資安管理

網路戰爭發展與資通安全管理研究探討

空軍上校　吳嘉龍

提要

美國軍事學家亞當斯(James Adams)說：在未來的戰爭中，電腦本身就是一種武器；前線無處不在，至於奪取作戰空間控制權的並非砲彈或子彈，而是在電腦網路系統中流動的位元組。由於資訊科技、網路技術發展的一日千里，21世紀已是資訊爭奪的世紀，「網路戰爭」成為一種新戰爭形態，更成為當代戰爭中相當重要的一環，「制網路權」可與「制空權」相提並論。美軍透過資訊科技基礎建設精簡整合，提昇資訊科技以及網路使用效能與安全性，並能有效防範網路惡意程式攻擊。資訊戰時代來臨，必須憑藉全民資訊安全共同因應，面對號稱「大國崛起」的中共處處與美國爭雄、競逐世界影響力，在「網路空間」的攻防更是時有所聞。本論文針對國防資訊科技發展趨勢與資訊安全理論技術加以深入探討，現代國防科技建軍應重視現代化作戰理論與資訊安全技術，結合未來作戰需求與整合軍民科技能量，分階段逐步發展穩固安全資訊基礎建設與自動化聯合作戰指管系統，以鞏固確保資訊優勢與國防安全。

關鍵字：網路化戰爭、惡意程式攻擊、資訊科技、網路安全管理、通資電優勢。

壹、前言

21世紀是電腦網路科技的世紀，資訊藉由網路傳輸既快速且無遠弗屆的流通與交換，科技進步孕育出全球化社會。進入資訊化社會，國與國之間的資訊戰也越演越烈，隨著網路的普及化，資訊安全的重要性更加凸顯，提昇政府單位資安防禦能力，便成當務之急的工作。資訊安全維護旨在確保資訊的機密性、完整性與可用性，我們應當落實最佳安全實務準則及縱深防禦策略，以因應資訊網路安全的威脅。有鑑於此，無論是防護機制建立、法令規範修訂、教育訓練與人才培養，均須落實執行。近期目標式攻擊越來越盛行，駭客不直接攻擊目標而採用迂迴的「水坑式」攻擊，從攻擊目標對象常去的網站著手，所有合法網站都有可能因為漏洞成為攻擊跳板，網站被駭原因很多，SQL injection, XSS網頁安全問題就可以讓駭客一再得逞。而DDoS攻擊威脅存在已久，近年來的變化速度卻愈來愈快，駭客利用網路協定所存在的漏洞，將各種網路設備變成殭屍電腦的一份子，例如：印表機、路由器、網路攝影機，再利用它們發動大規模DDoS攻擊，或是竊取裡面的資料。日前南韓攻擊事件以及美聯社Twitter帳號被盜等資安事件對當地造成股市大跌、影響金融社會秩序等重大衝擊。隨著APT攻擊的盛行，對於未知惡意程式(Malware)威脅偵測能力也受到重視。有鑑於此，RSA資安廠商的SIEM將由原本enVision平台轉換為收購來的NetWitness平台，名為Security Analytics，除了將log收錄外，其中全封包深度分析與鑑識功能則為最大特色[1]。

國防部、國安局與行政院資訊安全辦公室在立法院在2013年4月29日提出因應報告並接受質詢，國安局指出惡意程式攻擊38%來自本地而且嵌入式系統成新目標，立法委員並提出5臨時提案，要求國防部、國安局與行政院能積極培育並網羅資安人才、公布演練成效、強化關鍵基礎建設保護等[1]。就金融安全舉例說明，360互聯網安全中心發佈重大安全警報稱，“超級網銀”跨行帳戶管理功能已經成為駭客惡意利用的目標，近期全國連續出現多起各大銀行客戶被騙案例。掌握資訊已是軍事作戰重要的一環，而且，資訊本身已成為一種武器、一個作戰目標，根據美國國防部將資訊戰定義為「危機或衝突期間用以影響敵資訊，並保護己方資訊系統，以促進或達成特定目標之行動」，簡單來說，資訊戰的重點在於破壞或影響，敵獲得資訊的決策過程。事實上，資訊戰並非普遍認為的只是電腦網路攻防作戰而已，其核心的利器應包含：(一)心理戰：如大量傳送電子郵件、簡訊及撥打手機等，以影響動搖他人作戰意志。(二)軍事欺敵：如部署雷達、空射誘餌，誤導敵人攻擊錯誤目標。(三)作業安全：係藉由確保我方資訊作業全程安全，降低敵方攻擊的

