資訊安全

資訊安全技術與網路風險管理發展分析探討

上校教授　吳嘉龍

提要

國家實驗研究院科技政策研究與資訊中心2014年10月6日第201410004期資通安全電子報報導美國科技公司阿卡邁(Akamai)近日發表「網路攻擊」排行榜，公布網攻來源地比率，研究顯示，全球有43%的網路攻擊來自中國，排行第一，比率遠超第二名的印尼；美國則以13%排名第三，台灣也有上榜，以3.7%位居第四名。芬蘭上市資安公司芬安全(F-Secure)指出，從2011年迄今不到3年間，行動裝置惡意程式家族成長高達3倍，在Android平台上共有294個，這也意謂著每天發現的病毒數量超過3個，不法勒索軟體及殭屍網路將成為行動資安的兩大議題。本論文針對現代網路技術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，以鞏固與確保國防安全與資訊優勢。

關鍵字：資訊管理、惡意程式、緊急應變、網路威脅、行動資安。

壹、前言

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。隨著資訊安全與網路威脅的辯證發展，當今我們所面對的真正威脅，已不再只是單一國家或其內部的軍隊系統，而是一種具有全球性滲透的特性，以及呈現倍數成長的網路攻擊事件。這說明了網路攻擊已成為一種新的戰爭形態，表面看來，它似乎不及傳統戰爭來得嚴重，但事實上，它可能對國家目標與國家安全利益造成更大更深遠的不利影響。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。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，足以顯示因應現代戰爭型態對於資訊安全議題的重視[1]。

網路戰是一把雙刃劍，一旦運用網路部隊進攻別國的網路，導致網路癱瘓，而本國的網路作用也將急劇下降，所以國際間的網路必須靠合作，才能提升網路的便利性與使用價值。面對各國網軍較勁升溫的新形勢，未來的戰爭中電腦本身就是一種武器與戰場，前線無所不在，奪取戰場控制權將不只是導彈、飛彈和士兵，還包括電腦網路與數位通訊機制。科技日新月異，民眾上網行為也不斷變遷，跨平台上網已成為全民運動，近9成民眾會於多元裝置上安裝即時通訊軟體，即時通訊軟體已成為必備的溝通管道。，惡意威脅因應跨平台趨勢不斷衍伸變種，資安威脅數量與攻擊管道大幅增加。多家資安公司指出，目前網路作業系統出現了一個名為「Shellshock」(或稱「Bash Bug」)的重大漏洞，影響全球大約五億台網站伺服器和其他連網裝置，包括手機、路由器、網站主機、醫療裝置等，讓有心人士遠端透過惡意程式操作伺服器，可導致企業機密和個人隱私外洩，嚴重甚至可使網站服務中斷，或變成殭屍電腦攻擊指定目標。外電報導，美國政府的電腦緊急應變小組和科技專家已發出警告，Shellshock會影響「以Unix為基礎的作業系統」，包括Linux和蘋果Mac OS等部分電腦作業系統存在漏洞，駭客恐利用此漏洞發動攻擊[2]。

貳、無形戰爭資訊安全威脅無所不在

資訊戰可分為防衛資訊戰與攻擊資訊戰(Defensive Information Warfare and Offensive Information Warfare)，現階段國際情勢為後冷戰時期，中共隨戰爭形態改變進行軍事事務改革，積極投入信息化作戰的研究，中共藉由提升軍隊高科技及高技術的電子化作戰能力，藉由惡意程式攻擊以竊取國防重要機密資料和攻擊以癱瘓對方軍事內部系統及擾亂社會經濟秩序。中共信息化戰爭透過通資網路與航太

通訊科技技術以惡意程式採取攻擊性資訊破壞作為，我國所面對的資訊安全威脅，除戰略資訊作戰外，還包括媒體文宣、心理宣傳等方式，並對我國家，政治、經濟、金融、社會及軍事等方面進行計畫性資訊作戰，戰術指管作戰、傳統作戰、戰略資訊作戰，其影響的層面相當廣泛。資訊戰可區分為資訊取得、探測、傳輸、處理、顯示、存儲、使用等技術，而資訊戰攻擊行為目的就是取得控制權，資訊戰攻擊行為一方面表現則為通過資訊技術手段對自身資訊取得、處理、傳輸、使用等的控制，表一為資訊系統安全衡量表，表二為資訊系統安全維護技術分析表[3-4]。

表一、資訊系統安全衡量表(自行整理)

特性	資訊系統安全特性衡量
資訊保密性(Confidentiality)	保證資訊不洩漏給未經授權的人
資訊完整性(Integrity)	防止資訊被未經授權的篡改，保證真實的資訊不失真的送達目的地
資訊可確認性(Authenticity)	可確認性表示出資訊之來源可以無誤的辨識
資訊可用性(Availability)	保證資訊確實為授權使用者所用，防止電腦病毒或相關人為因素造成系統拒絕服務權限管理
不可否認性(Non-repudiation)	不可否認特性可以保證資訊行為人不能否認自己的行為

表二、資訊系統安全維護技術(自行整理)

