ISSN2221-8319

資訊戰爭呈現的新特點與地面部隊因應之道

提要：

茲軍事科技將由於第三波資訊產業的發達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。

鄉資訊戰在平時或未來戰爭所能發揮的特點有虧戰爭界限更加模糊；豐武器裝備投入數量相對減少；鄉安全保密問題更加突出；鄰資訊不對稱的情形更為突顯；霣作戰目標以破壞敵人資訊優勢為主；藹火力運用從面的打擊轉為「點穴作戰」；齏指揮架構趨於扁平化；懇以自動化提升效率；璽以最少代價，達成作戰目標。

蘭中共近年來積極發展資訊戰，目前，中共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），已可對我構成實際資訊戰之威脅。

關面對中共資訊戰我因地面部隊應作為有虧落實全民國防，確保國家安全；豐落實資訊基礎建設與新技術研發；鄉全面詳細評估資訊戰之損害；鄰提高保防警覺，維護系統安全；霣培養資訊人才，提升資訊戰力；藹加強人員審查，負起管理責任；齏重視安全措施，強化網路安全；懇綿密情資蒐整，開發防毒軟體；璽儲存備份資料，儘早恢復運作；闢結合民間科技，增強資訊戰力；器組建數位化部隊，強化傳輸能力；歖持續推動戰力整合，提升作戰效能；灅強化電磁脈衝防護，保存資訊戰力；續強化軍民心理建設教育。

ISSN2221-8319

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、以及電子戰等[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 年的波灣戰爭，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，他們預測在未來十年以內,軍事科技將由於第三波資訊產業的發達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，我地面部隊應針對未來資訊戰特點，深入研究分析，並強化因應作為，才能勝兵先勝。

貳、未來作戰將呈現之新特點：

美國軍方現正埋首擘畫未來以電腦武器攻擊的戰爭型態，維吉尼亞州北部的『情報安全指揮部』湯克斯理上校指出，將來美國的聯邦遭到集權國家威脅時，不必立即派遣百萬雄兵或大批艦隊上陣，而可能改以先進的電腦軟體設備，不斷的向敵方散播『現代傳染病』─電腦病毒。首先，他們會將電腦病毒注入對手的電話切換系統，造成電信系統的全面癱瘓；其次，再以可設定破壞時間的電腦軟體，摧毀負責全國鐵路運輸和軍事補給的電腦系統，造成交通大亂。在此同時，透過無線電接受後方命令的敵方戰地指揮官，將無法察覺命令早被移花接木，使敵軍的調動更因此毫無章法和效率可言，然後派遣受過特殊心理戰訓練的美國軍機，將鼓吹敵國百姓造反的宣傳畫面傳入當地電視臺強行放送，便大功告成，整個過程不費一兵一彈,即達到擊敗敵人的任務[2]。顯示未來資訊戰在未來戰爭的重要性，對此趨勢，我們應加以正視，資訊戰在未來戰爭所能發揮的特點如下[3]：

茲戰爭界限更加模糊：(圖一)

傳統意義上的戰爭有前方和後方之分，但在資訊高度發展的今天，縱橫交錯、四通八達的電腦網路，使每一個有心參戰的個體，都可利用手中的個人電腦，破譯敵人密碼，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，是恐怖份子侵入該公司路徑對美國發起之攻擊。

[1]吳福生譯，＜資訊戰的新世界＞《，國防譯粹月刊》，第 24 卷第 6 期，民國 86 年 6 月 1 日，頁 29。
[2]《自由時報》(台北)，民國 86 年 7 月 3 日。
[3]《前衛報》，2001 年 9 月 3 日。

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

鄉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與傳輸速度提升，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

蔭安全保密問題更加突出：

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，就可很容易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，幾個人或是一個人就可以發動戰爭。

闕資訊不對稱的情形更為突顯：

國防科技發達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，先期摧毀敵指、管、通、情、監偵系統，使敵我資訊不對稱的情形更為突顯，更能主控戰場。例由近年來之第一次波斯灣戰爭、科索沃戰爭、阿富汗戰爭、第二次波灣戰爭可看出，科技發達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、通信系統等展開攻擊，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。

