空軍軍官雙月刊 154
Air Force Officer Bimonthly

資訊管理

網路惡意程式攻擊威脅與資訊風險管理技術探討

空軍中校　吳嘉龍

提要

隨著資訊科技時代演變，網際網路訊息傳遞快速更容易接觸與取得資訊，資訊安全防護技術發展，主要目的是為解決惡意程式攻擊威脅所應運而生的資安漏洞。大部分的電腦使用者誤認靠著防火牆、入侵偵測系統、防毒軟體工具可維護網路以及電腦的絕對安全，但是隨著駭客技術及工具的演進，包括通訊、水力、鐵公路、航空站，甚至核電廠等基礎設施，都已成為網路戰的攻擊目標，如何做好最佳的防護變得越來越重要。資訊安全防護技術在身份識別與存取管理考慮包括不同應用軟體、硬體平台與作業系統外，更須針對不同的儲存方式、目錄管理、存取管理、使用者管理與申請流程、密碼管理以進行審核與規範管理，並落實網路安全風險管理與有效強化資訊防禦能力，以因應層出不窮的資安威脅。

關鍵字：資訊風險管理、網路安全、惡意程式攻擊、弱點攻擊、資訊戰。

壹、前言

資訊軍事事務革新正對軍事產生全面影響，資訊優勢已成為克敵制勝的關鍵及聯合作戰的重心，網路攻防戰更徹底改變了作戰形態。隨著資訊科技的日新月異，瞭解包括資訊作戰型態相關資訊科技與環境的運用與控制以及如何在傳統戰場與無限網路空間，遂行防禦與攻擊戰略戰術的行動，已成為相當重要的議題。二十一世

紀的網路戰(Cyberwar, CW)可定義為涵蓋攻擊電腦系統和網路，或防禦敵人攻擊友方系統和網路「電子作戰序列」(electronic order of battle，EOB)等一切作戰行動。波灣戰爭之後的軍事事務革新，名為「資訊軍事事務革新」(info-RMA)，能夠迅速做出有效決策，其應用性已成為所有戰場不可或缺的戰場管理技術。善用此技術不僅提昇現行系統之作業互通性，有效支援「效能作戰」(effects-based operation，EBO)，如同不對稱兵力倍增器，同時也符合隨著聯合、系統體系觀點而來的變革作為，以及不對稱作戰原則。在現今資訊科技不斷更新與網路蓬勃發展的結果，帶給民眾生活無限便利與品質提昇，但也衍生許多新的社會與犯罪問題。因為資訊科技的發達，只要一個動作，訊息就可以藉著網路傳播出去，但也因為如此，許多網路使用者常常因為一時疏忽大意或是知識上的不足，將不該暴露的資訊傳播出去，或是接收到有害的資訊。如果我們的電腦沒有安裝適當的軟體，或者一些存有大量個人資料的機關疏於防備，便極有可能遭到不法人士入侵而使自己或是多數人的權益受損，反觀軍事機密亦是如此。隨著美國政府遭受網路攻擊的次數逐年升高，美國國內開始呼籲在反恐之餘，更應重視網路資訊安全的重要性。由過去戰爭可知，戰爭獲勝的重要關鍵因素是戰時相關資料，但這些以往由人管制的重要資訊，在科技發達的現今社會，卻已全部交由電腦集中管制，資訊安全與保密方面應具備新思維與新觀念，在平時應建立電腦緊急應變中心作好周全的資安預防機制，不斷提昇資訊防護技能；戰時才能有備無患，確保機密資料不外洩，如何做好資訊安全防護也益加重要[1]。根據韓國媒體《朝鮮月刊》近期報導指出，南韓重要軍事機密《5027作戰計畫》在2009年11月中旬遭到北韓駭客竊取，這份軍事計畫包括北韓入侵初期，南韓的軍事應對措施。隨著北韓駭客部隊能力增強，報導指出，北韓已經有發動網路戰爭的能力。南韓軍方在2006年發表的報告中指出，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，也將北韓列為第八位，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[2]。

