資訊安全

網路攻防理論策略發展與資訊安全研究分析探討(上)

教授　吳嘉龍

提要

21世紀資訊科技運用的普及與網際網路的蓬勃發展，使資通訊科技應用儼然已成為每個人日常生活中的一部份，並改變了人類生活模式，然令人擔憂的是資訊科技帶來的資通訊安全問題，促使資通訊安全議題成為各國關注的焦點。網際網路為人類帶來便利與快捷，然而伴隨網路普及化與消費者行為改變，引發的網路犯罪及個資保護等課題，已逐漸成為影響國家安全、社會安定的隱憂，全球正面臨嚴峻的資安威脅。網路戰爭定義為一個民族國家為滲透另一個國家的電腦或網路進行破壞和擾亂的行為，中國大陸自1985年起開始積極發展網路戰能量，中國網軍於2006年積極展開先進持續威脅APT(Advanced Persistent Threat)攻擊模式，據報導網軍目前已突破18萬人，結合客製化病毒文件或連結的釣魚信、社群網路、程式漏洞以及後門程式等技術，先鎖定目標對象之社群朋友，將客製化的惡意程式包裝於文件檔案中，透過寄釣魚信先感染任一社群朋友，待此朋友寄信給目標時再將惡意程式包裝於文件，利用朋友間的互信感染目標，然後長期監控目標。我國政經情勢特殊，面對全球詭譎複雜多變的資通訊環境，以及日益嚴重的資通訊安全威脅，持續落實建立資訊優勢並精進各項資通訊安全防護工作，實屬必要。中國在2009年底時以APT模式攻擊美國32家高科技公司竊取資料，經美方調查，攻擊源頭為中國兩個大學，後續還發現多個類似手法的攻擊團隊。因應網路惡意程式攻擊威脅，美國自2009年成立「美國國防部網戰司令部(United States Cyber Command)」，整合全軍資源在網路上進行全面攻防作戰。網路聖戰惡夢一旦成真，所帶來的全球性災難將讓各國付出慘痛代價，本文針對網路攻防理論技術策略與資訊安全科技發展發展分析研究，以有效強化資安意識與建立資訊優勢確保國防安全。

關鍵字：網路戰爭、惡意程式攻擊、資訊安全、資訊優勢、網路資安威脅。

壹、前言

網路戰爭定義為「一個民族國家為滲透另一個國家的電腦或網路進行破壞和擾亂的行為」，並已成為全世界各國的首要任務。軍事戰略規劃目的在使國家武力之整建、發展與運用等一切軍事工作，能在整體考量下，密切協調配合，循一定之目標、戰略構想與統合之政策，做有系統之規劃與建設，以達成創機先制與危機應變的有效國防。實體世界恐怖攻擊採取不對稱戰爭形態，多數選定製造社會恐慌不安的對象、公共建築或政府機關進行攻擊；虛擬世界的網路戰爭，輕則癱瘓電信、商務網路，重則攻擊依靠電腦運作的鐵路運輸系統、油氣輸送管線、核電廠等，造成實體破壞的後果更難以想像，摧毀國家安全或危害人類的威力，更甚於恐怖攻擊。隨著資通訊科技日益蓬勃發展，如何提供安全、安心、可靠的網際網路使用環境，創新資安服務價值，掌握雲端運算優勢，朝向虛擬整合化資安服務，已成為邁向優質網路社會的關鍵議題。網路戰爭的攻擊是永無止盡的，在確立明確的攻擊目標、目的、時間後，執行單位就會開始規劃長期的攻擊計劃。以2013年3月份南韓Dark-Seoul攻擊事件為例，傳言北韓花了8個月的時間規劃攻擊，入侵防毒軟體更新伺服器，利用其更新機制將32000台電腦植入後門惡意程式(Backdoor program)，並刪除電腦資料使其無法啟動，更嚴重的是其中也包含了ATM提款機，這次事件除影響部分銀行停止運作，更造成南韓股市嚴重大跌[1-3]。

根據賽門鐵克網路安全威脅研究報告指出，臺灣有6成垃圾郵件夾帶惡意程式，我國垃圾郵件氾濫的比例從2012年的2.1%(名列全球第十二名)到2013年則增加為5.5%(名列全球第四名)，而駭客利用垃圾郵件夾帶惡意程式或惡意連結的比例，甚至高達6成(64.2%)以上。行動裝置上的惡意程式，也已經到倍數成長的狀態。像是趨勢科技也預測，2015年Android手機惡意程式將從2014年的400萬個，暴增到800萬個，不論是一般網路或者是行動裝置的網路威脅，越來越嚴重。我國一直以來都是被網軍鎖定的對象，依據趨勢科技調查，我國高科技企業一年有364天遭駭客入侵，是全球平均220天的1.5倍，且政府長達8.5個月才發現被駭。面對中國網軍部隊威脅，行政院資通安全辦公室主任蕭秀琴表示，台灣已成為中國駭客試驗場域、資安環境相當嚴峻，未來政府單位將分級因應，尤需加強日趨增多的進階持續性威脅ＡＰＴ網路攻擊的防禦，資安依據保密等級區分成Ａ、Ｂ與Ｃ三級分級管理，凡是涉及業務機密性、關鍵性基礎設施、全國性事務者列為Ａ級，如國防部、外交部、台電公司、內政部戶政司等，並依序類推Ｂ級與Ｃ級。Ａ級單位應建立自己的資安監控中心(Security Operation Center，簡稱SOC)，以達到聯防作用。行

