網路戰資訊安全探討與省思

梁華傑

提　　要

一、21世紀是網網相連的網際網路世界，掌握資訊優勢將成為掌握經濟與軍事優勢的基本條件，而資訊優勢的建立，是建立在資訊安全基礎上。

二、國家重要基礎建設(NII)與國防基礎建設(DII)兩者間形成互賴關係，在資訊安全領域中之互相滲透性與互賴，程度日深，通資安全成為國家綜合安全重要的一環。

三、「資訊安全」是一個寬廣且複雜概念，從龐雜無章的安全問題中，建立資訊安全機制，關鍵在制訂乙套「行之有效」的安全規範，方是從根本消除安全漏洞與罅隙的重要途徑與正本清源作法。

四、滿足資訊安全須依循「機密性(Confidentiality)」、「完整性(Integrity)」及「可用性(Availability)」三個基本原則，簡稱為「CIA」，絕不可為求「機密性」、「完整性」而妨礙「可用性」，亦不可為求「可用性」而忽略「機密性」與「完整性」。

五、「有效嚇阻、防衛固守」為臺澎防衛作戰戰略指導，就「網路戰攻防」言，應全面整合有限國防資源，建構多層次安全防護機制，以有效扼制中共網軍／駭客之威脅，「寓守於攻」、「形於無形」，蓄積磨礪戰略性資訊戰攻防能力。

六、在「網路戰攻防」領域與範圍內，具有多樣性、多變性的網路攻擊方式與手段，攻者形於無形，防不勝防，故就資訊安全領域言，惟有建構多層之安全防護機制，並以「勤能補拙」思維，主動提供技術支援服務，才能將資訊安全提升到一定的層次，資訊安全充滿挑戰與機會，應體認資訊科技所帶動的軍事轉型與威脅型式變化，妥採防衛措施。

七、創造資電優勢、蓄積戰略性資訊戰攻防能力、網路戰攻防及資訊安全，關鍵完全在「人」；人才培育及留用為前三者之基礎；而所有電腦使用者之安全操作能力與知識，為資訊安全之根本，關鍵在技術人員之主動支援服務。

關鍵詞：網路戰攻防、資訊安全、資訊安全規範、網路戰將、以小博大

壹、前　　言

資訊科技的日新月異發展，電腦、資訊系統與網際網路已成爲日常生活與職場工作無可避免的使用工具，網路戰隨著資訊科技的發展，巧然威脅著人們所使用的電腦、資訊系統與網際網路，致資訊安全躍升爲國家、社會、政府機關（含國防軍事機構）、企業、家庭，甚至於個人的重要安全領域之一。爲確保電腦、資訊系統與網路安全，各種防毒（駭）軟體、防火牆與資訊安全技術，不斷演化進步，市場產品琳瑯滿目，然「駭客」、「有組織之攻擊者」及「惡意程式（含電腦病毒、木馬程式）」亦隨著技術進步發展而日趨新穎，且更具威脅性，所造成的損害，年年都在增加，各類型入侵與攻擊，防不勝防，而爲加強通資安全所投注的大量金錢與心力，卻仍難達預期防範效果。21世紀是網網相連的網際網路世界，掌握資訊優勢將成爲掌握經濟與軍事優勢的基本條件，而資訊優勢的建立，必須是建立在「網路戰攻防」的資訊安全基礎上。

2001年，舊金山電腦安全研究所與美國聯邦調查局對500位電腦安全專家進行調查研究（這些電腦安全專家大都在大公司或政府部門工作），顯示：有90%的專家在電腦系統中安裝防火牆，有60%的專家使用具防盜警報裝置的應用軟體來偵察入侵，然卻有90%的專家表示，難以抵擋外來入侵。經統計歸類，2001年所發生的安全狀況，包括感染病毒、網站遭破壞、信用卡資料遭竊，及公司機密資料被入侵竊取，其中以金融詐欺案最爲嚴重，每件案子損失，平均高達四百六十餘萬美元[註一]。依2006年《美國國家安全報告》指出：美國國防部電腦系統2005年上年度遭到駭客攻擊的次數總和達21,124次，平均每次防護攻擊需耗資150萬美元，故爲對付駭客，美國防部每年要付出三百多億美元的代價。顯見，僅管是電腦安全專家，仍難以防犯蓄意攻擊者、駭客及電腦病毒的入侵、攻擊、破壞。

國軍對資訊安全工作向來相當重視，尤以近年來，在中共網軍與具有惡意企圖的駭客環伺下，爲確保資訊安全，可說是祭出重懲、重罰，企圖扼制疏忽所肇生的資訊安全事件。然就整體系統化觀察所制定的資訊安全政策、資訊安全相關規定（範）、實際運作情形，及從已發生的資安事件分析，以資訊安全向度言，仍亟待改善；另部分限制性規定（範）與措施，未符「國際資訊安全管理標準體系BS 7799(ISO 17799)」，實有待商榷及改善。

爲避免以往探討資訊安全文獻的專業生澀，本文將以指參人員（使用者）向度出發，深入淺出的探討資訊安全相關觀點與安全性措施，並置重點於廣大使用者必須具備的資訊安全基礎知識與技能，期在「網路戰攻防」對抗中，對國軍資訊安全做出省思與些微貢獻，並提升電腦、資訊系統與網路使用者的基本專業知識與技能。

貳、何謂資訊安全

由於資訊科技的快速發展與日新月異，對生活、社會型態、政府組織運作、國際溝通交流及軍事作戰運用等，都產生重大且深遠影響。又因資訊安全涉及層面廣泛，加之資訊科技發展快速，新技術、設備與軟體不斷推陳出新，產品生命週期大幅縮短，以致於要對「資訊」提出一個適當定義，的確困難。若從現有的文獻資料來歸結出「資訊」

註一《清流月刊》，民91年5月1日，頁44。

的定義，在一定時間後，所歸結出之定義可能已不符合現實潮流。

此外，各領域對「資訊」一詞所下的定義亦不盡相同。在資訊管理界，將「資訊」定義爲「凡與管理決策有關的訊息，都稱爲資訊」，故在探討管理決策領域上則屬適當，但卻無法解釋資訊與社會和生活間的密切關係[註二]，更無法解釋國防軍事領域之資訊運用，遑論「數位化戰場」、「網狀化作戰」之複雜關係。1970年後，隨著電腦科技的發展，電腦的主要功用變成「處理資料」，故被認爲在電腦中處理的資料就稱爲「資訊」，於是「資訊」被界定爲「由資料中萃取出來有用的訊息」[註三]。

人類是透過各種感覺器官從環境中獲得各種訊息，形成對事物的一種感性認知，再經大腦處理後形成理性認知，這個過程稱爲「能知」，而人所知道的所有事物統稱爲「所知」。人可以透過各種途徑（如，聲音、文字、圖像、色彩、線條等），將「所知」表達出來而形成「溝通」，也稱之爲「訊息交流」。據此，可以對「資訊」下一個廣泛且通用的定義：「資訊就是所知表現在報紙[註四]、書籍[註五]、電視、電腦、網路[註六]等媒介上的形式」。

由於科技的發展進步，進入以數位化技術而產生的數位媒介，將所有的「資訊」以0與1兩種型態儲存，而且可以取代任何傳統媒介，如轉換爲電子報、電子書、網路廣播、網路電視等。利用「電腦」作爲數位媒介，可匯集大量資訊，並對資訊進行處理，增進對資訊的利用能力[註七]，而透過「網路」這種數位媒介，則能將大量的資訊傳送至網路所及的廣大範圍，於形成以「網路」數位媒介爲載體的資訊世界。

同樣，資訊科技也廣泛運用於國防事務與軍事作戰領域，並大量採用商用的軟、硬體與數位媒介，大幅增進國防與軍事資訊的傳播速度與範圍，也增進處理國防軍事資訊的量與速度。因此，在資訊科技時代的戰爭型態，已由傳統的線性作戰轉爲非線性作戰，由接觸作戰轉爲非接觸作戰，由時間序之接戰行動轉爲同步化作戰行動。國家重要基礎建設(NII)與國防基礎建設(DII)兩者間形成互賴關係，在資訊安全領域中之互相滲透性與互賴，程度日深，通資安全成爲國家綜合安全重要的一環。

