作者/Bindiya Thomas　譯者/黃文啟　審者/劉宗翰

網路反恐新概念：網路應變能力

Resilience: The Solution to Cyber Terrorism?

取材/2016年7-8月德國軍事科技月刊併刊(*Military Technology*, July-August/2016)

面對日益嚴重的網路安全威脅，各個政府及民間組織除了採取預防措施外，還需要建立具有強大應變力之網路防護能量，俾因應不斷演進的威脅。

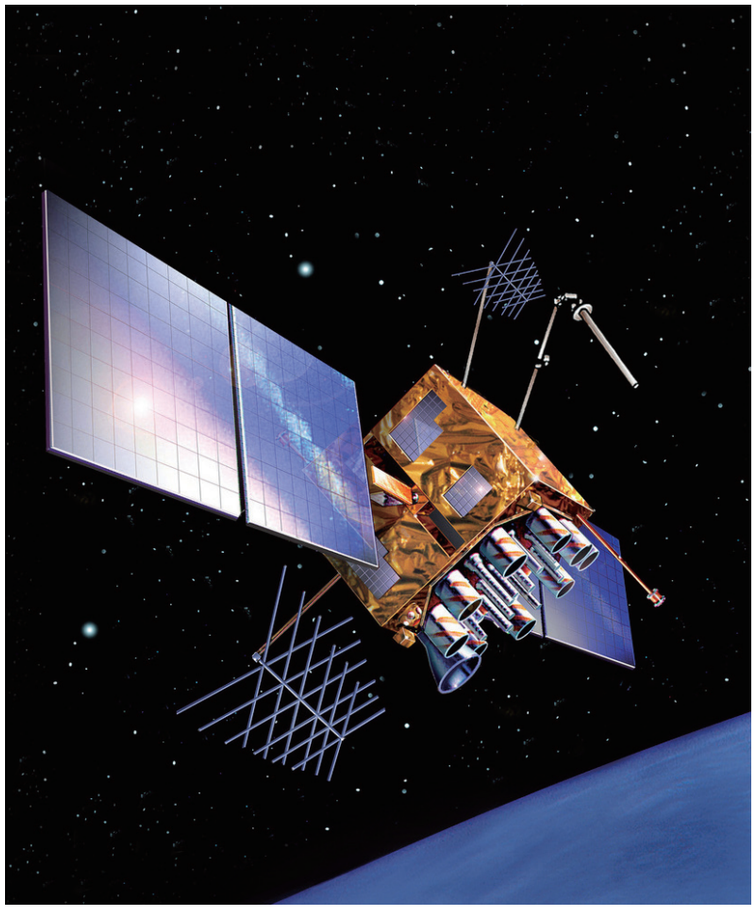
隨著電腦運算在人文和企業領域扮演日益全面性的角色，創新與發展機會持續大幅增加。由於這些機會帶來了更多的網路連結、更多的智慧型日常生活裝置，以及必然發生的癱瘓性資料漏洞、網路攻擊和勒索軟體，因此隨著企業蒐整大量客戶、夥伴、供應商和政府機關的資料，這些相關面向更令人感到憂心。

微軟公司估計全球到了2020年會有40億人口使用網路──約為今日人數的兩倍──高達500億個裝置將會和網際網路連結，而網路資料量將會比今日高出50倍。

2017年網路安全威脅預測指出資訊安全極度危險的畫面。國際安全論壇(International Security Forum, ISF)在其年度「威脅地平線」(Threat Horizon)報告中表示，資訊安全威脅惡化的步調和規模仍在不斷加速，危及誠信組織的完整和聲譽。該論壇列舉了2017年必須關注的九個最重大威脅：超大容量網路連結已超越各種防護措施的負荷；犯罪集團急速進步；科技排斥主義者製造混亂；對關鍵基礎設施的依賴變得危險；系統化弱點成為武器；舊有科技瓦解；數位服務受阻導致當機；全球整合危害競爭；安全與資料漏洞影響急劇升高。

國際安全論壇常務董事杜賓(Steve Durbin)在討論組織犯罪的研究中說明：「他們在彼此溝通和建立卓越中心方面具有極高效率和效能，因而會設法利用人類今日已經擁有的高度先進科技，」渠並進一步指出，「這點已充分顯現人類必須以更高效方式進行溝通和合作。」

