◎資訊安全宣導

—從臺菲網路戰說起—

說到先前最熱門的新聞莫過於菲律賓公務船槍擊我國籍漁船，並造成漁民死亡的事件。事件發生後不久，我政府部分官方網站陸續傳出無法正常開啟的狀況，經由反查發起攻擊的 IP 位置，發現原來是遭到來自菲律賓的 IP 對我政府官方網站所進行的阻斷式服務攻擊；而我國網友們也不甘示弱地紛紛向菲律賓政府網站發起攻擊，讓菲國許多網站飄揚著我國國旗，甚至使菲國總統府官方入口網站一度成了全球色情網站的分享載點。從這起事件我們清楚得知，網路攻擊無論是政府授意也好、個人自發作為也罷，已成為各國用來嚇阻、甚至攻擊敵方的手段之一。

基於民族意識的個別駭客，往往只針對流量的表層攻擊，多數不會真正危害系統。雖然這樣的行為已違反刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金」，但網路攻擊活動不易產生明顯的跡象，而且往往要在真正遭受實際損害時，才能從中找出責任歸屬，更何況這些攻擊經常來自境外，甚至是無法得知的地點，更遑論要將違法的駭客起訴。不過更令人擔憂的是，可能有由政府支持的駭客組織，以竊取公務、國防及商業機密為目的；其主要手段包括社交工程攻擊、入侵電腦布建跳板等，以建立情蒐網絡，由於攻擊的對象往往是針對特定的目標，故使防護更加困難。根據聯合國統計，全世界四分之一的國家設有網路作戰部隊。而網路上的攻防戰，既看不到漫天烽火，也聽不見震天聲響，更不用說實際的人員傷亡，只要在電腦前輸入特定指令就可以癱瘓敵方網路，甚至奪得敵國基礎設施的運作控制權，造成該國的動盪。

多年前朝鮮半島劍拔弩張之際，南韓境內多家電視台以及相當多的金融機構，突然都因遭受不明網路攻擊，造成三萬多台電腦及伺服器全面癱瘓，南韓民眾甚至想在金融機構領點錢都無法辦到。以如此網路入侵的手法擾亂敵國的社會秩序，將造成該國內部的極大壓力；而受攻擊方甚至不知敵從何來？數量有多少？受到破壞的程度為何？

剎那間一切彷彿陷入迷霧之中，不知何從反擊。

在《下一場世界戰爭》這本書中，著名軍事學家亞當斯就說過：「在未來的戰爭中，電腦本身就是一種武器，前線無所不在；奪取作戰空間控制權，不是砲彈或子彈，而是電腦網路系統中流動的位元組。」就以西班牙政府在４月間逮捕一名荷蘭籍的駭客來說，他在一輛自用的貨車內就發動足以影響荷蘭、瑞士、英國和美國網路伺服器的大規模分散式阻斷服務攻擊，其攻擊最大強度甚至高達每秒三千億位元。正因為網路攻擊的力量如此強大，故而美國特別將網路空間視為海、陸、空和太空以外的「第五戰場」，並加強國防部網路方面的開支，以攔截來自中共、伊朗、俄羅斯及其他國家逐日升高的網路威脅，並加強政府和民間電腦網路的防護措施。而我國國防部也將成立新的資電作戰部隊，藉由提高網路作戰投資，以強化「科技」與「速度」兩項攸關網路戰勝負的關鍵要素，並透過各項演練驗證相關資電作戰以及資訊防護成效；此外，更規劃在北、中、南、東建立地區資安防護管理中心，整合資安事件通報及應變機制，為的就是期望能夠掌握先機，應變制變。正因資訊安全易攻難守，在不計其數的網路攻擊中，攻擊方只要成功一次，可能就足以致命；而在防禦方，不論就經費或是人員訓練上來講，所有相關作為都比攻擊方所付出的代價高出許多，就因如此，攻擊方在網路戰中可說是占有極大的優勢。此一威脅，無論政府公務部門還是民間企業，甚至是一般民眾，均不能掉以輕心。

隨著智慧型手機的普及，以往在電影上看到駭客使用攜帶型輕巧裝備，在短時間內癱瘓政府網站、竊取國家機密的場景，已悄然遊走在你我之間。而在看似便利的雲端架構下，資訊安全問題對國防、金融、基礎建設等方面可能造成的傷害，將比以往更大。所以每個人都應有「資訊安全，人人有責」的認識，建立「預防重於治療」的觀念，才能在享受資訊設備與網路服務所帶來便利之際，同時確保各項資訊的安全。

臺中榮民總醫院提醒你!也關心你!