題目：資訊科技對作戰之影響兼論因應之道

作者簡介：
王進玄少校，陸軍通信分科班87年班、空軍航空技術學校電子戰正規班91年班，曾任排長、副連長、連長、通信官，現為步兵學校軍聯組通化小組教官。

提要：
一、軍事科技將由於第三波資訊產業的發展而出現劃時代的革命，所以未來的戰爭也將會呈現與以往不同之新型態。
二、資訊科技對未來作戰之影響有：㈠戰爭界限更加模糊；㈡武器裝備投入數量相對減少；㈢安全保密問題更加突出；㈣資訊不對稱的情形更為突顯；㈤作戰目標以破壞敵人資訊優勢為主；㈥火力運用從面的打擊轉為「點穴作戰」；㈦指揮架構趨於扁平化；㈧以自動化提升效率；㈨以最少代價，達成作戰目標。
三、共軍近年來積極將資訊科技融於作戰運用，目前其資訊戰力之優勢主要為衛星通信、偵察技巧及非核子戰術性電磁脈衝武器（EMP），已對我構成嚴重威脅。
四、對共軍應用資訊科技作戰我因應之道：㈠落實資訊基礎建設與新技術研發；㈡結合民間科技，增強資訊戰力；㈢建立軍民兩用航天體系，有效整合C⁴ISR系統；㈣加速更新通信裝備；㈤建構網狀化作戰網路；㈥培養資訊人才，提升資訊戰力；㈦強化資訊網路安全管理；㈧強化電磁脈衝防護，保存資訊戰力。

壹、前言：

由於科技的進步，隨著電腦微處理器、高速通訊設備、網際網路和精密感應器的普及，資訊戰爭的時代已到來。所謂資訊戰廣義而言，包含心理戰、欺敵、安全措施、實體破壞、資訊攻擊、及電子戰等[1]。資訊戰爭的觀念隨著美國近年來歷次的軍事行動而逐漸孕育成熟，其中1991年第一次波灣戰爭，更是美國首次將資訊科技運用在作戰上，可謂資訊戰爭的先驅。美國軍方和國防專家皆認為，資訊戰爭將是未來的戰爭趨勢，他們預測在未來10年以內，軍事科技將由於第三波資訊產業的發展而出現劃時代的革命，所以未來的戰爭，也將會呈現與以往不同之新型態。本文旨在介紹資訊科技對作戰之影響、共軍運用資訊科技融於作戰之發展現況，並提出

[1]吳福生譯，＜資訊戰的新世界＞《國防譯粹》，第24卷第6期，民國86年6月1日，頁29。

我因應之道，俾供建軍備戰之參考。

貳、資訊科技對作戰之影響：

資訊科技的日益發展，使作戰指揮、管制、偵察、監視、情報傳達更為快速，提高戰況體認共享程度、並將資訊優勢專換成戰力。作戰節奏也更為緊湊。美國自2006年積極推動3項資訊作戰，亦即電腦之網路作戰、「支配」（Influence）作戰及電子作戰。在這些新戰鬥領域中，敵人及其行動結果變化莫測，且狀況遭遇亦極不明確[2]。美國國防部官員2009年4月曾對法新社透露，正在籌畫成立新的網路軍事指揮部，負責電腦戰爭的防衛與攻擊。美國總統歐巴馬認為網路威脅是美國所面臨最嚴重的經濟和國家安全挑戰，其於2009年5月29日宣佈將任命一位「網路沙皇」(cyber czar)，負責協助美國政府與民間遏阻日增的網路攻擊，確保美國數位基礎建設的安全[3]。未來資訊科技對未來戰爭有相當重要之影響，對此趨勢，我們應加以正視。一次波灣戰爭、阿富汗戰爭、二次波灣戰爭已顯示出擁有資訊科技優勢之國家，能有效掌控戰場，以最小之傷亡、快速結束戰爭。近年來資訊科技對作戰之影響如下：

一、戰爭界限更加模糊（圖一）：

傳統意義上的戰爭有前方和後方之分，但在資訊科技高度發展的現代，縱橫交錯、四通八達的電腦網路，使每個有心參戰的個體，都可利用手中的個人電腦，不必機動到敵國度內，隨時隨地便能發起網路攻擊。在911事件後，美國遭受網路攻擊，經查攻擊來源為我國內某公司，又再仔細詳查，是恐怖分子侵入該公司路徑對美國發起之攻擊。