賽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；而未來的資訊作戰，則透過資訊攻勢手段，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，而贏取勝利先機。

滓火力運用從面的打擊轉為「點穴作戰」:(圖三)

電子資訊戰的特點是以精度、速度、超視距打擊為基本火力運用方式，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，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，此具中國文化特色的「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

輸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連繫；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

[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。

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]。

頯以自動化提升效率：

除了在指、管、通、情、電、監、偵系統方面實施自動化外，為減少軍事作業成本，亦可於後勤系統實施自動化，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，以直接向遠處、上級的維護人員以及裝備製造商，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]。

嫚以最少代價，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，使得科技發達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，提升了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。如美軍於波斯灣戰爭及阿富汗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、中共資訊戰之發展現況與對我之威脅：

筵中共資訊戰之發展現況：

第一次波灣戰爭後，中共研究認為：「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，中共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聯線工程外，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。其他有關資訊戰發展敘述如下[7]：

虧積極發展太空監偵及通信系統：

唐通信系統方面：

中共軍方認清，現代戰爭要求高機動、高效率的作戰部署。因此，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。目前已完成總長一百餘萬公里的光纖通訊工程及建立全大陸

[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。

[6]同註5，頁40。

[7] 同註4，頁76～77。

「八橫八縱」的傳輸網路基礎。另於「九五計劃」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，構成完整的地、空鏈結通信網路（圖四、五、六）。

圖四　中共車載式衛星接收站

資料來源：http://www.people.com

圖五　中共地域通信網路節點交換中心

資料來源：http://www.people.com

圖六　中共野戰通信團新通信裝備演練

資料來源：http://www.people.com

書太空監偵系統方面：

中共於第一次波灣戰爭後，著手打贏「高技術條件下戰爭」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，並於 2000 年發射 6 枚衛星，且載人太空船神舟 5、6 號已發射成功，增強其太空監偵能力（圖七、八）。

圖七　中共神舟 5 號發射情形
資料來源：http://www.sina.com

圖八　中共神舟 5 號運行情形
資料來源：http://www.sina.com

豐持續構建支援資訊作戰的指、管、通、情系統：

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。

貉加強普及資訊作戰訓練：

共軍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（如圖九、十），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（十一、十二）；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。

圖九　中共電腦基礎教育訓練情形
資料來源：http://www.sina.com

圖十　中共資訊作戰訓練情形
資料來源：http://www.people.com

圖十一　中共電腦模擬訓練情形（一）
資料來源：http://www.people.com

圖十二　中共電腦模擬訓練情形（二）

資料來源：http://www.people.com

鄰持續研發實用軍事科技及進行資訊戰戰略研究：

中共國防科學研究院已宣稱，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。

黌發展癱瘓敵資訊戰武器：

中共已具備小型核彈、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[8]。

翿積極發展資訊戰戰術戰法[9]：

依林中斌博士的蒐整及歸納,中共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「作戰人員及作戰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。

[8]＜陸軍電子戰需求探討＞《陸軍通信兵八十九年度軍事學術研討會》。

[9]同註 4，頁 77。

齊發展資訊作戰系統網路：

中共為執行資訊作戰，已構建完成中央與各軍區司令部的系統鏈路聯線，未來可透過大螢幕掌握戰區戰略態勢。餘如建置野戰自動化指揮系統、戰術資料鏈傳輸系統、指管中心機動化、完成23條光纖通信網路(總長32000公里)、以數據融合技術籌建自動化指揮系統、籌設信息戰模擬中心、以及積極開發太空C^4ISR系統等。