通資科技與數位媒介的廣泛結合與運用，在數位媒介中大量傳輸與處理的「資訊流」與「資訊」，亦涵蓋國家機密、國防軍事機密、商業機密、科研機密及個人隱私等，故確保在數位媒介中之「資訊流」與「資訊」的安全，就成爲資訊時代極爲重要的課題。基此，所謂「資訊安全」，就是「爲確保資訊免遭破壞、竄改、未經授權存取等侵犯，使資訊得到保全」。

註二 張博竣，《資訊安全管理實務》，臺北市：文魁資訊股份有限公司，2004年4月，頁1-2。

註三 前揭書，頁1-2。

註四 報紙和書籍是使用「紙」爲媒介，是大多數人每天接觸各種資訊的主要途徑，使用者可以直接閱讀；惟此類媒介的資訊都是事先排版的，發行後就無法變更，且媒介中所承載的資訊量有限。

註五 同註四。

註六 電視、電腦及網路是使用「電子」爲媒介，是利用粒子、電波、電磁介質、光電介質的能量變化，或能量的狀態發生改變，進而傳達不同的資訊。通常要獲得這些媒介中的資訊，須使用特定能量，在媒介上將電能轉化爲聲音、光能、熱量等形式的能量，俾以將資訊轉換成各種可看、可聽的形式，且爲維持持續獲得資訊，能量必須持續補充，一旦失去或沒有能量，電子媒介將恢復原本的靜止狀態。

註七 張博竣，《資訊安全管理實務》，臺北市：文魁資訊股份有限公司，2004年4月，頁1-3。

「資訊安全」的概念，是泛指與電腦相關領域的安全措施，根據電腦的實體組成及電腦使用上的因素，資訊安全可分爲下列三種：[註八]

一、硬體安全：包括電腦硬體環境控制、機房管理、硬體設備使用安全。

二、軟體安全：包括系統安全、應用程式安全、個人資料安全、公務資料安全。

三、個人安全：包括人身安全、個人隱私安全、網路通訊安全。

參、資訊安全規範

「資訊安全」是一個非常寬廣且複雜的概念，要從看似龐雜無章的安全問題中，建立資訊安全機制，關鍵在制訂乙套「行之有效」的安全規範，方是從根本消除安全漏洞與罅隙的重要途徑與正本清源作法。

在資訊安全的複雜領域中，要滿足資訊安全有三個基本原則：「機密性(Confidentiality)」、「完整性(Integrity)」及「可用性(Availability)」，簡稱爲「CIA」[註九]原則。「機密性」是指透過對資料進行加密，以達到保護資料之目的；「完整性」是指透過對資料的保護，避免遺失、被竄改等；「可用性」是指確保資料即時可用，能夠滿足各種使用需求，三個基本原則必須不偏不倚，相互均衡，絕不可爲求「機密性」、「完整性」而妨礙「可用性」，亦不可爲求「可用性」而忽略「機密性」與「完整性」。

世界上各政府組織(GO)、非政府組織(NGO)、國防軍事機構、企業機構的資訊安全規範，大多以「CIA」三個基本原則[註十]爲基礎，並整合各種安全技術，包括授權控制、存取控制、稽核控制、資料驗證及實體驗證等五項機制，據以發展出適應組織環境運作的「資訊安全規範」。

一、授權控制(Authorization Control)：係指每個需要存取的使用者，都有「唯一識別碼」，透過該識別碼判斷是否允許使用者登入和存取資源。

二、存取控制(Access Control)：係根據使用者職位或工作類型來設定資料的存取權限，控制使用者對資料的存取行爲。

三、稽核控制(Audit Control)：係記錄系統或使用者的活動，以便追蹤資源的存取情況。

四、資料驗證(Data Authentication)：係爲避免資料遭到未經授權存取，所建立之資料驗證機制。

五、實體驗證(Entity Authentication)：係爲避免冒名頂替者之存取資源，所建立之實體驗證機制，在確認實體身分後，方可允許其存取資源。

「資訊安全規範」須由具有權威的單位制訂，在臺灣雖然有國家資通安全應變中心制訂一些相關的資訊安全規範，但國內（含國防軍事機構）所認可的資訊安全規範，大多是由「國際標準機構(ISO)」所制訂定的規範而加以修改引用，如ISO 13335、13569、17799等都是被廣泛採用的安全規範。基此，國軍所引用暨修改自「國際標準機構(ISO)」所制定之資訊安全規範，能否

註八 同註七。

註九 岸田明著，林雯譯，《資訊安全的第1本書》，臺北縣：博碩文化股份有限公司，2003年10月，頁74。

註十 機密性、完整性、可用性三個基本原則，是1992年由「經濟開發合作機構(OECD)」所提出的；而GMITS則在此三個基本原則外，加上「追蹤性」、「眞實性」、「可靠性」等原則；「歐洲電腦工業會(Extended Commercially Oriented Functionality Class)」則又加上「非觀察性(Unobservability)」、「匿名性(Anonymity)」、「無關連性(Unlink ability)」、「課金性(Pseudonymity)」等原則。

「行之有效」則成爲能否落實資訊安全的關鍵與基本防線。

如何才能確保資訊安全？又如何評定安全風險呢？可透過國際資訊安全管理標準體系BS 7799(ISO 17799)來判斷。以下將簡單探討「國際標準機構(ISO)」所制定的資訊安全規範，並請讀者反芻國軍的資訊安全規範是否合理且行之有效。

一、ISO 17799/BS 7799安全規範[註十]

「ISO 17799」係源於「英國標準協會(BSI)」在1995年2月所提出的「BS 7799安全規範」；「BS 7799」包括「BS 7799-1（資訊安全管理實施規則）」及「BS 7799-2（資訊安全管理體系規範）」兩個部分。

「ISO 17799」對資訊安全管理提供很好的建議，可做爲資訊安全部門在建置、規劃、管理、維護資訊安全時使用。「ISO 17799」提供127個安全控制措施，以協助企業、組織、政府機構（含國防軍事機構）在運作過程中，以控制對資訊安全有影響的因素。這127個安全控制措施可分爲十個面向：

㈠安全政策面向：係制訂資訊安全措施，爲資訊安全提供管理指導和支援。

㈡組織安全面向：係建立資訊安全基礎設施，管理組織範圍內的資訊安全，以維護其他人存取組織內資訊的安全。

㈢資產分類與控制面向：係稽核所有的資訊資產，以便對組織資產提供適當的保護，並做好資訊的分類。

㈣人員安全面向：係關注員工工作職責的分配，以確保相關人員接受與安全知識有關的教育訓練，並確保授予使用者適當的使用權限。

㈤實體和環境的安全面向：係規定安全區域，避免未授權者非法進入；保護設備安全，防止因資訊資產遺失、損壞而導致服務停止。

㈥通訊和操作安全面向：係確保在網路通訊過程中，資訊的安全受到保護；制訂系統規劃和操作規則，確保資訊處理方法的正確和安全操作；防範惡意程式，保護軟體和資訊的完整性。

㈦存取控制面向：係制定存取控制機制，以控制使用者對資訊的存取行爲；建立以使用者身分爲基礎的存取管理，避免資訊遭到未授權存取；對網路存取加以限制，保護網路服務；建立以作業系統爲基礎的存取控制，防止對電腦的未授權存取；監控系統存取和使用，監測未授權的活動。

㈧系統開發與維護面向：係控制系統的安全，防止系統中使用者資料的遺失、被竄改或刪除；使用密碼控制機制，保護資訊的完整性、機密性。

㈨業務持續性管理面向：係減少業務活動的中斷，確保關鍵業務可以持續執行。

㈩符合性面向：係規範資訊系統的設計、使用、管理須符合法律要求，避免違反法律、法規、義務合約或任何安全要求，定期審查安全政策和技術是否符合標準要求，建立系統稽核機制。

二、其他資訊安全規範

除「ISO 17799」外，還有許多資訊安全規範，分別在不同的領域有重要作用，本文僅簡單介紹「橘皮書」、「紅皮書」、「RFC 2196規範」和「ISO 13569」：

㈠橘皮書

「橘皮書(Orange Book)」是美國「國

註十 張博竣，《資訊安全管理實務》，臺北市：文魁資訊股份有限公司，2004年4月，頁1-19～1-21。詳細原文內容則請參考《ISO 17799/BS 7799》文件。

