探討太陽風網界戰

●葉俊雄／前國家高速網路與計算中心主任

路透社（Reuters）於去（2020）年12月13日報導，駭客入侵多個美國政府屬性敏感的機構。美國資訊安全公司火眼（FireEye）在五天前發佈聲明，有他國的網軍侵入其公司，意圖竊取他們開發的測試用攻擊性紅隊工具。火眼立即進行調查，禍源來自資訊科技公司太陽風（SolarWinds）的網路管理軟體「獵戶座」（Orion）被值入後門（backdoor）所致，因而揭露此震撼全球的資安事故（incident）。

此事故的被駭者眾多，包括美國九個政府機構（含國土安全部、國家安全局、能源部、財政部、司法部）和上百家民間企業，以及世界多國的公私部門。其所造成的傷害規模甚為廣大慘重，可能是近年來最嚴重的資安事故，而且，根除與復原工作十分困難，可能要持續數年。依目前的資料，大都指向俄國的情資單位SVR（Foreign Intelligence Service）所為。有人認為此已是網界戰（cyber warfare）的行為[1]。

據專家研判，駭客技術老練、行事謹慎、很有耐心，知道如何避開偵測和消除蹤跡，留下很少線索，非常難於察覺。但由於貪圖也是資安高手所開發的工具，導致行踪敗露，鑄成大錯。

此次的攻擊手法屬於供應鏈攻擊，也就是駭客先攻擊資安防護較弱的廠商，將惡意程式植入其開發的軟體裡，再藉由廠商的更新機制，將惡意程式散佈至下游的客戶群，入侵客戶的資訊系統。客戶愈多，散佈就愈廣。又因上下游機構之間的信任關係，不易被偵測出來，所以，既有效率又隱密。

軟體系統愈來愈龐大複雜，已非單一組織能夠完全自行單獨開發全部的軟體，致使必須依賴其他軟體公司供應部分（甚至全部）的軟體。對於高資安強度的機構，藉由資安能力薄弱供應商的途徑進行攻擊，可以省下不少力氣及時間。供應鏈已是資安的破口，這種間接迂迴的攻擊模式逐漸為駭客所喜歡而採用。

太陽風有逾三十三萬家用戶，這些用戶涵蓋美國政府單位和大型企業等重要機構，正是他國網軍的理想攻擊標的。不過，太陽風宣稱少於一萬八千家用戶曾下載中毒的更新軟體。依專家分析，此次攻擊極具針對性，其企圖可能是竊取高度敏感的機密情資，所以，真正的攻擊目標大約只兩百家有高價值的機構，目前，尚不清楚駭客竊取了什麼資料。

事故爆發後，美國公私部門立即啓動緊急應變措施。美國國土安全部下屬的網界安全與基礎設施安全局（CISA）當晚發布緊急指令，要求所有政府機構將獵戶座系統及受其影響的系統斷線或關機。微軟立即移除惡意軟體所用的數位身份認證文件，並與火眼和GoDaddy連手建造「扼殺切換（kill switch）」，以此切斷惡意軟體和駭客的通訊管道，使它不再受駭客所控制或傳送竊取的資料給駭客。微軟的資安產品Windows Defender若偵測到它的特徵碼，就將它隔離（quarantine）鎖住，火眼也公布數百種反制措施。

然而，這只是初步的止血舉動而已。接下來的根除惡意軟體與復原工作十分艱鉅，加上人才欠缺，此工作可能要持續數年。受害者可能的補救措施包括：立刻執行事故應變計畫、以正確的順序從事矯正舉措、清查是否有資料被竊取或被破壞、持續緊密地偵測仍在組織內的惡意軟體、稽核資訊系統和應用程式、強化混合雲運作環境。此外，有人認為，美國情資單位重攻輕防的策略需要嚴謹檢視，必須重新思考資安的總體方向和佈局，也有人提議美國需要重新建構整體網路系統。

依據多家美國資安公司的調查和分析，此次攻擊可能早在2019年10月駭客就已入侵太陽風的軟體開發更新平台（Orion build system）。起先未植入後門，只做試驗性的運作。2020年3月才將名為Sunburst的後門植入獵戶座的更新軟體裡，再藉由太陽風的更新機制，將後門傳播至客戶群。惡意軟體成功入侵受害者的電腦系統後，就會與駭客聯繫，然後再下載另一惡意軟體Teardrop，以建立額外的管道，方便進出受害者的網路，這可讓駭客易操作中毒的電腦。之後。惡意軟體就靜靜地待在這些中毒的電腦內，不做任何行動，等待駭客下達新指令，如同間諜藏身在群眾裡，伺機出擊。