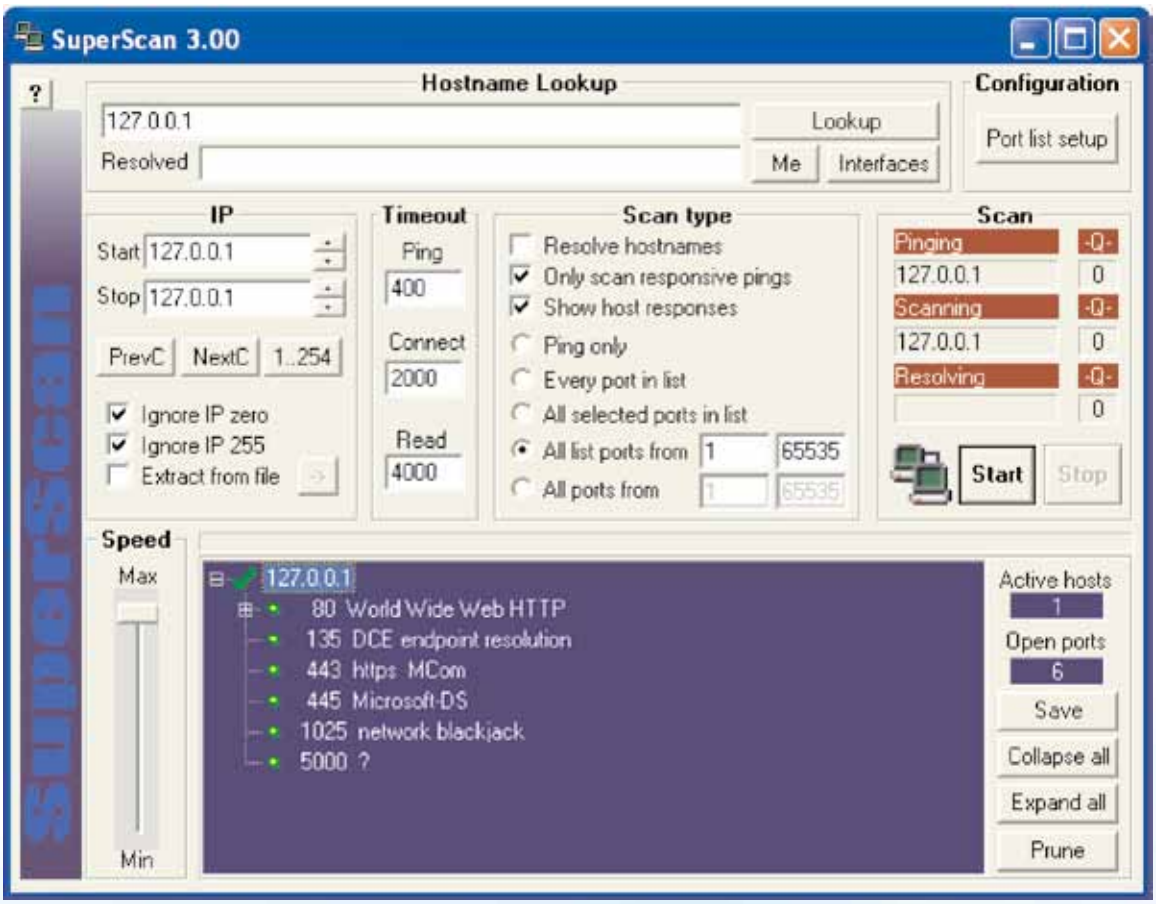
技術	資訊系統安全維護技術
植基於密碼學資訊安全基礎建設	對儲存資料進行加密處理與為保障資料傳輸安全建置公鑰基礎建設等
加強作業系統安全防護	作業系統是資訊系統中樞必要時須採行隔離措施
強化資料庫安全	對儲存資料加密，保障一致性，對資料維護統整性，並防範統計攻擊
保護網路安全作為	安裝防火牆、防毒軟體或實體隔離等措施

圖一、美軍資訊管理弱點掃瞄示意圖[6]