家安全局(NSA)」下屬的「國家電腦安全中心(NCSC)」，於1983年8月頒布的「官方系統安全標準」，該標準的全稱是「受信任電腦系統評量標準(Trusted Computer System Evaluation Criteria；簡稱TCSEC)」，由於封面爲橘黃色，故又稱爲「橘皮書(Orange Book)」。因「美國國家電腦安全中心(NCSC)」是專門負責對電腦系統和安全產品進行測量評估的單位，所以「橘皮書」是目前最權威的電腦系統安全評量標準。

「橘皮書」根據可信度將電腦系統由高至低區分爲A、B、C、D四個等級，凡符合特定安全條件、標準的電腦系統，即可歸類爲某種安全等級，較高等級的安全規範覆蓋較低的安全等級。每個等級的規範概述如后：

1. D級：爲「最低保護(Minimal Protection)」，凡沒有通過其他等級測試的系統，皆屬於D級。

2. C級：爲「自訂保護(Discretionary Protection)」，本等級規定系統中的物件（如，檔案、資料夾），都可以作爲安全存取實體，由系統的主體（管理員、使用者或程式）自訂存取權限，如使用者A可以自行決定某個檔案是否允許其他人讀取。C級依照安全性高低，又分爲C1和C2兩個等級，各種UNIX及複製品(clone)屬於C1安全等級，Windows NT/2000/2003則屬於C2安全等級。

3. B級：爲「強制性保護(Mandatory Protection)」，本等級規定必須由系統強制保護安全，在這種安全等級中，系統中的每個物件和實體，都必須有自己的「安全性籤頁(Security Label)」，系統可以根據使用者的安全等級賦予不同的存取權限。B級依照安全性高低，又分爲B1（頁籤式安全保護[Labeled Security Protection]）、B2（結構化保護[Structed Protection]）及B3（安全域[Security Domain]）等三個等級。

4. A級：爲「已驗證的保護(Verified Protection)」，目前定義的等級只有A1，其安全等級相當於B級之B3標準，可證明該等級系統之安全原則和安全規範的完整性和一致性。

㈡紅皮書

「紅皮書」是由「美國國家電腦安全中心(NCSC)」頒布的「官方網路安全標準」，與「橘皮書」對應的是封面爲紅色，故稱爲「紅皮書」，該標準的全稱是「受信任網路註釋(Trusted Network Interpretation，簡稱TNI)」，是保護不同類型的網路，及提供不同類型的網路架構。

㈢RFC 2196

「RFC 2196」安全規範是由IEFT定義的標準，其目的是讓網路管理員制訂連線到網際網路之電腦系統安全原則，「RFC 2196」安全規範亦提供沒有連線到網際網路的電腦系統有用的資訊，列出管理員在設定自己的安全原則時，必須考慮的因素，並在許多相關領域提供大量的建議。

㈣ISO 13569

「ISO 13569」安全規範是目前國際對金融資訊相關業務所制訂的安全標準，由ISO技術委員會「ISO/TC68銀行、債券及它項金融服務」及下屬委員會「SC2資訊安全防護管理及一般銀行運作」編製而成，其目的是建立銀行和相關金融業務的資訊安全防護標準，使其執行工作和系統運作更具效率。

肆、網路攻防與安全

「有效嚇阻、防衛固守」爲國軍防衛作戰之戰略指導，就「網路戰攻防」言，當應全面整合有限國防資源（甚或國家資源），建構多層次安全防護機制及組建「網路戰將」，以有效扼制中共網軍／駭客之威脅，蓄積磨礪戰略性資訊戰攻防能力，「寓守於

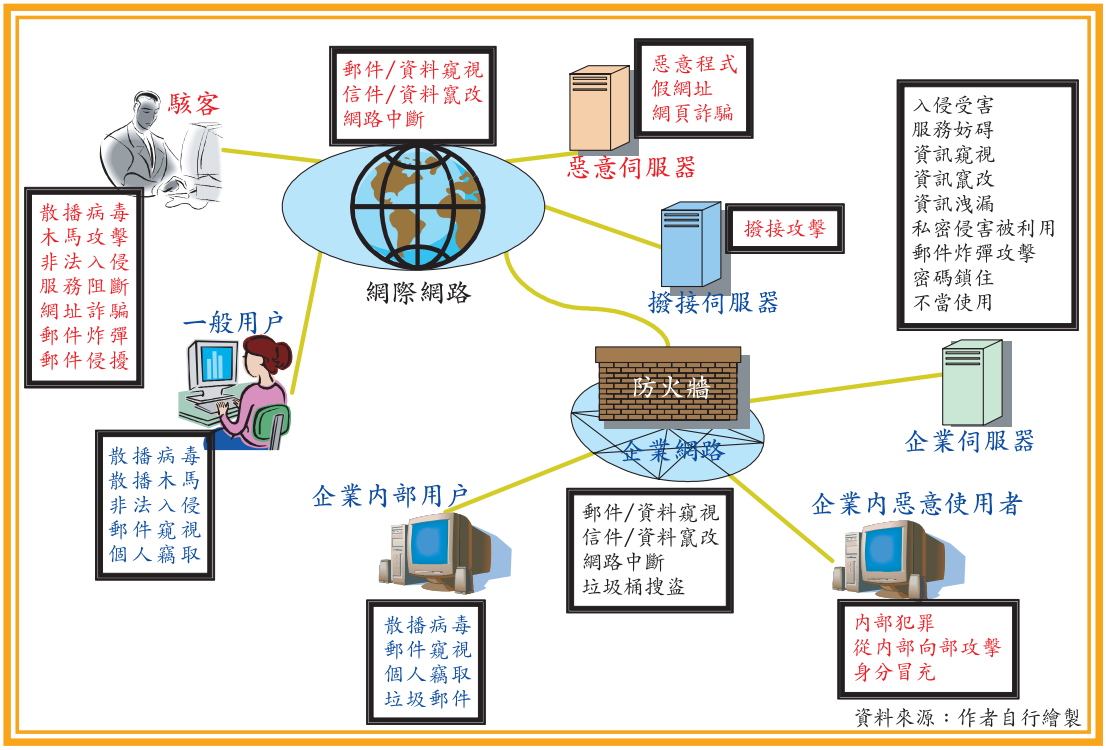

圖1　資訊系統與網際網路攻擊示意圖

攻」，「形於無形」，爲以資訊科技的戰爭型態奠定「以小博大」利基。在網際網路與資訊系統中所進行之資訊攻擊與手段，係指攻擊者（敵對者或潛在對手或出於好奇的入侵者）透過網路，對被攻擊之資訊系統、裝備及資訊流運作，實施阻絕、衰退、擾亂、竊取、詐欺、竄改、破壞、摧毀等之作爲（如圖1）。基此，各種資訊、資訊流、資訊系統與裝備、資訊基礎建設等，均可作爲網路攻擊之目標。國軍負有防衛臺澎金馬安全之任務，國防資訊系統、指管系統與指參人員所使用之公務電腦及相關儲存媒體，經常儲存各類型機敏資料與資訊，稍有不慎將對國家或國防造成不同程度損害[註十]，故首要爲建立乙套「行之有效且合理」的資訊安全管理規範，並要求所有電腦、資訊系統與網路的使用者、管理者遵循外，對資訊系統與網路攻防更須具有正確清晰概念，始能避免成爲網路攻擊下的「受害者」；而資訊技術專業人員、系統管理員，在確保資訊安全前提下，必須做到主動支援服務，始能防微杜漸而達成資安確保任務[註十一]。

註十　並不是所有國防與軍事資訊與資料都具有機敏性，故如何明確清晰定義與劃分機敏性資料，爲工作任務推展效率及效能之基準，依筆者意見，應以「正面表列」方式清楚指出機敏資料，以避免用歸納式將指涉範圍無限擴大與無限上綱。

註十一　以報章雜誌所公開報導的我國政府機關及國防軍事機構所發生的資安事件觀察，電腦資訊裝備與數位媒體的使用者，因未能接受必要的訓練，使用層面所應具有的資訊安全知識與基本操作技術多未具備；在此情形下，資訊技術專業人員、系統管理員更未能主動支援服務，致使遭受網路戰攻擊的使用者（受害者）處於孤立無援的狀況。這些情況如不能儘速改善，儘管是嚴刑峻罰，資安事件仍將層出不窮，而在此種狀況下的所有受害者，必將累積對公務部門的怨懟，無形中，在兩岸網路戰的攻防中，已屈居於下風，且自傷戰力。

一、常見攻擊行爲[註十四]

