著資訊科技進步，網路戰爭已演變為一場無聲無形的戰爭。面對中共網軍攻擊，我國除應落實資訊安全管理制度等作為，降低危安因素外；更應根據科技進展，強化對未來資安威脅的防護，完善防衛能量。若在使用時疏於防範，則個人電腦中重要資訊將輕易落入有心人士手中，進而發生一連串的負面效應，其危害程度可危及國防安全，實在不容小覷。我們應保持高度警覺，熟悉相關資安管控規定，精進各項管理作為與方式，工作上確實依照標準作業程序，建構最縝密周延的資安防護，才能有效降低風險與危害，維護國軍資訊安全。

關鍵字：國防安全、網路戰、資訊管理、網路安全、通資電優勢。

壹、前言

國家實驗研究院報導指出2013年網路攻擊有增無減，根據最近B2B International和卡巴斯基實驗室(Kaspersky Internet Security Lab)進行一項調查表示，在過去一年中，91%的被訪企業曾遭受過至少一次網路攻擊，9%遭受過針對性攻擊

，這是專為感染某個組織的網路基礎設施而精心策劃的攻擊。執行長卡巴斯基(Eugene Kaspersky)表示，隨著國家和單位組織在網路犯罪和間諜案日增，採取行動保護敏感資訊下，全球政府可能被迫築牆隔絕他們的網路系統[1]。另外卡巴斯基實驗室在2013年發現了Icfog攻擊，這預示著新型網路攻擊和網路雇傭軍出現，明年行動裝置和儲存在雲端的數據恐面臨更多威脅。網路犯罪節節攀升，加上美國國家安全局承包商前雇員史諾登(Edward Snowden)揭露的機密檔案，凸顯科技公司對間諜活動的疑慮。在史諾登爆料文件指控美國國家安局以間諜監控為目的，取得進入民間電腦網路管道後，蘋果(Apple)、谷哥(Google)和微軟(Microsoft)等公司更進一步呼籲美國政府，帶領政府的監控行為改革[1-2]。

國家實驗研究院在2013年12月31日第201312022期資通安全電子報報導德國「明鏡周刊」揭露美國國家安全局駭客部門作業內情，披露美國偵監人員如何攔截電腦交貨、利用硬體漏洞，甚至劫持軟體巨擘微軟公司的瑕疵回報系統，以監控他們的目標。美聯社報導，明鏡周刊(Der Spiegel)踢爆的內容與美國國家安全局(National Security Agency)轄下特定入侵行動辦公室(Tailored Access Operations，TAO)有關，特定入侵行動辦公室被稱為駭客菁英團隊，專精於竊取最難入侵目標的資料[3]。

惡意程式攻擊威脅無所不在，日本NHK電視台2013年12月26日引用資安公司NetAgent的資安威脅分析報告，報導日本百度所推出的免費日文輸入法軟體Android Simeji、PC Baidu IME，均有盜取使用者輸入資訊的可能性。日本文部科學省與內閣官房資訊安全中心(NISC)在無法確認機密資料是否會通過此類輸入法外洩的情形下，在新聞報導同時已先行發文籲請國內約140個政府機關、大學、法人與研究機構等單位，停用日本百度相關軟體以免重要機密資訊外洩[1-3]。

2013年10月22日，美國國家標準與技術研究所(NIST)頒佈了公司和基礎設施網路的《網路安全框架》草案，該草案意在幫助包括電力、運輸和電信在內的管家技術設施的所有者和經營者減少網路安全風險，NIST計畫在2014年2月發佈正式的《網路安全框架》官方檔。透過資訊系統的建置、資訊安全設備的防禦及落實資訊安全管理制度，可降低危安因素；但因應攻擊手法、技術不斷更新，發展資訊戰能力已是當務之急。我們應當建立對資安威脅的警覺性，資安防護不能只重視目前的威脅，唯有植基科技演進，強化未來資安威脅的防護，才能擁有完善資訊防衛能量[3]。