政院資通安全辦公室表示，目前最多的攻擊方式就是ＡＰＴ，這是一種駭客長時期低調潛伏在網路中研究，以現有技術很難發現，但是一旦他們偷資料，ＳＯＣ就會發現。科技部表示，資安中心業務範圍包括攸關國家安全而需對外保密或民間產業無能力執行的資安業務，在遭遇資通攻擊或威脅情況下，支援及協助相關單位進行反制等。成立經費2.6億元，成立後將擴增至3.2億元，中心人數編列120名。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。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，迂迴遂行網路網路滲透陰謀，對我攻堅範圍有擴大情形[4-6]。

2014年11月24日是美國索尼影業(Sony Pictures)最黑暗的一天，駭客入侵公司內網示威，銷燬硬碟資料、外洩還沒有上映的電影檔案，甚至包含4,864個資料夾、33,880個檔案，及15,232個在職員工的社會安全號碼外洩。外洩資料檔案推估達1.5TB，Sony集團股價在1周內跌幅高達1成，市值蒸發超過新臺幣600億元。面對層出不窮的資安攻擊，強化資安心防與意識，可以辨識不合理系統存取、資安威脅，就可提高企業組織的安全性。國防部高天忠次長指出，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。國際上資安威脅已從個別、單純的炫耀，演變成有組織、以經濟或政治等特定利益為目的的入侵行為。近來網路犯罪組織趨於高度專業分工，加以網路戰發起不受時空條件限制，具首戰即決戰之特性，已使國家安全之概念及範圍產生實質變化。事實上，我國相關機關從2001年開始委外廠商維護電腦安全，這項政策則成為中共網軍入侵的管道，因此一定要有完善的配套來防範。國家安全局李翔宙局長指出，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。我國國家安全局表示，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。對於中共網軍攻擊的手法，中共先廣泛蒐集我政府部門、學術研究機構、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嵌入動態或特定網址，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[7-9]。

貳、網路惡意程式攻擊威脅型態發展分析

安全問題向來是國家生存的優先考量，同時也是處理的第一要務，傳統的安全乃是以軍事安全為主軸，但隨著全球化國家互動與互賴的影響，安全的概念不斷地擴展與延伸，安全議題也穿越國界，安全變得無所不在，舉凡政治、經濟、社會、文化、環保、生態等議題均涵蓋其中。駭客透過電子郵件社交工程或利用網站應用程式漏洞、網頁掛馬等方式，在受害電腦植入惡意程式，以竊取個人隱私資料，並與犯罪集團合作，進行金融詐騙。例如2011年4月，日本Sony PSN(Play Station Network)遭駭客入侵，導致近8,000萬筆個資外洩。美國之所以能夠運用有限的資源進行兵力架構的重組，其實也是經過風險的評估與考量誠如美國所評估，在2015年之前，美國主要的假想敵對國家中共與俄羅斯，尚不足以成為美國的同儕競爭者;因此，美國擁有充裕的時間實施國防全面體檢，進行現代化與重組的工程。在數位經濟時代，重要資通訊設施一旦遭受破壞，勢將影響經濟、民生及整體政府運作；而各類關鍵基礎設施(Critical Infrastructure，CI)的監督控制與資料獲取系統(Supervisor Control And Data Acquisition，SCADA)，通常較無堅實的資安防護設計，兩者均為網路駭客重要攻擊目標。進階持續威脅攻擊之特徵為針對特定目標、低調、隱匿、手法多變、客製化等。近期美、英、法、德、紐及澳等國政府，均相繼傳出疑似遭APT攻擊，企圖竊取該國政府重要及機敏資料，表一為APT攻擊與傳統攻擊差異分析。進階持續性滲透攻擊是一種最近常見的網路攻擊型態，攻擊者往往都是相當龐大且有組織的駭客集團，而並非像一般的駭客事件可由單一駭客所為。駭客集團會針對特定的攻擊對象設計一套專屬的攻擊策略，攻擊的手法除了以電腦入侵方式外，也會透過其他的傳統的手法達到竊取資料的目的(如電話竊聽等)。APT的攻擊者往往都會透過長時間且持續性的潛伏及監控，趁使用者稍有疏忽時竊取其所需要的資訊，對於資訊管理的人員來說，APT的防禦模型顯得更加的重要，基本上面對如此有組織的滲透攻擊，管理人員能做的