㈠入侵網站

「網際網路(Internet)」上有數以萬計的網站，這些網站都可以提供電腦使用者透過網路任意存取，於是安全性較低的網站，就成爲攻擊者下手的目標。

㈡攻擊Internet網域名稱伺服器

「網際網路(Internet)」中分佈的根網域名稱伺服器，一旦受到攻擊不能提供正常服務，所有網域名稱解析將失效，甚至導致整個「網際網路(Internet)」癱瘓。

㈢阻絕服務(DoS)攻擊

阻絕服務攻擊可導致其他電腦無法工作或活動，攻擊者通常將大量的垃圾訊息傳送至網路，導致網路癱瘓或者將其電腦系統的資源消耗殆盡，而達成阻絕服務的目的。

㈣分散式阻絕服務(DDoS)攻擊[註十五]

分散式阻絕服務攻擊（如圖2）係透過挾持多臺電腦，同時向攻擊目標發出大量的封包或資料要求，導致目標主機無法執行正常服務工作。利用多層踏板攻擊的方法，被攻擊目標幾乎不可能在短時間內找出攻擊來源。

㈤利用惡意程式碼攻擊

惡意程式是程式編寫員刻意寫出來的，通常惡意程式碼會對目標主機造成一定的危害，常見的是病毒程式及木馬程式。

㈥利用應用程式或作業系統的緩衝區滿溢

在設計上有缺陷的應用程式或作業系統，通常會造成緩衝區滿溢的問題，多餘的資料將被寫入緩衝區中，覆蓋原來的程式碼，攻擊者便可以獲得電腦的控制權。

二、常見攻擊手段[註十六]

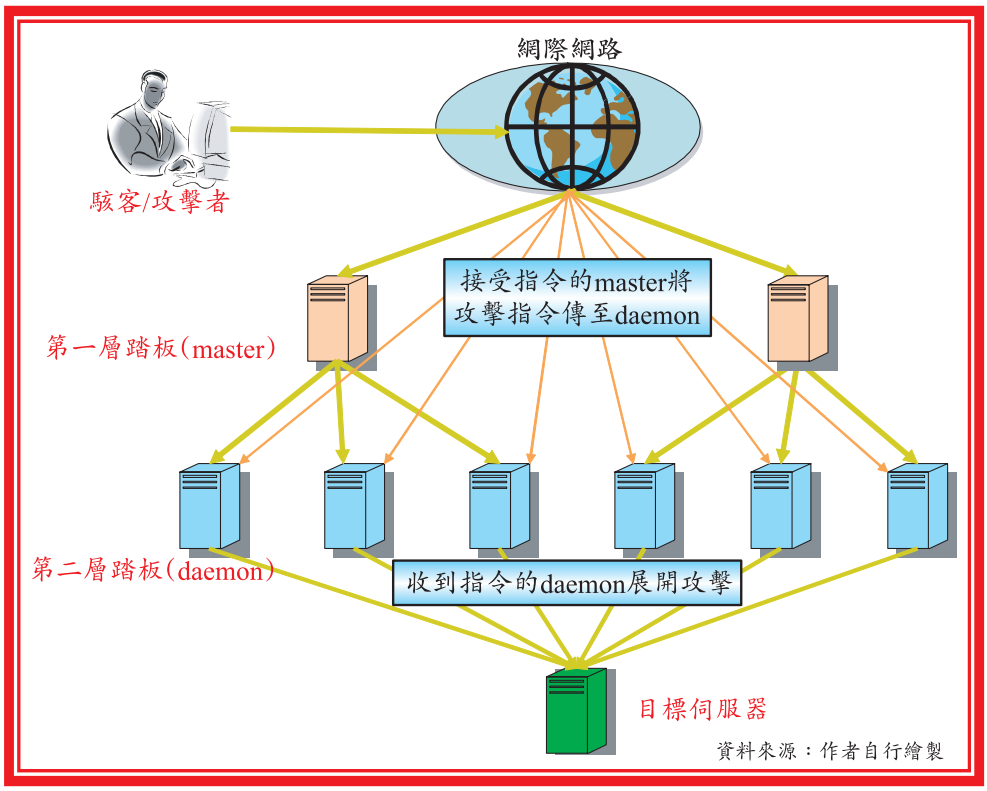

圖2　分散式阻絕服務攻擊示意圖

註十四　梁華傑，《網際網路戰（含資訊安全）》，國防大學戰爭學院正規班民96年班資訊作戰課程第七單元講義，桃園縣：國防大學，頁3-7～3-10。

註十五　駭客或攻擊者在攻擊前，先確定有許多踏板，被利用的踏板多爲管理欠完善或完全未加以管理的伺服器，駭客或攻擊者以非法存取的手段侵入該踏板，裝置攻擊程式；執行攻擊時，駭客或攻擊者先將指令送達第一層踏板，第一層踏板再將指令傳至第二層踏板，最後，被攻擊目標同時遭多臺踏板攻擊，業務服務陷入癱瘓。攻擊手法爲「持續送達連接要求、利用伺服器程式不方便處理例外等」。

註十六　同註十四。

㈠電腦病毒[註七]

電腦病毒是一種小型程式，具有潛伏、感染、發作、破壞等典型的行爲特色，有如生物病毒一般。電腦病毒一旦於資訊系統及電腦內感染、發作，經常會在極短時間內或特定時間造成極顯著的破壞與大量的傳染散播。

㈡變種病毒

爲一種程式工具，可依策略參數而產生大量的變種電腦病毒。

㈢木馬程式[註八]

爲一種任務導向的間諜程式，經常具有潛伏、窺探、匿跡、遙控等特色。一旦資訊系統及電腦被植入木馬，經常可對其進行長時間的秘密入侵而不被發現。

㈣邏輯炸彈

爲一種任務導向的惡意程式，可被設計成獨立運作而不需與原攻擊方聯繫。一旦資訊系統及電腦被植入邏輯炸彈，可於特定的時間或條件下，自動發作而破壞資訊系統及電腦。

㈤飽和攻擊

對被攻目標產生大量的垃圾資訊，以消耗其網路頻寬或系統資源，使其減低或喪失功能。

㈥弱點攻擊

利用被攻目標的系統弱點或電腦弱點所進行的攻擊，使其系統發生錯誤、被入侵或當機。

三、資安防護

面對資訊安全的威脅與挑戰，已轉變爲「道高一尺、魔高一丈」的形式，既然是「人」所製造出來的，自然也能採取相適應的手段與方法來進行防護，以提升電腦使用者的資訊安全；然任何資安防護手段與作爲，都無法保證百分之百安全，只有靠「勤能補拙」，始能將所有使用者的電腦與網路提升安全度。以下的探討將擺開電腦專業的生澀，並就使用者個人層次至網路資訊系統層次探討：

㈠安裝防毒、防駭軟體

於個人所使用的電腦（含筆記型電腦）上安裝防毒、防駭軟體[註九]（如圖3），提供使用者的電腦安全防護，以進行病毒與惡意程式掃描、過濾，以達防毒、防駭。

而各類大型資訊系統中之各種伺服器，則須由「系統管理員」安裝高階功能之防毒、防駭軟（硬）體，以對網路上收發之郵件、瀏覽之網站（網頁）、電子檔案等所有流通之數位資訊進行病毒與惡意程式掃描、過濾，使資訊系統後端的使用者（電腦終端平臺）具有多層之安全防護，以達防毒、防駭。

安裝防毒、防駭軟（硬）體的措施與作爲後，使用者必須時時更新防毒、防駭軟體之病毒定義檔，使其掃描、過濾功能處於最佳狀態，然最多僅能達80%-85%效果[註十]。

註七 電腦病毒產生迄攻擊過程，包括（但不限於）以下幾個階段：「病毒程式設計」、「在網路傳播」、「潛伏在電腦中」、「病毒觸發」、「病毒發作」、「進行攻擊」。

註八 木馬程式(Trojan Horse)：依大英百科全書定義爲：「隱藏在其他程式中的安全破壞程式，如地址清單、壓縮檔案、遊戲程式或者病毒中」。木馬程式都不是單獨出現的，而是結伴而行，可包括兩部分，分別是木馬伺服器端(Server)和木馬用户端(Client)，木馬伺服器端用來植入受害者電腦中，並開啓後門，準備回應駭客或攻取者的請求。