杜賓對人們依賴關鍵基礎設施的情況亦表達同樣關切。其舉美國國土安全部於2011年的研究為例，當時即已發現美國的15項關鍵基礎設施系統中，有11項是以全球衛星定位系統做為核心組成要素。據國土安全部在研究中指出，全球衛星定位系統的任何差錯，都可能造成災難性後果。同樣地，網路攻擊者在2013年也曾控制美聯社(AP)的推特帳戶，藉此報導白宮一場爆炸造成美國總統受傷。這個假推文引發一場股市風暴，直至發現為駭客攻擊事件後才告解除。



全球衛星定位系統(GPS)爲美軍廣泛使用，係牽一髮動全身的科技工具。(Source: Lockheed Martin)

《英國金融時報》(*Financial Times*)於2016年2月的報導中指出，世界第三大國防工業公司──英國航太系統公司(BAE Systems)，據悉每週至少會遭到兩次網路攻擊。該公司應用情報部門常務董事泰勒(Kevin Taylor)還向金融時報補充道，英國航太系統公司平均一年都得擋掉100次以上「潛在國家攻擊」的事件。該公司亦發現某些是由網路罪犯所發動，包含利用網路犯罪行為詐取金錢的業餘犯罪者，亦即所謂「騾子」(mule)；或是想要在同儕間炫耀的「脫逃者」(get-away)，他們因為知道自己年紀太小無法移送法辦，所以敢肆無忌憚地做出一些大膽行徑。

雖然網路空間為許多頂尖組織創造諸多機會，但整個環境卻是充滿不確定性和潛在的危險性。駭客運動分子和網路罪犯在這樣的環境中不斷精進技術，各國政府也不斷推出各種新規定和法案，以因應重大意外和大眾的關切。各種組織被迫持續進行調整並快速進行處置。國際安全論壇在報告中補充指出，那些具有知識和做好準備進行改變的人，仍須相當多的努力才能確保未來安全。

英國國家電腦緊急應變小組主任吉卜生(Chris Gibson)依其小組的紀錄指責道，「安全議題中有80%來自於不良的安全措施。」他在2016年3月所舉行的公部門資訊暨通信科技高峰會(Public Sector ICT Summit)發表演說時表示，擴大運用基本安全措施「可以積極提高對確認新威脅的重視。……如果從網路基本要件來看，人們都知道相當簡單的事情是──密碼、修補程式、建立治理程序等──就可以讓八成的麻煩瞬間消失。……只要能落實網路基本工作，實際上就可以降低人們對零時差弱點的已知破壞效果。」

網路安全問題多數來自不良措施與不佳防護習慣所致。

邁向應變之道

為因應當前和未來的網路事件，一種新的學門──網路應變──已開始成形。吾人應認清網路預防已不再是各類型組織和政府機關的可靠選項，還要衍生以應變、準備、持續評估和處置為重點的新趨勢。雖然網路應變在目前還沒有一個國際性認可的定義，但愈來愈多人都認同微軟公司在2016年2月部落格文章中所提出的說法，「儘管在面對長期性壓力源和嚴重震盪情況下，複雜網路系統仍可持續提供所望結果」，這是定義網路應變的適切敘述。

應變的網路系統所展現之共同應變屬性包含(1)狀況覺知，(2)多元性，(3)整體性特質，(4)自主規範，(5)調適能力等。此外，最有效瞭解和在某種程度上評估網路應變的方式，是瞭解其在整備、反應和重新改造方面的能量和能力。由這些特質可以明顯看出，網路應變絕非某個組織──或某個城市──可從廠商手中買到的商品。微軟公司的可靠電腦運算部門(Trustworthy Computing)資深主任尼古拉(Paul Nicholas)進一步解釋說，此種應變必須透過領導統御、團隊合作、最佳冒險、信任、彈性，以及致力促進和持續翻新數位城市的作為才能建立。

2015年底，蘇格蘭政府公布了一份網路應變戰

略，希望「協助發展一種網路應變文化，同時創造必要環境，俾確保蘇格蘭在滿足網路專技人才日增需求上成為領導者。」在其任務說明中，這份應變戰略列舉了蘇格蘭政府和公共業管部門所需採取的步驟，其中至少包含：在蘇格蘭部會中增加一個專責戰略治理的機關，以督導該戰略的有效落實與成效評估；將網路應變納入所有國家和地方政府政策內容；建立網路事件回報機制，並且結合更廣泛的資訊通信科技/數位與企業持續運作計畫；在發展新產品、服務和程序時，將網路風險與應變評估列為必要部份；以及考慮公部門共同開發或採購具網路應變的系統和工具。