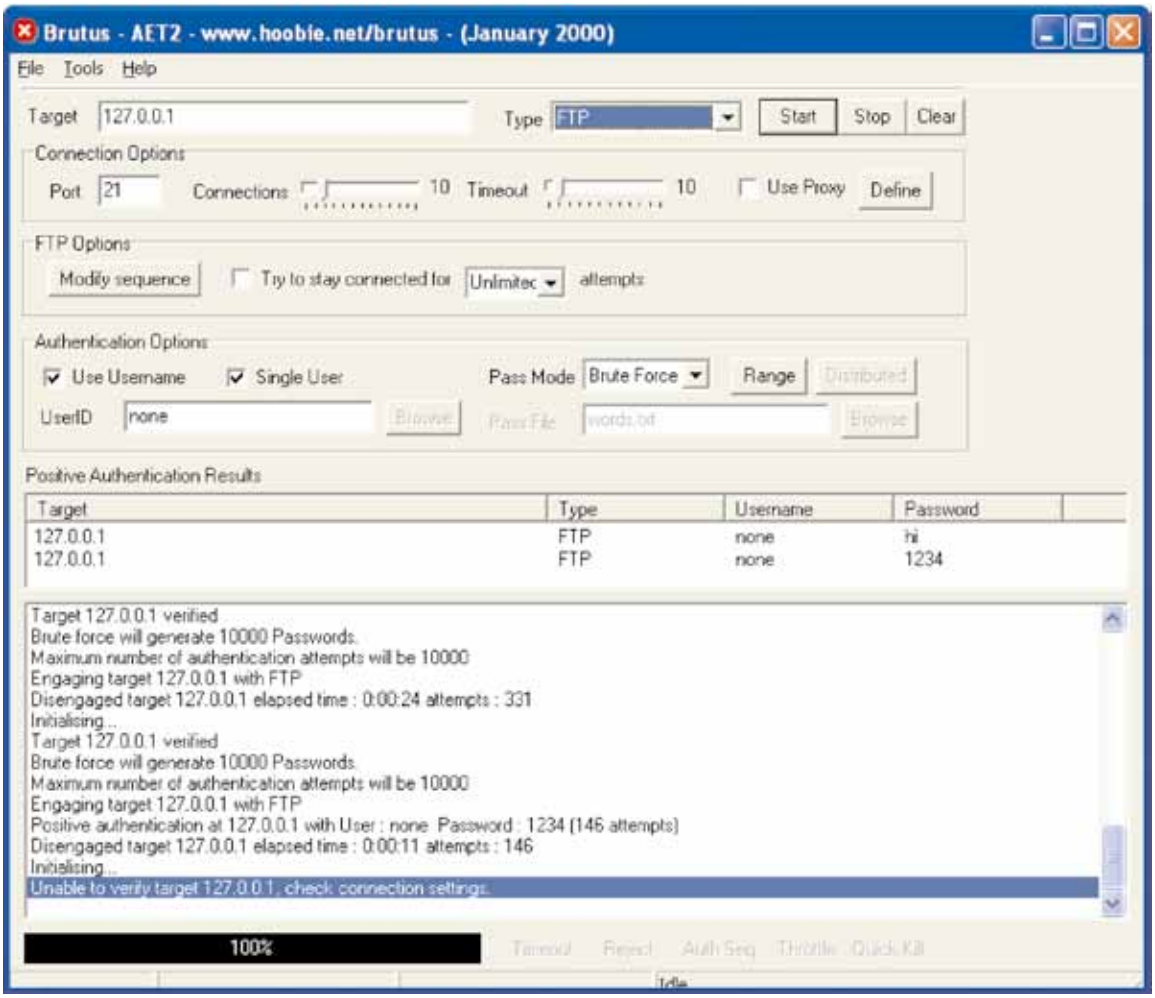
2013年2月10日，美國《華盛頓郵報》刊載美國國家情報委員會《國家情報評估》結論：美國是大規模、持續性網路間諜活動的目標，威脅著美國經濟競爭力，中共是意圖滲透美國企業機構電腦系統的最積極國家。美軍有鑑於資訊科技發展健全與否嚴重攸關國防戰力提昇，因應戰略考量遂對電子戰武器不斷提昇與更新，而美軍對武器系統發展的指導

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，圖一為美軍資訊管理弱點掃瞄示意圖。面對現代資訊安全威脅，資訊安全網路攻防議題須重視如何爭取資電優勢，尤其是能掌握資訊戰多層次與縱深防禦理論技術，並且加強人員的教育訓練防止資料外洩建立資訊安全風險管理觀念以落實多層次防護[5]。

資安威脅無處不在，惡意程式攻擊日新月異，舉例說明，2009年6月底伊朗爆發首座核電廠遭到Stuxnet蠕蟲惡意程式攻擊，2010年初Google報導Gmail受到中國2014年NSS Labs防毒軟體測試報告報告研究中全球雲端資安領導廠商趨勢科技針對國人上網行為進行調查，跨平台上網已成為全民運動，惡意威脅因應跨平台趨勢不斷衍伸變種，資安威脅數量與攻擊管道大幅增加。由於缺乏資安意識與防護未隨之提高，台灣不僅為全球最常造訪惡意網站的前五名，網路詐騙案件更較去年成長123%，相當容易誤觸資安地雷。因應跨平台上網風潮，惡意程式不斷變形，惡意



圖二、SuperScan資訊管理弱點掃瞄示意圖[11]



圖三、Brutus Password Cracker通行碼破密技術示意圖[11]

威脅數量及傳播管道都大幅提升。針對端點安全防護技術研究，SuperScan的是一個強大的TCP端口掃描器，包括一個額外的網絡工具，如各種的ping，traceroute的，使用HTTP HEAD，Whois，圖二為SuperScan資訊管理弱點掃瞄示意圖，它採用多線程和異步技術，形成極其快速和多功能掃描。可以執行ping掃描和端口掃描使用任何IP範圍，或者指定一個文本文件中提取地址。其他功能還包括HTML報告，TCP SYN掃描，UDP掃描，內置端口的描述數據庫，Windows主機列舉，banner grabbing。針對Brutus Password Cracker通行密碼破密技術說明，AET2通行碼破密技術authentication方式包括HTTP(Basic Authentication)、HTTP(HTML Form/CGI)、POP3、FTP、SMB與Telnet，圖三為通行碼破密工具之暴力攻擊方式技術示意圖[6-12]。