註九 使用者所安裝之防毒、防駭軟體，應使用正版軟體，避免自網路下載破解版使用。

註十 防毒、防駭軟體無法偵測、掃描新產生的病毒及木馬程式，是因爲防毒軟體的病毒定義檔未更新，或新病毒／木馬程式之病毒定義檔未開發出來所致。

圖3　例舉商場上幾種防毒（駭）軟體

㈡架設軟、硬體防火牆[註二]

個人所使用的電腦須安裝架設軟、硬體防火牆，以管制非法進出之用户與存取服務，以防制外部入侵。若受限於預算，最起碼在個人使用的電腦作業系統，必須具有軟體防火牆功能或安裝防火牆軟體。

各類大型資訊系統中之內部網路（區域網路）與外部網路（廣域網路或網際網路）間應架設多層次之軟、硬體防火牆[註三]，以保障於資訊系統後端之電腦使用者安全防護，以管制非法進出之用户與存取服務，以防制外部入侵。

安裝與架設之軟、硬體防火牆，雖可防制外部入侵，管制非法進出系統與存取服務，但遇到技術高明的駭客，仍然無法保證百分之百安全，故多層次安全機制，僅是在提高非法入侵的技術難度。

㈢設定密碼

設定密碼是使用電腦與資訊系統的基礎防護，可分爲個人使用之電腦，及連接於大型資訊系統的終端機平臺兩個層次探討。在個人所使用電腦之層次，須設開機密碼、使用者帳號與登錄密碼，以確保他人無法輕易開啓你所使用的電腦。在連接於大型資訊系統（含指管系統）的終端機平臺之層次，終端機平臺部分，與個人使用電腦之密碼設定

註二　軟、硬體防火牆雖然可阻擋大多數的外來的入侵，然遇到高明駭客或如大陸網軍的針對性攻擊，軟、硬體防火牆仍然無法阻止這類入侵，基此，系統管理員在系統上仍須建立「可疑入侵偵測系統」，以爲系統管理員即時接管入侵處理與防制。

註三　大型資訊系統所安裝架設之多層次軟、硬體防火牆，除須著意於安全參數設定外，惟應特別注意不要影響使用者使用系統的效能與功能。當兩者不能兼顧時，則必須依恃安全、可靠與實用的資訊安全政策來決定，故此時亦是檢視資訊安全政策與資訊管理規範是否適當的時機之一。

相同，惟在登錄到系統主機或伺服器存取系統資料前，則須建立使用者身分識別及密碼，通過識別與密碼驗證後，方能取得使用權。

由於大型資訊系統（含指管系統）的資料庫(Data Base)儲存龐大資料，更須提高其安全層次，故登錄至系統的使用者身分識別，最好採取「生物特徵辨識器」，如指紋辨識、聲紋辨識、視網膜辨識等技術平臺；而使用者之登錄密碼，最好採取「一次性使用密碼[註三]」，以回應主機的密碼盤問識別，以撤底杜絕非法使用者侵入系統。

啓用個人電腦或進入大型資訊系統（含指管系統）之「密碼」，既爲最基礎之安全防護作爲，該「密碼」之設定就必須具有複雜度，密碼長度最少在8碼以上，並且文、數字及符號混合編碼，以大幅度降低入侵者破譯密碼的成功率，尤其是登錄到大型資訊系統（含指管系統）之密碼設定尤然。

㈣加密處理

「加密處理」係針對使用者所產製之各類型電子檔案。使用者在產製電子文件後，儲存於各類型儲存媒體時，須使用「加密軟體」對該電子檔案進行加密處理後，再予以儲存，尤其是儲存於移動式儲存媒體之電子檔案尤然。

透過網路傳送／接收之數位電子檔案，更必須使用「加密軟體」完成加密處理後，再進行傳送；此運作機制下之所有使用群組，當然必須使用同樣的「加密軟體」，才能對所接收之加密檔案進行解密，惟電子檔案加密後之「密鑰」，必須以安全的方式告知接收電子檔案的使用者，方能成功開啓該傳送之電子檔案。若該加密之電子檔案在網路中遭人截收，截收者如無該「密鑰」，欲破譯該電子檔案之「密鑰」，恐需大費周章；然天底下沒有破譯不了之「密鑰」，惟就安全機制言，已大幅提高安全度。基此，必須選購或研發一套加密邏輯複雜度高之「加密軟體」，且加密所使用之「密碼設定」，也要符合複雜度原則，方能達到相對高度的安全性。

此外，涉及國防軍事、外交與國安等高機敏性機關，或大型事業機構，若有充足預算，除採用前述「加密軟體」之運作機制外，同時可考慮在使用者／接收者連接網路之端點，各裝置同一類型與程式之保密器（模組），對所傳送之電子檔案／資訊進行自動加解密，以「複式加密機制」，以達資訊傳輸安全。

㈤使用媒體內嵌器（軟體）

運用媒體內嵌器或軟體，將機敏性資料內嵌於無敏感性之多媒體影像中隱藏，唯有知道其內嵌過程及解密密鑰，才能解讀隱藏於其中的機敏性資料。如，將重要文件內嵌於風景照片、將一段影片內嵌於另一影片。

就個人使用的公、私個人電腦或家中連接網際網路的電腦言，個人因無足夠經費預算來安裝架設軟、硬體防火牆及防毒、防駭軟體，層層安全防護機制不足，使用者也可能不具備使用電腦與網路的安全專業技術，故這些工作者及工作平臺與電腦，在儲存隱藏機敏性資料時，即可藉用媒體內嵌器或軟體，來提升自身的安全度。

就大型資訊系統言，理論上不應將系

註三 所謂「一次性使用密碼」，又簡稱爲「一次性密碼」，係由進入欲使用的系統以亂數方式自動產生，經使用者（登錄者）使用後，即失效或自動銷毀，以防杜他人使用，主要是必須配合進入使用系統的身分識別之重複審認、辨識。

統資料或檔案儲存於個人使用的終端平臺或電腦，而應建立檔案伺服器及磁碟陣列來管理存取系統資料、檔案與參數，透過系統管理的層層安全機制（含身分識別、通行密碼、使用人安全等級區分、資訊存取分類、檔案加密等）進行全般與整合性管理，故不宜運用媒體內嵌器或軟體來執行機敏性檔案之隱藏。

㈥運用弱點掃描器[註四]

對大型資訊系統或連接於網際網路的資訊系統，系統管理員必須負責於防火牆後端工作者使用電腦終端平臺的安全工作環境，因此必須架設安裝與運用弱點掃描器，對網路上的網路伺服器（如：郵件伺服器、檔案伺服器、網頁伺服器、網域名稱伺服器等）、個人工作站及使用者之個人電腦，以弱點掃描器及技術進行有系統之掃描，以發現系統弱點存在，並立即進行修補，以確保所有使用者的安全。

由於大多數的電腦使用者，並無足夠的資訊安全防護技術與知識，系統管理員運用弱點掃描器偵測出安全弱點後，不能僅盡告知義務，而必須立即馳援使用者以協助其完成安全弱點修補。任何企業、公私立機關、團體與行號，眞正重視資訊安全者，均對資訊安全支援服務具有高度執行力，這絕對是資訊系統管理員的責任與義務，更是以「服務」爲宗旨的資訊社會所必須具有的使命感與工作熱忱[註五]。

㈦安裝架設入侵偵測器[註六]

管理大型資訊系統（含指管系統）或管理連接於網際網路的資訊系統，爲提供所有工作者使用系統或工作平臺（電腦）的安全環境，絕對必須架設安裝「入侵偵測器及系統」，實施即時線上偵測、掃描及巡邏，以偵測網路攻擊與非法入侵等行爲。

「入侵偵測器及系統」可分爲主動式與被動式兩種，主動式入侵偵測器及系統可即時阻絕攻擊與入侵，被動式入侵偵測器及系統僅能產生警示或制止部份攻擊或入侵。

「入侵偵測與反應」是資訊安全緊急應變機制極爲重要的一環，其重要性與「弱點掃描」的「主動支援服務」是資訊安全應變的雙核心，是系統管理員責無旁貸的工作與義務，也是資訊安全工作朝向「零資安」的最有效途徑。