圖一　四通八達的電腦網路使戰爭沒有前方和後方之分

資料來源：http://www.yahoo.com

[2]Adam j. Hebert，周敦彥譯，＜資訊戰爭＞《國防譯粹》，第33卷第12期，民國95年12月1日，頁29。

[3]蔣天清，〈歐巴馬將任命網路沙皇 遏止網路攻擊〉，pchome網，http://news.pchome.com.tw/science/cna_business/20090530/index-12436444213770122005.html

二、武器裝備投入數量相對減少：

由於太空監偵及無人偵察系統日益發展，並藉由資訊科技提升傳輸速度，再加上配備有全球定位系統的精確導引武器，可精確打擊敵人關鍵部位（圖二），使武器裝備投入戰場數量相對減少。

圖二　太空監偵系統可協助精確打擊敵人關鍵部位

資料來源：http://www.yahoo.com

三、安全保密問題更加凸出：

美國國防部在一份報告中提出警告：「敵人甚至不用進入美國本土作戰，就能破壞美國的電腦網路系統而達成戰爭企圖。」從事網路戰爭的關鍵是要能破譯敵人電腦系統之密碼，尤其是核心密碼，極少數人就可以發動戰爭。

四、資訊不對稱的情形更為凸顯：

資訊科技高度發展之國家與一般國家作戰時，因所能掌握戰場資訊較一般國家多出許多，且利用此一優勢，先期摧毀C^4ISR系統，使敵我資訊不對稱的情形更為凸顯，更能主控戰場。例由近年來第一次波灣戰爭、科索沃戰爭、阿富汗戰爭、第二次波灣戰爭可看出，資訊科技先進之國家可在戰場投入相當數量之衛星偵察系統、無人飛機，偵察後再經由通信衛星、網際網路等迅速傳輸，經電腦分析後，便可對敵雷達偵測系統、通信系統加以定位並展開攻擊，而遭攻擊之國家，則因雷達偵測系統與通信系統遭敵摧毀，無法蒐集到足夠戰場資訊，就有如盲眼者對明眼者之決鬥般，盲眼者毫無招架之力。

五、作戰目標以破壞敵人資訊優勢為主：

昔日戰爭的執行多以攻城掠地、消滅敵人有生戰力為目標，而現代作戰則可透過資訊攻勢手段，干擾或打亂敵方的作戰決策程序，使其無法採取協調一致

的作戰行動，贏取勝利先機。

六、火力運用從面的打擊轉為「點穴作戰」（圖三）：

過去「地毯式」轟炸、打覆蓋面的火力運用方式將成為歷史。取而代之的，將是採取非傳統式的「點穴」方式，以精度、速度、超視距打擊為基本火力運用方式對高科技作戰系統實施關鍵點的結構破壞以癱瘓敵戰力。事實上，具有中國文化特色的「點穴」作戰模式，以資訊科技的發展趨勢，達到「隔空點穴」的作戰效果，已非空言[4]。

圖三　高科技作戰系統可實施關鍵點的結構破壞以癱瘓敵戰力

資料來源：http://www.people.com

七、指揮架構趨於扁平化：

「需求頻寬」的成果顯示機械處理與傳送資料的能力遠勝於人工處理；在藉由網路系統提升作業速度的過程中，決策者可能成為阻礙改革的主要人物。由於資訊系統具有較佳的過濾與顯示效果，如再對操作人員施以合宜的訓練，就可突破人類智慧的極限。不過，資訊系統速度的大幅提升後，可能必須裁撤中間決策過程的參與者。在最高指揮層級與戰鬥感測器或武器系統間建立直接的通信鏈路，可去除指揮與執行者間的干預層級，而使金字塔形的指揮階層「扁平化」。此種「扁平」式與「高度中央集權」式的架構，將使戰鬥部隊可直接與最高指揮部聯繫；1996 年美海軍陸戰隊所舉行之「狩獵戰士先進作戰實驗」，即為此種指揮結構的典型代表。在此次演習中，由於裁撤中層的指揮階層，使得命令的下達與回應速度都增快許多，但是卻造成連、營級幹部回到後方區域。就傳統的戰鬥指揮觀念而言，這是個很重大的變革。雖然這並不代表美海軍陸戰隊未來的組織型態，但該演習的經驗，卻顯示網路連線的作戰方式，再也不可能讓連級軍官擁有「全權授與」的權責[5]。