網路空間已經成為全新的作戰領域，在這個新戰場，美軍積極採取最先行動。與實體空間一樣，美軍採取一系列措施，努力保持其網路戰能力的領先優勢。美軍

網路空間司令部大幅擴編，宣佈成立40支全球作戰網路戰部隊，秘密制定網路戰規則，並由北約率先推出“塔林手冊”，塔林手冊適用於網絡戰的國際法，由於成立於2008年的北約卓越合作網絡防禦中心總部(NATO CCD COE)設在愛沙尼亞首都塔林，這份手冊也因此而得名。發布該手冊旨在證明國際法現行規範意圖作為網路戰國際法典，美軍網路空間國際化步伐明顯加快[4]。

貳、資訊安全管理與惡意程式威脅分析

針對戰爭戰略研究討論，資訊科技的運用也成為另一重要的戰爭型態－資訊戰。而對抗資訊戰之道並非只有攻擊而無分析與防禦，現在網路上有許多隨處可得的攻擊程式與入侵工具，雖然這些惡意程式的撰寫方式十分複雜，但利用這些工具來進行破壞的攻擊者卻不需具備太多的攻擊「知識」，只要懂得如何使用攻擊「工具」，就可以輕易地發動攻擊，導致成為網路攻擊者的門檻越來越低，因此網路入侵、攻擊、詐騙事件便層出不窮。近年來企業組織及重大關鍵設施遭駭客攻擊(含病毒攻擊、駭客植入木馬入侵、蠕蟲等)事件頻傳，若遭受攻擊的是國家重要設施，將可能威脅到國家、人民的安全，因此這些惡意程式及攻擊手法自然引起各國政府的高度關注，以下表一為中共網軍入侵事件分析統計表。

針對資訊安全風險管理規範，行政院研究發展考核委員會於97年4月1日函頒「行政院所屬各機關風險管理作業基準」，風險管理是資訊安全與個資管理的最重

表一　中共網軍入侵事件分析(自行整理)

日期	中共網軍入侵事件內容
2003.8	威盛電子、中華電信、警政署、中選會、國防部等 88 個政府和民間單位電腦遭到湖北與福建網軍入侵，植入木馬程式。
2004.3-2004.6	網軍利用總統大選期間入侵總統府、國安會內部網站竊取資料。民進黨官方網站與軍聞社網站被中國網軍入侵。
2005.3-2005.6	國軍大直衛山指揮所電腦被中國網軍入侵。外交部電腦被中國網軍入侵植入木馬程式竊取資料。美國 CardSystems Solutions 電子付款資料處理公司，因為遭到駭客入侵植入了惡意程式，導致 4000 萬筆帳戶資料外洩。
2006.5	美國退伍軍人事務部筆電、儲存設備遭竊，而造成 2600 萬退伍軍人資料的外洩。
2007.1	美國折扣零售集團 TJX 資料庫遭駭客入侵，4570 萬筆課務資料遭竊。
2007.8	華文世界最大的 BBS 批踢踢實業坊(PTT)發生有史以來最大的安全漏洞，長達 20 分鐘時間，新登入使用者都享有站長權限，可以瀏覽版友們的真實個人資料，近百萬名網友的個人隱私外洩。
2008.1	駭客以 Storm 殭屍網路作為跳板的釣魚攻擊，對英國等數家銀行發動攻擊。
2009.3	攻破美國五角大廈防火牆，竊取 F-35 戰機資料。
2011.8	美防毒軟體 McAfee 指中國駭客過去 5 年入侵 14 國，72 個政府、組織或企業。
2012.9	《紐約時報》記者電子信箱遭攻擊，入侵美國白宮，駭客侵入到控制核武密碼網域。
2013.1-2013.3	1-3 月入侵美國《華爾街日報》、CNN 網站並且攻擊臉書，竊取推特的個資。

要的核心工作之一。風險是潛在影響組織目標事件發生的可能性及影響度，風險管理的重點在預防，降低發生可能性與影響度。透過系統化機制與評鑑方法，並與組織日常管理、業務流程結合，鑑別組織的資訊資產，評估其可能面臨的威脅、弱點、風險等，並據以研擬適切風險管理計畫，透過風險避免、移轉、降低或接受等方式，對各項風險加以監控。資訊風險評鑑依照以下步驟執行：鑑別資訊資產、分析營運衝擊、鑑別威脅與弱點、鑑別現有控制、鑑別風險發生可能性與影響程度。關於風險管理的國際規範，目前主要有ISO27001、ISO20000、BS25999、BS10012等國際標準，ISO27001是國內推動資訊安全管理系統最普遍使用的國際標準，然而，面臨已經上路的個資法，ISO27001對企業而言還是不夠的！ISO27001對風險評鑑僅有提供原則性的要求內容(what)，卻沒有提供實務性的指南內容(How to do)，而國際標準ISO27005則為組織資訊安全、個人資料的風險管理提供實務上的執行指南(Guideline)。目前，國防部、空軍司令部暨所屬61個單位，已部份範圍導入、建置ISO27005：2008版要求，並以「一級輔導一級」的方式陸續擴大單位範圍，分階段完成全組織導入與建立ISO27005風險管理的工作。

