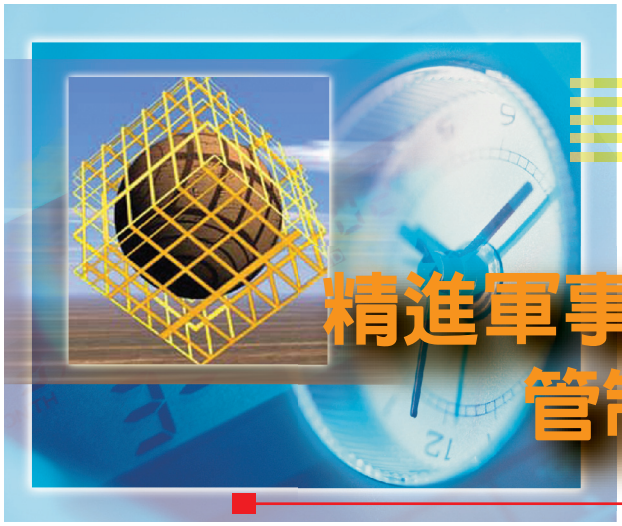


# 精進軍事資訊安全管制作為之研究

作者/林明昌 中校

## 提要

資訊科技的快速發展與廣泛運用除爲現代戰爭帶來全新的面貌外，亦對整個軍隊編制與戰術運用造成極大的衝擊。從近幾年發生的網路大戰中，可以明白看出－即使敵人相隔遙遠也可以實現作戰，只是火力來自於鍵盤，而非槍砲等。因此對於「網路安全問題」之要求又再次的被重視，然而如何在最大限度使用高科技的同時，還能兼顧資訊安全之要求，並能增加自主智慧財產權的創新度，乃成爲目前國軍訂定資訊安全管制作爲時需特別重視的。因此本篇文章除探討共軍的信息戰發展概況及其網路戰能力外，並研判其對國軍實施網路攻擊可能的方式。文中同時說明國軍資訊戰發展概況及目前資訊安全管制機制，並進一步提出個人對精進國軍資訊安全防護措施的一點心得與建議，期能改善國軍資訊安全管制作業的缺失，進而提昇整體戰力與效能。

## 前言

隨著時代的發展，網路和資訊愈來愈重要，摧毀、襲擊和破壞網路體系將對人們的生活造成危害。從近幾年發生的中美網路大戰中，可以明白看出－其實雙方是兩敗俱傷的，因爲中國駭客在攻擊美國網站的同時，諸多中國網站也遭到破壞，總體損失可能遠大於美國，美國駭客的攻擊有組織，專業水準高，技術先進且效率明顯。中美雙方的駭客將傳統的戰爭提前改變，即使敵人相隔遙遠也可以實現，只是火力來自鍵盤，而非槍砲等。因此「網路安全問題」又再次被重視，然而資訊的安全與不安全是相對的，如何在最大限度使用高科技的同時，還能兼顧資訊安全之要求，乃成爲軍方訂定資訊安全管制作爲時需特別重視的。換句話說，除了電腦硬體、軟體、網路路由器和伺服器要朝自主研製發展，且不能將機密以上的資料儲存在這類平台外，駭客入侵的實戰驗證技術也可轉化成爲軍方資訊網路安全的教材及經驗。

然而網路攻防戰永遠是一種競技性行動，因此在資訊和網路安全問題上必須要有強烈的憂患意識和危機感，並配合務實的資訊安全管制作爲，如此方能持續站在勝利的最前端。因爲未來戰爭的勝利者是屬於具有

憂患意識和超前思維的智者。

## 共軍「信息戰」發展及對國軍實施網路戰可能採取之作為

### 一、共軍信息戰發展概況[1]～[3]

㈠基礎建設

中共在過去的五年中，除舉辦多次的研討會並利用大量的軍事出版物，再三強調高科技局部戰爭的重要性外，實質上亦編列了大筆國防經費投資在各項信息戰的基礎建設中。

㈡人才培育

固然硬體設施可以用錢來達成，然而軟體設施卻是無法一蹴可及的。因此共軍乃成立培訓資訊及指揮通信專業人員之信息工程學院，用以提昇解放軍人員素質。

㈢模擬訓練

爲節省訓練成本及便於驗證各項信息戰研究成果及戰法，乃籌設「信息戰模擬中心」，用以進行對抗演練，藉以提昇遭遇實際狀況之緊急應變能力。

㈣彈性編裝

於廣州軍區成立高科技特種部隊，配備高科技武器裝備，平時用以驗證各項資訊戰作爲，戰時則遂行各類型資訊作戰。另外解放軍已經開始考慮彈性縮小軍隊規模，以適應不同的情勢。並開始強化兵種聯合作戰的能力，在編制上除了重點的海、空軍與二砲部隊之外，同時重視技術兵種的建設，加強陸軍航空兵與電子對抗部隊，進行高科技編組，實現作戰部隊的高度合成，並根據作戰的需要實施多樣化的編制。然更受人矚目的是第四軍種－「網軍」的編成，用以實施高科技的網路攻防戰。