4　曾瑞章，《兩岸電子資訊戰發展比較上》（台北：尖端科技，1999 年 7 月），頁 73。

5　陳振農譯，＜資訊科技之文化挑戰＞《國防譯粹》，第 26 卷第 1 期，民國 88 年 1 月 1 日，頁 39。

八、以自動化提升效率：

除在C[4]ISR系統方面實施自動化外，為減少軍事作業成本，後勤系統亦已實施自動化，以降低裝備停用時間及維護成本。因此，未來將會開發即時的後勤網路回報系統，其中包括將感測器植入主要裝備組件中，以直接向遠端、上級的維修人員及裝備製造商，持續且自動地回報狀況。其構想乃是透過即時作業以及零組件取得與技術援助過程的自動化，大為降低維修時間，並可減少維修人員編制。自動化回報網路系統並可讓上級單位掌握各連線站台的物資籌補狀況，甚至可自動提出單位裝備損害報告，使上級單位可有效地授權現場指揮官決定單位作戰與物資籌備[6]。

九、以最少代價，達成作戰目標

資訊裝備、電腦網路、通信設施、監偵裝備不斷精進，使得科技發展之國家可洞悉戰場狀況、作戰準備快速、火力運用靈活，又由於指揮扁平化的關係，提升其作戰速度與靈活度，使敵在來不及準備之情況下，屈服其意志，減少己部隊在戰場之傷亡。如美軍於第一次波灣戰爭、阿富汗戰爭及第二次波灣戰爭都是以最少代價，達成作戰目標，便是資訊戰典型代表。

參、共軍運用資訊科技融於作戰之發展現況：

第一次波灣戰爭後，共軍研究認為：「資訊作戰乃是一種包含偵察監視、作戰全程整合C[4]ISR作業效能、資訊策略欺敵、資訊心理作戰、電子作戰、戰場資訊防護、資訊系統實體摧毀及保障等『軟殺傷』及『硬摧毀』交互實施的作戰模式」。此種作戰模式旨在保障己軍指、管、通、情的資訊獲得及運用能力，並以癱瘓敵軍心理士氣及癱瘓敵軍C[4]ISR及作戰能力為目的。基於上述認知，共軍乃著手進行資訊作戰的建設工作。中共於「總參二部（軍事情報部）」下設「科學裝備局」，除已於1992年完成三軍情報自動化指揮系統的連線工程外，亦已針對運用電腦網路竊取、竄改資料、散布謠言及散播病毒程式等犯罪行為加以監控防制。近年來由於經濟快速成長每年皆大幅增加國防預算，積極運用資訊科技提升其部隊現代化，其有關運用資訊科技作戰之發展敘述如下[7]：

一、積極發展太空監偵及通信系統：

㈠太空監偵系統方面：

共軍於第一次波灣戰爭後，著手打贏「高技術條件下局部戰爭」的準備，包括資訊戰、高解析度偵察衛星、彈道飛彈及空射、陸射、海射巡弋飛彈等，並

[6]同註4，頁40。

[7] 同註4，頁76～77。

於2000年發射6枚衛星，且載人太空船神舟5（圖四）、6號已發射成功，2008年已完成神舟7號發射及執行航太員出艙活動試驗，2009年預定建立太空實驗室[8]，依照中共的規劃，2009～2012年完成目標飛行器對接技術，2015年建立永久太空站[9]。共軍在太空系統發展於軍事運用上，可對軍事目標進行精確測量與定位，並將訊號傳送至武器系統運用。

圖四　中共神舟5號運行情形
資料來源：http://www.sina.com

㈡通信系統方面：

現代戰爭要求高機動、高效率的作戰部署。因此，共軍積極建立軍用全球衛星定位系統及光纖網路，以爭取戰場軍事優勢。2001年已完成總長一百餘萬公里的光纖通訊工程及建立全大陸「八橫八縱」的傳輸網路基礎。另於「九五計畫」期間，建立戰備通信網路，將以太空衛星為主體，以地面衛星接收站為輔（圖五），構成完整的地、空鏈結通信網路（圖六）[10]。