弱點，如加密、實體隔離等。(四)電腦網路作戰：誠如大家熟知電腦網路攻擊(如分散式阻斷攻擊、邏輯炸彈、病毒、特洛依木馬)、防禦及網路安全加解密等，甚或是新發展的網路武器。(五)電子戰：如干擾全球定位系統(GPS)接收、雷達系統、敵我識別系統、導引飛彈及無人飛行載具(UAV)等，均係藉由完整掌握電磁頻譜，干擾或制壓敵人通信與遙測系統武力[2]。

貳、資訊科技發展與網路安全威脅

Google於2009年12月發現中共駭客侵入其Gmail系統，便展開反制與蒐證，其工程人員發現位於臺灣的一部電腦被利用來發動網路攻擊，經調查，不僅在這部電腦發現攻擊Google的證據，另至少還有33家企業遭駭證據，包括Adobe系統、諾斯洛普格魯曼等。Google認為事態嚴重，通報美國情報和治安機構，並共同蒐集證據，證明攻擊者不在臺灣而是在中國大陸；所發現的許多細膩攻擊證據，強烈指向是中共所發動(或是獲得中共官方認可)。此波Google等企業所遭受的網攻，規模是歷年來數一數二的[3]。2013年2月10日，美國《華盛頓郵報》刊載美國國家情報委員會《國家情報評估》結論：美國是大規模、持續性網路間諜活動的目標，威脅著美國經濟競爭力，中共是意圖滲透美國企業機構電腦系統的最積極國家。美眾議院情報委員會主席羅傑斯當日亦提出警告：美國遭到的網路攻擊，恐有導致金融服務關閉、企業每日運作所需資訊遭摧毀之虞；百分之九十五民間部門網路十分脆弱且絕大部分已遭攻擊，並特別點名中共和伊朗，不僅竊取軍事機密，也竊取企業用以成立生產線，製造商品的創意。《國家情報評估》除點名中共外，更提及涉嫌竊取經濟情報的俄國、以色列、法國等三個國家，但其規模與中共相比，是小巫見大巫。《國家情報評估》是代表美國情報機構的共同見解，指出過去五年在能源、金融、資訊科技、航太、汽車產業等已是駭客入侵目標；網路間諜曾是美國情報與軍方的主要關切點，現在則被視為是國家經濟利益的直接威脅，造成美國百分之零點一至零點五GDP的損失(約二百五十億至一千億美元)[3]。

根據2013年5月賽迪網-IT技術訊報導，國內DNS服務提供者114DNS官網微博消息：新發展DNS釣魚攻擊已經突破國內安全防線，可能已經導致數百萬用戶感染。目前遭受攻擊的主要對象已從政府機關、駐外館處，擴大到民間智庫、電信業者與委外廠商，而主要攻擊標的也轉向包括車輛交通號誌儀控設備、寬頻路由器、工業微電腦控制器、網路儲存系統等嵌入式系統上。隨後，安全軟體及服務商騰訊電腦管家通過官方微博對此消息予以了證實，並向廣大用戶發出了安全風險警告。而相同的DNS攻擊，曾在2009年製造了轟動全球的“銀行劫持案”，導致巴西最大銀行