此次攻擊的駭客應為國家級的網軍小組所為，他們有長期的規劃，但分階段進行。佈局嚴謹、技術精進細緻、行事謹慎、有紀律和耐心。他們開發的惡意軟體善於自我掩護，避開身份的認證。並且，採用多種新穎及現有的不同技術，如使用一個很難察覺的軟體瑕疵作為攻擊手法、使用已過期或現存的網域名（domain name）、將惡意行動混在正常的太陽風活動裡、藏身在正規的網路通信協定中、將竊取的資料儲存在合法的檔案內，這都讓它能長久不被偵測出來。他們的終極目標是經由某受害組織的內部系統入侵微軟的雲端服務系統Azure Office 365。

近年來，全球資安攻擊頻繁快速、規模變大、技術精進、新樣態的攻擊也增加。去年12月，台灣遭受網路威脅的單月次數就有九萬九千兩百九十三件，雖然大多數的攻擊都被擋下，但潛藏的威脅仍然不可忽視。又如業務敏感特殊的外交部，長期以來是中共網軍攻擊的主要目標，依2020年的統計資料，兩年間的資安警訊數量增加數十倍。

資訊安全是一場易攻難守永不止息的戰鬥，隱藏於四面八方的黑帽駭客隨時隨地伺機出擊。他們時時在尋找有漏洞的設備或警覺性低的個人，進而攻擊這些特定目標，竊

取重要資料或控制其設備做為跳板。駭客一詞易使人誤認為資安專業人士只是在入侵他人電腦以竊取資料（即黑帽駭客）。其實，多數資安人士從事資安防護和降低風險（如尋找資訊系統漏洞）的工作（即白帽駭客）。他們一方面使用工具及設備協助防衛，也要隨時留意異常現象，以及分析一堆雜亂無序的巨量資料，判斷是否有被駭的跡象。

駭客不僅來自外部，也很有可能藏在組織內部（俗稱內賊的員工），這表示資安防護很難有明確的邊界。資安攻擊可從外圍、供應商、外包廠商、合作夥伴、分支／出差／居家等遠端辦公之處、或組織內部出手。而防守方只能預測可能的攻擊樣態，依此建立防線，以及規劃遭入侵時，如何快速回應和降低傷害。一個高強度的資安防護系統必須同時全面性地涵蓋管理、技術和實體三面向。

近三十年來，資訊科技快速進步，進而促使其應用領域及使用數量大增，已成為人類生活的必需品，其重要性不可言喻。這也造成資訊生態變得相當複雜，資訊科技與資安生態的相關發展大大影響資安防護的演變和挑戰度，在此列出幾項關鍵性的發展。

一、自英特爾（Intel）開創出微處理器（microprocessor），使得設備及裝置的功能可藉由軟體實現而無需變更硬體設計。由於軟體非常有彈性且容易更動，這使軟體成為絕大多數設備及裝置的最核心組件。隨著來自各行各業的需要，人類創造的設備數量驚人且種類繁多，程式也愈來愈龐大和複雜，以致於很難去除所有的瑕疵（bug）。絕大多數大尺度的軟體系統已非單一組織所能獨自開發，需要依賴第三方（third-party）提供部分程式，或者使用開源（open-source）軟體套件。而且，為了搶先對手上市或其他業務需要，必須儘速推出產品，在時程的強大壓力下，只好犧牲資安的需求。在這些多重錯綜複雜的因素下，自然就產生了為數可觀的軟體漏洞。

二、約十五年前，雲端系統和服務的興起開始改變資訊生態。小公司可以使用雲端服務，而不必自己購買資訊設備及雇用技術人員。大機構為了節省成本及彈性調度計算資源，也將部分軟體系統移至雲端，但高機密性的資料與系統則仍留在自家的資料中心。雲端系統的計算資源管理涉及多方參與者（如雲端系統擁有者、客戶／使用者、軟體及服務提供者），資安防護的責任必須所有參與者協調分擔，有時難免有灰色地帶或考慮不周之處。而且，駭客也可以是正規的使用者，有其應有的資源使用授權。所以，雲端系統的廣泛使用提高了資安防護的複雜度及挑戰性。