根趨勢科技研究發現，2014年第二季所攔截之惡意檔案數量高達31億，較2013

年成長一倍，每月平均攔截58億個威脅，截至今年7月更有1,000萬筆個資遭到外洩；據今年11月《蘋果》壹傳媒遭受駭客攻擊可觀察中共的網軍攻擊更進化，被駭的型態從打掛網路伺服器的阻斷式攻擊(Denial of Service，DoS)，變成竄改、刪除網站後台資料庫的穿透式攻擊，且祭出簡稱APT(Advanced Persistent Threat)的「先進持續威脅」，用釣魚信、社群網路、程式漏洞、木馬程式等技術送出客製化病毒惡意程式攻擊。由於民眾喜愛瀏覽社群網站、看網路新聞與影片，駭客常透過熱門新聞、話題關鍵字或影片散播釣魚網站連結及惡意程式，社群網站、即時通訊軟體也常作為惡意威脅傳播平台或詐騙管道。大多數企業、政府單位所面臨的資訊安全問題，主要來自於病毒、間諜程式、惡意程式入侵等問題，在使用者瀏覽網站或是下載軟體的過程中，經常會不小心的在電腦被植入木馬而不自知。由於我政府及國人行動裝置，包括智慧型手機、平板等需求持續攀升，去年就達到1053萬人，中共除持續攻擊政府網通裝備外，研判將著手研製各類惡意行動APPS應用程式，駭侵個人行動裝置，以從中竊取特定目標敏感資訊，如電郵帳密、通聯情形甚至通話內容。據政院統計，2013年政院平均每周遭遇近2000次網路攻擊，每月約有450次電子郵件攻擊。除了政院外，中國網軍偏好攻擊的部會網站，包括手握大筆機密資料的外交部、國防部。而涉及兩岸談判部會，像經濟部、財政部、衛福部等，也是中國網軍熱門的偷盜對象。此外由於作業系統、應用程式本身的安全性漏洞，很可能被駭客加以利用，經由外部網路連線入侵到企業內部網路，竊取重要機密資料[3-6]。

一旦機密資料經由間諜程式、駭客入侵竊取，便有可能導致機密資料被販賣、勒索，輕則戰演訓資料外流影響軍譽，重則對國家目標與國家安全利益造成更大更深遠的不利影響，我們因此更需小心謹慎。根據報導2014年11月在立法院質詢報告中國安局長李翔宙證實，中共網路戰總體戰力有18萬人，目前我國正在規劃在情治單位設立「網軍」。此外，國防部次長高天忠表示，我國軍目前僅是進行電子防護，並以模擬紅軍方式對國軍進行攻擊與防護。李翔宙指出，中共網路戰任務分工於總參各部、7大軍區、國防科研機關與各級院校等，平時主責網路竊密及滲透、戰時負責網路攻擊，並暗中扶植民間駭客組織從旁協助「網路間諜」活動，據「美中經濟委員會」報告評估，中共網路戰總體戰力約18萬人；另成立「中央網絡安全及信息化領導小組」，以統合相關部會職能，藉頂層設計、統籌規劃、創新發展，努力將中共建設為網路強國。對於中共網軍攻擊的手法，李翔宙表示，中共先廣泛蒐集我政府部門、學研機構、黨團組織等人員或幕僚個資後(含電郵帳號、工作職務、聯絡電話等)，並選擇適當時機，如新聞事件、首長行程等，利用「社交工程

」手法。採外圍到核心關聯方式，散佈惡意郵電誘騙目標開啟。另外中共也會在惡意程式內崁入動態或特定網址，導向已部署完成中繼站後，再採遠端連線通道保護方式操控中繼站，遂行滲透竊密或實施毀癱攻擊。依據調查指出，國安局2013年公開網站遭到侵擾達到722萬次6657次，其中惡意行為次數計有23萬8764次，均遭到國安局所偵測與阻絕，未產生危害。然而，現在各政府部門資訊系統、網防設備等，多採委外方式研建或維管，中共利用這項漏洞，輾轉駭侵各機關委外廠商、軟體開發或服務供應商，盜用廠商維管人員遠端管理權限，迂迴遂行網路滲透陰謀，觀察對我攻堅範圍有擴大情形[6-8]。

參、重視網路漏洞落實資訊安全防護

根據《防衛科技》網站報導，美國海軍一支全新「網路警示特遣部隊」(TFCA)於2014年8月成軍，這支部隊將致力於建立網路通訊協定、找出網路安全漏洞、加強網攻威脅警示，並強化登入美國海軍內部網路的安全性。因為現代武器愈來愈仰賴網路，在操作平台與系統製造出大量的數位資訊，領導TFCA的史瓦茲表示：「我們在數年前開始發現，網路攻擊所造成的損害已不可同日而語時，建立這支部隊的想法也隨之而生。」。App廠商在行動App開發時，經常進行前後端的分包，而鮮少將後端控制運用搭配於前端手機應用程式中，而後端亦忽略了行動平台的特殊性而疏於伺服器安全的防護措施，包含後端的服務、API、資料庫、網站本身等，App後端需要有對應的Web Service提供服務，同樣會存在SQL Injection(資料隱碼注入攻擊)問題、應注意資料傳輸過程中的保護，如SSL安全性、Session是否有抵抗重送攻擊以避免被截錄後利用、傳輸的資料是否敏感，如身分證字號、卡號、密碼應避免在網路上傳輸等[2]。OWASP(Open Web Application Security Project)是一個開放社群、非營利性組織，其主要目標是研議協助解決Web軟體安全之標準、工具與技術文件，協助瞭解並改善網頁應用程式與網頁服務的安全性基本的網站安全，基本網站安全風險表整理如表三。OWASP Top 10 Mobile Risks所提到十種行動裝置風險類型，整理「電腦系統資訊安全檢測辦法」如表四。加密演算法是安全防護的最後一道防線，當駭客取得了帳號密碼，可以簡單地使用一些破解軟體包括線上服務進行破解[3-8]。