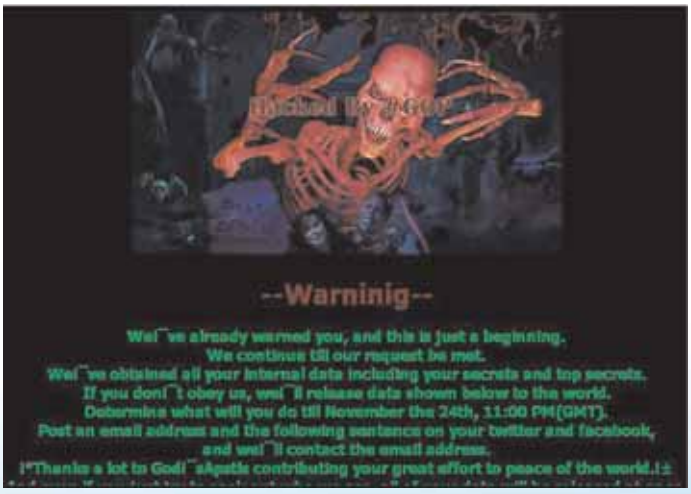
表一、APT攻擊與傳統攻擊差異分析表(自行整理)[12]

傳統攻擊	APT 攻擊分析
攻擊前需知道攻擊對象之設備位置或 IP 區段	攻擊前需搜集攻擊目標的電子郵件等個資
以電腦與資訊設備為攻擊單位	有針對性質以特定 IP 網站為攻擊單位，惡意攻擊散佈範圍較小，但對於受害組織影響卻很大
透過攻擊系統弱點取得控制權	利用社交工程或零時差攻擊使攻擊者傳遍整個目標網路以獲得敏感機密資料

就是勤加監控網站或是資料庫的存取記錄，以便能從記錄中辨識出攻擊的事件，並阻擋該來源的讀取權限，圖一為進階持續威脅APT惡意程式攻擊生命週期示意圖[10-13]。

圖一、進階持續威脅APT惡意程式攻擊生命週期示意圖[10]

根據2015年1月16日第201501003期資通安全電子報報導，法國網路防衛主管官員庫斯提耶爾表示，自巴黎上週遭伊斯蘭極端分子連續攻擊以來，約有1萬9000個法國網站遭受網攻，許多網攻是由「多少有組織」的團體所發動，包括一些知名的伊斯蘭駭客團體。這些網攻似乎多屬程度相對輕微的阻斷服務攻擊(DoS attack)，攻擊對象多樣，資安威脅不斷。Sony Pictures在2014年11月24日遭到駭客入侵，導致內部網路及電腦全數停擺，除影片及員工資料外流，並傳出內部電腦資料全數遭刪除。包括趨勢科技、賽門鐵克、卡巴斯基實驗室，與Blue Coat等資安業者都分析了FBI所提及的Destover惡意程式，發現該惡意程式專門鎖定Sony Pictures，熟悉其內部電腦架構。除了記錄Sony內部主機名稱與IP位址的關係，還含有許多可進入共享網路的使用者名稱與密碼。當滲透到Sony網路之後，惡意程式就會開始運作，包括刪除使用者的檔案，刪除近端或遠端磁碟的檔案還有用來開機的主啟動磁區(MBR)，此外，Destover中還有一個BMP桌布檔「Hacked By #GOP」畫面(如圖二)與Sony被駭時所出現的電腦畫面一致[14-15]。美國資訊網路公司Mandiant針對APT攻擊歸類成五個生命週期，週期分析如表二。簡單來說，APT其實就是有組織且有針對性的網路間諜活動，類似目標式攻擊(Target Attack)的進化版。一旦判斷遭受APT目標攻擊就必須果斷回應，回應APT目



圖二、Sony被駭時所出現的電腦畫面示意圖[15]

標攻擊有幾個部分：控制威脅、加以消除和確認損害範圍。第一步是立即隔離或控制威脅規模，可進行的步驟包括隔離受感染機器或將被入侵的服務離線。最終目標是防止攻擊進一步的擴展。值得注意的是，中國國家網際網路緊急應變中心(CNCERT)自2008年起，每年撰寫中國互聯網絡安全報告，CNCERT功能與世界各國的網際網路緊急應變中心(Computer Emergency Response Team，簡稱CERT)相仿，都是接受資安事件通報、緊急處理、評估測試及預警通知等。此報告內容涵蓋網絡安全形勢宏觀判斷、安全監控數據分析、危害案例分析、網路安全政策及安全技術發展等，值得注意的是行動通訊網路資安問題嚴重，中國指出我國D-Link路由器

表二、APT攻擊生命週期分析表(自行整理)[10]