㈤尋求外援

共軍爲補其技術之不足，並求短期內提昇其整體資訊作戰能力，因此利用各種方式積極尋求與美國之外的其他先進國家實施技術合作發展計畫。除可立即獲得合作利益外亦可同時藉以縮短其相關技術的研發期程。諸如尋求從法國商用衛星得來的資料，移轉作爲軍事用途；和以色列共同合作發展攻陸巡弋飛彈以及空中預警機；與法國及巴西合作進行追蹤太空衛星的建設及技術移轉；與德國的DASA航太公司合作建立通訊衛星；並從英國移轉小型衛星發展技術等，以提昇其整體戰力。

### 二、共軍之網路戰能力

中共資訊網路戰的能力究竟爲何？根據美國的研究專家表示，其能力應足以實施網路攻防戰[4]、[5]。已經過證實的網路戰作爲有：

㈠法輪功網站入侵事件

當法輪功事件發生後，美國、英國、澳大利亞、加拿大等地的法輪功網路也同時遭受多次的駭客攻擊，目前已確定是中共公安部門所爲。

㈡兩國論事件

前總統李登輝先生提出兩國論的論調後，兩岸展開了一連串的網路駭客戰爭，由

註１：廖宏祥，「台海資訊戰爭的評估與展望」，台灣綜合研究院戰略與國際研究所研究論文。
註２：陳友武等著，資訊作戰概論，國防部通信電子資訊次長室編印。
註３：軍事重地資訊網站，「資訊戰」，http://tacocity.com.tw。
註４：同註３。
註５：曾復生博士，論戰略—中共的戰略性趨勢。

官方的資料顯示，兩岸三地相互攻擊網站達萬次，雖然其中大部分是民間人士之作爲，但其中仍不乏中共的官方作爲或授意。

㈢南京大屠殺事件

日本方面有人否認南京大屠殺之後，日本電腦網路即遭遇一連串駭客攻擊事件，研判大部分爲中共發動網路戰的作爲。

㈣中美軍機擦撞事件

中美軍機擦撞事件發生後，中美雙方駭客即展開一連串之網路攻防。茲將相關研究成果整理說明如後，此次中美駭客攻防戰中計有竄改首頁、刪除文件、取得管理者使用權限、阻斷式服務攻擊(簡稱DoS)、格式化主機硬碟、強迫關閉網站服務等主要的攻擊項目。主要攻擊手段有阻斷式服務攻擊、電子郵件炸彈、網路監聽器、特洛伊木馬程式及緩衝區溢位攻擊等方式。而所攻擊的對象概略可分爲商業網站、政府網站、民間網站、軍事網站及其他網站等五大類別網站。