由於網路使用的普及性，導致駭客無所不在，所呈現出的是一場「看不見敵人的戰爭」，現代戰爭勝負幾乎取決於瞬息之間，任何軍事機密如被敵人刺探掌握，均可能造成勝負逆轉的關鍵性影響[7]，資訊時代來臨影響所及，隨著資訊安全與網路威脅發展，當今我們所面對的真正威脅，已不再只是單一國家或其內部的軍隊系

表三、OWASP Top 10網站安全風險分析表(自行整理)

攻擊類型	基本網站安全風險分析
Injection(注入攻擊)	網站應用程式執行來自外部包括資料庫在內惡意指令，SQL Injection與Command Injection等攻擊包括在內。
Cross Site Scripting (XSS)(跨站腳本攻擊)	網站應用程式將執行請求送回瀏覽器執行，使得攻擊者可擷取使用者的Cookie或Session資料而假冒登入為合法使用者。
Broken Authentication and Session Management(身分驗證功能缺失)	身分驗證功能缺失風險分析如下，網站應用程式中自行撰寫的身分驗證相關功能有缺陷。例如，登入時無加密、SESSION無控管、Cookie未保護、密碼強度過弱等等。
Insecure Direct Object References(不安全的物件參考)	攻擊者利用網站應用程式本身檔案讀取功能任意存取檔案或重要資料。進一步利用這個弱點分析網站原始碼、系統帳號密碼檔等資訊，進而控制整台主機。
Cross Site Request Forgery (CSRF)(跨站冒名請求)	(CSRF)(跨站冒名請求)風險意指已登入網站應用程式的合法使用者執行到惡意的HTTP指令，但網站卻當成合法需求處理，使得惡意指令被正常執行。
Security Misconfiguration(安全性設定疏失)	系統的安全性取決於應用程式、伺服器、平台的設定。所有設定值必須確保安全，避免預設帳號、密碼、路徑。
Failure to Restrict URL Access(限制URL存取失敗)	網頁因為沒有權限控制，使得攻擊者可透過網址直接存取能夠擁有權限或進階資訊的頁面。例如管理介面、修改資料頁面、個人機敏資訊頁面洩漏等等。
Unvalidated Redirects and Forwards(未驗證的導向)	網頁應用程式將使用者Forward或Redirect至有驗證機制的頁面或網站。攻擊者可將受害者導向至釣魚網站或惡意網站，甚至存取受限制的資源。
Insecure Cryptographic Storage(未加密的儲存設備)	網站應用程式沒有對敏感性資料使用加密、使用較弱的加密演算法或將金鑰儲存於易取之處。
Insufficient Transport Layer Protection(傳輸層保護不足)	網頁應用程式未在傳輸機敏資訊時提供加密功能，或者是使用過期、無效的憑證，使加密不可信賴。舉例說明如：攻擊者竊聽無線網路，偷取使用者cookie；網站憑證無效，使用者誤入釣魚網站。

統，而是一種具有全球性滲透的特性，以及呈現倍數成長的網路攻擊事件。網路攻擊已成為一種新的戰爭形態，它可能對國家目標與國家安全利益造成更大更深遠的不利影響。資訊安全則是隨著我國資訊系統運用的普及化，資訊及網路安全已成為日趨重要的國家安全課題，而且國家安全目的是準備戰爭或從事戰爭，進而追求與保障和平[8]。微軟2014年11月25日公布一份全球七大數位犯罪趨勢報告，指出亞洲已經成為駭客攻擊的一級戰場。有鑑於此，微軟去年底時已經成立數位犯罪防治中心(Digital Crime Unit)，並組成國際專業團隊，以大數據分析及定位技術協助執法單位偵搜數位犯罪區域，讓駭客及殭屍病毒等犯罪手法無所遁形[9]。

在行動App開發時，經常有不同的承包商進行前後端的分包，前端App與後端Web Service傳輸過程沒有使用HTTPS而使資料暴露，針對Web攻擊類型分析如表三。值得注意的是，部分App直接與後端資料庫直接連通，導致資料庫傳輸內容亦暴

露於網路。而App廠商鮮少將後端控制運用搭配於前端手機應用程式中，而後端亦忽略了行動平台的特殊性而疏於伺服器安全的防護措施，包含後端的服務、API、資料庫、網站本身等，App後端需要有對應的Web Service提供服務，同樣會存在SQL Injection(資料隱碼注入攻擊)又稱為SQL指令注入攻擊問題、應注意資料傳輸過程中的保護，如SSL安全性、Session是否有抵抗重送攻擊以避免被截錄後利用、傳輸的資料是否敏感，如身分證字號、卡號、密碼應避免在網路上傳輸等。檢測App本身處理資料儲存與該資料的保