貳、弱點攻擊與惡意程式攻擊

美國資訊安全策略目標有三，包括(一)：預防對於美國重要基礎建設的網路攻擊；(二)減少國家遭受網路攻擊的脆弱性與(三)當網路遭受攻擊時減低受損程度並降低系統所需之回覆時間。然而，防火牆、防毒軟體、IDS/IPS等等各式各樣的資訊安全防禦工具越來越多，功能越來越強，可是為什麼還是一直被駭客攻擊成功，其原因在於電腦使用者常誤以為防火牆與防毒程式可以擋掉所有駭客的攻擊，或者認為可以靠IDS/IPS將攻擊抓出來，靠防毒軟體將病毒掃掉。事實上，在惡意程

式攻擊手法與策略的進步與複雜化，傳統的資安防禦方式也勢必要做相對應變革，完全仰賴防火牆加上防毒軟體的觀念，幾乎已經無法阻擋目前的資安外部威脅。防火牆只能防制外部對內部的攻擊，而且無法辨識仿冒或是假的IP。傀儡網路攻擊涉及資料竊取外洩，這些都是顯而易見的網路犯罪行為，若網路駭客無法靠資料搜集與系統掃瞄取得有用資訊時，駭客將開始運用列舉入侵技術取得目標網路主機的使用者帳號或資源共享資料，進行攻擊。法務部調查局便指出，很多電腦使用者者往往是直到執法單位通知才發現系統被入侵或帳號密碼被竊取冒用。各種網路犯罪中，網路釣魚受害最廣，但傀儡程式受害最深[3]。弱點攻擊方式分析如下：包括撰寫不良的程式碼、緩衝區溢位、路徑跳脫攻擊、資料隱碼與電子郵件攻擊。應用程式弱點攻擊中包括無效的輸入值、存取控制不嚴謹、身分見別及連線管理不嚴謹、緩衝區溢位、不恰當的錯誤處理、阻斷服務與不安全的組態管理，弱點攻擊方式項目與分析內容如表一[4]。

針對資訊安全的威脅與日俱增，分析敘述如下，英國政府去年6月表示，國際網路犯罪者透過工業間諜和信用卡詐欺等活動，令英國經濟每年損失「數十億英鎊」，研判該等威脅來自中共和俄羅斯等國家、恐怖團夥、犯罪團夥和惡意的駭客[17]。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，能在有限的範圍內摧毀敵方的電子設備和電腦。2008年春天，北韓實施了一次網路武器試驗；2008年十月，北韓進行首次邏輯炸彈試驗，邏輯炸彈是一種含有惡意代碼的電腦程式，在某些事件或在某個預設的時間點就會自動執行，能夠導致電腦當機、資料數據被刪除等電腦災害。2009年3月5日，北韓駭客對南韓陸軍第三軍司令部發動24小時的網路襲擊，盜取了第三軍司令部下屬的國立環境科學院化學物質安全管理中心的安全密碼；之後，再利用密碼盜取

表一　弱點攻擊方式項目與分析內容(自行整理)

弱點攻擊方式分析項目	弱點攻擊方式分析內容
撰寫不良的程式碼與應用程式弱點攻擊	根據開放網站的應用程式安全計劃網站應用程式造成會被攻擊的弱點，可以歸類為以下幾種：Invalidated input、Broken access control、Broken authentication and session management、Cross-site scripting flaws、Buffer overflows、Injection flaws、Improper error handling、Insecure storage、Denial of service、Insecure configuration management。
緩衝區溢位與路徑跳脫攻擊	因為程式撰寫不良最常見的弱點就是緩衝區溢位，當程式程序沒有限制使用者所提供資料的大小所造成的弱點，讓攻擊者可以強迫程序儲存比預期中還要多的資料。而這個過大的資料複寫到記憶體中儲存的重要職，讓攻擊者可以控制這個程序進行插入或者執行惡意的指令。
SQL injection資料隱碼與電子郵件攻擊	攻擊方式會造成伺服器最重的毀損就是injection attack。SQL injection(資料隱碼)攻擊對於依個僅開80通訊PORT，對於使用資料為基礎的網站來說，是一個很嚴重的威脅，而且，此種攻擊的技巧非常的容易學習，甚至是在系統已經安裝所有更新程式的狀況下還是可以造成整個系統被入侵。
SSL封包明文解碼中間人攻擊	SSLstrip工具可在公開的無線網路環境中使用，從中獲得帳號密碼，以中間人攻擊攔截無線網路SSL封包將亂碼轉為可閱讀的明文，必須運用更嚴謹的EVSSL(Extended validation SSL)認證與謹慎使用帳號密碼才能避開此類攻擊。
利用系統漏洞入侵列舉Enumeration分析攻擊	駭客入侵列舉Enumeration分析攻擊，運用與目標系統主機連線，在Windows系列的作業系統利用Net Bios Null Sessions漏洞，建立連線後，惡意攻擊者再使用NetBIOS、SNM、Active Directory與Zone Transfer列舉，以取得使用者帳號等資料。