圖五　中共車載式衛星接收站
資料來源：http://www.people.com

[8]應天行，〈中共與美國合作進型態空探索的可能性探討〉《中共研究》，第38卷9期，2004年9月，頁92。
[9]桑治強，〈中共航行戰略發展與我國應採取之策略〉《國防雜誌》，第22卷6期，民國96年12月1日，頁87。
[10]劉德彥，〈論中共電子戰戰力與我因應之道〉《陸軍月刊》，第41卷481期，民國94年9月1日，頁57。

圖六　中共野戰通信團新通信裝備演練

資料來源：http://www.people.com

二、持續構建支援資訊作戰的指管系統：

自 1990 年代迄今，中共已研發完成「野戰自動化指揮系統」及「野戰自動化指揮車」等戰場指管裝備，正進行戰略指揮系統的研發與部署。

三、加強普及資訊作戰訓練：

共軍將資訊戰界定為「知識戰爭」，是高智慧人才力量的特殊較量，不僅引進前蘇聯解體後的大批科學家，改革後的歸國學人也能補充所需，共軍已編製一套資訊課程以培育人才[11]。現其已成立培訓各級資訊及指揮通信作業人員之「信息工程學院」，除各類軍事院校加強電腦基礎教育外（如圖七），並增設相關資訊作戰技術的課程，另針對新配備的光纖通信、數位通信、衛星通信、微波通信等裝備，加強實施專業人才培訓，並將新裝備運用於戰役演練中，至於作業單位所需的資訊系統設備，正持續普遍設置。近年來共軍已運用電腦數位科技，完成多種戰機、火砲、戰車、飛彈等武器的模擬訓練系統（如圖八）；開發各類戰役模擬的電腦兵棋軟、硬體，並交由聯訓基地或軍事院校進行測試，持續研究與精進。

圖七　中共電腦基礎教育訓練情形

資料來源：http://www.sina.com

[11]梁正綱，〈臺海衝突中的戰略資訊戰〉《國防雜誌》，第 23 卷 1 期，民國 97 年 2 月 1 日，頁 52。

圖八　中共電腦模擬訓練情形

資料來源：http://www.people.com

四、持續研發實用軍事科技及進行資訊戰戰略研究：

共軍國防科學研究院宣稱，已成功完成「模糊邏輯」人工智慧開發環境的構建，「杭州大學」則開發成功新型500瓦雷射光束加工機（可用於焊接積體電路晶片等用途），此等科技的突破對中共發展資訊作戰有相當助益。另外，中共已成立一處軍事戰略研究中心，旨在研究如何贏得「資訊時代的資訊戰爭」，此等結合科技研發、軍事智慧及戰略研究的努力，均將為中共資訊作戰能力建構相當基礎。

五、發展癱瘓敵資訊戰武器：

共軍已具備小型核彈、中子彈技術，具備研發電磁脈衝與高能微波武器之能力，其可用於強力干擾摧毀戰機航電系統與反輻射飛彈、干擾各式衛星電子系統，以及大規模摧毀指、管、通、情中心與資訊網路節點等。研判共軍在首波對臺攻擊中，可能運用海空軍武力、彈道飛彈、巡弋飛彈、反輻射飛彈、電磁脈衝武器、電腦病毒攻擊，對臺進行「點穴戰」，癱瘓我防空網、軍用機場以及指管通情系統[12]。美國國防部2006年報告指出，共軍「可能」已建立能夠「發展病毒攻擊敵人電腦系統與網路」以及「保護友軍電腦系統與網路之方法」的資訊戰部隊。該報告指出，中共資訊戰作戰構想「強調電子作戰的整合運用、（電腦攻擊）及針對關鍵C^4節點實施有限的動能打擊，以破壞敵人的網路系統」[13]。

六、發展網路攻擊能力：

根據被美國五角大廈倚為智庫的「國防科學評議會」發表報告說，除美國以外，包括俄羅斯、中共、北韓、伊拉克、伊朗、印度、埃及、古巴、利比亞和敘利亞等10個國家都有能力發展資訊戰爭，美國「國家安全局」（ＮＳＡ）更估計全球有120多個國家有「電腦攻擊能力」。共軍於1997年10月10日首度進行戰役層次電腦網路病毒對抗演練，由瀋陽軍區某集團軍所屬的兩個師指揮所，相互以電腦病毒進行攻防，共軍三軍總部及各部隊的電子戰專家都在現場觀摩。另共軍自2000年開始研究結合民兵與後備部隊，於緊急狀況中，以駭客攻擊與網