APT攻擊生命週期	APT攻擊生命週期內容分析
初步的入侵	利用一些釣魚網站或電子郵件來做為入侵的媒介。
建立立足點	植入Rootkit等惡意程式以掌握使用者系統。
取得管理者權限	利用破解密碼等方式取得該電腦管理者權限。
內部偵查與平行擴散	找尋該主機附近的其他主機或伺服器，並伺機取得其內部資料庫儲存之機密資料。
持續監控並完成任務	持續掌控資料庫伺服器或是主機，並將資料匯出達到竊取機密的目的。

表三、中國CNCERT網際網路發展與威脅分析表(自行整理)[13]

項次	CNCERT針對中國網際網路威脅分析
一	網際網路域名(Domain Name)是隱憂，因為分散式阻絕攻擊(DDOS)之故；風險主要來源為通用軟硬體缺失(佔42.1%)、信息洩漏(佔15.3%)、權限繞過(佔12.7%)、SQL Injection(佔12.0%)、弱通行碼(佔11.2%)等。
二	2013年感染木馬病毒的主機為1,135萬台，伺服器16萬部，分別較2012降低22.5%及44.1%，成效可觀，足見中國全力打擊駭客地下產業鏈不餘其力，資訊治理與資安實力不容小覷。
三	2013年偵測到70.3萬個惡意程式，其中Android作業系統佔99.5%。CNCERT在2013年偵測到惡意行動程式活動12,956,836次，是2012年的23倍，牽涉網域有15,427個，IP有60,976個。
四	電子金融安全威脅增加，面臨跨平台風險---駭客主要利用簽名驗證繞過漏洞，仿冒知名銀行行動服務，竊取認證資料，完成銀行交易、轉帳等操作，牟取利益；2013年共偵測到30,199個釣魚頁面，4,240個偽IP；隨著支付寶等第三方支付蓬勃發展，行動付款的安全也跟著受到威脅
五	中國政府網站面臨威脅，地方政府網站成重災區；2013年有2,430個政府網站被攻擊，較2012年上升34.9%；其中反共駭客較活躍，持續對黨政軍機構、企事業進行攻擊；匿名者及阿爾及利亞駭客也常發動攻擊。
六	CNCERT已經與59個國家、127個組織建立合作協調關係，處理跨國資安事件數量共5,498件，較2012增長加35.3%。目前與CNCERT合作的公司有網秦、安天、金山、恆安嘉、奇虎、洋浦、網御星雲和卡巴斯基等，這些資安公司全天24小時密切在監控網路上的活動，並將他們所監測到的行為，通報CNCERT。
七	CNCERT於2012年總共接到31,655通報事件，其中處理了31,180件；通報事件中僅971件有關網路安全，較2012下降19.1%；足見中國資安防禦能力提升；通報事件大都為軟硬體漏洞(佔34.5%)。
八	2013中國被植入後門程式網站主要是.com(佔58.3%)，其次是.net(佔7%)和.gov(佔3.2%)；駭客常利用動態網域名從國外進行攻擊(掛馬)，最主要網域為www.snda5188.com；釣魚網站主要是仿冒.com(佔51.1%)網頁；其次是免費的.tk(佔16.8%)和.net(佔8.3%)；2013年CNVD(CNCERT的子部門)蒐集到的網路漏洞總計有7,854個，其中高危險的有2,607個。

有後門；駭客地下產業鏈則是用來套取個資，轉售給商家，作為發廣告信之用，中國國家網際網路緊急應變中心網路發展與威脅分析如表三。可以觀察到中國正積極為資訊戰作準備，報告指出包括APT攻擊(例如Icefog，紅色十月、特洛伊木馬等病毒、利用漏洞植入後門程式、網路釣魚Phishing或零時差攻擊)是資訊戰中常用武器；2013年有境外3.1萬台主機，對中國6.1萬台主機進行遠端控制；攻擊主要來自美國(6,215台美國主機控制15,349台中國境內主機)；境外釣魚網頁承載主機主要來自美國、韓國和香港；在殭屍網路方面，中國1,090萬台主機被境外2.9萬台伺服器所控制；其中美國有8,807台主機控制中國的(448.5萬)台主機、其次是葡萄牙控制了(398.8萬台)和韓國(83.9萬台)，值得注意的是，中國大陸在「十二五」規劃中提及，將推動國家七大戰略新興產業，而其中的新一代資訊技術，並將雲端運算發展列為重要發展項目。2015年1月15日，工業和信息化部中國電子信息產業發展研究院聯合網際網路經濟雜誌社在北京舉辦“2015年中國網際網路發展和網路安全

表四、中國2015年網路安全十大趨勢預測分析表(自行整理)[19]