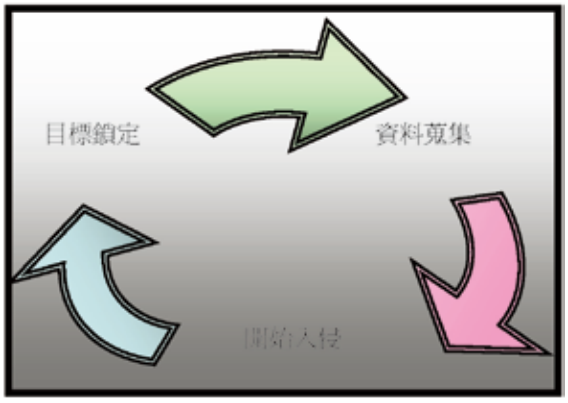
Bandesco銀行近1%客戶遭到釣魚攻擊。在2012年，世界各國許多電腦系統、包括美國政府的系統都不斷遭到入侵，其中某些入侵似乎是由中國大陸政府和軍方直接發動。根據國安局調查，目前的攻擊僅4.9%是直接來自於對岸，38%是以台灣本地的殭屍電腦或其他周邊國家電腦做為攻擊跳板，許多工業電腦由於沒有防火牆保護因而成為駭客攻擊中繼站。國家實驗研究院科技政策研究與資訊中心於資通安全會報分析指出，環球時報綜合報導“包括愛國者導彈系統、F-35戰機等重大武器專案都受到中國駭客的攻擊”，美國國會從2000年起要求國防部針對大陸軍事發展發表年度報告；路透華盛頓2013年5月7日報導指出美國國防部今天首度在年度報告直指北京當局試圖入侵美國國防電腦網絡，利用間諜活動獲取加速軍事現代化計畫的技術[4-5]。面對資訊安全威脅的快速發展，美國國防部長海格6月1日在第12屆亞洲安全會議(香格里拉會談)上，以「美國對區域安全的策略」為題進行演講，直接公開點名中國大陸政府、軍方的網路駭客，不斷重覆地侵入美國敏感的資訊情報系統。美國對網路干擾威脅增加已表達高度關切，其中又顯示與中國政府及軍方有關係。美國國防部在提交國會的83頁大陸軍事發展報告也指出，北京當局在研發先進匿蹤戰機和打造航空母艦方面取得進展。中共航空母艦有助大陸在外海進一步投射軍力。報告也說，中國利用網路入侵能力，來支援對美情報偵蒐，矛頭指向美國外交、經濟和支持國防計畫的國防工業基礎部門。大陸的網路窺探活動已成為「重大隱憂」，且由於大陸網路窺探活動包括入侵技術與執行網路攻擊所需技巧相當類似，因此形成更嚴重資安威脅[2-6]。

圖一　美國國防部長海格在香格里拉對話會指責大陸網路駭客入侵美國資訊情報系統[6]

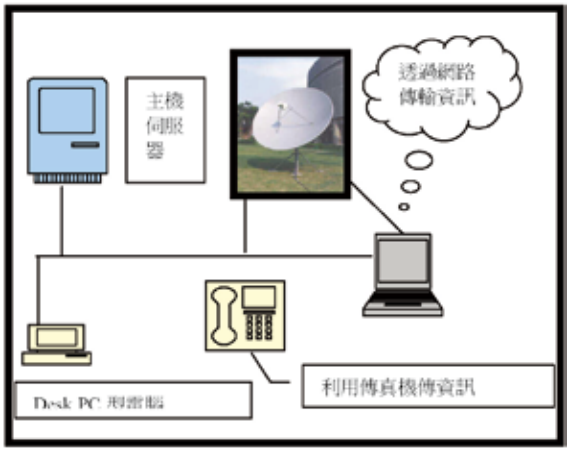
參、美軍資訊網路作戰發展分析

隨著網路安全形勢的日益嚴峻以及網路攻擊複雜程度和惡意程度的不斷加深，安全的責任問題就變得越來越重要。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，焦點已轉向APT(Advanced Persistent Threat)，高級持續性

滲透攻擊，圖二為駭客入侵的程序示意圖，圖三為網路監聽示意圖，指未經使用者允許而利用網路探聽資訊，圖四為網路攔截示意圖，攔截指利用網路竊取別人的資訊。美軍有鑑於資訊科技發展健全與否嚴重攸關國防戰力提昇，因應戰略考量遂對電子戰武器不斷提昇與更新，而美軍對武器系統發展的指導是：高精度、高摧毀力與高受攻擊承受力(經得起敵之攻擊)等來發展三軍武器裝備，以長制短求得本身安全與接敵先制。而自波灣戰爭後，C⁴ISR(指管通資情監偵)系統更被重視且已被公認為有效之「戰力倍增器」。C⁴ISR系統目的在預先獲悉敵人犯我之動態，對敵情隨時進行威脅分析、研判，適時提出確切應變處置方案以能即時傳遞指揮命令，持續掌控任務執行狀況，遂行克敵致勝作戰[6]。



