# 資訊戰國家戰略

●廖宏祥／國防大學軍事學院榮譽講座、台灣和平基金會研究中心主任

據2000年的美國國會資訊戰研究報告指出，解放軍數年前即已全力研發資訊戰力。而中國人民解放軍疑似運用其「網軍」，從今年3、4月開始，陸續入侵我國政府機關部分網站與資訊系統。這支網軍的攻擊對象甚且廣及世界各國。

美國高級戰爭及資訊研究中心（Institute for Advanced Warfare and Information Studies）對資訊戰有如下之定義：「為了在軍事及商業領域獲得優勢，採取攻擊及防禦之手段，使用計算機科學與資訊系統來利用、誤導、以及摧毀敵人之資訊系統，同時亦保護自己之相關系統」。

於廣義之「資訊戰」中，潛在敵國可將我國對資訊之產生、獲得、傳送、分配、利用、儲存等設備，列為戰爭目標；並以前述之資訊型態直接作為戰爭武器，或以政治、經濟、心理、軍事等作輔助手段，以達成戰爭目的。就狹義之「資訊戰」來說，敵可將我電腦網路列為高科技攻擊目標；透過造成電話、電力中斷等破壞，削弱我國之實力。資訊戰利用的正是現代社會對電腦與資訊之依賴，影響所及包括電子通訊、電力供應、金融業務，及空中交通管制等。發展資訊戰計劃之國家，顯然瞭解攻擊敵國前線與後方電腦系統之價值。資訊戰對整個國家社會結構之破壞，如經濟、商業、通訊、與交通等，可能不亞於傳統總體戰爭之程度。如忽視資訊系統之潛在戰場運用，僅純仰賴有形之軍事戰力，無異建造一條一夜之間可能徹底崩潰之現代馬奇諾防線。

於傳統戰爭中，自動員、整備乃至部署，均為戰爭前不可避免之階段。然資訊戰使這些必要階段變得更為快速。甚至可能於傳統戰爭未行開戰之前，資訊戰已將一方之戰力瓦解，或使一方屈服於政治、軍事壓力，致因戰意及戰力之喪失而結束戰爭。正如核戰爭之「先發制人」——若將敵之核戰力先期予以殲滅，顯然先發動攻擊之一方，將取得決定性勝利；在資訊戰範疇亦可能有相同之效果。換言之，假如欲發動攻擊之一方，先發制人將敵方所有與資訊相關之設施及產業，完全於短時間內予以摧毀，那麼遭摧毀之一方，將無還擊能力。

資訊時代之到來，亦可能引發全球性政治及軍事關係之不穩定。正如冷戰時期有核嚇阻之理論研究，在資訊時代可能亦有資訊嚇阻之理論出現。所不同的是，危機管理與政治決策等領域，在資訊時代，戰爭節奏加快，可能已超乎傳統之政治領域所能想定。故討論資訊戰應納入以下人員：政治人物、科技專家、軍事專家、以及商業領袖等。資訊時代之來臨對戰爭型態及社會所產生之影響極其深遠。因此各種領導人物接受資訊教育，了解資訊時代

所應有之決策過程至為重要。

廣義而言，資訊戰的目的就是在影響甚至瓦解敵人的決策機制。戰略性國家資產不但是政府和社會正常運作的指標，也是國家能遂行抵抗行動的能力，更是民心士氣賴以維繫的基石。因此，當我們努力維護台海軍事平衡的同時，保衛國家資訊基礎建設更是不可或缺的一環。台灣為了在未來的資訊戰中瓦解敵人攻勢的有效性，並幫助我保有第二擊的能力，自應未雨綢繆、及早因應。

為了防衛美國的重要基礎建設，美國總統在1998年5月下令在聯邦調查局下設立「國家基礎建設防護中心」及商務部下設立「重要基礎建設保證局」，以統合美國政府各部門對相關重要基礎建設的系統性分析，以提升美國對潛在弱點的威脅評估與反應能力。

基於此，我國可能亦需要設立一個新的政府機構或小組以協調並協助建立各部會，如經濟部、財政部、交通部等，應付資訊戰的挑戰。此「資訊戰小組」初期應可設於國安會。「資訊戰小組」應整合國內與資訊相關的研發單位如資策會、中研院資訊所、大學院校，與眾多民間產業，並協助撥款分工研發如：網路監控、駭客辨識、損害評估、攻擊後重建、編碼與解碼、網路與資訊安全等系統軟體與程序。「資訊戰小組」應協調政府各部會資訊系統使用者與管理者，確認各該系統的主、次要功能與服務、結構弱點、與邏輯漏洞等，並建構國家整體資訊系統藍圖，與各系統的相對重要性。供我國於準備資訊戰的過程中，做全面系統性的分析，以削弱敵人攻勢資訊戰的有效性。