風險分析(Risk Analysis)是以預測模式推估未來風險事件發生可能機率，並依據分析結果建議可行管理措施以降低危害。整合性風險管理係以組織整體觀點，系統性持續進行風險評估、風險處理、風險監控及風險溝通之過程。資策會ISO27005資訊安全與個人資料風險管理認證訓練透過講解與實作研討闡述系統化風險管理的內涵，結合資訊安全管理(ISMS)、資訊技術服務管理(ITSM)、營運持續管理(BCMS)、個人資料管理(PIMS)及個人資料保護法與對風險評鑑要求，教導風險評鑑步驟，練習風險評鑑詳細執行細節，以培養風險評鑑小組人員建置與維運能力。資訊風險管理依照以下步驟執行：評估風險管理建議、決定風險管理方案、彙整風險管理計畫、執行風險管理計畫工作事項與追蹤風險管理計畫工作事項進度，97年12月8日行政院為進一步強化機關危機處理能量，將前開基準納入危機處理專章，並配合將名稱修正為行政院所屬各機關風險管理及危機處理作業基準，機關各層級作業基準運作時須注意設定政策目標、規劃及建置架構、執行與操作、監督審查與矯正預防及改善等作業[5]。

事實上，面對一個新形態的戰爭，我們不僅在觀念上必須擺脫傳統思維的束縛，從全球性、區域性及國家性三個層面去加以思考，才能有效掌握「網際網路相互通聯與相互依存」的特性，進而採取可行的因應對策；而且在實務上必須針對敵人可能採取的攻擊行動，如竊取資訊、資料或程式碼，或在網路上進行「阻斷服務」行為或以散布病毒方式，造成資訊喪失、作業中斷、文件受損、伺服器遭清除等情

況，予以立即性、可控性及預防性之反制作為[2-5]。資訊戰可定義為：藉由對資訊或資訊資源進行保護、利用、破壞、阻絕、摧毀的行為所組成，以比對方達到更重大的優勢、目的或取得勝利。資訊戰攻擊能力與行動預判包括：(一)具電腦病毒破壞能力，可透過多種植毒管道，直接攻擊、破壞我政、經、軍等資訊系統。(二)具電磁脈衝炸彈，大規模干擾、癱瘓我C4ISR指管通情系統，及影響我武器系統的功能性。(三)具資訊偵收能力，特別是藉助駭客的力量，竊取我機密資料。這種隨著科技的進步而轉變到全球化、全民化的作戰方式，形成一種新的戰爭形態：在軍事上的特徵就是以有限手段打無限戰爭，因為是超越一切界線和限度的戰爭，故又可稱為超限戰。值得注意的是，同時發動資訊戰的主體應為國家或是區域聯盟，方能超脫於國家法令進行攻擊行為[6]。

網際空間具備獨特的作戰特性、戰術、技術與程序，隨著網路攻擊複雜程度和惡意程式攻擊力道的不斷加深突顯網路安全問題越來越重要。中國駭客於2011年攻擊了網絡安全公司RSA Security，中國並將盜竊來的技術攻擊入侵軍事攻擊目標。之後美國國防承包商洛克希德・馬丁(Lockheed Martin)網絡並遭到中國駭客入侵。針對惡意程式攻擊，過去最關注的資訊安全威脅往往是全球病毒爆發事件，從2011年起，惡意程式攻擊焦點已轉向高級持續性滲透攻擊(APT：Advanced Persistent Threat)，APT攻擊作為一種複雜且多方位的攻擊，對於企業的安全保障構成了極大的風險。儘管全球化企業在安全控管上都投入了龐大的資源，但是APT攻擊仍然滲透進這些企業，並使韓國金融企業、Adobe等遭遇了重大損失。這些事件警示了APT攻擊的複雜性與巨大破壞性[3-5]。