十大趨勢	中國網際網路發展和網路安全十大趨勢分析
網路空間國際軍備競賽加劇	一、西方國家繼續建立或增設網路部隊，依據聯合國裁軍研究所統計，全球已有近50個國家建立了網路戰部隊。美國2014年《防務評估報告》首次明確網路戰部隊的建設目標。俄羅斯、以色列、日本等都在擴大網路部隊規模。二、各國加強網路武器和新型網路對抗技術研發。三、各國加強網路戰演習。據歐盟網路與信息安全委員會(ENISA)報告，各國開展網路演習的頻率大幅提高。四、美等西方國家通過北約組織加快構建網路軍事同盟，以實現集體防禦。
可能發生有組織大規模網路攻擊活動	一、美國更多的網路監控和網路攻擊行為將遭到曝光，多個國家加快發展網路攻擊能力。二、出於政治目的的駭客行動主義將更加泛濫。三、受經濟利益驅使，網路犯罪團體將針對有價值目標開展更密集的網路攻擊，攻擊行為發生頻率越來越高。
行動網際網路安全事件增加	伴隨著行動裝置動網際網路的高速發展，網路安全問題將更加突出。一、針對Android設備的網路攻擊持續增加。據卡巴斯基統計，2014年針對Android設備的攻擊是2013年的4倍，每5個用戶就有1個面臨過移動威脅。有機構預測，2015年針對Android設備的惡意軟體數量將是2014年的2倍。二、行動付費將可能成為網路攻擊的新目標，通過攻擊系統漏洞、製造網上銀行病毒等，網路犯罪分子可能獲取金融敏感信息或劫持賬戶。三、BYOD(Bring your own device，自攜行動裝置)的興起將帶來更多針對企業或機構內部網路的攻擊。
智慧型網路設備成為網路攻擊新目標	IOT(Internet of Things，全球物聯網)快速發展，越來越多的設備接入網路，車聯網、智慧型家居、可穿戴設備等應用日趨成熟。智慧型互聯設備應用帶來便利，但駭客將可能利用這些設備中數據，執行更複雜、更嚴重的破壞任務。已有安全研究者利用智慧型汽車、醫療可穿戴設備的安全漏洞，實現對這些設備的遠端程式控制，對設備使用者人身安全構成威脅。2015年針對物聯網的攻擊將可能成為現實，攻擊者可能對家庭路由器、智慧型電視和互聯汽車等發起攻擊，以獲取敏感資訊數據、採取進一步破壞行動，但大規模攻擊還不會出現。
工業控制系統安全風險加大	APT進階可持續性攻擊的目標正在從傳統的IT系統，轉向石油、天然氣、航空運輸等行業的工業控制系統。近幾年大量的實際案例中，這種趨勢越來越明顯。2015年，工業控制系統的安全風險持續加大，美國、歐盟等都在採取措施加強關鍵領域控制系統安全保護。而在中國80%關鍵系統都使用了相同的控制系統，由於依賴國外組件、安全意識低、持續接入網際網路等原因，更容易受到攻擊。

將發生大規模資訊洩漏事件	近年來，全球大規模數據洩漏事件頻繁發生，如美國Target超市7000萬客戶資料，摩根大通帳號資料被竊取，iCloud泄露出大量好萊塢影星私密照片，國內12306用戶身份證等敏感信息泄露。據Verizon《2014年度數據洩漏調查報告》，2014年全球共發生63737起網路安全事件，經確認的數據洩漏事件1367起。2015年大規模資訊洩漏事件可能再次甚至多次發生，掌握大量個人資訊的政府機構、大型零售企業、金融機構，以及移動應用服務提供商成為資訊竊取的重要目標。
網路安全事件造成更大損失	據美國戰略和國際問題研究中心報告，網路犯罪每年給全球帶來高達4450億美元的經濟損失。2015年，隨著網路威脅更加激烈，網路安全事件將帶來更大損失。一、針對關鍵資訊基礎設施的網路攻擊一旦成功，將帶來不可估量影響，能夠導致化工廠爆炸、火車碰撞、大面積停電等重大安全事故。二、駭客攻擊手段和工具更為強大，將可對更為複雜的資訊系統實施網路攻擊，從而造成更大影響和損失。三、隨著智慧型行動裝置與務聯網互聯設備成為網路攻擊的新目標，網路安全事件將不僅造成經濟損失，還可能危害設備使用者人身安全。
網路空間國際話語權的爭奪更加激烈	2015年針對網際網路關鍵資源管理與網路空間國際規則等問題熱烈探討，各國在網路空間國際話語權的爭奪將更加激烈。國際話語權是指以國家利益為核心、就國家事務和相關國際事務發表意見的權利。它體現了知情權、表達權和參與權的綜合運用。一、在網際網路關鍵資源管理上，仍然存在國家主導和利益相關方主導的管理模式競爭，國際社會將積極推進網際網路資源管理權的變革，以改變美國等少數國家掌控網際網路關鍵資源的局面。二、各國對網路空間規則制定主導權的爭奪將更加激烈。網路空間尚缺乏一套完善的網路空間國際規則，以美國為首的西方國家，以及俄羅斯和中國等都推出了網路空間國際規則設想，但尚未形成共識，誰能掌握制定游戲規則權利，誰就能掌握網路空間話語權和制高點，可預見未來爭奪將更激烈。
中國資訊安全產業高速發展	在一系列利好政策的刺激下，2015年中國信息安全產業將高速增長。針對網路安全威脅加強技術研發，推出更加智慧型的資訊安全設備和服務。另一方面，面對愈演愈烈的網路攻擊和網路犯罪，政府、金融、能源等重要行業的資訊安全需求大幅增長，帶動了信息安全市場的快速發展。預計，2015年資訊安全產業增長率將達到30%。
中國網路安全立法計畫將取得新進展	中國預測2015年，中國網路安全法治建設進程將顯著加快。一、適應網路安全形勢需要加快修訂原有法律，例如，在刑法修訂中增加關於網路恐怖主義的相關規定；修訂網際網路資訊服務管理辦法，針對新應用建立有效的資訊服務管理模式。二、圍繞關鍵信息基礎設施保護、跨境數據流動、信息技術產品和服務供應鏈安全等一系列重大問題，全國人大及相關單位開展更深入的研究。三、中央網信辦等加快推進網路安全審查等法律制度建設。