圖二　駭客入侵的程序示意圖(自行整理)

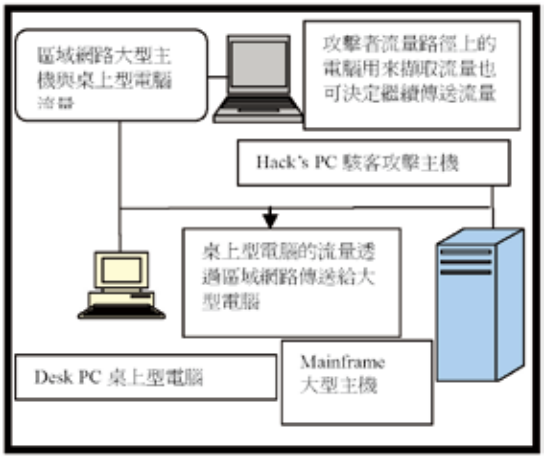


圖三　網路入侵監聽示意圖(自行整理)

現代化戰爭形態，已由兵器與人力導向，轉為技術與知識導向，因此必須分偵蒐、通信、指管三方面，建置自動化的C⁴ISR系統，方能透過數據鏈路傳遞各項情資，然後經由指管系統整合現有武器裝備，進而建立「偵測系統不限載台、指管決策不限位置、武器載台不限軍種」之聯合作戰能力。資訊戰相關研製，就期程而言，應先以發展資訊戰策略及防護系統為主；其次發展資訊戰攻擊系統；然後再持續強化資訊戰防護及攻擊系統。如此可逐步建構資訊戰全方位的防護、支援及攻擊技術及系統能量，因應資訊戰快速變動特性。美軍事務革新係以配合現今科技分階段性：第一階段是要求有限度的軍事傷亡、遠距攻擊與準確性、資訊之主導等；第二階段則涵蓋非致命性、心理科技、自動化防衛與其它突發應變事項[1]。美國軍事革新常在歷史教訓中檢討、改革，從各種不同的角度與觀點來考慮問題與理念，經「戰鬥實驗室」(Battle Lab)配合，就可能找出鼓勵自由思維的方法與新的解決方案，然後再將之制度化納入準則運用[6]。

中新網2013年5月24日《華爾街日報》中文網報導，美國現任及前任官員稱，

伊朗駭客對美國企業的發起網路攻擊，入侵並監視能源公司的電腦網路。資訊技術(包括電腦、感測器及數位化武器)的迅速發展，更加快了美國陸軍資訊戰因應與整備，並因此1973年成立陸軍訓練作戰準則司令部(Training and Doctrine Command，TRADOC)，未來戰鬥系統是美國陸軍邁向新世紀作戰形態重要的一環，著重於制敵機先的概念，了解與掌握戰場全貌，提高機動性、致命性，強化防護力為其系統發展的著眼。美國海軍1995年10月啟用了艦隊資訊戰中心(FIWC)，該中心向部署在海上的船艦作戰群及兩棲戒備大隊的指揮控制作戰參謀提供有效資訊作戰支援，透過先進的部隊網路，各艦縱使分散於海域，仍可即時共享戰場狀況，艦隊運用也趨於一體化。美國空軍資訊戰專家更積極致力奪取戰場制空權與掌握作戰資訊控制權，電腦化指管通資情監偵為強而有力戰力的加乘因子，以整合發揮戰力優勢遂行網狀化作戰，表一為美軍資訊戰發展演變分析表[7]。



圖四　網路入侵攔截示意圖(自行整理)