## 三、共軍對國軍實施網路攻擊可能採取之作為

從國防政策白皮書、前行政院長唐飛先生的國防報告書及美方研究中共信息作戰專家的研究報告中之研究推論，預判公元2005年中共的信息戰應已具備以下的能力。

㈠運用電腦建立神經中樞網路，已可執行聯合模擬作戰。

㈡完成野戰自動化指揮系統，可供部隊機動及戰場使用。

㈢完成戰術資料鏈傳輸系統，可使資料傳輸系統標準化。

㈣指管系統完成數位化，可整合並提昇自動化指揮系統。

㈤已可藉由衛星及空中預警機，達成三軍聯合作戰。

㈥具衛星導航能力。

㈦具撰寫電腦病毒程式能力，可透過多種管道攻擊國軍資訊系統。

㈧具電磁脈衝炸彈，可大規模干擾、癱瘓我$C^4ISR$系統。

㈨具資訊偵蒐能力，可竊取我軍事機密。

根據以上推論，可以進一步預估中共若侵犯台灣，其可能採取之作爲除傳統的戰術思維外，應該還包含了新的資訊作戰運用。因此就個人淺見提出以下推論：

㈠以各式彈道飛彈攻擊機場、港口、海空軍基地和國軍指管設施，實施第一波攻擊，藉以癱瘓大部分國防基礎設施。

㈡配合第一波攻擊，以電磁脈衝炸彈實施電子戰，藉以癱瘓國軍指管通情系統。

㈢以特工人員實施破壞，摧毀橋樑、水庫及電力系統（含輸電設施、高壓電塔等），藉以阻斷各項後勤支援能力。

㈣以三棲武力進犯攻擊本、外島。

㈤以網路戰癱瘓軍、民資訊網路及廣播電視媒體，並攪亂台灣金融系統。

㈥海外散播謠言，混淆美國視聽並引起對台政策分歧，並以心理戰擾亂軍、民心理。

至於中共侵台時可能採取之網路戰作爲則預判有資訊網路攻擊、病毒作戰及駭客入侵等三大主軸，說明如後：

㈠對國軍資訊網路展開攻擊

1.襲擊國軍資訊系統

藉以破壞國軍決策機制與指揮作業程序，並配合先進偵察系統、指管系統與精確導引武器，摧毀國軍指揮中樞及要害，達到實質性之破壞。

2.干擾國軍指管系統、網路

藉以切斷或迫使國軍改變指管模式。給予或植入錯誤資訊，以混亂指管決策系統，甚而竊取、破壞、欺騙、摧毀資訊系統或傳輸網路。

㈡對國軍展開病毒戰

1.中共可能採取的病毒入侵管道－內部攻擊

就國軍網路而言，中共特工人員可以藉由任何一台電腦或工作站開始散播病毒，並經由伺服器及國軍網路骨幹傳給其他國防單位。

2.中共可能採取的病毒入侵管道－外部攻擊

雖然基於資訊安全的考量，國軍目前對於軍、民用網路採取實體隔離的政策，然部分單位因爲特殊的需要或因資安措施實施的不周延，而給予中共藉由網際網路將病毒傳給國軍單位的機會。

㈢中共網路駭客入侵

中共駭客入侵的流程如圖一所示，其可能採取之網路攻擊作爲有阻斷服務攻擊、偵測防護系統攻擊、系統弱點攻擊、資訊窺探攻擊、網頁式攻擊及情資蒐集等。

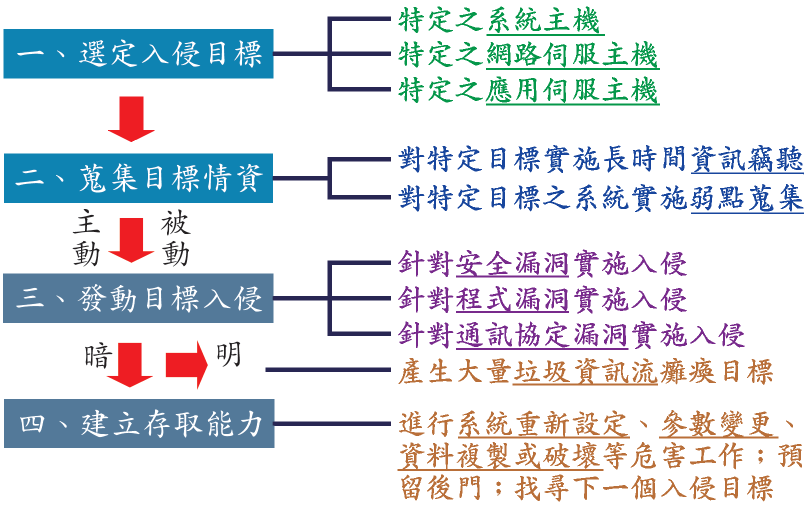
從以上的討論中可知，目前中共的網路戰能力已不可忽視，尤其是從成立所謂第四軍種（網軍）以後，更加致力於資訊網路戰之戰術戰法研究及驗證，因此預期爾後之資訊網路攻擊將對國軍通資系統造成系統功能癱瘓、網路傳輸受阻、洩漏軍事情資、指管判斷不實等重大影響，因此值得所有國軍幹部深思及警惕。

## 國軍資訊戰概況

### 一、國軍資訊戰發展及資訊安全相關規定

㈠國軍資訊戰政策發展

近年國軍鑑於資訊科技的快速進步及電腦處理各項工作的高度效率，並爲了因應資訊化作戰，故研擬了國軍資訊發展政策，諸如整合通信及資訊以建立指管通資情監偵系統平台、推動國防管理資訊系統轉型，以支援戰略規劃與聯合指揮，以及在國家資訊




▲圖一　中共駭客入侵流程

基礎建設上發展國防資訊基礎建設等作爲，期望充分運用高效率的通信、資訊網路整合科技，有效實踐三軍聯合作戰「看得見、聽得到、能指揮」之目標與三軍整體後勤的建軍備戰要求。目前國軍資訊的整體規劃與發展，係依「有效嚇阻、防衛固守」之戰略指導及聯合作戰需求，達成爭取資電優勢、鞏固國防、制敵機先之目的；策定優先順序，本平、戰時結合之理念，詳實檢討規劃訂定發展策略。現階段主要政策爲：加強國防資訊基礎建設，提昇國軍網路的運作效益與戰場存活率；落實國軍業務資訊化作業，建構國軍知識共享共用之平台、達成公文管理電子化、行政作業數位化；推展委外政策，有效提昇人力的運用及創造國內就業市場。