[12] 陳子平，〈中共「不對稱作戰」的發展影響——從美國2006中共軍力報告的觀察〉《國防雜誌》，第21卷6期，民國95年12月1日，頁178。

[13] 同註2，頁30。

路入侵，或以其他型式的網路戰，攻擊敵人的軍事與商用系統，並同時防護共軍的網路。加拿大網路研究機構「資訊站監督人」研究人員於2009年3月28日表示，一個來自中共的間諜網絡已利用惡意軟體駭入103個國家的政府與私人機構電腦，並竊取電腦裡的機密檔案[14]。另英國情報單位警告英國政府當局，由於英國電訊新架設的通信網路是採取中共華為電信的技術，中共或許已能運用其架設的器材癱瘓英國電信網絡，進而破壞仰賴電腦運作的水電供應、食物分配、金融體系與運輸系統，使整個英國陷入停擺[15]。

七、積極發展資訊戰戰術戰法[16]：

依林中斌博士的蒐整及歸納，共軍已積極探討資訊作戰的實施方式。目前，中共資訊作戰基本的戰略戰術概念，是研究如何將「作戰人員及裝備形成的作戰運作體系」與「資訊流及資訊裝備所形成的功能體系」兩大部分，進行實質或無形的破壞戰術，使敵人因不能結合此兩大運作系統，而達到癱瘓其戰鬥力的目的。林博士所蒐整的中共資訊戰戰法如附表一：

附表一中共資訊戰戰法

戰術面	攻擊面
首戰即決戰	戰端一開，戰略、戰役、戰術行動即相互滲透，高度融合。首戰迅速而直接地發展成為決戰，勝負一戰便見分曉。
指揮控制戰	攻擊指揮體系，使之癱瘓。摧毀個別關鍵設施，就可破壞敵作戰系統的整體性。
多兵器結合	充分利用砲兵、航空兵、戰役戰術飛彈、綜合攻擊C^3I系統。
用特種分隊	利用特種分隊、潛入敵縱隊，襲擊敵偵察、指揮、控制、通信系統、以及戰術火箭等重要目標。
實施軟打擊	充分利用心理戰、戰術欺騙等，對敵實施軟打擊。
小散遠直	戰場行動的特徵是部隊小型、人員裝備分散、打擊距離遠、指揮層次少而直接。

參考資料：曾瑞章，《兩岸電子資訊戰發展比較上》（台北：尖端科技，1999年7月），頁77。

肆、對共軍應用資訊科技作戰我因應之道：

一、落實資訊基礎建設與新技術研發：

資訊戰能力，根植於國家資訊基礎建設，現今世界先進國家，莫不制定長程計畫積極進行。我國於民國86年行政院即設置「資訊通信基礎建設推動小組」

[14]〈中國網軍　駭入103國公私電腦〉《自由時報》（台北），民國98年3月20日，版A4。

[15]〈網絡採用中國技術　英國恐遭癱瘓〉《自由時報》（台北），民國98年3月20日，版A4。

[16]　同註4，頁77。

負責國家資訊基礎建設（NII）的推動，期使我國能成為世界最先進的資訊化國家，提升國家競爭力；並置重點於國防資訊基礎建設（DII），期以奠定資訊戰良好建設[17]。現今共軍在資訊建設方面不遺餘力，我們更應利用國內資訊人才優勢，對於未來資訊工業發展進行評估，同時結合工研院、資策會、中科院等單位，對於資訊戰的關鍵技術持續進行研發，俾使國家資訊戰在軟硬體上保有相對優勢。

二、結合民間科技，增強資訊戰力：

捍衛國防雖為國軍的天職，但要鞏固國防則必要整合各方共同強化，從資訊戰的觀點而論，無論運用、防護更非國防部一個單位所能獨立完成。換言之，資訊作戰涉及國家整體戰略，本無平時與戰時之分，亦無軍事與民生之分、政府與民間之別，故須結合產、官、學整合強化防護戰力。以我國資訊科技人才之豐，科技水準之強，相信不難在各方資源的界面整合下，展現卓越的資訊作戰與防護戰力，嚇阻中共輕啟資訊戰的動機。