表一　美軍資訊戰發展演變

軍種	美軍各軍種資訊戰發展演變內容
陸軍	資訊部隊負責蒐集敵人武器系統，培訓指揮員確定這些系統如何使用，擬定資訊戰新指南收錄在《FM100－6 資訊戰》手冊中。資訊處理器使指揮員能夠將整個戰場傳來的各種資訊綜合起來並運用這些資訊有效判斷敵人動向
海軍	艦隊資訊戰中心負責研究海軍及各軍種聯合資訊技術、過程和訓練，作為新軟體的試驗場所，有一個整個艦隊電腦安全設置全天候服務危機反應中心，可以為大型海上演習訓練提供資訊戰假想敵來支援反恐作戰或監視區域危機
空軍	美國成立空軍資訊戰中心，其任務是制定一套戰略和戰術，保護美軍的指揮、控制和通信(3C)資源，有效遏制敵方利用空軍指管通資情監偵資訊系統

美國國防部在全球88個國家與地區擁有超過4,000個軍事基地與至少1,500個次級電腦網路，軍方的指揮管制、情報後勤、軍事研發與部署均仰賴網路的通信整合，美軍網路司令部由國防部長蓋茲2009年6月下令建立，以統一協調保障美軍網路安全，進行網路攻擊與防禦等與電腦網路有關的軍事行動[5]。美國空軍戰略司令部(USAF Strategic Command)司令奇爾頓上將2010年3月16日表示，五角大廈已完成美軍網路司令部(U.S. Cyber Command)籌備工作。當美軍愈來愈依賴網路的同時，來自網路的威脅也越來越多，為強化網路安全，美軍已成立網路戰司令部，約4萬人投入與網路戰的相關工作；日本方面則組建一支編制5,000人由陸海空自衛隊電腦專家組成的網路戰部隊。美國網路司令部整合美軍全球行動，並且與國家安全局協力維持美軍指管通情系統的安全與通暢，同時為美國的非軍事部門與國際夥伴

提供相關支援[8]。2013年4月29日國安局副局長張光遠表示，目前遭受攻擊的主要對象已從政府機關、駐外館處，擴大到民間智庫、電信業者與委外廠商，而主要攻擊標的也轉向包括車輛交通號誌儀控設備、寬頻路由器、工業微電腦控制器、網路儲存系統等嵌入式系統上，可以瞭解到現代資訊安全危機隨處可見[4]。

肆、戰爭型態演變與國防資訊科技應用

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，美軍充份運用各種高科技設備，掌握敵兵力部署，並講求指揮管制，充分掌握「電子戰與資訊」[14]。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]。

美軍於2003年3月20日對伊拉克發動空中攻擊，開啟「第二次波斯灣戰爭」序幕。本次作戰，美軍運用特種部隊作戰及高科技武器精準打擊，並配合地面部隊快速挺進，戰果豐碩。此期間，美軍不但在軍事科技、武器裝備系統有所精進，作戰理論亦隨之改變，其所執行的「震撼與威懾」(Shock and Awe)理論以及特種部隊作戰、快速機動、精準打擊、後勤支援等優勢作為，皆為現代戰爭典型，震撼與威懾透過人膽戰心驚的打擊與威懾，利用火力優勢打一場不需要傳統規模部隊的戰爭，利用心理宣傳打擊敵人的意志，使用決定性或壓倒性大規模空襲導彈精準打擊，使衝突或戰爭可於短時間內結束[4]，表二為美軍因應「震撼與威懾戰」之核心特性(自行整理)。