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[2]。針對臺灣而言，傀儡網路攻擊案件媒體曝光率雖然不高，但臺灣卻是全球感染傀儡程式、遭受傀儡網路攻擊最盛的國家之一。傀儡網路攻擊和病毒、垃圾郵件相比，傀儡網路攻擊比較不受重視，這類攻擊通常不會發生立即性破壞，然而這些潛在攻擊，往往也因為沒被發現，而能夠為所欲為。傀儡網路攻擊造成重要損壞，主要的原因還是在於寬頻網路及無線網路普及。因此，傀儡程式隨著高速網路對企業帶來的傀儡網路攻擊(Botnet)，相關危害將不可忽視。相對於會影響企業系統作業的病毒、垃圾郵件等顯而易見的資安問題，傀儡程式往往潛入企業後便按兵不動等待時機，或者已經長期監控、竊取資料，而不被系統察覺，從傀儡程式被植入到被發現，最短1週～3個月，半年以上才發現的比比皆是，超過1年以上也不在少數[5]。

DoS(阻斷式服務)攻擊是指利用傀儡電腦發出的封包，癱瘓受駭電腦的系統，導致緩衝區溢位，或使封包超過頻寬。這些攻擊若從單一機器對單一主機發動，目的在使系統主機超載，則是DoS攻擊；但若攻擊是從多個機器針對單一系統發動，則為DDoS。而IDS/IPS對目前許多後門加密通訊、網頁應用程式攻擊、SQL injection與駭客精密加工的後門行為並無法達到完全防禦，針對防毒軟體的弱點設計的木馬程式攻擊(rootkit與修改source code技術等)更是日益升級，更重要的是，傀儡程式除了可以聽命竊取資料外，更可以發動DDoS(分散式阻斷式服務)攻擊。另外，駭客也可利用監聽網路流量(Sniffering Traffic)，取得其他傀儡網路電腦的資訊。根據青年日報報導，在2009年7月，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、近兩萬部個人電腦受到「傀儡電腦」(Bot)惡意程式入侵攻擊，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[2]。根據美國CERT定義，傀儡網路攻擊基本定義是指：一個可自動執行的電腦程式非法安裝在電腦系統中，而駭客可以透過病毒或其他惡意程式，散佈該傀儡程式在多臺電腦上，以控制該臺電腦；該臺電腦也可以被1個或多個以上的駭客控制、存取[6]。有鑑於網路威脅的安全因應，美國率先組建網路司令部，美國國防部長蓋茲2009年6月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。美國公布的官方報告指出，2009年美國國會與其他政府單位遭網路攻擊的案件暴增，估計每月達16億件[17]。

參、身分識別與資料安全儲存技術

美國國家安全局局長Alexander表示，資訊戰爭隨時可能發生，因此，國家的策略需先對國家安全網路與機敏網路分級，進而防護，以維繫重要的資訊流通不中斷。而平日與國土安全部進行資訊分享經驗、技術與訓練的防護專家，應當隨時提高安全意識，戰時則足以發揮關鍵效用[18]。全球每日有10000～35000個不等的傀儡程式，利用各種管道，活躍地、散佈在全球各個不安全的系統上。根據資安公司CipherTrust資料統計，傀儡程式每天影響超過25萬個系統；而這個影響的系統，除了50％是家用電腦網路系統外，40％的攻擊是針對大型以及中型企業。全世界第一個寫出來的傀儡程式，是在1993年針對Unix主機所寫的程式，名稱為：Eggdrop Bot，迄今還有針對微軟視窗作業系統的傀儡程式：Eggdrop Bot for Windows存在著。目前傀儡程式大致可分成幾種管道散佈，其中，「網路聊天室(Internet Relay Chat；IRC)的散佈是傀儡程式最原始的散佈方式。」。這些IRC Bot通常都走TCP通訊協定，包含TCP 6667通訊埠等。