至於資訊作戰的整備，由於國內電腦科技已普遍受到國際社會肯定，尤其對電腦防毒軟體的相關研究與網路防護產品更受到廣泛的注意。因此，現階段國軍的資訊戰發展以建立資訊防禦能量爲主要重點，尤其著重於國軍資訊系統之安全防護工作。

然因國軍整體的資訊戰組織體系尚未臻完備，大部分均採任務編組方式來遂行資訊戰準備工作，因此執行成效仍有待加強。至於資訊安全政策發展，從83年令頒國軍資訊發展策略規劃報告、國軍資訊發展（84-93年度）指導綱要計畫及執行計畫後，即致力於資訊安全政策發展，隨後並成立「通資安全處」以綜整國軍資訊戰策略規劃及指導。目前主要任務爲因應未來資訊戰之需求，國軍指、管、通、資、情、監、偵系統($C^4ISR$)及國防資訊基礎建設(DII)，藉通資安全管理與防護技術，以確保資訊優勢並阻絕敵人偵蒐、入侵、竊取、僞冒、篡改、破壞等企圖，有效剋制敵資訊攻擊作爲，進而建立主動監偵能量發展反制作爲，以削弱或摧毀敵戰場管理能力，俾確保國軍通資優勢，創造有利之戰略態勢。

㈡國軍資訊安全相關規定

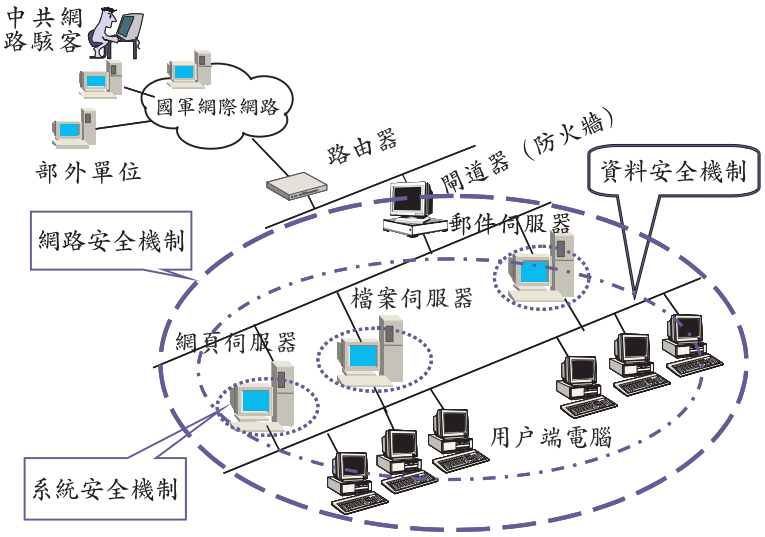
國軍目前有關資訊安全之主要相關規定計有國軍資訊安全工作指導要點、資訊安全工作手冊、國軍各級單位連結國際網際網路管理作業規定、國軍通資保密違規違紀處分規定等約18項具體作業規定，其中包含指導要點、作業規定、管理規定、保密規定、監察作業及違規違紀處分規定等六大範疇。

## 二、目前國軍之資訊安全管制機制

國軍目前之資訊安全管制機制以國防部爲主，各軍總部爲輔。國防部之整體安全應變機制已初具架構，而各軍總部則在相同架構下依其軍種特性及網路建構情形訂定其CERT（電腦緊急應變處理）應變作業。

雖然國軍資訊網路在國防部多年積極經營下，現已漸具規模並繼續推動中，惟現階段之各項安全防護系統及資訊安全基礎建設仍未臻完善，對於國軍資訊網路之規劃與發展造成極大的影響，因此如何確保國軍資訊系統對外往來的通道安全，建立安全的電子郵件系統及內部憑證管理，並設置適度抵禦入侵的防護牆及資訊網路安全防護功能檢測機制，乃變得十分重要。目前國軍整體資訊安全機制規劃如圖二[6]，茲摘要說明如後：