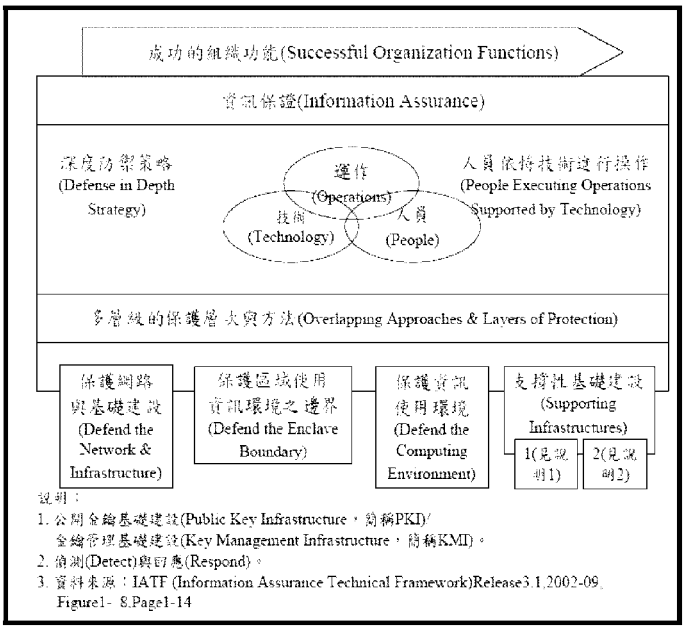
表二　美軍因應「震撼與威懾戰」之核心特性

核心特性	因應震撼與威懾戰核心特性說明
戰場認知	充分瞭解敵我狀況與環境，掌握優勢戰場知覺並能超越優勢期望
運用速度	迅速統合運用速度、時效與靈活度，以期掌握震撼後的戰場情勢
卓越特性	確定卓越作戰與執行標準以有效消弭戰場誤擊以及確定作戰節奏
掌握環境	實際掌握地面、海面上下、空中與太空等空間之資訊傳遞與接收

圖五　美軍網路戰司令部作戰平臺[8]

先進的C⁴ISR系統可以整合共

通作戰圖像，以實現數位化戰場管理，並且可以連結三軍主戰兵力，發揮戰力倍增效能。要建置先進的C⁴ISR系統，其核心技術在於指管決策自動化、智能化以及相關的作戰效能、武器效能預估能量的建立。資訊科技的發達，促進了實現網狀化作戰的動力。事實上，網狀化作戰的實現，除了資訊基礎建設之外，能夠適當融入作戰想定、指揮方式、組織形態和人員專業的指管系統，才足以發揮整體戰力[5]。針對中共網軍威脅與日俱增，美國與英、法約60個國家締結相同的資訊安全協定，同時於2007年與日本簽署「軍事資訊共同安全協定」因應中共駭客惡意攻擊，並於五角大廈成立一個新的網路戰爭指揮中心，積極為網路戰爭做準備。特別值得一提的是，美軍陸軍、海軍、空軍與陸戰隊紛紛組建各自網路戰部隊，並在2009年建立各自網路指揮部並組建多達20種大型軍事網路完成網路整合能力，五角大廈並大規模招聘與訓練網路安全專家，為即將正式運作的網路司令部儲備人力。美國陸軍與海軍分別基地資訊中心與艦隊資訊戰中心建立「電腦應急應變(Computer Emergency Response)分隊」，以積極因應戰術層次網路威脅，圖五為美軍網路戰司令部作戰平臺示意圖[8]，圖六為美國2002年提出資訊保證技術框架(Information Assurance Technical Framework)示意圖。



圖六　美國資訊保證技術框架示意圖[11]

伍、結論與因應作為

隨著資訊科技快速進步，組織的各種資料、資料90%以上都是以電子文檔和資料的形式保存。資訊化在企業生產經營中起到越來越重要的支撐作用。隨著資訊技術的發展，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」。面臨戰爭革命和資訊科技各種變化與挑戰，世界先進國家的軍事發展，莫不以強化兵力投射、專業化、資訊戰、C⁴ISR、精準、戰場數位化，以及聯合作戰等能力的提昇為急務，國軍資電優勢關鍵研究發展分別針對「C⁴ISR」、「電子戰」及「資訊

戰」積極整備與籌建相關能量[12]。美國政府資訊網路對於網路入侵事件與系統異常現象的問題相當重視，美國政府社會面對網際空間威脅，透過整體審視與稽核的策略，結合官方、學術界與產業界的合作，以建構堅實的資安防禦與基礎建設[13]。擔任白宮網際安全協調官的Howard Schmidt並在會議中宣揚對資訊網路安全的作為，包含CNCI(Comprehensive National Cyber security Initiative)的12項目標與計畫。預計縮編收納4000條政府單位資訊系統線路至100條，達到可信賴之網際連線(TIC)目標，並建置Einstein2與Einstein3系統用於偵測政府資訊網路之入侵事件與系統異常現象；以及針對國外商業間諜之反情報計畫，以偵測、阻絕資訊戰諜報問題，保護公私領域網路與智慧財產之損失[14-19]。