隨著加密通道的盛行，為了逃避常規檢查，傀儡程式也會選擇諸如：https通訊協定傳播(TCP 443埠)或其他8000埠、500埠等，未來點對點(P2P)的傳播方式將更為普遍。傀儡程式主要是聽命發動者發布命令而動作，不論是自動更新其版本，或者命令傀儡程式攻擊某個網址，藉此發動DoS(阻斷式服務攻擊)。大型Botnet能夠進行廣泛的DDoS，小型Botnet利用偽造IP的方式，發動攻擊，以避免其植入傀儡程式的電腦被發現。分散式阻斷服務攻擊主要的目標在於「阻斷」任何人去使用應用程式，而且是透過大量的網路流量，來攻擊這些伺服器以及網路裝置上的應用程式。DDoS攻擊用來對特定的公司或組織攻擊，進行勒索或破壞他們的電子保護機制，而且任何人都可以在網際網路蒐集到各式各樣用來發起DDoS攻擊的工具[7]。

結合許多被植入傀儡程式形成的傀儡網路攻擊，電腦資料加密安全措施可有效完成儲存安全規劃，而儲存管理人員將必須做網管人員落實『存取、識別與原則控制』縱深防禦策略，遵循稽核與報告、資料加密、身份管理與資料存取鎖定，強化伺服器與主機安全性，以及強化儲存設備、元件、交換器，與相關通訊連線的安全性。值得注意的是，實體隔離使用加密方式，將資料加密後才拿到外部網路傳送，在技術上已經遭駭客破解，先透過USB Worm建立起傳輸管道，透過Hook API的方式，搶先攔截加密前的明文資料，使加密方法形同虛設。虛擬化是集中儲存策略的主要元件，所有自動化、異質儲存的管理策略都將會需要一個虛擬化的環境來掩護所有在其下錯綜複雜的儲存設備。而虛擬化也已經實際出現於網路儲存環境的每個部份：RAID控制器、伺服器配接卡、磁碟陣列、路由器、網路設備、交換器、虛擬磁帶櫃加密等。

SAN(Storage Area Network)技術廣泛的運用得以提供高速的、可管理的、具容錯能力的、富彈性的儲存服務。SAN技術包括：辨識與評估儲存介面、建立風險範圍、監視與控制實體存取、建立資料安全遵循的標準、保護外圍資料、瞭解機密暴露的風險與實作適當的服務聯貫性。它是一種服務架構，結合多種硬體(光纖、HBA卡、高速交換機、伺服器、磁碟陣列等)與軟體(管理軟體、target軟體、驅動程式等)的技術。採用SAN的架構，可以將各個單一的儲存設備連結起來，提供整合性的管理與應用[8-10]。SAN最大的用途不僅在於做為資料的儲存，而是在於其容錯與災難備援的能力。這也是SAN技術得以普遍運用的主要原因，一方面可以將所有的儲存資源妥善的管理，另一方面可以提供不中斷的營運服務，在遇到天災外與電腦病毒時，可以在最短的時間內，最有效的復原，從而避免損失，SAN(Storage Area Network)技術優點分析如表二[11-12]。

表二　SAN(Storage Area Network)技術優點分析(自行整理)

SAN技術優點項目	SAN(Storage Area Network)技術優點分析內容
具經濟效益	透過網路架構儲存設備分享，所有的用戶端不必直接連接到特定的儲存設備上就可以使用期資源。
可有效管理	透過管理軟體有效管理，可以更有效的管理儲存的資料與制定備援計劃。
具容錯能力	SAN 提供多種容錯功能能降低資安服務風險，從 mirror 到進階 snapshot，可以減低資料遺失或是企業服務中斷的風險。