註6：國防部通信電子資訊次長室網站，http://www.cei.mnd.mil.tw/。




▲圖二　國軍整體資訊安全機制示意圖

㈠資料安全機制

1.公開金鑰基礎

在系統運作中，規劃使用者的合法簽入、伺服器間的認證、資料傳遞的加解密、應用程式與資料庫在網路上交易協定等安全機制之建立。

2.電腦病毒防毒機制

辨認病毒、偵測並防範病毒的危害，可清除郵件附加檔案中隱藏之病毒，並自動發出警訊給信件所屬雙方及系統管理者。規劃多層次防毒架構都有專屬防毒軟體提供完善的保護。

㈡網路安全機制

1.網路防火牆

規劃外部防火牆及內部防火牆，以防止不相關人員取得國軍網路上之資料。

2.虛擬私有網路

建立虛擬私有網路，用以達成網路間的整合與保密傳輸，並區分基本虛擬私有網路及特定虛擬私有網路，形成如同防火牆之機制，避免駭客取得連線。

㈢系統安全機制

1.弱點掃描機制

現有的作業環境以微軟視窗作業系統爲主，已知微軟視窗系統有許多駭客可攻的弱點。弱點掃描機制乃針對現有系統的主機及網路通道，利用自動駭客程式掃描以檢測有無駭客可攻擊之弱點，並檢測網路設備如路由器、交換器、防火牆、伺服器等環節存在之漏洞，提出補強以減少入侵的威脅。

2.入侵偵測機制

於網路環境中裝設入侵偵測防護系統，當有入侵事件發生時，可立即反應並予以截斷。入侵偵測防護，可分爲網路式的防護及主機式的防護兩種類型，二者搭配運用以爲互補。網路型式的入侵偵測是透過網路活動的即時監控，對入侵行爲的提早反應，僅對網路訊息作處理；主機型式的入侵偵測，則可確定入侵行爲的成功與否。除此之外，尚需一入侵偵測主控台，用以顯示入侵

警訊並緊急控管。

3.損害預防機制

損害預防機制，分爲硬體與軟體兩類。硬體採實體磁碟陣列與容錯備援等機制，軟體採微軟視窗2000中內建之相關機制，主要以資料自動備份爲主，確保資料儲存安全。

## 如何精進國軍資訊安全防護措施

### 一、國軍資訊安全防護規範現況

現階段因受限於網路安全技術及硬體配置，因此依據國軍資訊傳輸主幹網路作業安全規範，目前國軍的管制權責劃分爲國防部通信電子資訊次長室負責資訊安全政策、計畫及技術規範之研議、建置、評估及稽核使用管理。總政戰局負責危害單位「資訊安全」之預警情資蒐集、資訊機密維護及調查等工作。各軍總（司令）部則負責資料及資訊系統之安全需求研議、使用管理及保護。使用單位執行網路資源管制作業並協助稽查系統保密安全。操作個人則負責處理資料及密碼保管之責。

而各軍種所屬單位若欲架設開放或公開伺服主機（如WWW、FTP、MAIL等各類型伺服主機）應先將其需求、運用範圍、系統建置軟、硬體、功能等規劃計畫，呈報各軍總部（司令部）核准後始可開設；國防部聯參及直屬單位則比照軍種執行方式呈報總長奉核後開設。各軍總部（司令部）通資安全部門應建立其資料庫管理，並將資料提送國防部通信電子資訊次長室統一納管。目前有關資訊安全防護的具體規範有：

㈠國軍內部網際網路

所使用的瀏覽器應作防火牆代理伺服器設定，全球資訊網路伺服器應透過組態設定，使其啓動時不具有系統管理者身份，對HTTP伺服器可存取的範圍限制在網路區段的某一特定區域。

㈡單位內部網路

透過身分認證及收發認證等服務，提供通訊資料的完整性、來源確認和不可否認等安全功能，以確保參與收發雙方之權益。單位之間資料如透過專線傳送（封閉網路系統），則視資料的安全等級，根據相關安全條文做適當加解密。單位之間機敏性資料如透過國軍內部網際網路傳送，應經由虛擬私人網路，以確保機密資料的隱密性與一致性。單位內部的公文電子化，需要電子簽章的安全機制，以便內部人員進行公文的簽核或機密文件的調閱。

㈢電腦作業系統連線，應使用軍設專用電路爲原則，網路全部使用軍用電路，可傳遞「密」級（含）以下等級資訊。網路中有一段以上爲軍租電路時，於未加裝保密裝備時，限傳遞無機密等級資訊。使用軍用電路或軍租電路配合資訊保密器時，可傳遞與保密裝備相同機密等級資訊。

㈣因業務需求，得依規定由權責單位核定連線網際網路，依網際網路作業管制要點，除管理人員外，嚴禁更動原系統設定。連接網際網路之電腦應獨立設置，電腦內僅儲存連接網際網路之相關軟體及資料，嚴禁與業務用電腦混用；電路（含網路及電話線）應與單位現有作業系統實體隔離，不得搭接或混用。網路使用，應詳實登載記錄，並由保密軍官每日實施稽核。

㈤緊急事故應變與災害復原處理

各重要網路設備應有備援，並對網路

硬體設備加裝避雷措施及不斷電系統，以防止雷擊與不正常的斷電狀況。爲確保單位內部網路與外部網路的服務持續暢通，連接應有一個以上的替代路徑。對於網路系統中各主要主機伺服器應有備援主機，以因應主要主機無法正常運作時之用。網路如有被入侵或有疑似被侵入情形，應立即拒絕入侵者任何存取動作，防止災害繼續擴大；當防護網被突破時，系統應設定拒絕任何存取；或入侵者已被嚴密監控，在不危害內部網路安全的前題下，得適度允許入侵者存取動作，以利追查入侵者。