註四 「弱點掃描」是透過自動且完整的弱點檢查，以提供系統管理者有關受測系統現有的弱點資訊。系統弱點發現後，系統管理者可以依照弱點檢查所產生的結果尋求補救方法，進而防禦網際網路上的攻擊。「弱點掃描」概分爲「遠端弱點掃描檢測」及「本地端弱點掃描檢測」兩大類。兩種弱點掃描檢測差別在於，「遠端弱點掃描檢測」是模擬駭客的動作對系統作攻擊，但並不會如駭客在攻擊後對系統作出造成危害的動作，因此「遠端弱點檢測」是由遠端藉由駭客的觀點來對系統作弱點檢測；「本地端弱點掃描檢測」是提供遠端檢查無法檢測到的本地端系統弱點資訊，如蠕蟲檢測，就屬於本地端弱點掃描檢測。

註五 從國內所發生的資訊安全事件觀察，當受害者被告知遭到病毒、木馬等惡意程式攻擊及駭客惡意入侵時，都是處在孤立無援狀態，甚至於受害者還遭受到企業、機構、組織的懲處，令人質疑與心寒的是，這些擁有專業技術知識的系統管理員或資訊安全部門人員，爲什麼都只在冷氣房上班，而無具體的緊急服務支援可言，在以「服務」爲宗旨的時代，又爲何未能支援到使用者；反觀資訊安全事件非常少的企業、機構、組織，他的系統管理員及資訊安全部門，又何以能做到「即時服務支援使用者」，歸根究底，就是「心態」與「制度」都不是建立在「主動服務」上，而是建築在「官僚型式主義上」。

註六 「入侵偵測」主要目的是即時提供目前系統遭受攻擊的資訊。「入侵偵測」提供資訊以提醒系統管理者系統是否遭受攻擊，使系統管理者能對正在發生的攻擊進行合宜的對應動作，並且提供系統所遭受侵害的資訊便於系統管理者修補攻擊後的系統。此外，並可加入適當的反應措施，如，若偵測到某個網路位址的網路封包爲攻擊模式，則過濾掉此封包並紀錄其來源位址。

㈧使用有位址過濾功能的路由器

大型資訊系統間的網路，或連接於網際網路的資訊系統，或公、私場域個人所使用連接到網際網路的電腦，連接到網路所使用的路由器，須具有「位址過濾功能」，以利過濾假冒內部位址的外來封包，或假冒外部位址的外送封包，以減少各式以位址假冒爲基礎的網路攻擊。

大型企業、公、私機關、團體與行號，因有較多的可用預算經費，故採用具有「位址過濾功能」的路由器，較無困難；然個人使用者因無足夠預算經費支援，則必須充分整合運用前述第㈠至第㈤等項資安防護方法，以提升個人使用電腦的安全度。

伍、國軍網路資訊安全省思

國軍追求創造「資電優勢」，多年來投入龐大資源與預算，以提升通資網路基礎建設，並不惜巨資籌建C^4ISR系統，同時在組織編裝上也配合進行適度調整。由於資電作戰、數位化戰場及網狀化作戰之領域範疇過於廣範，故欲對國軍網路資訊安全檢視，範圍應限縮於網路與其相關之資訊安全，而且是以「網路戰攻防」觀點來進行省思體察，始能透穿迷霧，並得出較爲眞實因果。由前揭「何謂資訊安全」、「資訊安全規範」、「網路攻防與安全」的探討與分析，及觀察國軍資訊安全實務工作的現象，以系統化整體觀進行體察，概可歸納出以下幾點省思。

一、寓防於攻、貫穿全程

網路戰（或資訊戰）攻防之特質是「無平、戰時之分」、「打破地理疆界侷限」、「可異地同時、異地異時全時域攻防」、「網路戰士無年齡限制」、「戰／技術充分融合之無聲行動」、「網路戰效益拓殖於戰略／作戰／戰術各層次」。《民九十三年國防白皮書》揭示，且在《民九十五年國防白皮書》再次強調的資電作戰任務爲：「平時在執行指管系統之資電安全防護與監控，遂行全天候、全方位、高速率、高品質、高可靠度之通信資訊支援，……；戰時防制敵網路入侵、破壞、封鎖、竊取，……」[註壬]。就已揭露公開資訊觀察，顯然平時僅遂行通資網路的防護與監控，誠屬被動式作爲，而於戰時始進行防禦性資訊戰，且重點置於防制敵網路入侵、破壞、封鎖、竊取，故自平時至戰時，完全未觸及資訊戰情報／網路情報作爲，及網路戰之攻勢戰略與作爲，因消極性與被動性防護策略，故能否達成「防禦性資訊戰」或「網路戰攻防」目的，誠屬難料。

另，就國防科技執行現況方面，以資訊戰系統言，爲建立資訊戰攻防能量，防止中共以電腦病毒及駭客對我電腦網路及通信系統實施攻擊，正積極從事光纖網路建設、研發指揮自動化系統、資通安全防護系統、培養電腦網路人才等作爲，爲「資訊戰」作準備。[註六]就已揭露公開資訊觀察，仍處於萌芽發展階段，且諸多配套作爲尚無具體規劃，或僅就技術層次著手，無法達到戰／技術融合要求，其中，又以「複合式人才」及「戰／技術融合人才」無長遠性計畫培育，故能力與能量實有待商榷。

「網路戰攻防」實乃「寓防於攻」的整軍備戰，故首重攻防二者綿密整合，且就網路發展歷史軌跡觀察，只要存在網路，只要運用網路來遂行廣範的資訊作業與作戰指管，就存在難以兼顧的弱點與安全性，故發展「網路戰攻防」與建立資訊安全，絕對必

註壬《中華民國九十三年國防報告書》，臺北市：國防部，頁122。
註六《中華民國九十三年國防報告書》，頁176。

須建築在攻勢基礎上來遂行防禦，同時須著眼於貫穿全程。

二、超前建設，注重合作

美軍「2010年聯戰願景」及「2020年聯戰願景」將資訊優勢視爲聯合作戰的主要因素，相當重視資訊網路的攻防研究與建設，以求奪取未來資訊作戰的主動權。在網路攻擊方面，美軍要求未來網路戰應具備「對所有目標網路的偵察能力」、「靈活精確的電腦網路攻擊能力」、「對網路攻擊效能的評估能力」、「具備先進準確的網路攻擊武器以對目標實施百分之百的精確打擊」；在網路防禦方面，美軍要求要達到「完成電腦網路防護評估程序與作戰指揮程序的整合」、「定期向有關人員提供客觀、簡潔的電腦網路防護狀況報告」、「完善各級司令部、各軍兵種及各部門間的即時資訊共享」、「開發國防資訊系統和資訊基礎設施結構圖的動態繪製工具，包括關鍵系統對網路依賴程度，以輔助確定網路系統對完成任務的影響程度」等[註元]，以超前的資訊設施建設走在網路戰前趨，以跨部門、跨領域之團隊合作加速整合發展，維持資訊優勢。

「網路戰」已發展爲弱小國家的廉價核子武器，然以美軍超強軍事強權之姿，尚且如此重視「網路戰攻防」，故國軍在追求資電優勢上，實應學習與仿效美軍，並發展出具有海島國家特色的「網路戰攻防」戰略／術融合，以超前戰略思想觀念，掌握資訊界之資訊運用關鍵技術，及自我開發獨特性關鍵攻防技術，落實於資訊基礎設施的先進超前建設，並成立「超本位主義、跨部門、跨領域」專家團隊，講求「Team Work」綿密合作，方能在防衛作戰上有能力去爭取與維持網路戰的相對動態優勢。時光荏苒，國軍不只硬殺武器系統推陳更新緩慢與遭遇困境，連臺灣本身極具世界資訊優勢的「網路戰攻防」建設與耕耘，亦停留在民間駭客式的攻防思維與窠臼，且難以排除本位，遑論動態「Team Work」之無間合作，而「跨部門、跨領域專家團隊」更難以組成，遑論戰／技術領域的充分整合運用，前此都是吾人當應痛定思痛，大膽啓用具有執行力與創造力之戰將人才，力挽狂瀾，以於未來具有爭取「網路戰攻防」之戰略優勢。

三、展開網路偵察、奪取網路先致

現在與未來之網路戰與電子戰將並駕齊驅，並構成資電作戰兩大支柱。作戰以情報爲先，在「網路戰攻防」中更是如此，首應重視獲取作戰目標的相關情報，惟有在掌握足夠的資訊情報並經分析處理後，才能做到「知己知彼，百戰不殆」。而「資訊網路偵察」不僅爲掌握戰場主動，亦爲充分發揮軍事謀略競爭而奠定取勝的基礎，故亟須展開網路偵察，並獲取充分完善之網路目標情報，以達成「知彼」爲目的之資訊網路情報偵察，以奠定有效的網路戰競爭手段，並企達軍事謀略競爭優勢。