雖然現存的官僚體系可能會排斥這個新機構，但在起始的最低程度上，國家安全會議應建立任務編組以：

（一）確認我國資訊基礎建設的主要組成元件、量化我現有的攻勢及守勢資訊戰能力、規範我資訊戰應達到何種水準、並建立具體衡量指標；

（二）蒐集及評估資訊戰的威脅與風險，如潛在的弱點、可能的威脅、攻擊的效果及其造成的連鎖效應等；

（三）協調國內及國際的執法單位，以促成國際間對資訊戰的情報交流，並促進與國際間的資訊產業合作；

（四）促使經費提撥以研究發展能夠監控、追蹤、辨認、重建及攻擊與損害評估的技術，而密碼及網路安全的技術研發亦屬不可或缺；

（五）提供政府及民間單位資訊戰的教育，以警覺防範措施；因應各單位需要，協助其制定守勢資訊戰準則及程序；

（六）規劃政府緊急通訊系統、最低必要緊急通訊網路，以作為「必要的最少資訊設施」（Minimum Essential Information Infrastructure）的基礎；

（七）建立資訊戰的戰術預警指標、攻擊評估、損害評估及緊急反應與應變措施；同時宣告資訊戰的報復政策，以達成某種程度的嚇阻；

（八）制定一套安全調查程序，以廣泛吸納民間資訊工業能量並與產業界合作建立伙伴關係，擴大與民間合作的基礎；

（九）建立資訊戰認證標準；並建議政府提供政策上的誘因，鼓勵公民營單位獲得資訊戰認證；

（十）協助建立國家軍事資訊戰戰略，強調指揮管制通訊系統的建設及能量提

升，同時全面進行以資訊為基礎的軍事事務革命。

在戰史上，經過精心設計的欺敵劇本層出不窮。一般以為欺敵不過是偽裝、佯攻、或是散佈假情報而已；其實，欺敵更是結合作戰彈性與謀略，來操縱敵人的認知與行為的計劃過程。正如美國空軍的資訊戰中心所揭櫫的，欺敵除了可以阻撓敵人的情蒐行動，更可破壞其資訊戰能力。

據「中國國防報」報導，解放軍已組成一支民兵偽裝分隊，專門從事製造與部署假導彈、戰車等武器裝備的工作。顯示解放軍瞭解在現代高科技資訊戰的精確打擊下，採用偽裝以增加存活率的重要性——雖然這些欺敵精神和兩千年前農業時代戰爭所使用的並無多大不同。

然而欺敵不只是軍事上的運用而已；它更是在防衛重要國家基礎建設上的一種謀略。當我國正日益仰賴資訊系統提供日常生活必要的功能時，資訊安全就變得無比重要。但是因為今日的科技無法提供百分之百的資訊安全防護，故資訊欺敵應是防衛我重要資訊基礎建設的優良選項之一。而經過良好規劃的資訊欺敵措施能以大量的假目標迷惑入侵者、提供假資訊情報以混淆敵方的決策、或誤導攻擊者進入陷阱系統中，因而瓦解敵之攻勢作為。

然而資訊欺敵僅是眾多能增加系統存活率的技術之一而已。處理系統存活率的問題應當從四個要項著手：辨認、抵抗、報復、與復原。辨認是偵測敵人攻擊模式與損害評估的能力；抵抗是擊退攻擊保護己方資產的能力；報復不但是解除敵再次發動攻擊的能力，更是嚇阻敵冒然進犯的利器；至於復原是在攻擊時，維持重要系統功能、降低攻擊損害、及攻擊後迅速恢復正常的能力。

由於資訊系統不斷演變得更為複雜，因此資訊安全必須是一個動態的觀念。系統複雜化雖然可使攻擊者較難下手，但是也會使防禦者難以了解與控制潛在的弱點與威脅。雖然防禦者不遺餘力的使用資訊強化等手段來防範未然，但是由於現今科技的限制，沒有任何一種技術可以保證資訊安全。因此，不但在技術上要能了解敵我雙方系統的任務、功能、與架構之外，提升存活率更需要風險管理的觀念與策略。

同時，當我們處理威脅及弱點的問題時，所要考慮的應不只是硬體、軟體、及科技而已；就像戰爭的本質與人性因素和文化脫不了關係一樣，資訊防護更重要的還有人的因素。在資訊時代科技似乎是一切的原動力，因此「資訊戰士」常會將注意力集中在如加密和防火牆這些技術上，但卻忽略了如訓練、動機、和程序等人為和操作的問題。

準備防衛資訊戰千頭萬緒；然而，吾人更應牢記人——而不是系統－是最容易被操縱和利用的一環。畢竟，戰術可以改變，結構與組織也可以改變；但是，不論科技如何演變，戰爭中人性的本質卻是亙古不變的。 ◎