針對資料儲存理論技術分析，在SAN採取的是Client/Server架構，其中提供儲存能力的一端稱之為Target，而要求資源的一端稱為Initiator。Target與Initiator之間，透過高速的網路連結，這通常是光纖，SAN(Storage Area Network)技術防護分析如表三。而提供連接的介面我們稱之為HBA(Host Bus Adapter)，建構網路的方式則是光纖交換機。然而隨著技術的演進，SAN亦有支援IP的介面出現，可以運用現有的Ethernet、SAN/IP與iSCSI技術來達成[11-14]。

表三　SAN(Storage Area Network)技術防護分析(自行整理)

SAN技術防護	SAN(Storage Area Network)技術防護分析內容
存取控制與身份管理	目的在阻礙未經授權人士獲得存取儲存管理工具與設備權限，以辨識嘗試進行存取的使用者或系統，獲得合適的存取權限。
可架構在任何伺服器與主機之上	要避免對有資訊安全漏洞伺服器儲存系統發動攻擊，系統應用程式開發人員熟練伺服器安全設定，儲存管理人員控制權應越少越好。
設備與交換器間通訊安全	設備會被鎖定負責實際安全，在設備與交換器執行最新版本作業系統，並安裝目前所有的更新套件，還有定期為所有的裝置更改密碼。

Cisco思科的網路存取控制方案(NAC，Network Admission Control)與Microsoft微軟的網路存取防護方案(NAP，Network Admission Protection)均注重事前防禦機制(pre-ad-

表四　NAC/NAP的Post-admission控制功能(自行整理)

Post-admission控制項目	NAC/NAP Post-admission 控制功能技術分析內容
強制採取身分為基礎的網路存取	資源網路應該採用身分識別決定權限，限制擁有合法存取權利的功能，而且，限制匿名到訪者及非授權者的擅入。
防止受害範圍惡化	網路安全措施雖然無法完全杜絕攻擊的存在，不過，起碼它要能防範攻擊行為的擴散，以確保整體網路的運作安全。
減輕企業營運的負擔	尤其是勞力密集性質的工作，需透過自動化管理，可讓 IT 團隊提供企業更高品質的服務。藉由透過 pre-admission 機制，可輕易察覺有問題端點情形，並改善管理主機狀況。

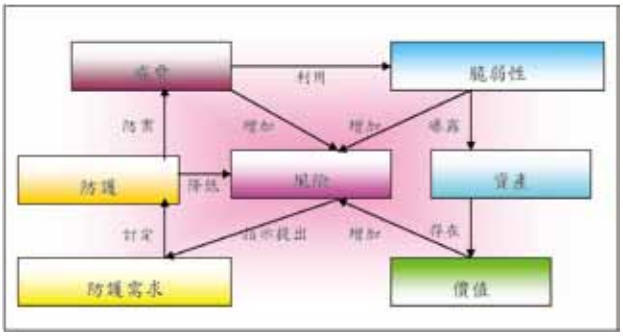
mission)，採取post-admission方式，確保端點遵守安全政策。其目的就是安全隔離有問題、不安全的端點主機，以抵禦多形態的網路攻擊。資訊安全屬服務性質，條列出三項有關NAC/NAP的post-admission控制功能分析如表四[12-15]。