蘇格蘭政府資訊長莫西絲(Anne Moises)指出，「應變需應用到幾乎所有企業職掌的關鍵基礎設施，而政府當局必須確保在所有新數位服務設計的面向上，將應變納入考量。建立滴水不漏的網路威脅預防措施是一個無法達成的目標，因此重點必須轉向偵測、快速反應和復原。吾人必須想像所有不可

美國政府各機構刻正協力提升網路安全性。(Source: REUTERS/達志)

預期的狀況、預先規劃並練習處置作法。達成此一目標的方式，在於確保所有網路應變想定和網路意外反應計畫都能經常進行檢視、驗證和演練。」

同樣地，2016年2月，美國白宮也公布了「網路安全國家行動計畫」(Cybersecurity National Action Plan, CNAP)，未來將致力防止聯邦政府各部會遭到類似兩年前美國人事管理局(US Office of Personnel Management)所經歷的網路攻擊型態。根據白宮所發布的聲明稿，行政當局已經設置聯邦資訊安全長(Federal Chief Information Security Officer)一職，以推動聯邦政府所有機關的網路安全政策、規劃及執行方式。此外，美國國土安全部、商務部及能源部也挹注了各種資源和能力，成立國家網路安全應變中心(National Center for Cyber security Resilience)，提供所有企業和各個產業組織一個封閉環境，測試其系統安全性，諸如模擬輸電網路遭到網路攻擊的情境。

此外，該新聞稿亦指出，國土安全部、總務署(General Services Administration)及其他聯邦機關將增加各個地方政府在資訊科技和網路安全共享服務方面的可用能量，希望藉此使各個單一機關免於單打獨鬥地建立、持有和操作其自身資訊

科技設備的業務，代之以更高效率、效能和安全的選項，以及確保所有機關都不會淪落自力對抗最精密威脅的窘境。

北約組織也採取類似步驟，以確保網路應變的遂行。2016年2月，在北約企業網路夥伴關係(NATO Industry Cyber Partnership, NICP)的架構下，北約通信暨資訊局(NATO Communications and Information Agency)宣布與防特網(Fortinet)公司簽署協議，推動雙向資訊共享，尤其是針對網路威脅情報的交流。此種方式通常對於加強網路應變及消弭網路攻擊弱點方面，是具有較高影響和效率的方式。北約通信暨資訊局執行總監吉斯博斯(Koen Gijsbers)在官方聲明中表示，「北約當前所面對來自全世界各地的網路安全威脅，可能對各國經濟和民眾構成極其重大的衝擊。為避免此種情況，北約通信暨資訊局堅定支持及早與全世界包含防特網在內的頂尖大廠，進行各種威脅和弱點資訊分享作為。」

藉由此項倡議，負責運作和保衛北約組織所有網路的北約通信暨資訊局，將可強化整個北約防衛供應鏈的網路防護、協助各個產業組織參與多國「巧防衛」(Smart Defence)計畫、同時改善在網路攻擊常態威脅下的操作專技、資訊和經驗分享，包含諸如惡意程式資訊分享等相關威脅與弱點資訊。該局也將致力提高各界認知，並且強化對各種網路風險的瞭解、運用民間產業各項發展來建構自身能力，並且在發生網路意外時提供高度效率與充分的支援。

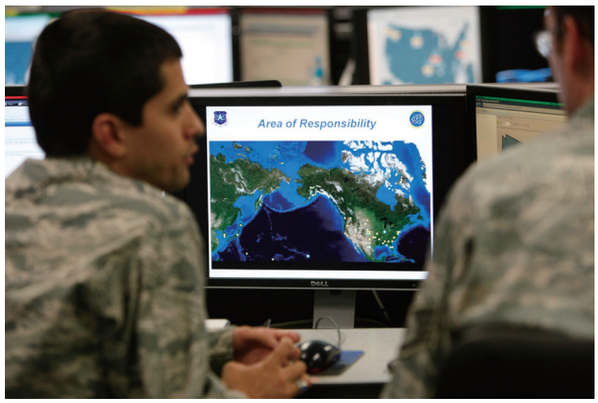
強化網路應變能力已成為美國和北約確保國家安全與防衛的重點。

解決各項關鍵性問題

2016年2月，微軟、甲骨文(Oracle)及其他五家網路安全產品與服務的頂尖廠商，聯手創設「網路安全政策暨法律聯盟」(Coalition for Cybersecurity Policy and Law)，這個全新組織將置重點於教育決策者並爭取渠等合作，以解決與網路安全相關日益複雜的立法和規範政策問題。這個聯盟的創始會員包含Arbor網路、思科(Cisco)、英特爾(Intel)、微軟、甲骨文、Rapid7和賽門鐵克(Symantec)等公司。