㈥網路安全稽核

除可偵知違反系統安全策略事件，以達到嚇阻不法及入侵偵測的雙重目的外，並可對未來稽核查詢系統加入經驗法則以加強入侵偵測的能力。

㈦運用相關法令查處

若發生涉及違反電腦設備安全及資訊保密案件時，得參酌有關法規查處。

## 二檢討並規範國軍資訊安全規定及相關作業程序

依據文獻記載及2001年國家資通安全會報資料，網路安全潛在威脅因素中環境的因素約佔15%~17%，而人爲因素則約83%~85%。綜合檢討目前國軍網路所面臨的安全問題可分爲病毒感染、資料外流、非核定使用人員入侵、使用人員不務正業（違規使用公務電腦上網際網路或玩電腦遊戲）、遭不明人士竊聽或僞裝等五大類。另一方面，由軍方目前的主要資訊安全缺失（詳如附表）可看出，仍然以個人操作習慣不良及保密觀念不足佔絕大比例。因此個人認爲現階段國軍的資訊安全應置重點於－如何規範國軍資訊安全規定，訂定相關標準作業程序，並輔以適當的處分規定與監察制度，以利整體資訊安全防護作業。

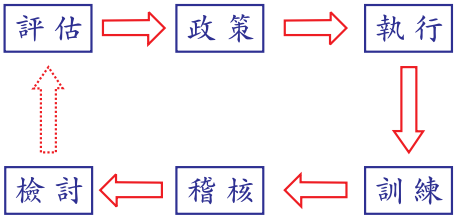
然而，資訊安全應考量的範圍包含管理制度、作業流程、人員、軟體、硬體、通信、資料文件、媒體儲存、實體設施等九大範疇，各範疇之間看似獨立卻又息息相關。因此國軍在規範相關資訊安全規定之前，必須先確認國軍的安全需求爲何，並確實做好資訊安全整合規劃後，方配合國家政策來研究訂定國軍資訊安全政策及相關規定，並依據實際狀況與實施步驟來逐級逐一訂頒標準作業程序，以利各層級遵循與作業管制。

目前國軍資訊安全應具有的基本需求，包含基礎網路架構、資訊內容、應用程式使用及操作安全等四大部分。但若以整合的觀點而言，資訊安全則應包含個人電腦、伺服器、網路、病毒及認證等系統，再配合政策與稽核以求得完善之資訊安全系統。

根據以上推論，國軍的資訊安全政策至少應包含實體安全、撥接存取、服務存取、資料加密、電腦病毒防範及身份認證等六大種類。其具體作爲則應包括安全管理、數據通訊裝置、隱私權、對侵入之反應指導原則、程式軟體引進原則、可容許引進原則、安全警報程式及違反原則之處置等八大要項。至於資訊安全的實施步驟則如圖三所示，其中必須特別注意的是檢討後的回饋資訊，以便作爲評估及修訂資訊安全政策之參考依據，唯有如此不斷執行、稽核、檢討及修正，方能求得最佳化之資訊安全防護措施。然而，必須注意的是－制定資訊安全政策後應指定專人或專責單位負責，並依程序進行後續的維護與檢討工作。在此必須特別

| 區分 | 資訊安全缺失 | 原因 |
|---|---|---|
| 個人 | ·軟碟片引入病毒<br>·防毒軟體安裝不確實與未及時更新病毒碼<br>·使用帳號未嚴格管制<br>·安裝來源不明軟體<br>·無備份資料習慣<br>·不當或未依規定開設資源分享<br>·違規使用撥接線路或手機上網搜尋資料 | ·操作習慣不良<br>·保密觀念不足<br>·法紀觀念不足 |
| 組織 | ·公開金鑰身份認證機制尚未建立<br>·各單位防毒機制未集中控管，定期更新病毒碼<br>·網路傳輸資料時未區分安全等級<br>·尚未建置可偵測蓄意侵入者之監督軟體 | ·整體安全防護機制尚未建置完畢 |
| 訓練 | ·資訊作業規定及資訊安全要求不熟悉<br>·錯誤的安全認知，僅作簡單的保護<br>·密碼不夠安全或設定過於明顯、草率<br>·不安全的連接太多<br>·主機管理疏忽或設定錯誤 | ·基礎教育不足<br>·資安教育不足<br>·保密觀念不足 |
| 法令 | ·作業單位、場所及個人未設置或缺乏資訊作業手冊、規範及相關處罰規定<br>·單位自訂之資訊安全管理規定違反部頒作業<br>·部分資訊作業無相關法令依據或規範 | ·法令未臻完善<br>·法規未依實際需要及層級頒發 |