據媒體2003年9月5日報導，發現中國駭客企圖大規模癱瘓我國電腦系統，經查臺灣有88個企業及政府單位遭駭客入侵植入「木馬程式」，追查結果發現駭客入侵的方式共分四層，第一層(被入侵的機關機構)計88家；第二層(被利用當跳板)計8家；第三層(潛伏駭客或隱藏當跳板)計2家；第四層(隱藏駭客)計2家。刑事局偵九隊偵察8家民間企業，完全使用國際標準監控，發現最後都定點回報到中國湖北及福建兩地，其中臺灣被監控的定點，也發現有其他國家會定時向這些定點回報，電腦網路防禦、反駭(hack back)與有效反制阻絕敵人運用網路更顯得更加重要[3-5]。

參、中國與美軍資訊網路作戰發展分析

美國總統歐巴馬在美國的國情咨文裏提別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在中國大陸上海浦東的

圖一　NATO和俄羅斯聯合電子戰演練圖[8]

大同路208號十二層樓高的駭客部隊61398部隊。中共組建「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「863專案」的培植人才。不是只有軍方人員，民間企業及學術機關也都在解放軍總參謀部二部的資助下，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，負責偵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、美國航空太空總署NASA、美國太平洋司令部、紐約時報與華盛頓郵報。美國官方與時報調查報告指出，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，除了竊取資訊外，並企圖掌握美國基礎設施，像電力網、變電所、淨水廠、汽油及天然氣設施等[5-6]。

Jgospel 2010年9月17日報導北大西洋公約組織和俄羅斯最近宣布將進行聯合信息戰演練，以便於雙方能更好地保護國家的關鍵數字基礎設施，努力提高數字安全性，圖一為NATO和俄羅斯進行聯合電子戰演練圖。一份長達32頁的報告闡述了即將進行的網上襲擊模擬框架，雙方將進行相互觀察和科學合作，為發展脆弱性評估和重要設施排名的標準一同努力。雙方建議擴展現有網絡犯罪應急反應系統和全年無休的全球網絡保護框架，評估針對“網絡戰”交戰國家的關鍵基礎設施，並聯合ITU開發一個可信任基於公鑰的基礎結構框架[8]。

資訊作戰不受時、空限制，也沒有平、戰時與軍、民之別，基於綜合性的國家安全考量，如何有效因應與防制，已成各國至為重視的課題。根據CSI/FBI (Computer Security Institute/Federal Bureau of Investigation)2006年的電腦犯罪與安全性調查報告指出，回覆的313家公司遭受病毒攻擊的損失高達1,500萬美元，未經授權的存取損失約1,000萬美元，綜合各種損失將近5,200萬美元。美國曼迪安網路安全公司稱中國現有超過20個積極活動的駭客團體，但其中代號為「APT1」的組織竊取機密的數量最多。Mandiant分析其6年來141個受害者，種種跡象顯示61398部隊就是「APT1」。針對61398部隊6年來141件入侵案中，美國佔115起，台灣有2

起，而且台灣曾被當駭客跳板，有6部該部隊的伺服器被查出擁有台灣IP位址。中國駭客部隊擁有數千名中國最頂尖駭客成員，麥迪安公司從2006年開始追縱美國政府與企業所遭到的網絡攻擊事件，發現其中有141家企業長期遭到來自中國大陸的駭客攻擊[3-6]。

圖二　美軍網絡司令部司令積思・亞歷山大[9]

美國奧巴馬總統2009年宣布，網路安全關乎國家和經濟安全。美國《華盛頓郵報》報導，網絡攻擊種類繁多，可能破壞美國電力系統、阻礙金融交易或致癱互聯網服務器，可謂防不勝防。Jgospel 2010年11月8日據新華社電美國媒體6日報導，美國網絡司令部(Cyber Command)統管美軍網絡安全和網絡作戰指揮。美國網絡司令部司令積思・亞歷山大提議，美國當局授權網絡司令部可在全球範圍展開網絡攻擊，以便有效維護美國網絡安全，亞歷山大所領導的網絡司令部設在馬里蘭州，與國土安全部、國家安全局等部門密切合作。。按照亞歷山大的構想，網絡司令部具備“進攻能力”，採取“先發製人”打擊策略。美國網絡司令部隸屬美軍戰略司令部，2009年6月根據國防部長羅伯特・蓋茨的命令組建，今年5月正式啟動，由國家安全局局長積思・亞歷山大兼任網絡司令部司令，圖二為美軍網絡司令部司令積思・亞歷山大公開演講圖[9]。