此一聯盟的協調員、前白宮總統網路安全特別助理史瓦茲(Ari Schwartz)表示，「本聯盟的所有會員均致力於建構美國公共和民間網路安全基礎設施，藉由渠等專業知識和參與，將對美國政府網路安全政策方面的決策作為發揮關鍵性作用。今日世人所面對的數位威脅範圍可謂前所未有，涵蓋包含犯罪集團和國家背後支持之攻擊行為等，而本聯盟在與決策者合作發展因應這些威脅的最有效處置作為過程中，將代表產業界發聲。」

此一聯盟的任務，是欲集結所有頂尖公司的力量，協助決策高層制定共識性政策解決方案，以促成蓬勃且堅實的網路安全市場、支持發展與採用各種網路安全創新作為、同時鼓勵不同規模的各種組織能採取諸般改善其自身網路安全的步驟。2016年2月，網路安全政策暨法律聯盟在聲明中表示，身為政府機關、研究人員和企業



美軍積極部署網路領域。(Source: Reuters/達志)

廠商等不同領域的交流介面，其將代表網路安全產業向國會、聯邦機構、國際標準機構、產業自律專案及其他相關決策管道發聲。同時，美空軍也在同年2月12日宣布其已達成一項重要階段目標——網路空間弱點評估/獵殺(Cyberspace Vulnerability Assessment/Hunter, CVA/H)武器系統已經達成全期運作能力(Full Operational Capability, FOC)目標。此種系統是一種網路防禦工具，主要用於受防護網路系統的應用範圍內。美空軍將把網路空間弱點評估/獵殺系統配備於網路防護小組。這項裝備將可提供搜尋、定位、追蹤、鎖定、攻擊和評估空軍資訊網內優先網路區塊內，各項任務所遭遇之高階持續性威脅。

美空軍在新聞稿中表示，「達成全期運作能力目標，意味著網路空間弱點評估/獵殺武器系統已完全可以滿足協力空軍資訊網路中，主要區域防禦平臺執行優先性傳輸的需求。此種武器系統可有效遂行弱點評估、敵意威脅偵測和遵守規範評估。」美空軍太空司令部(AFSPC)所屬整體空中、太空、網路空間與情監偵作業處(Integrated Air, Space, Cyberspace and ISR Operations)處長惠廷(Stephen Whiting)准將在簽署全期運作能力公告文件後表示，「這項成就凸顯出空軍對於美國網路司令部網路防護小組任務的承諾，以及保護國防部資訊網路中空軍部分優先網路空間區塊。網路空間弱點評估/獵殺系統可以捍衛美空軍在空中、太空和網路空間飛行、戰鬥和致勝的能力。」

網路空間弱點評估/獵殺系統的操作人員側重在提供弱點評估和獵殺任務，後者的能力提供第24空軍部隊指揮官與受支援聯合作戰指揮官一套部署型精準戰力，俾確認目標、遂行網路範圍內追擊、消除影響各種關鍵鏈路和節點的網路威脅，以及支援戰區或專業部隊作戰行動。美空軍表示，網路空間弱點評估/獵殺武器系統所提供的網路安全能力，可以深入評估諸如電腦、基礎設施、應用程式、數據及網路作戰等方面資訊系統資產。

其他網路空間武器系統還有美空軍的網路空間防禦武器系統(Cyberspace Defense Weapon System)、網路安全與管制系統之武器系統(Cyber Security and Control System Weapon System)、網路指揮管制任務系統之武器系統(Cyber Command and Control Mission System Weapon System)和網路空間防禦分析武器系統(Cyberspace Defense Analysis Weapon System)等。

作者簡介

Bindiya Carmeline Thomas係駐印度邦加羅爾(Bangalore)的戰略事務與國防記者，為德國軍事科技月刊定期撰稿者。

Reprint from *Military Technology* with permission.