表四、OWASP行動裝置風險類型表(自行整理)

攻擊類型	行動裝置安全風險分析
M1-Weak Server Side Controls	伺服器端安全控制脆弱
M2-Insecure Data Storage	不安全的資料儲存於用戶端
M3 - Insufficient Transport Layer Protection	傳輸層保護不足
M4 - Unintended Data Leakage	非故意/意外造成資料外洩
M5 - Poor Authorization and Authentication	身分鑑別與授權機制不嚴謹
M6 - Broken Cryptography	加密方法不嚴謹或失效
M7 - Client Side Injection	用戶端注入攻擊
M8 - Security Decisions Via Untrusted Inputs	對於不受信任輸入來源的檢測處置
M9 - Improper Session Handling	連線階段處理不適當
M10 - Lack of Binary Protections	封裝檔案保護不足

表五、Web攻擊類型分析表(自行整理)

項目	Web 攻擊內容
Cross-site scripting	中文翻譯為跨站腳本攻擊 Web 應用程式直接將來自使用者的執行請求送回瀏覽器執行，使攻擊者可擷取使用者的 Cookie 或 Session 資料，而能直接登入成使用者。
Injection Flaw	Web 應用程式執行來自外部包括資料庫在內的惡意指令，SQL injection command injection 等攻擊都包括在內。
Malicious File Execution	Web 應用程式引入來自外部的惡意程式檔案，並執行檔案內容。
Insecure Direct Object Reference	攻擊者利用 Web 應用程式本身的檔案讀取功能，任意存取檔案或重要資料。
Cross-site Request Forgery	已登入 Web 應用程式的合法使用者，執行惡意 HTTP 指令 Web 應用程式卻當成合法需求處理，使得惡意程式卻被正常執行。
Information Leakage	Web 應用程式的執行錯誤訊息包含了敏感資料，舉例來說錯誤訊息顯示了系統檔案路徑。
Broken Authentication and Session Management	Web 應用程式中，自行撰寫的身分驗證相關功能缺陷。
Insecure Cryptographic	Web 應用程式沒有針對敏感型資料使用加密，或是使用較弱的加密演算法，甚至將金鑰儲存在容易被取得之處，都是這類攻擊的起因。
Insecure communication	在傳送敏感資料時，未搭配使用 HTTP 或其他加密方式。
Failure to Restrict URL Access	某些網頁因為沒有權限控制，使得攻擊者可透過網址直接存取，允許直接修改 wike 或 Blog 網頁內容等行為。

護方式包含將用戶敏感資訊、系統敏感資訊存放於用戶端裝置中，而未給予適當的保護，可能造成這些資料被存取、解析來使用，間接造成其他傷害，表五為Web攻擊類型分析[8-10]。

表六、電腦系統資訊安全檢測辦法(自行整理)

檢測類型	電腦系統資訊安全檢測項目
網站安全檢測	原始碼檢測或黑箱檢測、網站目錄與存取權限、滲透測試、異常處理與弱點掃描
安全設定檢視	AD群組原則、檢視Firewall與VPN、ACL(存取控制清單)與特權管理監控
網路架構檢視	建立資訊系統安全基準進行網段劃分、單點故障最大衝擊與風險承受力分析
設備安全檢測	網路設備、伺服器與終端機更新管理、金鑰管理、系統密碼複雜度及檢測系統設定等設備檢測
網路活動監測	網路設備與伺服器存取紀錄、封包側錄、資訊設備監控記錄、識別及警示機制

對於資安漏洞安全防護，資訊風險管理技術作網路封包分析，除了能夠找出異常的行為和網路流量之外，也可以用來學習各種不同通訊協定，是網路管理人員不可或缺的技能。網路提供使用環境，人類是網路的使用者，許多在真實社會發生的事件，仍然會在網路上重演，但是更為隱匿，這也是發展資訊安全技術的重點所在。在App與後端的資料傳輸過程中，未施以合適的傳輸層保護，如其中有重要的資料傳輸，則容易被揭露或攔截使用。開發者將API的Key Chain、密碼與商業邏輯撰寫於App中，這樣可能會被逆向分析出原始資料或動態執行時遭到截取，而導致敏感資料洩漏。App與後端溝通時，使用明碼的身分識別與密碼，或部分App將身分鑑別與授權內容綑綁行動裝置UDID或IMEI，可能導致未來裝置遺失時有更高的風險，表四為電腦系統資訊安全檢測辦法。應用程式可能經由惡意攻擊者精心設計，或是應用程式遭攻擊者透過Client Side Injection攻擊方式來消耗可攜式行動裝置的硬體資源或提升權限情形。行動平台檔案也有可能被逆向分析而發現其中的明文訊息或隱藏資訊，若透過簡單的工具即可做到還原大部分的內容，則保護便顯得不夠充足，表六為電腦系統資訊安全檢測辦法[11-15]。