現今資訊作戰形態已無平戰時區分，更沒有時間、空間限制，只要透過網路駭客攻擊，輕者能夠竊取個人資料與錢財，嚴重者則足以讓國家軍事機密資料外洩或運作遭癱瘓[17]。網路致能作戰(Network-Enabled Operation)可以運用迅速分享的構聯網路傳遞訊息，相對來觀察中共為使其「網軍」發揮預期效能與戰力，由中共「國家國防動員委員會」負責協調人力與物力、軍隊與政府、戰爭與經濟關係，至今已協調聯繫運作具有相當規模的「信息民兵部隊」，並對全世界的資訊與網路安全造成威脅。共軍在信息作戰方面的犯台模式，已逐漸從全面封鎖、攻擊國軍有生力量，轉變為包括企圖採資訊戰攻擊或破壞我方的C^4ISR系統[18]。鑑於此，國防部除訂頒「國軍資訊安全」相關規範，嚴格落實資安管控措施外，並針對戰演訓部分，策頒「國軍演訓資通安全維護整備要點」，期能從軟硬體乃至於「人」的因素著手，避免違規情事肇生，建立安全的資訊作業環境，進而強化國軍整體資安防護能力[17-19]。

我們瞭解『他山之石可以攻錯』的道理，針對美國國防部資訊安全作為在此提供我國軍事安全防衛的借鏡參考，美國資訊安全重點在於：其一、保護機敏資料的安全；其二、使資料安全快速方式共享；其三、確保資訊科技基礎建設以利網路戰爭期間確保可靠無虞；其四、保障任務指揮官存取網路空間的能力；其五、以迅速高效能的方式運用新興科技。總而言之，以資訊為核心所建構的國家基礎設施，新形態網際網路所衍生的電腦駭客等安全漏洞問題，已經是防不勝防，無論是國防科技或軍事武器等重要情資外洩，均將牽一髮而動全身，若透過敵方後門程式的植入或個人帳號的套取，導致資訊流的阻斷、篡改與監控，並肇生資訊安全危機將使敏感機密資訊受極大威脅與造成國家安全利益重大損失，因而需要提昇全民國防與資安防護觀念，使用網路資源時，要有維護網路安全基本素養，確遵安全規範，讓全體國人均保有高度資安警覺與防制能力，落實更綿密的國防資訊安全防護作為

[20]。

陸、參考文獻

〔1〕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。
〔2〕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.
〔3〕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。
〔4〕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。
〔5〕路透社，駭客入侵國防網路、美首點名大陸，http://www.reuters.com/，2013年5月7日。
〔6〕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。
〔7〕Eric L. Haney and Brain M. Thomsen著，國防部譯，論21世紀超越震撼與威懾，國防部軍官團教育參考叢書-613，2010年3月。
〔8〕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。
〔9〕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。
〔10〕中華民國資訊軟體協會，行政院「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。
〔11〕樊國楨、黃健誠，資訊安全管理系統要求事項之應然與實然初探「技不如人」還是「要求事項不如人」?，第二十三屆全國資訊安全會議，2013年5月23-24日。
〔12〕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。
〔13〕奕平，青年日報專論：歐洲神經元無人戰鬥載具，2007年6月4日。
〔14〕洪蘊華，青年日報專論：迅速之眼-實現全球精確、快速打擊目標，2007年9月12日。
〔15〕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。
〔16〕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。
〔17〕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。
〔18〕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。
〔19〕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。
〔20〕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。

作者簡介

空軍上校 吳嘉龍

學歷：中正理工學院電機系電子工程組77年班、美國俄亥俄州空軍理工學院電腦工程研究所碩士84年班、國防大學理工學院國防科學研究所電子工程組93年班博士。

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：空軍航空技術學院一般學科部航空通訊電子系專任教授兼任系主任。