肆、資訊安全風險管理理論技術

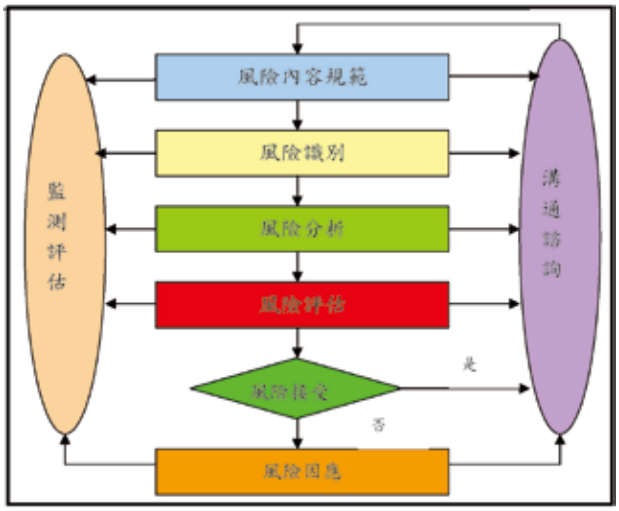
由於社會逐漸數位化及資訊化，加上中共「網軍」四處蒐集機密資訊，導致世界強權的美國也預測透過「網路911」的攻擊模式，就能夠延遲、甚至癱瘓整個美國社會的正常運作，因此美國總統歐巴馬決心成立網路戰司令部，以整合當前美軍的網路作戰資源[16]。美國《華盛頓時報(Washington Times)》2010年3月18日報導，資深國防記者比爾・葛茲(Bill Gertz)在「五角圈內」(Inside the Ring)專欄指出，美國五角大廈遍佈全球的龐大電腦網路，在2008年遭遇一個經由隨身碟進入電腦的惡意軟體攻擊，美國戰略司令部(US Strategic Command)指揮官空軍凱文・齊爾敦將軍(Kevin Chilton)在今年3月16日眾議院聽證會上表示，美軍已發展出新的網路監視和評估系統，並努力掌握網路的安全需要。戰略司令部正積極為網路戰爭做準備，包括籌設一個新的網路戰爭指揮中心，諸如此類的惡意滲透與入侵正是當前網路戰爭面對的威脅模式[20]。美國國防部依據2000年通過的國防授權法案，每年針對當前暨未來20年中共軍力發展趨勢，2005年向美國國會提出評估報告，同時對外公佈中共武力已衝擊亞太區域安全，並對美國全球安全地位造成威脅。現代的戰爭形態早已隨著資訊工業的快速發展而起了激烈的變化，在進入太空時代的現在，所有的先進武器都已電子化，而網際網路科技上的能力更是決定戰爭勝負的一項重要因素，相對於資訊的流通便利，如何落實「風險管理」就成為一門極為重要的課題。

自2002年2月，資訊技術安全評估共同準則(簡稱共同準則)公布缺點修補之評估方法增補(Supplement)之後，IBM、Microsoft、Netscape、Oracle、RedHat、SuSELinux等公司紛紛遵循共同準則之要求，建置其產品缺點修補程序，並通過審查與測試之驗證程序。共同準則定義的缺點修補安全保證之目的，在於要求開發者追蹤與更正所發現的安全缺點，包括配發缺點更正措施之需求，ISO/IEC 17799:2005(E)已大量使用風險管理、網路安全、入侵偵測、金鑰管理與資訊安全事故管理等技術及作業控制之標準，在共同準則方面，於2004年1月9日及4月12日，經濟部標準檢驗局依序公布「資訊技術－安全技術－資訊技術安全評估準則」CNS 15408系列標準之第1部、第2部及第3部[21]，圖一為ISO/IEC TR 13335-1規範下資訊安全系統風險管理關係圖。

國際標準化組織(International Organization for Standardization, ISO)於2007年10月規劃「重要民生基礎設施資訊安全」標準的制定計畫，我國也於2007年12月31日通過CNS 27001(ISO/IEC 27001:2005)資訊安全管理系統(Information Security Management System, ISMS)驗證之重要民生基礎設施防護。國際標準化組織與國際電工委員會於2008年6月15日制定第一版ISO/IEC27005:2008(E)資訊安全規範風險管理的標準，制訂單位是ISO與IEC之第一聯合技術委員會(ISO/IEC JTC1)的第27資訊技術分組委員會(SC27)，制定標準參考根據ISO/IEC 27001:2005、ISO/IEC 27002:2005及AS/NZS 4360，CORAS是一個開放原始碼的軟體，以JAVA程式語言開發完成，可安裝在Windows及Linux作業系統中，屬跨平台的軟體，同時也是一個整合風險評鑑方法的平台，圖二為CORAS模組流程圖[22]。表五為ISO/IEC 27005：2008(E)風險管理步驟，風險管理步驟項目包括風險內容規範、風險評估、風險處置、風險接受、風險溝通、以及風險監控與審查等六個步驟，其中值得注意的是，風險評估步驟必須列出所有可能遭受威脅事件的資產清單，並找出可能產生威脅事件的弱點，並且對這些弱點、脆弱性及威脅事件加入風險發生時的後果推論及判斷，而風險監控與審查步驟則應隨時掌握新的弱點及威脅事件，並且更新，以維持組織風險管理機制的正常運作，保護組織的資訊安全[22]。



圖一　資訊安全系統風險管理關係圖(ISO/IEC TR 13335-1)(自行整理)