三、建立軍民兩用衛星體系，有效整合C^4ISR系統：

發展衛星系統經費所需不貲，我國防預算有限，無法與中共做此方面競賽。基於尖端太空科技有95%皆具有軍民兩用性質，故我應善用民間資源，建構軍民兩用航天體系。並藉由通信衛星建構一套迅速、可靠且各軍種通用的軍事通信系統，以期整合與強化C^4ISR系統，提升整體戰力[18]，進而爭取台海「制天權」。

四、加速更新通信系統：

敵軍電子戰裝備日新月異，我軍部隊之通信系統尚未全面完成換裝，現行VRC-12系列通信裝備反電子戰能力薄弱，故我應加速更新部隊通信系統，強化我反電子戰能力。另應持續蒐整敵電子戰裝備發展與戰術戰法，以掌握通信系統換裝時機，以免形成反電子戰力空窗期，予敵可乘之機。

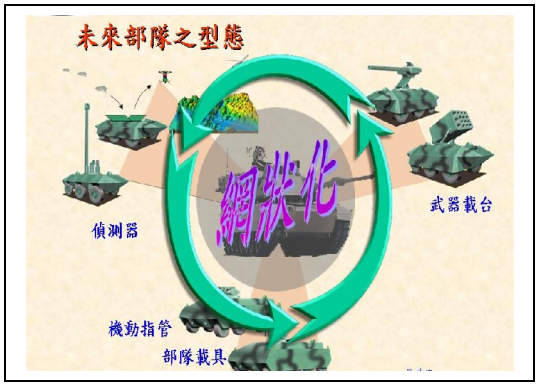
五、建構網狀化作戰網路（如圖九）：

未來的作戰運用將朝向聯合、機動、快速、多元、精準的方向發展，而以網路路由器作為連結之核心，並以此為基礎發展全新型態的指管模式，目前國軍資訊網路之架構已面臨轉型之階段，我們應全面檢討網路政策，以解決未來通資架構整合瓶頸，有效整合「指揮管制中心系統」、「情資分析系統」、「戰鬥勤務支援管制系統」、「防空系統」、「電子戰系統」、「火力與支援系統」、「海、空支援系

[17] 《戰略性資訊作戰的崛起》（台北：國防部史政編譯局譯印，民國89年5月），頁81。

[18] 張德方，〈台海安全策略研析——美國軍事介入臺海軍事衝突研究〉（桃園縣：國防大學，2005年），頁222。

統」、「機動性通信管制系統」、「資訊管理系統」、「資訊安全系統」、「數位化地圖系統」等，方能發揮戰力統合功用，且整個戰場管理系統能使司令部－作戰分區－旅級－營級－連級－個人形成串聯，使橫向聯繫增加，由樹狀指揮體系變為網狀指揮體系，提高指揮靈活度。



圖九　建構網狀化作戰以資訊增加武器效能

資料來源：步校發展室參數資料庫

六、培養資訊人才，提升資訊戰力：

共軍通信指揮學院以其跨學科組織專家、教授完成「信息作戰指揮控制學」和「信息作戰技術學」專著為理論體系，首創信息戰指揮控制這門新興學科，為其數位化部隊建設提供了理論基礎。該院先後為共軍培養了4批300多名信息作戰人才，使中共信息戰幹部大量增加；組織專家至總部機關、部隊和院校巡迴講課；出版製作有關信息戰讀物和多媒體教學軟體。為因應未來戰爭需求，國軍除廣與民間各校系所合作外，並應在軍事院校納編學有專精師資，針對部隊需求廣招學員，分組專題研究，且授予學位。利用長期的研究、發展，大量培養資訊戰人才，以提升我資訊戰攻擊及防護能力。

七、強化資訊網路安全管理：

依2006年《美國國家安全報告》指出：美國國防部電腦系統2005年上半年度遭到駭客攻擊的次數總和達21,124次[19]，顯見資訊網路很難防範蓄意攻擊者、駭客及電腦病毒的入侵、攻擊、破壞。故資訊網路安全管理相對重要。