自2008年起，先進惡意軟體Regin就已經被用於針對許多跨國目標的系統性間諜活動中，Regin是一款複雜的後門木馬惡意軟體，其結構設計具有罕見的技術能力。根據攻擊目標，Regin具有高度可定制化功能，能夠使攻擊者通過強大的框架進行大規模監視，並且已經被用於監視政府機關、基礎設施運營商、企業、研究機構甚至針對個人的間諜活動中。資安人編輯部於2014年7月31日專欄報導指出2014年十大資安技術以利資安管理者掌握最新的技術趨勢規劃與執行資安風險管理計劃，2014年十大資安技術整理如表七[4]。

表七、2014年十大資安技術與安全檢測分析表[4]

資安技術	電腦系統資訊安全檢測項目
雲端存取安全中介服務(Cloud Access Security Brokers; CASB)	雲端存取安全中介服務是一套可以在企業內或雲端運作的軟體，位於雲端服務使用者與供應商之間，負責在員工存取雲端資源時套用企業安全政策，通常具有加解密、稽核、防制資料外洩(DLP)、存取控制、與異常行為偵測等功能。
適應性存取控制(Adaptive Access Control)	適應性存取控制是一種基於內容感知的存取管控機制，其具備內容感知與動態降低風險兩種特性。所謂內容感知是指，根據提出資料存取請求時的狀況。
沙箱分析(內容引爆)及入侵指標(IOC)確認	沙箱分析可能在雲端或資安設備端進行，運作模式為將郵件附加檔案或網址連結先丟到沙箱去運作，倘若內含惡意程式，可以模擬惡意程式在端點執行後可能會有的行為。
端點偵測及回應解決方案(Endpoint Detection and Response Solutions	從端點(平板、伺服器、桌上型電腦與筆記型電腦)找出駭客在內網擴散軌跡，透過掃描工具分析網路拓撲、透過 NG-IPS 或網路封包側錄工具(Sniffer)進行分析，進行端點行為分析及端點鑑識以防禦 APT 攻擊。
新一代安全平台的核心：巨量資料安全分析	面對大量資料(Big Data)儲存、管理、處理、搜尋、分析與智能應用等處理資料的能力也將面臨新的挑戰，建立安全資料倉儲存放監控資料支援回溯分析，藉長期資料儲存分析，納入情境及外部威脅與社群情報，建立正常行為模式，進而利用資料分析來發覺真正偏離正常的情況。巨量資料分析強調偵測並立即回應違規行為。
機器可判讀的威脅情報，包含信譽評等服務	判斷是否允許終端使用者存取內部網路或資料時，除了可以考慮使用者身份與當下所使用的裝置外，也可將 URL 和 IP 位址的信譽評等納入決策因素裡。
建立控制和隔離為基礎的資安策略	在病毒與惡意程式變化速度加快的情況下，傳統依賴特徵碼來判讀的方式效果有限，新的策略是將所有未知執行檔都視為不可信賴，並傳送至隔離環境加以執行，如此就不會對日常運作系統造成損害，也無法利用該系統當成跳板，攻擊其他資訊系統。
軟體定義的資安	隨著 CPU 運算效能提升，讓軟體定義的資安具備可行性，將原本各自獨立的資安設備集中在一個硬體上，再透過軟體去實現各種不同的資安功能。
互動式應用程式安全測試	應用程式的安全測試分成動態與靜態兩種，動態應用程式安全測試(DAST)是從外部入侵(Outside in)的角度來測試 AP 有沒有安全漏洞，靜態應用程式安全測試(SAST)則是由內而外(Inside out)，檢視原始碼、位元碼與二進位程式碼有沒有問題。
針對物聯網的安全閘道、中介服務與防火牆	從傳統專屬通訊協定走向標準化網際網路通訊協定(IP)，形成相連的物聯網環境，資安風險也跟著大幅增加，營運設備高度自動化，不需要人為介入彼此通訊，使得資安防禦變得更重要。

肆、資訊安全網路風險管理作為與結論

針對資訊安全風險分析，近年來中共駭客屢遭各國政府、跨國企業指控竊取軍事或商業重要機密資訊可知，中共在國際間諜活動相當頻繁，所涉及國家廣泛，且

目標與手段多元，從破獲的案例更可看出，其情蒐部署的時間往往長達數年以上。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[16]。資安攻擊手法越來越精密，突破傳統資安防線不再是件困難的事，病毒、惡意程式與資安功擊型態變化的速度越來越快，駭客資料探勘利用whois查詢、nslookup查詢以發掘一些潛在的IP位址範圍、員工姓名、電話號碼、網域名稱伺服器、郵件伺服器等等的資訊。為了快速掌握威脅情資，新一代資安平台多半具備整合與自動判讀外界情報資料的能力。針對APT鎖定特定目標的攻擊手法，資安防禦新思維為如何在第一時間察覺入侵跡象，讓駭客無法造成太大損失或匯出敏感資料，成為防禦此類攻擊手法的關鍵，資安技術廠商開始在設備中引進沙箱技術(Sandbox)，包括APT解決方案、次世代防火牆、郵件閘道器等結合沙箱技術的工具。從沙箱技術來看，目前分成模擬器(Emulation)與虛擬化(Virtualize)兩種，模擬器技術沙箱透過底層硬體直接記錄與分析，比較不需要在作業系統額外安裝系統分析工具，相較於虛擬化技術的沙箱來看，比較不容易被惡意程式偵測出沙箱環境。模擬器技術的沙箱是藉由分析CPU指令集以及觀察記憶體的存取資訊，來判斷惡意程式與行為，避免因為應用程式與版本的差異而無法分析出惡意程式的風險[17-18]。