三、物聯網系統的建置必將導致小型裝置（如感應器、攝影機）暴增。這些裝置雖有計算和通訊的能力，但由於空間及成本的限制，計算和儲存容量與資安防護能力則相對不足，不易抵擋駭客的入侵，這絕對是資安的大破口及嚴峻考驗。

四、人工智慧（AI）歷經兩次寒冬之後，於本世紀初，有顯著的技術突破而再掀風潮，成為今日極為重要的科技顯學。先進國家都投入資源從事AI與資料分析的研發並探尋其應用，業界致力於相關產品的開發或將AI置入產品中。白／黑帽駭客當然不會坐失

良機，且朝自動化的方向前進，這使得資安交戰更加激烈和強大。

五、約二十幾年前，資安生態開始改變，其中一項重大改變是諸多國家開始建立「正規網軍」（與陸海空及太空軍並列五大軍種），同時也「支助」民間駭客並派遣任務，網軍的活動已不那麼神祕，不時見諸媒體報導。有別於（不合法的）民間駭客（無論是孤鳥或集團），網軍受到國家保護，且有充足的經費和資源。然而，有些國家的網軍不只從事軍事情蒐行動或開發資安攻擊或防禦工具，也竊取他國的商業機密、智財資料及個資，甚至於散佈不實訊息以製造社會分裂與威脅他國關鍵基礎設施的安全。這與傳統的戰爭迥然大異，一場無煙硝的網界戰或資訊戰已經開打了。

此次太陽風事故震驚美國資安界，有諸多論述與改善之道紛紛發表。美國總統拜登（Joe Biden）上任前就聲明優先處理太陽風資安事故，也要政府各階層將資安列為最重要的任務。今年3月中，美國政府職掌資安的高階主管強調，資安防衛的重要策略就是要快速協調民間企業，共同聯手應對資安事故。並擬現代化資安防衛體制，以及籌備「統一協調組」（Unified Coordination Group），由白宮國家安全委員會主導，以因應往後大規模的網攻，且把傷害國安的他國科技公司列入黑名單。他山之石可以攻錯，美國的資安策略值得借鏡。

太陽風事故實為一場典型的網界戰役，俄國總統普廷（Vladimir Putin）亦擔憂美國的報復。而台灣時時遭受中共網軍的無形攻擊，也經常受到中共飛機及飛彈的有形威脅，情勢萬分險峻，所幸蔡總統高度重視國安與資安。有鑑於此，筆者從技術面、政策面、法規面、教育面提出數項芻議，以供政府、組織決策者及資安先進參考與討論，期盼能對台灣的資安體質有所助益。

一、技術面：首先，必須強化整體資安架構，以建構完善的國家資通安全環境。設計資安防護機制必須遵循一些重要原則，如合宜可行的資安政策、風險評估與管理、最小授權（least privilege）原則、零信任（zero trust）原則、系統備援、網路分隔（segmentation），即對資料／使用者／設備做機密分等，依此，分隔內部網路的虛擬區域。其次，對自家的內網務必透澈了解，所有連上內網的裝置及軟體要有文件紀錄，而且，要嚴格警覺地監控網路，並做行為分析，如網路流量、進出信息、使用者登錄、資料存取、異常連線、黑名單網址等等。也可引進先進技術（如AI、數據驅動防護、集體防禦）以強化防禦系統，此外，要採用多因子認證、不定期檢查設定，更正錯誤或不良的設定，軟體更新，以及定期資料備份和病毒掃描。

二、政策面：國家的資安政策是整體國安的一環。蔡英文總統高度重視資安與假訊息的防範，曾多次宣示「資安即國安」，也將透過專業訓練，強化情研戰力。而且，行政院根據《資通安全管理法》要求關鍵基礎設施提供者須做好資安管理與維護。這些都是正確的方向。

國防部近期公布2021年《四年期國防總檢討》報告，報告強調：「落實各項資安管控機制，提升防護能量，建立嚴密阻絕防護，並與政府及網路安全機構建立夥伴關係，建立軍民一體的聯合網路防護架構體系，精進資安人才培育。」政務委員郭耀煌就規劃中的數位發展部表示，其功能定位之一為：「強化跨機關資安聯防及應變機制，掌握自主資安科技，提升早期偵知、預警機制，降低損害風險；希望積極扶植台灣資安產業，政府與民間串成公私協力的資安國家隊。」這些宣告清楚地顯示出政府高度重視資安，期盼也能擬定合宜可行的執行策略和行動方案，並儘速確實有效能地落實這些良好的構想。