十大趨勢”研討會，會中發表預測2015年網路安全十大趨勢如整理表四[16-19]。

參、因應網路戰爭資訊安全威脅網路防護策略發展研究

中國大陸在國家中長期科學和技術發展規劃綱要中，提出將資訊產業及現代服務業列為國家長期重點發展產業，在面向核心應用的資訊安全中點出關鍵資安技術方向，且以研發減稅、政府採購、軍民合作及國際合作四大面向之鼓勵措施，推進中國資安技術發展。韓國大型企業並和學術單位合作，並投入大筆資金，發展出韓國相當重要的資訊研發成果。南韓藉由「e-Korea Vision2006」政策，推動高速寬頻網路服務，並因應資安威脅所帶來的衝擊，在「Broadband IT Korea Vision 2007」政策中，將資安列為國家基本政策。日本政府為了增強國家競爭力與維持社會經濟發展，近年資安政策發展方向著重提升國家安全與系統安全、增強資安教育

、促進國際合作等。中國於2008年第16屆中國共產黨四中全會，將資訊安全列為國家安全的重要組成部分，明確提出「增強國家安全意識、完善國家安全戰略」，以確保「國家的政治安全、經濟安全、文化安全與信息安全」。美國早於2002年小布希總統簽署了總統令要求各部門制定網路攻擊策略，2005年，美軍組建專門負責網路作戰的“網路戰聯合構成司令部”。2003年2月，美國發佈第一份專門針對網路空間國家安全的戰略報告《網路空間安全國家戰略》。值得注意的是《美國網路空間國際戰略》，它成為美國處理網路問題的“指南針”和“路線圖”。國防部緊接著出臺《美國網路空間行動戰略》，強調將與盟友和國際夥伴合力加強集體網路安全，具體行動體現在兩個方面。從2006年起，美國每兩年舉行一次“網路風暴”演習，以全面檢驗國家網路防禦水準和實戰能力。演習中，由美軍網路戰專業力量擔任“藍軍”，承擔演習中的網路攻擊任務。於2009年歐巴馬總統上任後，針對過去美國的網路安全政策與現況進行綜合性評估，建立可靠堅固的資通訊基礎，並宣布加強美國網路安全的新計畫，將資安提升至國家安全的層次。2011年9月15日，美國與澳大利亞在雙邊防禦協定中增加了網路共同防禦條例。美軍與日本自衛隊雙方合作針對駭客攻擊展開磋商並共用具體應對措施。美韓軍事演習的網路戰也已成為常態化課目，2010年8月舉行的美韓聯合軍演中，已增加網路戰防禦課目。2011年，北約空襲利比亞的“奧德賽黎明”行動實施時，一個國際非營利性組織啟動了“網路黎明-利比亞”項目，利用美國Palantir(分析軟體提供商)公司強大的網路情報分析軟體，對利比亞互聯網進行了全面監控，為北約軍隊提供評估報告。可見，美國主導的“網路北約”已進入實質性運行階段。2013年3月18日，英國《衛報》報道，一份為北約撰寫的網路戰手冊已經發行。位於愛沙尼亞首都塔林的北約卓越合作網路防禦中心邀請了20名法律專家，在國際紅十字會和美國網路戰司令部的協助下撰寫了塔林手冊。其內容強調，由國家發起的網路攻擊行為必須避免敏感民用目標，如醫院、水庫、堤壩和核電站等目標，規則允許通過常規打擊來反擊造成人員死亡和重大財產損失的網路攻擊行為。國防政策、軍事戰略與兵力架構三者息息相關，相互配合決定政策設計，同時影響國家目標與利益達成。2013年5月初，聯合國裁軍研究所(United Nations Institute for Disarmament Research)指出全球已有46個國家成立了網路部隊，美國國土安全部並於2013年6月12日公布改進關鍵網路架構分析報告，其中包含美國歐巴馬總統簽署執行命令Executive Order 13636(Improving Critical Infrastructure Cybersecurity)與政策指導PPD-21(Presidential Policy Directive-Critical Infrastructure Cybersecurity)，美國防部於2014年3月4日公布2014四年期國防總檢討(Quadrennial Defense Review，

