現代戰爭的前哨戰—網路戰

◎蘇啟維

現今科技發展迅速，「智慧型 3C 產品」、「雲端空間」、「Wi-Fi 及藍芽等無線傳輸」與「App 程式」等新型技術及軟硬體相繼問世，讓世人依賴電腦與網路執行各項工作日深；但伴隨而來的電腦病毒、駭客入侵及資料遭竊等資安問題，長期以來亦困擾著各國政府、企業及人民。而現在的「網路戰」更可兵不血刃地破壞對方的指管通資中樞，導致無法動用武器、指揮鏈癱瘓，達到不戰而屈人之兵的效果；若網路一旦遭到癱瘓，不僅政經建設受到影響，可能導致社會動盪，後果相當嚴重。面對日趨惡化的網路安全威脅，各先進國家莫不積極尋求對策，且將其置於極高的戰略位置來籌謀。

分析當今戰爭型態，在空間上不打全面戰爭，係以殲擊目標的局部作戰為主，所謂的「斬首行動」、「外科手術」當為貼切的用詞；為了要避免持久消耗，各國多改以霹靂行動速戰速決。欲達成此一作戰方式，尤其借重資訊網路的作戰能力，例如利用誤導、錯亂、阻絕、封鎖等手段，造成對手在開戰前即陷入「耳不聰、目不明」的狀態，無法正確決策。戰場的決勝固然受人員、武器、裝備等諸多因素的影響，但決定戰爭勝負的關鍵，則在於資訊作戰能力的利鈍。尤在兩軍對陣中，資訊戰力猶如人之中樞神經，致勝之道，一方面要提升資訊精確品質與決策能力；另一方面則須確保資訊安全，避免被敵入侵，陷入敵暗我明的險境。現代戰爭的發展趨勢，資訊戰不僅是前哨戰，更可藉由網路和通信技術，先期掌握情資，癱瘓敵方軍事系統，進而獲取戰場優勢。美國陸戰隊作戰發展司令部指揮官佛林表示，網路作戰與防衛能力越來越重要，美軍必須持續投資開發，因為現今所有戰力都離不開網路，不論是戰場情偵、目標鎖定，或是聯合作戰，都需要運用網路。

鑑於頑強且複雜的網路攻擊行為日益增多，為了建構足夠的網路作戰能量，全球至少已有 46 個國家成立網路作戰部隊。以軍事大國美國為例，即在 2014 會計年度投入數億美元擴大既有的網軍規模並安置所需設備；另外北約組織亦針對如何提高盟國應對現代網路戰爭的能力，以及北約集體的網路安全，召開首次的 28 國國防部長會議，在在說明資訊戰與網路戰已為當前各國重視的國防議題。而我政府團隊對資安工作的推動向來不遺餘力，資安防護策略係採深度、廣度及速度的三維度，包括協助機敏機關強化資安防禦縱深以降低損害；建立資安聯防擴大整體防護網絡，共同防範駭客攻擊；以演練及預警提升機關應變速度，落實資安防禦措施等。美、韓兩國先前陸續遭到駭客攻擊，美國第一夫人蜜雪兒及部分高階首長個人資料被公布在網站上。駭客的攻擊旋即引起國際社會的重視與撻伐，也宣告全球已邁入網路戰爭時代。

美國司法部長埃里克·霍爾德即曾公開表示：「中國駭客坐在電腦桌前，就能竊取維吉尼亞州一家軟體公司的程式碼；國防承包商員工只要敲幾下鍵盤，便能盜竊價值數十億美元的設計或程（公）式。」可見任何機密一旦缺乏完善的防護機制，便可能暴露於危險之中。軍事學家亞當斯（James Adams）在其《下一場世界戰爭》中亦強調：「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。」以全球發生的網路攻擊事件而言，南韓國內多家電視臺和銀行遭大規模駭客攻擊，肇致網路全面癱瘓；之前美聯社推特帳戶亦遭駭客入侵，發布假消息，直指白宮發生爆炸，歐巴馬總統受傷，造成紐約股市一度大跌。