根據J Gospel Net, Inc.報導，Jgospel 2010年9月28日據聯合早報網報導，美國國土安全部宣布，將與12個國家合作，舉行龐大的電腦網絡攻擊演習，以提高網上保安。據報導，該項網上攻擊演習名為“數碼風暴三”，將模擬重要基建設施受到大規模網上攻擊，各部門如何協作，減低影響。演習涉及多個部門、11個州政府、60間私人公司及12個國際夥伴，包括澳大利亞、英國、加拿大、法國、德國、匈牙利、日本、意大利、荷蘭、新西蘭、瑞典及瑞士，圖三為美國聯合網絡司令部統管美軍網絡安全和網絡作戰指揮示意圖[10]。

Jgospel 2010年11月8日報導首次在全歐範圍內進行的模擬網路戰結果將於11月10日發布，歐盟的22個成員國以及冰島、挪威、瑞士等非歐盟成員國的代表們參加了這一名為“歐洲2010網路”的演練，其他成員國則派觀察員參加。這是歐盟落實今年5月制定的《歐洲數字化議程》而採取的重要措施，主要目的是提高各國

應對網絡駭客攻擊的能力。全歐進行的模擬網路戰演練持續了7個小時，承辦方為歐洲網絡與資訊安全署和歐盟聯合研究中心。130名網路專家分成3組進行演練。此演練目的在於，在各國的互聯網聯系逐步受到嚴重限制，公民、企業和公共部門享受的重要網上服務受阻的情況下，如何避免網絡徹底癱瘓，網絡黑客日益頻繁地使用新技術，例如使用殭屍病毒(或Bot機器人程式病毒)進行攻擊。這技術是利用阻斷服務攻擊或分散式阻斷服務攻擊(DDoS：distributed denial-of-service attack)，此惡意程式攻擊將數萬萬個被感染的電腦組織成一個個控制節點，用來發送偽造包或者是垃圾數據包，從而使數萬台電腦癱瘓並無法提供正常服務。報告指出，德國國防部和國防軍2009年受“殭屍網絡(Bot)”感染，網頁無法打開和更新，進一步演練並將組織有IT行業及私營部門參加的演練，併計劃將演練從歐洲擴展到全球範圍，圖四為進行的模擬網路戰示意圖[11]。

圖三　美軍網絡安全和網絡作戰指揮示意圖[10]

圖四　全歐範圍內進行的模擬網路戰示意圖[11]

肆、國防資訊安全與通資電優勢

資訊攻擊屬主動性資訊作戰，係運用諸如電磁脈衝、電腦病毒、精確導引等高科技資訊武器，針對敵之指揮管制系統、交通樞紐、電力設施、軍事基地、經濟中心、重要工業等基礎建設，遂行指管攻擊、電子戰攻擊、網路攻擊、情報戰、心理戰、經濟資訊戰等資訊攻擊行動。資訊防護定義為防禦性的資訊戰對敵之破壞活動