簡稱QDR)，2014QDR報告指出美國面臨不斷迅速變化的安全環境，美國防部正重新定位，置重點於定義美軍未來的戰略挑戰與機會：新科技、新武力中心，以及更變化多端、更難預測、且在某些情況下對美國更具威脅的世界。美總統歐巴馬對網路安全問題十分重視，將把網路安全的重要性提升到大規模殺傷性武器的國家安全問題。針對網路作戰部署，美軍將投資於新增與擴充的網路戰力及部隊，俾加強遂行網路作戰與支援世界各地軍事作戰行動，並於作戰司令規劃與執行軍事任務時給予支援，同時反制對美國的網路攻擊，近年網際網路攻擊統計如表五[20-23]。

表五、近年網際網路攻擊一覽表(自行整理)

年份	近年大型網路攻擊型態分析
2009	極光行動(Operation Aurora)，是2009年12月中旬可能源自中國的一場網路攻擊，其名稱「Aurora」(意為極光)來自攻擊者電腦上惡意文件所在路徑的一部分。遭受攻擊的除Google外，還有20多家公司：其中包括Adobe Systems、Juniper Networks、Rackspace、雅虎、賽門鐵克、諾斯洛普·格魯門和陶氏化工。賽門鐵克將這個行動中，木馬程序(Hydraq/Aurora)的平台稱為「Elderwood Platform」，其攻擊目標包括機構組織和製造業供應鏈，最主要攻擊目標是國防承包商，次要攻擊目標是人權或非政府組織，許多被攻擊網站都與宗教、台灣、香港和中國大陸有關。攻擊方式大量利用Zero-day(零時差攻擊)漏洞，通過釣魚郵件和網站漏洞傳播惡意程序。
2009	美國網絡安全公司曼迪安特(Mandiant)長達78頁的報告中指出，位於中國上海的駭客團隊從2006年起開始至少對141家美國公司從事間諜活動，盜取了數百萬億字節的數據。2009年，電子間諜系統「鬼網」(GhostNet)被發現時，顯示中國的駭客不僅僅掌握可大規模實施間諜行為的技術，並會把這種技術付諸於行動。當時大約有100個國家的政治和經濟機構遭到了「鬼網」的滲透。國際研究組織曾表示，操控「鬼網」的電腦位於中國，從覆蓋面上來看，「鬼網」是迄今為止被發現的最大的網絡間諜攻擊之一。
2010	超級工廠(Stuxnet)，又稱作震網，是一種Windows平台上的電腦蠕蟲，2010年6月首次被白俄羅斯安全公司VirusBlokAda發現，其名稱是從代碼中的關鍵字得來，它的傳播是從2009年6月開始甚至更早，首次大範圍報導的是Brian Krebs的安全部落格。它是首個針對工業控制系統的蠕蟲病毒，利用西門子公司控制系統(SIMATIC WinCC/Step7)存在的漏洞感染資料採集與監控系統(SCADA)，能向可編程邏輯控制器(PLCs)寫入代碼並將代碼隱藏。這是有史來第一個包含PLC Rootkit的電腦蠕蟲，也是第一個以關鍵工業基礎設施為目標的蠕蟲。此外，該蠕蟲的可能目標為伊朗使用西門子控制系統的高價值基礎設施。據報導，該蠕蟲病毒可能已感染並破壞了伊朗納坦茲的核設施，並最終使伊朗的布希爾核電站推遲啟動。
2011	2011年美國五角大廈武器供應商洛克希德馬汀資料遭竊，駭客鎖定該公司採用動態密碼供應商RSA演算法，美國國家安全局統計說，從2009年到2011年，針對美國的網絡攻擊大幅增加了18倍。美國國防部副部長威廉·林恩表示，美國面臨巨大網絡攻擊危機，國防部的網絡每天受到幾百萬次的攻擊，國防工業的網絡也面臨被滲透的危機。其中，重大網路戰攻擊事件就包括了：2011年3月：美國國防部網路遭侵，被竊2.4萬份資料等；2012年8月，防毒專家發現「火焰」病毒，專門攻擊中東地區政府機構；2012年9月，美國國土安全部指控伊朗駭客攻擊摩根大通與美國銀行網站。
2012	大紀元2012年10月03日報導美國白宮傳出遭到駭客入侵的消息，但強調沒有機密資料外洩，來自中國的駭客破解了白宮的軍事指揮網路，甚至接觸到了啟動核彈的密碼。儘管美國行政與立法部門，尤其是國防部一直將網絡攻擊比作戰爭行為，可以採取軍事反擊，但立法進程緩慢。據美國之音報導，白宮的軍事辦公室遭到駭客入侵，並侵入最敏感的指揮系統，企圖偷取美國核彈的指揮控制密碼。但白宮的國家安全官員則表示，這起事件是「針對非機密網絡的魚叉網絡釣魚攻擊」，駭客採用的是所謂「釣魚」(phishing)的電子郵件入侵手法。