圖二　CORAS標準風險管理程序模組流程圖

伍、結論與未來因應作為

資訊科技的發展與進步，提升網路應用的普及率，讓我們體會到網路無國界的便利；然而在網路便捷的環境下，必須思考如何架構良好的資訊安全環境，因此，

如何做好資訊安全風險管理就成為最重要的環節[22]。有鑑於網路襲擊恐怖主義對國家安全的衝擊日益升高，全世界對於資訊安全的重視程度也逐漸加深，中共自2000年建立「網軍部隊」後，即專事透過網路對目標進行遠距的駭客攻擊，許多國家為防範「網路911」發生，相繼成立資訊戰指揮單位。資訊安全工作並不僅限於防範駭客入侵一項，也非僅使用者開機時才進行的工作，而是使用者平時即應落實養成的態度與習慣。特別是當今網際網路運用的密集與多樣化，已取代傳統資訊通路，而不斷推陳出新的網路互動平台如即時通訊與大量流通的電子郵件，無異提供更多駭客入侵與惡意程式潛伏的路徑及空間。美國國防部為了反制駭客的入侵與危害，除積極強化各項防護與因應作為外，近年來更投入高達二百五十億美元的預算，運用於網路媒體的防護策略與專業部隊的建立，並在2009年6月宣布成立「網路戰司令部」，負責進行網路作戰，並加強防範日益增強的網路安全威脅[16]。英國政府通信總部2009年宣布將成立新的網路安全作業中心，負責協調英國國防部、內政部、軍情五處、軍情六處的相關任務，以確保英國的網路安全，2010年6月，英國安全事務大臣韋斯特宣佈，英國將成立新的「網路安全作戰中心」，並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，以確保網路安全[17]。我國現行網路攻防力量係由行政院資安小組負責網路安全與防護工作，警政署刑事警察局、法務部調查局負責整合產、官、學、民間專業人士，建構「民間網路攻擊力量」；國安局與國軍等單位負責相關情報作為，雖已建置肆應網路戰相當能量，但駭客無孔不入，仍須全民配合支持反制，方能克盡全功，身為國軍的一份子，應樹立「保密是軍人美德，洩密是軍人恥辱」的觀念，培養「人人以保密為榮、事事以保密為先、時時具保密警覺、處處行保密要求」的素養[23-24]。尤其，資訊安全工作已無平時與戰時的區分，是一個優患意識的建立與防患於未然的工作，要知道，平日養成風險管理的觀念，隨時做好資訊

表五　ISO/IEC 27005：2008(E)風險管理步驟(自行整理)

風險管理步驟項目	ISO/IEC 27005：2008(E)風險管理步驟內容
風險內容規範(Context Establishment)	內容規範包括制定與組織有關的資訊安全風險管理基本規則，內容必須持續符合ISMS的規範，詳細說明組織的資訊資產及精確定義組織的風險管理範圍與機制。
風險評估(Risk Assessment)	風險評估針對已制定之組織風險管理機制，列出組織內資產的擁有人、資產置放的位置及資產功能等，加入威脅事件的識別，依序列出風險的等級及對分可接受風險值的範圍，找出可能即時解決的方法，以降低風險發生時的意害狀況。
風險處置(Risk Treatment)	風險處置依據風險評估所列風險等級的優先順序加以處置，處置技術方法包括降低風險的產生及檢視組織內的活動項目，若活動易引起某些異常狀況而產生風險時，應加以避免或做風險移轉。
風險接受度(Risk Acceptance)	風險接受依據組織決策者對分之可接受的風險，做定期的文件紀錄檢視，因風險的可接受度不是絕對的是或否，仍需依照風險事件發生時的情況做評估。
風險溝通(Risk Communication)	風險溝通步驟持續蒐集風險資訊，以獲得新的資訊安全知識，除對組織的風險管理結果提供保證，並支持組織的決策，分享組織風險管理的結果。
風險監控與審查(Risk Monitoring and Review)	組織目前所制定之風險管理制度並非固定不變，風險的發生會隨著外在環境因素而改變，隨時會因新的弱點及威脅事件的產生而有所更動，因此必須持續監控組織環境的異常現象。