「資訊網路偵察」是電腦網路的基礎，並貫穿於「網路戰攻防」全過程，各種偵察技術在資訊網路偵察行動中均有其重要角色，其關鍵技術概有資訊截獲技術、密碼破譯技術、隱蔽偵察技術、滲透偵察技術等，此外，還可運用智能偵察技術，及使用反偵察技術，以保護己方的資訊安全。[註壬]

資訊系統與網路先天存在各種安全缺

註元 祝利，《軍事強國逐鹿網絡戰場》，北京：解放軍報，2002年5月22日，第11版，轉引自國防部，《共軍信息戰研究與發展專輯》，臺北市，民92年11月16日，頁127。

註壬 叢友貴，《關注計算機網絡偵察》，北京：解放軍報，2002年6月12日，第11版，轉引自國防部，《共軍信息戰研究與發展專輯》，臺北市，民92年11月16日，頁163-164。

陷，資訊系統與電腦技術不斷更新，且亦建構多層次防禦措施，然攻擊手段的多樣性與多變性，致硬體、軟體、通訊協定先天存在的缺陷，及系統安全政策所存在的漏洞，使攻擊者能在未授權的情況下入侵或破壞系統。但資訊系統與網路所存在的各種缺陷與漏洞，及所建構的多層次防禦措施，會隨著運用技術與資訊安全政策的調整而有所變更或強化。因此，在「網路戰攻防」領域與範疇內之「知敵知彼」各種偵察部署與作爲，爲奠定網路戰先致與確保資訊安全之根基。

四、廣育人才，留用人才

資訊科技的日新月異，網路戰已成爲現在與未來戰爭的重要型式，且網路戰於平時即在相互競逐，是一場貫穿平戰時的無聲息、無煙硝戰爭，潛在對手包括中共正規與非正規網軍、職業與業餘駭客（含中國大陸龐大的駭客群）、政府組織情治特工、非政府組織敵意入侵者，及利用網路的犯罪者等。而網路戰之對抗、競爭與資訊安全，除必須具備戰略／術素養外，更須具備高技術素養與專業能力，故培養與訓練一個具有戰略／術素養與高技術層次的「網路戰將」，誠屬不易。基此，爲貫徹國軍所揭示的「資電優勢」建軍指導與防衛作戰政策，並在「網路戰攻防」領域與範疇中奠定勝兵先勝及「以小博大」基礎，當應「廣育資訊作戰人才」，並「有效留用（住）人才」，始能打造功力深厚基礎。

資訊網路與電腦已成爲現代化軍人必備的工具，故首重教育訓練廣大職業軍人（使用者）如何進行個人使用之公、私電腦安全設定與基本防禦技能，而且是每一職業軍人必具之基本要件[註三]，就未來係以資訊科技爲主導之戰爭型態言，此乃當務之急，重中之重。

再則，培育「網路戰攻防」戰力，必須由深具戰略／術素養的職業軍人中，遴選出能接受資訊科技教育訓練的人才，將其培訓成戰／技術融合之「複合型人才」，組建成網際網路攻防團隊（網路戰將），從而由「網路戰攻防」之戰略／術觀點，以進化現行「堵、封、拆、斷」的資安作爲，實質的將國軍推升至「寓防於攻」之「網路戰攻防」與資訊安全。

全世界潮流都在進行「精兵式」裁軍，整個動態進程中，若無法將「戰／技術融合之複合型人才」，適職適任安置於適當位置[註三]，將極易流失人才。依戰史經驗，當處於戰爭型態轉型與發展的「時間框(Time Frame)」，不能留住人才的一方，臨陣對敵時必將是處於敗勢的一方。基此，當務之急，不僅要廣育「網路戰攻防」領域與範疇

註三 觀察國軍近年之資安事件，概均將事發後之責任歸究於個人，然進一步分析探討，國軍廣大使用電腦的職業軍人，絕大多數人均未接受正規的「網路安全設定、電腦安全設定與資訊安全」教育訓練，事發之際，當事人處於茫然與孤立無援狀態，甚至於如何遭到網路（木馬）攻擊大多完全不知，即陷入不斷的行政調查與約詢，試想連資訊安全專家都無法保證當遭到網路（木馬）攻擊時能全身而退，這些未接受過正規教育訓練的廣大職業軍人，又如何能幸免呢？倘若不回歸根本，從「網路安全設定、電腦安全設定與資訊安全」之教育訓練紮根做起，以目前處理方式與心態，再嚴厲的懲處，判將難以杜絕資安，只是無法預測下一個受害者是誰而已。

註三 所謂「適當位置」，並不是所有職業軍人都要循指揮職路線發展晉升，而是須建立精緻化的「專、通分流」制度與管道，讓「戰／技術融合之複合型人才」置於能發揮專才的適當位置，方能眞正的留住人才；當然在軍中不能適所適任留用，人才必然會掛冠求去而回到社會發展，而我們的敵人（中共），不正好以厚碌吸取這些人才爲其所用，因此，如何有效留住人才，應該是推動「精兵式」裁軍且置於戰略高度來思考與規劃執行的重中之重。

的戰／技術融合人才，更要將「網路戰」之精英人才有效留用（住），據以組建一支眞正「量小、質精、戰力強」的「網路戰將」菁英部隊，才能於未來不可預期的軍爭中，取得「以小博大」之勝兵先勝利基。

五、主動支援，全面資安

「Farmer法則」告訴我們：「電腦系統安全的降低程度與所使用的系統總量成比例」。[註三]Farmer認爲安全之所以會出問題，大部分是來自於人爲因素，而非電腦本身。系統管理者可能操作錯誤，或對系統做出錯誤設定，或使用者使用極易破解的密碼或非常馬虎的安全習慣。[註四]顯見要全面落實資安，就必須要有正確的資安政策，並建立符合國際標準規範的資訊系統與網路安全管理規範，系統管理員與網路管理員的正確安全設定和主動支援服務，及使用者了解一般安全設定等，任何一環鬆動或脫序，均可能筆生資安。

從國軍近數年來的資安事件進行系統性觀察分析，「資安政策」與「資訊系統與網路安全管理規範」必須重新審視與再建構，俾達國際標準規範水準[註五]，且須廣泛考量技術觀點、使用者觀點與確保效能觀點等著眼，始能建構與創造「資電優勢」基礎。

在「系統管理員與網路管理員的正確安全設定和主動支援服務」面向，所呈現的問題是，「系統管理員與網路管理員」對資訊系統的安全防護設定是否正確，雖屬專業安全軟體工具與系統管理員、網路管理員的專業技術能力[註六]問題，若安全設定錯誤或設了不能顧及效能發揮的安全設定，都將造成極大的安全風險，然實況是未能對此一層面進行完善的稽核與控管機制[註七]，完全由系統管理員與網路管理員逕行決定各種安全設定，且肇生之任何資安事件，都只檢討懲處端終使用者（受害者），幾乎未對系統管理員與網路管理員、稽核控管人員做出任何檢討，此一重大的安全罅隙，亟待謀求改進與建立完善機制。

此外，就資訊系統與網路管理言，均設有網（系）管、監控與預警機制，理論上任何入侵均可預警，並迅速應變與支援服務。然觀察國軍的資安機制，當遭受資訊安全攻擊的受害者，幾乎未得獲任何即時性之技術安全協助服務，即令是使用者終端使用平臺的技術安全設定支援服務，及此類安全設定

註三 Dan Blacharski著，李正源、簡崑鎰譯，《Network Security in a Mixed Environment（網路安全—在多重環境下）》，臺北市：文魁資訊股份有限公司，2002年2月，頁8-1。

註四 前揭書，頁8-1、8-2。

註五 「資安政策」與「資訊系統與網路安全管理規範」屬國防部階層權責，非本文探討重點，謹於本文「參、資訊安全規範」概略性提出各種可資參考的國際標準規範，由業管聯參本於職權與責任，重新審視與再建構，俾以確保資安，同時大幅減少國軍的資安受害者。

註六 系統管理員、網路管理員的專業技術能力，在資訊業界已存在一套專業技術能力的認證機制與機構，但國軍並未建立此類的專業認證機制與機構，現在擔任系統與網管的人員（尤是應變人員），是否有足夠的專業技術能力，則是無從稽核。