2013	2013年6月，全球最大國防武器承包商Lockheed Martin透露，該公司從2007年開始即密集的遭到駭客入侵；隨後中共在2012年推出的第二架隱形戰鬥機J-31，與美軍最先進的戰鬥機F-35有著驚人的相似之處。Lockheed Martin並指出中共駭客還一直試圖竊取該公司為英國量身打造的「聯合攻擊戰鬥機」的設計機密。五角大廈的一份報告指出，中共黑客入侵美國國防部機密網頁，並竊取多項尖端武器設計，包括美國為亞洲、歐洲和波斯灣等地區而設的核心飛彈防禦系統，以及海軍的神盾彈道飛彈防禦系統。
2013	2013年10月3日，Adobe宣布遭駭客攻擊外流290萬筆客戶資料，同時駭客也竊取了許多Adobe產品的源代碼，包括Adobe Acrobat和ColdFusion等，包括姓名、密碼及信用卡號；另外也有部分軟體的原始碼遭竊，可能產生另外的網路攻擊活動。目前對於客戶資訊與帳號遭劫，以及原始碼的遭竊，是否是相同攻擊者所為，仍不甚明確。。
2014	2014年5月22日大紀元報導，美國聯邦調查局指控中國偷竊SolarWorld數據財務資料，聯邦檢察官指控中國軍方在2012年侵入位於希爾斯伯勒(Hillsboro)地區SolarWorld公司計算機系統至少十次，從公司計算機竊取成千上萬電子郵件和文件用於貿易戰。美國司法部長Eric Holder2014年5月中宣佈對五名中國軍方官員網絡間諜罪指控。起訴書指控中國軍方官員有針對性對SolarWorld和其它四家美國公司，以及工會的網絡間諜行為。
2014	2014年7月13日大紀元報導指出，美國司法部指控一家中國航空技術公司的老闆蘇斌，從美國國防承包商竊取美國關鍵技術，這是美國刑事起訴美國官員所稱的猖獗的中國工業間諜的最新努力。美國官員長期以來指控中共駭客對許多美國公司構成威脅，蘇斌的案件證實了美國的指控。
2014	美國有線電視新聞網財經頻道(CNN Money)於2014年8月21日報導，自3月26日起，聯合包裹服務公司(UPS)在美國24個州的51間分店的電腦系統被一個駭客的惡意軟體入侵。這是自許多大公司如Target、Adobe、Snapchat、Michaels、Neiman Marcus、AOL、eBay、Albertson's和Super Value被駭客入侵電腦系統以來，最新的一起客戶資料洩露事件。
2014	2014年11月5日報導指出，加拿大媒體獲得一份最新文件顯示，加拿大最頂級的科研機構在今年夏天被中共駭客入侵。2012-2013年度花銷超過9億加元的加拿大國家研究委員會(NRC)是該國頂級研究機構，旨在幫助科研技術儘快轉化成加拿大工業界能夠運用產品。2014年夏天，該機構電腦遭到駭客入侵，加拿大聯邦政府將此次攻擊歸咎於中共政府贊助的機構。
2014	2014年12月網路安全公司Palo Alto Networks發現，在英國和美國銷售的中國製手機酷派(Coolpad)暗藏後門，酷派修改了Android系統，使得搜集使用者隱私資料的惡意後門程式CoolReaper深度植入在作業系統中，能躲避移動安全軟體的檢測，其動機是為了創造收入，但任何後門都可能會被濫用。而且這種官方植入的後門，用戶無法修改也無法察覺個人資料被竊。即使酷派沒有執行惡意程式，後門安全漏洞仍然能給駭客入侵的機會。
2015	2015年1月8日報導中國警方在其網站上披露一份14.9萬元的駭客入侵手機軟體合同，被刪除的頁面在Google網站上仍然可以看到，它顯示溫州經濟技術開發區公安局授予兩份合同給武漢虹信通信技術有限公司。它是中共中央政府一家主要信息技術公司的子公司。這份通知。這份簽署於2014年12月15日的合同顯示一個產品以49000元購得，可以讓中國警方向Android系統注入木馬病毒並解鎖蘋果的手機。

(文轉下期)

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、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、教授、系主任。現職：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。