表二　國防部資訊安全建軍重點方向

項　目	資訊安全建軍重點方向內容
有效整合通信網路	傳輸平台之建設為爭取「資訊優勢」之關鍵要素；本部指管通情及資訊傳輸系統之整合，係以建立三軍通用戰術聯戰網路為目標，結合國軍有、無線電通訊系統及民間通訊資源，形成軍民共用多重節點、複式網路的通聯手段，以充分有效運用整體國家資源，提升通資戰力，有效支援作戰。
強化電戰作業能量	依照國軍未來電子戰作戰構想及任務特性，積極強化電子戰對抗能力，策頒「國軍電子戰作戰構想及專業單位(部隊)規劃」，指導三軍電戰部隊定期演訓外，並責成中科院研製先進電戰裝備，加速推動國軍電子戰戰力整備，建立局部優勢跨陸、海、空域的整體電戰防護網，以發揮部隊整體戰力。
建立優勢資訊戰力	資訊戰的重點在網路安全防護，且以全方位思考與創意運用為原則；在發展安全防護機制與系統裝備之外，朝向構建自動化、系統化及資訊化之安全防護系統目標邁進。由被動性的防護進而建立主動性的監偵能量及反製作為，結合產、官、學、研界能量，構建國防自主能量，俾確保資訊戰場的優勢。
落實頻譜管理	加速「國軍頻譜資料庫自動化管理系統」之建置，以有效管理軍用頻率，確保通信紀律及通資安全，提升國軍無線電頻率使用效率
籌建聯戰指管鏈路	考量聯合作戰需求與指導整合三軍通資現有能量，充分運用民間科技，整體規劃並建置國軍指、管、通、情、資訊系統及三軍共通自動化數據傳輸鏈路，俾以整合、提升新一代兵力、武器系統之有效戰力。

，則具有防護或反制的手段。包括心理建設、指管防護、電子防護、安全措施、資訊網路安全以及資訊防護等。資訊防護屬被動性的資訊作戰，面對敵之資訊攻擊行動，應具備指管防護、電子防護、資訊網路安全防護、情報蒐集、心理建設、經濟資訊防護等資訊防護措施，以確保資訊優勢。前美軍參謀長聯席會議主席托馬斯·穆勒(Tomas Muller)預言：如果發生第三次世界大戰，獲勝者必將是最善於控制和運用電磁波譜的一方。美國海軍上將威廉·歐文斯(William A. Owens)指出，美軍「整合式系統」由太空、陸地和海空基地的感測系統聯合構成指揮、管制、通信、電腦、情報、監視、偵察的C4ISR系統[12-26]。

因應國防資訊安全重要性，國防部長嚴明在2013年11月舉辦的「102年通資電工作檢討會」中，期勉國軍運用通資電科技，逐步進行不對稱戰力的建構，期能滿足聯戰實需，有效掌握資電優勢，支援防衛作戰任務遂行。國防部依據「十年建軍構想」及「五年兵力整建計畫」，落實各項整備工作，以聯合作戰為目標，採「一種裝備、三軍共用、多種效能」理念，按規劃期程構建滿足聯戰需求通資電平臺與防護系統；另應運用專案管理模式定期實施進度管控，持續檢討與精進。國軍現有重要通資電系統需要爭取與積極評估軍種關鍵知識轉移需求項目，以建立系統自主維運能量，建立自我修護能量，朝國防自主目標努力邁進。國防部長在「102年通資電工作檢討會」強調維護資訊作業環境安全是共同責任，要求各級持恆落實執行

「國軍資訊安全政策」及「一級督導一級」工作，以打造安全的資訊作業環境。針對未來戰爭型態、電磁戰場環境、敵情威脅及軍種作戰需求，本部正全力推動國軍電子戰戰備整備工作。面對中共網軍具資訊戰能量之威脅，我們應該建立國家層級資訊戰指揮體制外，因應作為包含如下：(一)、具緊急應變與災後快速回復之能力，確保整體戰力。(二)、具備電磁脈衝的防護能力，防敵癱瘓。(三)、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。(四)、研發不易破解之加密技術，確保資料安全。(五)、結合資訊戰與軍中C4ISR指管通情系統，建置資訊戰反制能量。(六)提升使用中和建置中的各項資訊系統安全防護網，並建置安全的通資作業環境，國防部目前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，滿足軍種及三軍聯合作戰需求，有效提升國軍整體戰力，正全面性積極推展各項具體作為，並應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弱點分析，國防部資訊安全建軍重點方向執行重點整理如表二[27]。