安全工作，一旦遭遇病毒攻擊就可立即做好危機管控，能多做一分預防工作，就可以強化一分資安的戰力，每個人做好預防工作，就可以集結為更強而有力的資安防護戰力。總而言之，我們應建立平時即戰時的危機意識並建立電腦緊急應變相關機制作為，以落實網路安全管理與資訊風險管理觀念，如此才能將國防安全與科技的潮流相結合，確保國家安全的長遠發展。

參考文獻

一、青年日報社論(2010)，落實資安防護、確保軍機安全，新聞導覽，軍事新聞，2010年04月28日。
二、青年日報社論(2010)，北韓網軍竊密不斷、南韓積極綢繆防堵，新聞導覽，軍事新聞，2010年01月19日。
三、黃彥棻(2006)，揪出資安威脅藏鏡人－傀儡程式，ITHOME電腦報，242期，28－34頁，2006。
四、李倫銓(2006)，免殺木馬兵臨城下、資安防線節節敗退，資安人，35期，16-19頁，2006。
五、陳志杰(2006)，韓國資安市場概況-全方位資安服務將成主流，資安人，35期，20-22頁，2006。
六、資安人雜誌社(2006)，Symantec運用Intel vPro技術-解決電腦安全防護問題，資安人，35期，76-77頁，2006。
七、Mark Diodati(2006)，身分識別存取控制管理123，資安人，33期，35~54頁，2006。
八、Michael Cobb(2006)，起床號，資安人，33期，58~64頁，2006。
九、Alan Radding(2006)，只有加密資料夠安全嗎?，資安人，33期，86~89頁，2006。
十、ITHOME Online(2008)，儲存技術ABC之初談SAN(Storage Area Network)，http://ithelp.ithome.com.tw/question/10008219。
十一、ITHOME Online(2010)，HP推出新一代ProLiant伺服器，http://www.ithome.com.tw/itadm/article.php?c=60671。
十二、HP IDC白皮書(2009)，Gaining Business Value and ROI with HP Insight Control，2009年5月。
十三、HP白皮書(2008)，HP Dynamic Power Capping TCO and Best Practices」，2008年11月。
十四、Eric Ogren(2007)，將安全列管事後監控機制填補NAC/NAP的不足，資安人，38期，63~64頁，2007。
十五、Alan Radding(2006)，2007熱門儲存科技，資安人，38期，77~80頁，2006。
十六、青年日報社論(2009)，安全戰略環境丕變、美建構網路戰司令部，新聞導覽，軍事新聞，2009年7月19日。
十七、孫國祥(2010)，網路新冷戰資訊攻防引發東西對立，青年日報社論新聞導覽，軍事新聞，2010年6月3日。
十八、Information Security資安人科技網(2009)，RSA PART(二)：國安問題需分級防護並全面稽核，2009年5月4日。
十九、Information Security資安人科技網(2010)，RSA 2010(一)：舊問題亟需新解，2010年3月8日。
二十、尖端科技軍事新聞(2010)，遭可能來自中國攻擊-美軍積極為網路戰備戰，1107期軍事電子報，2010年4月30日。
二一、樊國楨、林樹國、鄭東昇(2005)，資通安全分析，專論T94003，T1：資通安全政策，資訊安全保證框架標準初探：根基於ISO/IEC 17799：2005-06-15之12.6.1節，2005年12月。
二二、傅雅萍、樊國楨、楊中皇(2008)，資通安全分析，資通安全專論T97022，T3：最新技術研究發展，ISO/IEC 27005風險管理標準整合CORAS之可行性研究：以電力公司為例，2008年12月。
二三、青年日報社論(2009)，落實風險管理、確維資訊安全，新聞導覽，軍事新聞，2009年8月7日。
二四、青年日報社論(2009)，強化資安肆應網路戰時代來臨，新聞導覽，軍事新聞，2009年8月7日。

作者簡介

空軍中校　吳嘉龍

學歷：國防大學中正理工學院四十八期電機系電子組、美國空軍理工學院電腦工程研究所、國防大學中正理工學院國防科學研究所電子工程組。經歷：電子官、教官、區隊長、講師、助理教授、科主任、系主任、國科會計畫主持人、副教授。現職：空軍航空技術學院一般學科部航空通訊電子系中校副教授。