面對網路攻防這場「沒有聲音的戰爭」，除需提升防駭技術外，保密觀念的建立亦是不可輕忽。

沒有聲音的戰爭

◎鍾永和

依據研究資料預測，到 2020 年全球將會有 500 億筆資料在網際網路中流通，並透過網路空間交換、取得及蒐集等。也就是說，眾多機敏資訊在轉瞬間，便流傳於網路空間，無形中增大滲透破壞與情蒐空間，不但極易肇生資訊安全危機，更將損及國家安全與利益。我們對資安的重視誠如馬總統所強調，對於駭客、網路攻防的重要性越來越高，可說是「沒有聲音的戰爭」，政府各單位應全面檢討，妥為因應。

再者，資安狀況不僅是電腦作業系統的問題，更是多數駭客透過網際網路平臺對特定電腦或網站實施攻擊與癱瘓的作為。經評估許多安全漏洞乃係出自人為疏失，意即輕忽資訊安全的觀念所致。美國哥倫比亞廣播公司新聞網曾報導，前美國中情局局長道奇即因使用家中無安全防護措施的電腦上網及收發電子郵件，結果導致機密資料外洩，落入外國間諜手中。就國內的情況而言，雖然軍事機密一直是中共處心積慮所欲得到的資訊，但對其他民間的資訊亦不鬆手，且部分民眾對資訊保密仍未建立應有的觀念，往往因此產生保密安全的罅隙，諸如文書作業為圖一時之便，違規將公務或機敏資料隨意存置於個人隨身碟，透過被控制的電腦傳送至駭客手中，衍生後續洩密疑慮等。探究普遍性缺失之主因不外乎是：人員未能遵守保密規定、資料存置未符規範、資媒防護仍有罅隙、保密警覺有待提升等，仍需加強資訊安全控管作業機制、電腦安全防護工作，以及積極致力結合產官學研各界力量，有效強化資安預警及網路防禦能力。

網路因具有虛擬特性，故安全性極易使人疏忽，美國《華盛頓郵報》曾報導，大批駭客經由中國大陸網站企圖入侵美國國防部、國務院、能源部、國土安全部，甚至武器承造商的網路，並成功入侵眾多民間公司企業的網路，當時駭客隨意進出電腦系統，既沒有犯下鍵盤輸入上的錯誤，也沒有留下入侵途徑，僅僅不到 30 分鐘，網路安全系統後門洞開，美國情治人員將這些被入侵的網路資訊拼湊後發現，駭客源頭最可能來自中共軍方，美國政府部門與企業事後都意識到問題的嚴重性，紛紛強化網路資訊安全設備與反偵測裝置。我國也正積極朝此方向努力與精進，需藉各部會能量的整合運用及國民的全力配合，才能事半功倍，確保網路資訊的「相

對性安全」。

中共領導人習近平在十八屆三中全會上，一方面特別強調網路和資訊安全，牽涉到國家安全和社會穩定，是新的綜合性挑戰；但事實上在另一方面，中共為遂行其非對稱及非接觸的作戰理念，早已成立電腦網路攻擊資訊戰的網軍，並設置資訊兵團以利單位組建資訊戰管；除此之外，中共還設置資訊戰武器及戰略之專責研究機構，並不斷進行虛擬實戰，不僅美國五角大廈等單位迭遭中共網軍攻擊，我行政院亦證實曾遭中共網軍以駭客模式有系統、有計劃地入侵包括警政署、健保局在內數十個政府單位的網站，被木馬程式竊取資訊或破壞癱瘓電腦網路，這些情況顯示臺海表面雖然無煙硝味，但中共早已透過虛擬世界對我攻擊破壞，我方若長期無法鞏固資訊安全，防杜保密罅隙，將予敵人可乘之機，招致洩密風險。

21 世紀是網路的世紀，掌握資訊優勢才能掌握經濟及軍事優勢，但機密資訊的保護亦不容忽視，網路具有即時性及無國界的優點，也因此帶給現今繁忙的社會無比便利，一方面可以利用網路進行資訊查詢、網路連線通訊或是跨國界的交易行為，但另一方面網路也使駭客有機可乘。若在使用時疏於防範，則個人電腦中重要的資訊將輕易落入有心人士手中，進而發生一連串的負面效應，其危害程度可能涉及國防安全，故不容小覷。

在面對複雜多變的資訊作業環境，為了保護本身的資訊系統不被敵人利用或破壞，除強化資安預警及網路防禦能力外，更要從政策面、管理面、技術面三管齊下，深植國人正確的資安保密觀念，建構嚴密的資安防護機制與資安管控措施，方能打造堅固的資安防護網，有效維護國家利益與國防安全。

林試所政風室製

資料來源：清流月刊