註七 「系統管理員與網路管理員的技術安全設定」層面的稽核控管，除系統與網路面的技術安全設定正確與否的稽核控管外，更重要的是系統與網路管理員的安全忠誠查核，因爲系統與網路的安全設定屬專業技術層面，但安全卻掌握在「系統與網路管理員」這些人身上，若「人」的安全忠誠有問題，系統與網路是無法達成安全的設定，且處於高階督導的政策人員亦不具這些技術的稽核與控管專業，基此，此一層面若無或不去建立良善的稽核控管機制，資安事件將仍接續肇生，嚴懲再多的終端使用者，均將無際於事，只是製造更多的怨懟。

的教育訓練，幾乎都付諸闕如。[註廿八]而更令匪夷所思與無法與企業界相提並論的是，資訊安全部門極端缺乏主動即時馳援服務的工作精神，諸般種種均須省思與亟待謀求改進，始能向「零資安」邁進。

六、建立電子檔案庫(分庫)，完善最後一尺網路設施

國軍迄現階段，除極少數之系統係採電子資料庫(分庫)儲存各類型電子檔案外，絕大多數機關、單位、部門之業參(管)，都將所產製之各類型電子檔案儲存於個人所使用的公務電腦上，且無任何備援機制，而業參(管)爲確保電腦當機故障後，仍有備份電子檔案可供使用，幾將備分燒成光碟或儲存於移動式磁碟或俗稱「姆指碟」上，造成所產製的電子檔案難以控管，凡此種種均是未運用檔案伺服器與磁碟陣列等技術與設施，建立儲存電子檔案總庫與備援儲存分庫等機制所致。這是一種很普遍的技術與設施，然每一電子檔案資料散失的資安事件，卻從未檢討及此，實是令人匪夷所思與深值警省。

造成國軍在內部進行資訊作業的動態進程中，需要使用移動式硬碟及USB抽取式姆指碟來進行電子檔案移動傳遞的最主要原因是，「未能完善最後一尺的網路設施建置」。國軍資訊網路號稱「實體隔離」，應是處於最安全的資訊網路工作狀況，但卻因「未能完善最後一尺的網路設施建置」，致使開會、簡報、提報等議事場所均無網路設置，故必須使用移動式電子儲存媒體來攜帶電子檔案，無法透過網路經檔案伺服器稽核機制至電子檔案總（分）庫存取電子檔案使用，造成一個電子檔案存管安全大缺口，亦從未檢討，實深值警省與亟待改善。

軍民網跨接，在美軍來講實屬平常，因美軍除「飛彈預警管制系統」此類極機敏系統爲專屬系統外，幾所有管理系統均架構在網際網路上，且每年歷經數萬次的網路攻擊，仍屹立不搖，亦未聽聞誰在資安攻擊事件中遭到議處法辦。但在國軍號稱「軍民網實體隔離」的規範中，卻使用USB抽取式姆指碟來進行軍民網電子檔案移動傳遞，而USB抽取式姆指碟在軍民網轉用中間，又設立「過濾檢疫平臺」，企圖杜絕病毒、木馬等惡意程式的感染破壞。然世上功能最強大的防毒、防駭軟體，最多能偵測出75%~80%的病毒、木馬等惡意程式，在無法完全偵測出所有病毒、木馬惡意程式前題下，看似安全的軍民網電子檔案的「過濾檢疫平臺」，就「網路戰攻防」言，實暴露在網路戰「間接摧毀攻擊（接力式摧毀攻擊)」的嚴重威脅下。

爲徹底減少電子檔案透過「USB抽取式姆指碟／光碟」等間接式的移動傳遞，絕對必須徹底做到「完善最後一尺網路建設」及「架構電子檔案總（分）庫」等之整合運用機制，始能眞正朝向「零資安」邁進。最後，電子檔案資料印製成紙本的習性[註廿九]，爲傳統留下來的作業習慣，究其根本肇因，

註廿八 以「不教而殺謂之虐」觀點言，未提供使用資訊平臺與電腦的使用者足夠的安全設定教育訓練，使用者只能將電腦或終端平臺拿來當打字機，使用者是不會也不懂如何實施安全設定，不是使用者不遵守安全規定，而是不會、不懂安全設定，而資安業管部門僅以資訊安全規定（通報）來規範使用者，卻未提供適當的教育訓練，而肇生資安時，使用者面對的是一連串無情調查與懲處，「不教而殺謂」，更不能「懷璧其罪」，眞正要落實資安，則必須提供給廣大使用者適當的資訊安全設定教育訓練。

註廿九 電子檔案資料印製成紙本，是傳統作業習慣所留下來的習性，沒有對錯，卻是未能與時俱進，不符數位化戰場與網狀化作戰的需要；就如「公務家辦」此一似是而非的論述，在以前電腦沒有普及使用時，「公務家辦」是用筆在紙張撰擬，再帶回辦公室交由文書兵使用打字打印，文件遺失洩密時有所聞，但卻沒有將

乃高階人員不會、不懂、不了解、不使用電腦所致；未來的數位化戰場與網狀化作戰，對高階人員來講，是將「敵我千軍萬馬拉進電腦螢幕」，指揮管制遂行是「倚靠電腦螢幕上的視覺化圖像」，戰場資訊、情資與戰管信文是「運用電腦網路傳送的即時／近即時(Real time/Near real time)格式化訊息與共同作戰圖像(COP/CTP)」，高階人員若繼續不會、不懂、不了解、不使用電腦，投資數百千億元的所建置的C^4ISR系統，恐未蒙其利先受其害，國軍又將如何立足於數位化戰場與網狀化作戰中爭雄與確保防衛安全。基此，高階人員應即學會、學懂、學了解、學會使用電腦，並據以透過電腦螢幕閱讀電子檔案，以徹底減少電子檔案資料印製成紙本的資安缺憾，若再整合電子簽章機制，連公文書的呈轉核批都可以完善。體系化與一體化的資安基礎建設、機制與規範，始能眞正達於「零資安」政策目標。

陸、結　　論

當國軍全力追求與創造「資電優勢」的動態進程中，「資訊安全」將成爲「國防安全」之一環；當軍事衝突進入以資訊科技爲主要戰爭型態時，「資訊安全」更是最根本的議題與關注焦點。「水能載舟、亦能覆舟」，何況「道高一尺，魔高一丈」，在這無煙硝更無聲息的「網路戰攻防」中，不能動輒得咎，自傷戰力，未戰而先敗，反必須積極培養戰／技術複合型人才成爲「網路戰將」，並在精兵式裁軍的「精進案」進程中有效留用（住）人才。

以資訊科技爲基礎的戰爭型態、數位化戰場的來臨及網狀化作戰指揮與管制，必須完善所有的基礎建設，並運用資訊科技來解決現存問題及克服可預見的困難，不當的「封、堵、拆、斷」人爲干預政策，只是造成更多寒蟬效應與頓挫數位化、網狀化、資訊化效能／效率，「網路戰攻防」與「資訊安全」必須建築在「寓守於攻」的絕對主動性上，網路偵察與情報必須進行深廣度佈局，更必須貫穿平戰時全程，「以小博大」爲確保與達成防衛作戰任務的本質，「精兵式」的「精進案」成功，絕對需要將人才留用（住）在軍中，更需要更一步的將人才培育成「跨領域」、「戰／技術融合」、「聯參化」的「複合式人才」，這場無聲息、無煙硝的資訊確保與「網路戰攻防」，才能固本紮根，打好基礎，致人而不致於人，甚且在未來的數位化戰場與網狀化作戰中，方能「以小博大」而達成防衛作戰任務。

收件：96年06月25日
修正：97年02月18日
接受：97年02月25日

作者簡介

梁華傑陸軍上校，陸軍官校73年班、陸軍砲校正規班137期、三軍大學陸軍指參學院83年班、國立政治大學外交學系戰略與國際事務碩士；曾任排、連、營長；防衛部、軍團、總部、參謀本部參謀及博勝案駐美IPT；現任職於國防大學陸軍學院。

「公務家辦」變成不可饒恕的禁止事項，只是要求要完善保護機密的工作罷了；然當電腦普及使用了，用筆在紙張的繕寫撰擬轉變成電腦打字的型式，電子檔案遭無法辨識偵測的木馬惡意程式竊取（能辨識偵測就不會發生），「公務家辦」卻成了不可饒恕的錯與禁止事項，且動輒得咎，但身爲長官者將公事、文案帶回家中批閱，卻未聽聞任何規範。