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。

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