㈠加強人員審查，負起管理責任：

資策會指出，電腦網路系統遭到入侵、破壞，根據以往的案例，外來的駭客只佔兩成，也就是說，有高達八成的駭客來自內賊或離職員工所為[20]。因此，我們對使用電腦相關人士，如電腦操作員、程式設計人員、及維護人員等可

[19]梁華傑，〈網路資訊安全探討與省思〉《國防雜誌》，第23卷2期，民國97年4月1日，頁87。

[20]《青年日報》（台北），民國87年11月24日，版4。

以接近敏感資料者，都必須加強人員的背景審核，以判定其是否足以信任。

㈡設置防火牆並不定時執行網路安全監控：

我們應將現已採用之網路密級傳輸資料管道，一律採取軟硬體兩種方式加密，並加置資料庫前端防火牆及資料庫使用權限等，但此舉對具備專業知識又有耐心的電腦駭客而言，依然無法達到百分之一百的效果。所以還應加上自動生物檢定系統（如檢查指紋、視網膜）及不定時執行網路安全監控等方法，如採不預警對各級資訊網路系統實施測試攻擊，以驗證其防護功能並找出漏洞，確保網路安全。

㈢綿密情資蒐整，開發防毒軟體：

一般的掃毒軟體係在二進位和執行檔中搜尋已知病毒程式碼，但其缺點是掃毒程式製造商必須在偵測和攻擊該病毒前，先獲悉其型態。一個撰寫極佳、未曾散布過、而且是為了攻擊特定目標而設計的特殊用途病毒，將很難被任何套裝掃毒軟體察覺，因此，如能透過綿密的情資蒐整，事先得知敵所發展出之電腦病毒型態，即能開發出效果較佳之防毒軟體，成為有效之防護利器。

㈣建立電子檔案庫，儘早恢復運作：

以電腦武器作為攻擊手段，它不一定完全是癱瘓電腦，有的只是破壞資料系統，或者是竄改資料系統。故應建立電子檔案庫，當資料遭到破壞或竄改時，即可使用備份資料，以確保戰備任務仍可遂行。

八、強化電磁脈衝防護，保存資訊戰力：

我國武器裝備多購自美國，大部分的武器系統皆在美設計防護電磁脈衝之前即已購置，例如，我們目前的主要防空武器，如鷹式飛彈、天弓飛彈及愛國者防空系統等，皆未進行嚴密的電磁脈衝測試，故對電磁脈衝的防護能力，值得懷疑。目前我們正積極發展自製精密武器，建議應加入防電磁脈衝的設計，避免將來武器系統開發完成後，無法因應新一代電磁脈衝武器。總之，電磁脈衝的防護工作，隨著國軍武器系統日漸更新，精密電子、資訊裝備的使用益見普遍的現在，變得愈重要與迫切，我們應教育幹部瞭解電磁脈衝效應，更要努力研發防護裝備，作為阻抗電磁脈衝之屏蔽，使能在遭受電磁脈衝攻擊時，仍能維持完整之指、管、通、情功能，遂行作戰任務贏得最後勝利。

伍、結語：

美軍的轉型就是以資訊科技為基礎，結合冶金、精密科技與管理、知識「創造與

掌握」軍事事務革命帶來的組織、思想與準則方面的變革[21]，成就為全球第一軍事強權。現共軍亦積極將資訊科技融於作戰系統中，在太空科技發展逐步縮小與美國之差距，已完成軍團以上自動化指揮網，現有的信息電子能力，配合反輻射飛彈、微波電磁脈衝彈、巡弋飛彈及網路攻擊，將會對我觀通雷達及指管系統實施干擾與攻擊，迫使我軍在惡劣環境下作戰[22]。面對未來持續利用資訊科技強化戰力的共軍，我亦應結合民間科技，增強資訊戰力，有效整合C⁴ISR系統，建構網狀化作戰網路，並強化資訊網路安全管理與電磁脈衝防護力，方能確保國家安全。

[21]曾祥穎，〈兩次波灣戰爭對中共建軍之啟示〉《陸軍月刊》，第41卷480期，民國94年8月1日，頁16。
[22]曾祥穎，〈中共高科技作戰之思維改變〉《陸軍月刊》，第41卷474期，民國94年2月1日，頁21。