伍、結論與因應作為

近年來隨著資訊科技的快速發展，讓人們的溝通管道、工作型態等均產生了許多的變化。人們現今透過網路取得新知、進行交易、認識朋友，甚至可跨國組合虛擬團隊。而人們的生活仰賴資訊科技的服務日益加深，相關資訊建設也成為先進國家不可或缺的關鍵基礎建設。從另一方面來看，資訊科技的重要性提高，在不法攻擊者眼中的重要性也隨之提高。由於網路戰並左右戰局勝負，加上中共自成立網軍已來，整體網路作戰能量大為提昇，包括美國、英國、法國、日本等主要國家，無不費盡心思採取因應之道。軍事學家亞當斯(James Adams)在《下一場世界戰爭》中說到：在未來的戰爭中，電腦本身就是一種武器，前線無所不在，奪取作戰空間控制權，不是砲彈或子彈，而是電腦網路系統中流動的位元組；美國蘭德公司亦曾指出，未來的網路戰是多元中心但理念單一的戰爭，其優勢在於運用高科技以提昇戰力。資安重點政策涵括「網路安全管理」、「國軍人員資安教育與督考評鑑」、「資安應變暨通報機制」、「資訊系統發展與管理安全」及「資訊資產管理」等五大要項，強調各單位除須貫徹軍網、民(學)網、作戰指管網、情報網等網路實體隔離，以及網路管理上恪遵專網專用、民網集中公開、網路線材分色標示等原則辦理；同時國軍網路應依機敏等級妥採分級措施，建立相對之安全防護能力；各單位防火牆強度應依據資安等級劃分檢討籌建。嚴密管控通資安全為當今國防的重點，為配合政府資通安全政策及因應近年國軍資訊網路蓬勃發展，國防部已積極規劃建置

國軍資訊戰防護及通資訊緊急應變、制變作業能量，更積極發展軍種積極資訊防護及主動網路監偵能力，以確保三軍部隊通資安全，以維持我國完整指通力、機動力以及打擊力，並且鞏固國防安全[20-24]。

鞏固國家安全建立完善的情監偵體系能在對的時間，將正確的情資提供給合適的決策者，其優於敵人的情報價值與品質，並可為戰場指揮官及作戰部隊創造出決策優勢，以制敵機先。網際空間是目前最新的作戰領域，一如情報、監偵與偵察在傳統作戰的重要性；所以，在此新領域的情監偵作為上，必須突破網際空間的複雜性與不確定性，方能取得有效情資，全面支持各種軍事作戰行動。中共企圖藉中國特色軍事變革，致力取得不對稱的資訊戰優勢，在2004年『中國的國防白皮書』中，人民解放軍立足打贏信息化條件下的局部戰爭，足以見得解放軍各類信息化條件下的攻擊型態均可能出現，包括「戰略信息戰」或「戰略資訊戰」。面對未來戰爭，作戰行動具備強烈的系統性與整合性，透過網路資訊的快速傳遞、資訊系統的資訊處理能力及現代武器裝備的快速反應能力，使各項武器的精準效能得以發揮，通信及自動化的指揮系統能在戰場上運用自如；但愈倚賴以資訊科技為核心的高科技武器及系統運作，愈易形成關鍵致命弱點，形成敵人遂行資訊攻擊目標。因應各種可能的網路攻擊，國防部統籌規劃國軍網路資安防護措施，持續發展綜合性資訊戰力，確保國軍資電優勢；並參酌各國電子戰發展趨勢，結合國軍電子戰發展作為，逐步提昇與整合未來電子戰指管平台，以建立全面聯合電子戰防護戰力[25-30]。

柒、參考文獻

〔1〕中央廣播電臺國際新聞，卡巴斯基：全球網路陷分裂危險，2013年12月15日，http://news.rti.org.tw/。
〔2〕資安人編輯部，Information Security資安人科技網，資料庫熱門新聞，RSA 2010（三）：政府該有的網路防災觀念，2010年3月8日，http://www.isecutech.com.tw。
〔3〕財團法人國家實驗研究院科技政策研究與資訊中心，資通安全資訊網電子報，2013年12月30日，第201312021期資通安全電子報。
〔4〕財團法人國家實驗研究院科技政策研究與資訊中心，資通安全資訊網電子報，2013年12月31日，第201312022期資通安全電子報。
〔5〕行政院研究發展考核委員會，風險管理作業手冊Ver 3.0，http://www.rdec.gov.tw/DO/DownloadControllerNDO.asp，存取時間：2013年12月31日。
〔6〕柯宏叡、王旭正、黃嘉宏、詹前　，資訊戰攻擊與入侵證據鑑　資通安全分析專論，T3：最新技術研究發展，2007年12月。
〔7〕Gospelcity.net，中美網絡戰已在開打-中國的61398部隊，http://jgospel.net/news/tech/，存取時間：2013年12月31日。
〔8〕Gospelcity.net，北大西洋公約組織和俄羅斯進行聯合信息戰演練，http://jgospel.net/news/tech/，2010年9月17日。
〔9〕美國之音(VOA)，美軍稱網絡司令部各編隊全面運作，2013年9月27日。
〔10〕徐芝泉，共軍駭客無所不在美「中」網路戰白熱化，青年日報，2013年2月28日。
〔11〕Gospelcity.net，美宣布將聯合12國舉行大型電腦網路攻擊演習，http://jgospel.net/news/tech/，2010年9月