網路攻擊適用範圍極為廣泛，「網路入侵被廣泛視為係一種對於國家安全、公眾安全和經濟最嚴重的潛在挑戰」。國安局長曾表示，我國遭攻擊次數已逾六百萬次，顯示情報機關與政府網路為駭客主要的攻擊目標。資安廠商趨勢科技不久前發表的白皮書也指出，80%的臺灣企業並不知本身已遭「進階持續性威脅」（APT）的攻擊；且由於一般資安處理方案並沒有辦法解決 APT 攻擊問題，致受駭目標除政府單位外，還包括高科技產業、金融業和中小企業等，因此建議企業界最好與專業資安夥伴合作，定期檢視安全死角，才能有效防禦。事實上，面對日益嚴重的資安威脅，美國安全公司目前調查發現，我國在全球 177 個網攻來源國排名第七，大陸則仍是網路攻擊來源之首。行政院江院長亦曾指出，政院平均每週遭逾一千九百次網路攻擊，每月約有四百四十次電子郵件攻擊，整體資安情勢頗為嚴峻。現今大陸網軍或駭客發動網路攻擊的消息時有所聞，根據國安局統計，該局遭駭客「刺探攻擊」的次數，累積高達三百二十七萬多次，其中「惡意攻擊侵擾」達到七萬多次。國安局相關報告更指出，大陸近年透過網路竊取我方資訊高達二萬六千多筆，而實際狀況恐更為嚴重。由此顯見大陸近年在國際進行網路攻擊相當猖獗，倘若這類攻擊活動均告成功，將造成我方莫大的損失，故而立法院外交及國防委員會審查「國家安全局 103 年度施政計畫及收支預算案報告」時，即有立法委員提案要求國安局研擬禁止 4G 電信業者採購中國大陸廠商的網路設備，以維國安。事實上，我政府去（102）年底曾對行政院所屬 33 個二級部會進行情境、實兵、社交工程郵件等演練評估；除了部分資安維護仍須強化，在社交工程郵件演練中，亦有少數機關有超過二成人員因好奇心開啟八卦、新奇、娛樂等模擬攻擊的社交工程郵件，凸顯保密工作之良窳，除應建立健全的軟、硬體設備外，更取決於人員對保密、資安觀念的落實！

雖然沒有隆隆砲聲與烽火硝煙，但是隱藏在數位中的網路戰爭更讓人防不勝防。從資訊保密的角度看，小從網路遊戲帳號密碼被盜，大到企業、國家的機密外洩，無不造成個人、團體與國家的傷害。從軍事的角度來看，則說明了兩軍對戰中，若要取得勝果，首先要落實情資管控，避免駭客入侵與資料外流，以因應無所不在的網路作戰威脅。為此，國防部向來極為重視資安防護工作，將通資安全視為國軍達成各項作戰任務、遂行資訊作戰的重要作為，積極從事國防資安整

備工作，除建置嚴密的資安防護機制、頒布多項資安管控措施、主動查察違規事件外，另從政策面、管理面、技術面三管齊下，落實資安工作，並將網路攻擊列入年度漢光演習重點驗證項目，未來也將成立新的資電作戰部隊，提升國軍資安能量。此外，為提升國軍資安防護強度，國防部規劃在北、中、南、東建立地區資安防護管理中心，並整合資安事件通報及應變機制，期能發揮「早期預警、即時應變」的功能。國軍除持續強化各項軟硬體基礎建設及防毒作為，並建構純淨的作業環境及各項保密與資安規定，嚴格要求國軍官兵澈底落實。

面對兩岸關係從昔日緊張對峙，到邁入和平與良性互動發展，惟中共仍持續強化國防武力建設，且不放棄武力犯臺；我們身處在「對立的和諧」局勢中，不能讓對方從內部攻破。有道是「不計其數的網路攻擊，只要成功一次，就足以致命。」因此，無論政府公務部門、國軍單位、民間企業，乃至一般民眾均不能掉以輕心。須知，資訊網路作戰是場沒有砲火的戰爭，也是不經宣戰就已全天候進行的戰鬥，換句話說，每一位電腦操作者都已在戰場上，都應自我提高警覺，遵守各項資安保密措施；各單位也必須展現集體約制力量，有效防範洩違密事件發生，共同確保組織與國家的安全。

臺灣屏東地方法院檢察署關心您