在風險管理技術研討方面，2014年3月推出的軟體定義防護安全架構(Software-defined Protection，簡稱SDP)，該架構分成三個不同的層次：管理層、控制層與執行層，透過統一的管理層，使用者能夠統一指揮安裝在執行層上的各種資安模組，並且可以在單一的主控台上，看見所有發生在網路底層中的事件。事實上，軟體定義資訊安全型態的軟體定義網路(Software-Defined Networking，簡稱SDN)技術，隨著發展日趨成熟，有些資安服務也可以透過SDN來提供。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，現今資訊作戰形態已無平戰時區分，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。網路致能作戰(Network-enabled Operation)運用迅速分享的構聯網路傳遞訊息，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，為能洞燭敵情掌握優勢，我們不得

不重視相關發展。

值得注意的是，針對資訊戰發展分析，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，轉變為包括企圖採駭客與惡意程式等資訊戰攻擊或破壞我方的C4ISR系統。面對近年我國政府機關及民間企業屢遭駭客組織與惡意程式入侵，國軍網路安全同樣面臨嚴峻挑戰，鑑於此，國防部除訂頒「國軍資訊安全」相關規範，嚴格落實資訊安全風險管控措施外，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」的因素著手建立正確觀念。網路防護可說是創新及不對稱戰力的重要憑藉，國軍為政府整體安全防護的一環，依行政院指導，負責網際防護體系的國防分組，以國軍網路防護為核心，負責規劃、推動資安防護及應變等工作。國防部將致力推動各項資安防護作為，確保資通安全。網路防護可說是創新及不對稱戰力的重要憑藉，國防部致力推動各項資安防護作為，確保資通安全，國防部依行政院政策指導，積極投入國防資源從事相關整備，以提升我國網路空間整體戰力；另國軍面對網路駭客不斷的攻擊，除持續落實風險管理機制以掌握網路威脅型態，並要求所屬單位綿密各項資訊緊急應變機制，以提升國軍整體網路安全管理與防護能量。建立包括防火牆、入侵偵測即時回應系統及誘捕系統，防止不當惡意網路連線，此外，也將建立國防部資訊網路中央防毒系統，運用集中控管、病毒碼派送機制，建立完整防毒系統與避免違規情事肇生，建立安全的資訊作業環境，進而強化國軍整體資訊安全防護能力[19-22]。

伍、參考文獻

〔1〕Information Security資安人科技網，“台灣名列全球惡意網站造訪第五名防護刻不容緩”，2014年10月3日，取自資安人科技網。

〔2〕Information Security資安人科技網，“金融資訊安全現況探討(下)以行動應用爲媒介的攻擊思維”，2014年6月25日，取自資安人科技網。

〔3〕E-NEWS，“Web Security網站安全基礎篇(二)，”2010年第15期，取自中央研究院計算中心通訊電子報。

〔4〕資安人科技網，“掌握未來十大資安技術，有效做好攻擊防禦”，2014年7月31日，取自資安人科技網。

〔5〕資通安全資訊網，“國家資通安全會報”，2014年1月3日，取自第201401002期資通安全資訊網電子報。

〔6〕美國國防部，《2010四年期國防總檢報告》(Quadrennial Defense Review Report， QDR)，2010年2月1日。

〔7〕陳清泉，“制霸網路者，制霸世界，”2014年8月14日，取自蘋果日報。

〔8〕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。

〔9〕資通安全資訊網，“國家資通安全會報”，2014年11月26日，取自第2014011018期資通安全資訊網電子報。

〔10〕李忠憲，“未來戰爭是數位戰爭”，2014年7月26日，取自蘋果日報。

〔11〕賴溪松，“資訊倫理與資訊安全”，成功大學電機工程系，http://www.twisc.ncku.edu.tw。

〔12〕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。

〔13〕Benson，“資安危機就是國安危機系列之三台灣可以成爲資安強國”，2014年7月24日，取自蘋果日報。

〔14〕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。

〔15〕林盈達，“媒體被駭政府怎能置身事外－資安危機就是國安危機系列之一”，2014年7月22日，取自蘋果日報。
〔16〕編譯崔敬熙/綜合外電報導，“加強防駭美軍網路特遣隊成立”，2014年10月28日，取自青年日報網。
〔17〕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。
〔18〕青年日報社，社論：恪遵保密規定確保軍機安全，2013年12月9日。
〔19〕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。
〔20〕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。
〔21〕青年日報社，“國軍落實資安防護整備-嚴防駭客攻擊手段”，2014年11月20。
〔22〕賴溪松，“資訊安全稽核”，成功大學電機工程系，http://www.twisc.ncku.edu.tw。

作者簡介

上校教授　吳嘉龍

學歷：中正理工學院48期電機系電子組、美國空軍理工學院電腦工程研究所、國防大學理工學院國防科學研究所電子工程組。經歷：電子官、區隊長，教官、講師、助理教授、科主任、校教評秘書、副教授、教授、系主任、資圖中心主任。現職：航空通訊電子系上校專任教授兼任資圖中心主任。專長領域：資訊戰，通資安全，無線通訊，網路通訊協定。