28日。
〔12〕梁華傑，青年日報專論：共軍駭客入侵劇增美掌控「制網路權」應戰，http://news.gpwb.gov.tw/news.aspx，2013年3月27日。
〔13〕陳志誠，資訊戰及其對國家社會安全之影響，資通安全分析專論，2005年12月。
〔14〕奇摩知識，第一次波灣的美軍所使用的高科技武器，美軍對武器系統發展的指導，http://tw.knowledge.yahoo.com/question，存取時間：2014年1月2日。
〔15〕張維君，資安人科技網，國安局：攻擊38%來自本地嵌入式系統成新目標，Information Security，http://www.informationsecurity.com.tw/article/article，2013年4月29日。
〔16〕新浪網，即時新聞-美國國防部長譴責大陸網路攻擊，http://news.sina.com，澳洲日報，2013年06月01日。
〔17〕吳冠輝，青年日報專論：嚴密資安管控-確保演訓安全，2010年4月25日。
〔18〕中國評論通訊社，美組建空軍網路戰司令部-多管齊下發動網路戰，2007年4月2日，http://www.chinare-viewnews.com。
〔19〕中華民國資訊軟體協會， 政院「完備我國資訊安全管 法規之分析」委託研究計畫期中報告(初稿)，2012年8月17日。
〔20〕Robert A. Miller and Daniel T. Kuehl.著，李育慈譯，二十一世紀之網域與「第一戰」(Cyberspace and the “First Battle” in 21st - century War)，國防譯粹，37卷，5期，21-31頁，2010年5月。
〔21〕青年日報專論，社論：落實資安防護措施-達成演習零缺失目標，2010年4月24日。
〔22〕Timothy M, Bonds et. al.著，黃文啓譯，美陸軍網路致能作戰(Army Network-enabled Operation)，國防譯粹，39卷，8期，39-43頁，2012年8月。
〔23〕梁華傑，青年日報專論：中共佈建網軍-全球資安隱憂，2010年4月24日。
〔24〕國防部通資次長室，建立資訊保密安全共識防堵資安漏洞，青年日報專論，2013年5月29日。
〔25〕柳育欣，正視中共網軍竊密-強化資安防護，青年日報專論，2013年5月17日。
〔26〕C4ISR Go South著，陳克仁譯，擴大籌建指管通資情監偵戰力(C4ISR Go South)，國防譯粹，40卷，5期，35-46頁，2013年5月。
〔27〕國防部，資訊戰綜合作法與成效，通信電子資訊局記者會資料，2005年6月。
〔28〕國防部，中華民國102年國防報告書，第三章聯合戰力與整備，第三篇國防戰力，存取時間：2014年1月2日。
〔29〕林明武，國軍應用「通資電」科技於不對稱戰力之研究，國防雜誌Defense Journal，第4期，第26卷，第87-102頁，2013年10月。
〔30〕梁正綱，臺海衝突中的戰略資訊戰，國防雜誌Defense Journal，第1期，第23卷，第51-60頁，2013年5月。

作者簡介

教授 吳嘉龍

學歷：中正理工學院48期電機系電子工程組77年班，美國俄亥俄州空軍理工學院電腦工程研究所84年班，國防大學理工學院國防科學研究所電子工程組93年班。經歷：電子官、區隊長，教官、講師、助理教授、校教評秘書、科主任、副教授、教授、系主任、資訊安全學會永久會員、危機管理學會理事、危機管理學會資訊安全主任委員。現職：航空技術學院一般學科部航空通訊電子系上校專任教授兼任系主任。專長領域：資訊戰，通資安全，無線通訊，網路通訊協定。