▲附表　國軍主要資訊安全缺失檢討




▲圖三　資訊安全實施步驟

提出強調的是－當最初資訊風險評估工作所根據的基礎變動時，此程序能重新檢討政策以因應變化。

## 三精進資訊安全管制之具體作為

儘管資訊安全攻防戰的方法與技術與日俱進，但無論由技術面或務實面來考量，網路系統被入侵之原因不外乎以下幾點：

㈠不重視安全性，沒有任何保護措施或僅作簡單之保護。

㈡密碼不夠安全或設定過於明顯、草率。

㈢系統程式有問題。

㈣不安全的連接太多。

㈤主機管理疏忽，如不完善的檔案存取控制、備份管理、稽核制度。

㈥錯誤的安全認知。

㈦惡意的內部人員。

因此預防入侵的具體作爲應包含以下五大範疇：

㈠健全網路安全管理及稽核。

㈡資訊安全技術之研發。

㈢防火牆設計與建置。

㈣偵測入侵行爲技術之研發。

㈤強化身份驗證之技術。

然而，各範疇所涉及之問題相當廣泛，且涉及資訊安全委外、資訊安全教育、採購預算編列等政策與規定。因此本文並不深入個別討論，以下僅提出較務實的做法以供參考。一般而言，預防入侵之必要作爲至少應包含：

㈠每日檢視系統記錄檔是否有不正常處理動作。

㈡每日檢視防火牆記錄是否有非法嘗試連線。

㈢每日檢視網路服務狀態是否有異常大量請求服務現象。

㈣使用入侵偵測系統，自動檢視系統是否設定正確。

電腦病毒防禦則必須完成以下作爲：

㈠建置網路病毒防護牆。

㈡建置網路防火牆。

㈢建置並落實辨識與認證機制。

㈣設置虛擬私有網路。

㈤建立網路遠端撥入防護。

㈥強化憑證認證管理。

目前國軍因部分資訊安全措施之規劃尚未完成或尚未建置啓用，因此現階段較務實的資訊安全管制作法，個人建議爲：

㈠落實人員管理機制

對於資訊系統相關之職務（位），應進行安全等級評估，並考量允許存取資料之敏感性、機密性，賦予各級人員使用資訊系統及存取資料之權限，並定期加強考核。負責重要資訊系統管理、維護、設計及操作人員，應予妥適分工，必要時得建立相互制衡的機制，並建立人員輪調及備援制度。人員離（休）職時，應立即取消其使用單位內資訊資源之所有權限。

㈡重視資訊安全訓練

定期對各級人員進行資訊安全教育訓練及宣導，並列爲重點教育訓練之項目，以求建立以下所列之基本網路安全知識。

1.不開啓來路不明的郵件。

2.小心郵件中的網頁。

3.密碼設定勿過於簡單。

4.嚴禁帳號及密碼外借他人。

5.加強伺服主機的獨立性。

6.架構網路安全防衛系統。

㈢嚴密資料安全管理

1.儘量減少磁片或可攜式資訊媒體之使用，並將資料加密後儲存於伺服器上。

2.極機密以上之資料，應加密後儲存於可攜式資訊媒體中，不得存放於伺服器或使用者硬碟中。

3.任何透過網路傳輸之公文或業務資料，必須予以加密並附加數位簽章，以有效防止備份資料遭到竊取與竄改。

4.透過伺服器列印之報表應於系統中留存稽核紀錄，並造冊簽領後，始得攜離電腦機房。

5.廢棄之報表應立即銷燬，不得移做他用。

㈣強化網路安全管理

1.各單位網路建置完成時應隨即建立單位內部及對外之網路配置圖，並於單位實

施保密安全檢查時，核對修訂最新電腦與網路配置狀況。各單位資訊部門應配合保防人員採定期（至少每月一次）或不定期方式，確實檢查單位有無私接線路或網路實體遭受破壞事件發生。

2.定期將各項資訊安全機制之稽核紀錄與檢查結果，分析並彙整關閉伺服器上沒有必要的網路服務及通訊協定，以減少伺服器遭到入侵之可能。

3.網路上之資源分享應設權限管制，以杜絕可能之洩密情事。

4.各單位對外連接點應加裝防火牆以防止外部入侵，對於內部有特殊安全需求之單位，可另加裝內部防火牆，以提昇該單位之安全防護能量。

㈤定期實施資訊安全稽核作業

各單位資訊部門應配合保防人員每日檢查資訊系統使用記錄，並找出可能之不正常訊息，以便及時修訂管理上的缺失或盲點。總部資訊中心應配合保防單位，於實施年度資訊安全檢查時，利用系統掃描軟體，協助受檢單位找出作業系統可能之管理漏洞，以利檢討修訂。各單位資訊部門則應於實施資訊教育訓練期間，安排資訊安全與正確電腦操作習慣之課程。另外各單位資訊部門亦應配合保防部門，不定期稽核單位之資訊安全執行狀況，並將缺失情形彙整，由資訊部門輔導改進。