除此之外，政府也宜思考其他資安核心要務，如攻防兼顧的資安佈局、國家整體網路架構的妥善性、現代化資安防衛體制，強化防衛縱深與體質，攻防技術能力的增強、全民資安意識的提升、深化國際交流與合作。例如，仿效美國國家標準與技術研究院（NIST），責成某政府資安單位（如正在規劃的數位發展部下屬的資通安全研究院或資安署）訂定技術規範或準則，在產品及服務的開發或採購上，供政府單位遵循和民間企業參考。也宜要求屬性敏感的政府組織及關鍵基礎設施提供者所屬的資安單位必須取得一家有公信力的國際機構所訂定的資安認證（如ISO 27001），並將這些單位的資安成熟度推向成熟模式的最高階。

民間企業也必須將資安視為最重要的任務，擔當起自家的資安防禦能量，如台積電加強自身的資安防護，也要求供應商建立起碼的資安規範，並將其列入例行稽核項目之中。

三、法規面：網軍的興起改變了資安生態，關鍵基礎設施與國家／商業／核心關鍵技術機密資料的保護更為重要且具嚴峻挑戰，資安相關的法規也應與時俱進。政府陸續修改《國安六法》和《營業秘密法》，行政院長蘇貞昌強調「相關修法要以國安角度思考盤整」，值得肯定。

鑑於此次太陽風事故，政府宜時時檢視現有法規的適用性，如訂定法規，要求提供政府機構軟體／設備／服務的廠商，當其公司遭駭時，應立即通報政府機構。此外，對於境外敵對勢力在網際空間的惡意行為（如蒐集、竊取）必須嚴格究責，依此原則做合宜的修法，如英國政府打算立法禁止特定供應商參與智慧城市的投標或整套系統的運作，或如美國商務部將華為納入實體名單，美國公司未經許可不得把特定技術或零組件出售或轉讓給華為。

四、教育面：此次太陽風事故固然對美國造成相當的傷害及出醜，但察覺後，多位專家聯合行動，快速阻斷惡意軟體的擴散並將其隔離，亦顯示美國的實力。美國資安的深厚實力深植於數百家既競爭又合作的民間資安企業，專業技能涵蓋各領域，從政策、策略、研究到產品／工具開發、系統建置及維運、諮詢和顧問服務皆有，有攻擊面也有

防禦面。如此多元的生態提供了一個培育人才的優良環境。

資訊安全是最實務的專業，所有的技術都要在網界（cyber space）裡展現真功夫。所以，資安人才的培育必須攻擊與防禦並重。同時，必須建置一個相當規模的獨立虛擬育才環境，具備各種攻防工具，不時進行紅籃隊攻防對戰，以打下紮實的基本功夫和知識。更必須投入實體的網際世界，參與實際運作及磨練以累積實戰的經驗。

資安防護是全體國民（及組織成員）的責任與任務，在網路時代，每個人都需具備資訊安全的基本知識。政府可結合民間，積極地撰寫或製作易懂有趣的文章或影片來介紹資訊安全（含網路詐欺及假訊息），藉由各類媒體傳達給民眾。也可與地方政府合作，不定期地到各地區，舉辦活潑生動的資安說明會，透過這些活動來提升國民的資安意識和認知。

太陽風事故雖然發生在美國，台灣政府也必須審慎嚴肅地看待此場網界戰役。資訊科技的快速發展與應用的廣泛擴增，促使資訊安全愈趨重要，已是國家安全不可或缺的關鍵一環。國家政策必須綜觀全局，嚴謹擬定國家資安的總體策略和佈局，管理、技術及實體三大面向都要顧及，攻擊和防禦技能並行發展，人才養成與資安意識的提升不容輕忽。

【註釋】

1. 本文以「網界」一詞對應Cyber，以此與Network的網路一詞區別。Cyber是指以網路為媒介而連結成的虛擬網際世界，而Network是指由諸多資通訊設備所建構的實體資訊傳輸和通信系統。◆