㈥平時之資訊安全防護作為

1.成立緊急危安應變處理任務編組，並反覆實施狀況演練。

2.完成作業軟體檢測。

3.進行裝備檢整。

4.落實網路安全檢查工作。

5.加強系統防毒作業。

6.加強網路監控。

7.完成作業場所電磁遮蔽及裝備接地措施。

8.定期實施資訊安全稽核作業。

9.網路系統的保護。

㈦戰時資訊安全管制作為

1.依緊急突發事件因應人員編組執行作業。

2.對作業系統、應用軟體及資料進行備份。

3.完成備用裝備、電力供應系統準備。

4.完成備用傳輸電路之開放。

5.實施全天候24小時監控作業。

6.重新設定網路參數，並派專人專職監控。

7.加強作業場所電磁遮蔽及裝備接地措施。

8.加強電子公文認證。

## 未來國軍資訊安全發展方向與展望

依據資訊科技的發展趨勢及爾後的資訊安全技術發展，並配合國軍的資訊安全規劃。國軍未來的資訊安全發展方向約可分為以下七大方向：

一、持續網路安全機制檢討及規劃以強化危機通報與預警機制，並研析先進技術與趨勢，蒐集成功企業之資訊發展與運用模式，評估引用於國軍資訊發展之可行性。

二、結合精進案，檢視國軍資訊發展與運用現況，發掘整體資訊發展瓶頸與運用需求，擬訂未來全軍整體資訊發展優先順

序，配合各項資訊建案，強化資訊安全規範。

三健全網路安全的相關檢查工作，加強事前防範措施與事發應變處理能力。

四健全各層級資訊安全稽核作業，落實安全防護。

五落實資訊安全教育及資訊作業規範，並釐定相關配套措施，建立資訊發展整體標準機制，提昇國軍整體資訊發展之品質與效益。

六積極開發網路安全的防護技術。

七加強與軍公民營廠商資訊安全技術合作。

八配合國家資訊安全法制，擬定國軍資通安全法規。

至於未來的國軍整體的資訊安全計畫是希望能包含防護體系、評估認證、資安教育及通報流程等方案並配合系統整合及資料庫管理等技術來持續更新，以達到加快資訊安全反應速度之目標。

## 結論

建置資訊安全體系可保護資訊不受各種威脅，確保組織運作並將傷害降至最低。然而資訊有多種方式的呈現，可以印刷或寫在紙上，也可以用電子方式儲存；可以郵寄或是電子郵件、也可以用影片播放或口語傳播。然而無論其形式爲何，使用何種方式與他人分享或儲存，都應以適當之方式加以保障。因此必須實行可靠的控管措施，包括資訊安全政策、作業程序、組織架構、軟體功能等。

孫子兵法虛實篇有云：「善攻者，敵不知其所守；善守者，敵不知其所攻」。恰巧描繪了今日資訊人員的困境。隨著科技的進步，入侵途徑的暴增，新的駭客不斷增加，舊駭客又不斷更新技巧的情形下，資訊人員根本不知如何防守起。因此除引進或研發資訊安全防衛軟體外，藉由強大研發團隊的不斷努力，從最簡單的自我檢查做起，進行弱點稽核，隨時掌握最新資訊安全情報，利用偵測器進行持續監測。

然而任何系統最薄弱的一環始終是人，因此資訊安全的警覺訓練仍是投資報酬率最高的資訊安全反制對策。而且利用資訊及保護資訊是同等重要的，一分事前的預防重於十分事後的補救。因此最後僅以「資訊安全，人人有責」來共同勉勵。

## 參考資料

一Joint Doctrine for Information Warfare, JP3-13，光碟版。

二榮泰生，資訊管理學，(台北：華泰書局，1999年)。

三Chris Brenton著，孫銘新，邱柏豪，廖殷淳編譯，精通網路安全技術，(台北：儒林書局，1999年)。

四William Stallings著，巫坤品，曾志光譯，密碼學與網路安全，(台北：碁峰資訊，2002年)。

五2001年資通安全報告書，國家資通安全會報，2001年12月。

## 作者簡介

林明昌中校，中正理工學院正47期、中正理工學院電研所22期、中正理工學院國科所博士16期。曾任排長、連長、組長、訓練官、參謀、教官、隊長。現任第六軍團第三後指部資訊室組長。