慰研發運用戰術：

根據《解放軍報》報導指出，中共探討的資訊作戰模式，計有下列五種：

唐欺騙性攻擊：

對敵辨識系統進行欺騙性信息攻擊。

書佔位性攻擊：

用大量無關緊要或雜亂的信息，癱瘓敵系統。

洇污染性攻擊：

向敵方提供雜亂、錯誤、矛盾的信息，癱瘓敵系統無法正常工作。

癸導向性攻擊：

在一段時間內向敵方大量傳輸、提供特定信息(真假依需求而定)，從而影響敵方決策，採取符合我方意圖之決策。

致揭露性攻擊：

適時揭露敵方當局的騙局和謊言，使對方和己方的民眾不受欺騙。

爾對我之威脅：

目前，中共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），中共也已對電磁脈衝破壞指管中心電子設備的攻擊，進行評估與試驗，預判非核子電磁脈衝武器已具成果[10]。依照我國防單位推估，中共在2005年已可對我構成實際資訊戰之威脅[11]。從紐約書評文章「網路上的中國」透露，民國88年8月在「特殊國與國關係論」被提出後，大陸駭客在一個月內曾對我發動7萬多次攻擊，其中有165次成功[12]，由此可見中共「資訊戰練兵的手段與企圖」，研判中共實施資訊戰對我之威脅如下：

虧積極戰力整合相對提升其戰力：

中共近年來積極發展偵察衛星、通信衛星、衛星導航定位衛星、無人偵察機、電戰預警機，且現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，並已研發完成「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

[10]《聯合報》(台北)，民國88年8月13日，版15。

[11]＜國防部長唐飛，國防部施政報告＞，民國88年11月1日，頁9。

[12]《聯合報》，民國88年11月13日，版13。

進行戰略指揮系統的研發與部署，除此之外，並全力研發各種火力系統之軟體技術，其中尤以射擊指揮程序及計算電腦的普遍運用，更處處顯露其戰力整合以相對提升其戰力[13]，對我威脅日益增大。

豐逐漸完成作戰準備：

中共各兵種、科研機構對信息戰理論之研究不遺餘力，近年來積極推行並落實於1997年步兵實兵演練與驗證中。另由「軍區信息作戰與訓練指導要則」建立作戰程序，組織「軍區計算機網路防護與攻擊技術研究小組」，及提出資訊對抗戰法，顯示中共對資訊戰相應之軍備、建制與作戰準則，現正逐漸配套形成中[14]。

貉資訊系統易遭破壞與癱瘓：

現我政府運作機制、經濟發展、社會民生與軍事運作等，逐漸升高對資訊系統之依賴，因而使國家在遭受敵資訊戰攻擊的脆弱性相對提高。針對我資訊系統點多線長，分布面廣，難以組織嚴密防禦等弱點，中共經由點穴、斬首、斷脈等方法，對我資訊系統關節點與資訊鏈路實施軟、硬打擊，先期摧毀、癱瘓我資訊作戰指、管、通、情體系及政、經、工、商業電腦網路系統，使我政府各機構無法正常運作與指揮，再利用我各級部隊混亂間隙，乘機實施快速打擊，達到瓦解我政、經、軍、心戰力之目的。

鄰國人心防易遭恫嚇：

民國88年7月間，我李前總統將兩岸定位為「特殊國與國」關係後，中共官方即開始對我展開一連串文攻武嚇，如其戰鬥機數次飛躍海峽中線挑釁；利用香港報紙、電視媒體等不斷放出中共演習消息與誇大中共軍力之報導，企圖影響我金融秩序與造成民眾心理恐慌；其駭客因不滿我方提出兩岸為『特殊國與國』關係，也數次對我各政府機關網站實施侵襲與散布不實之消息，而我民間組織，亦自動自發反擊；又如民國88年8月份大陸官方網站假中央社名義發出台灣海峽發生空戰的假新聞，僅僅在網路上流傳30分鐘，就造成我股市狂跌500點，造成人心惶惶。

肆、對中共資訊戰我地面部隊因應之道：

篤落實全民國防，確保國家安全：

基於中共有可能對我實施「資訊戰」，戰場已無前方與後方之差別，故未來戰爭若要贏得勝利，必須全民上下一心、團結一致；以目前中華民國在台灣而言，就是要全民建立「同島一命、同舟共濟」的生命共同體理念，並確實化為共同實際的行動才能達成。強大三軍所匯集的

[13]陳東龍，《中共軍備總覽》(台北：黎明文化，民國89年9月)，頁245。

[14]林海清，＜資訊戰與國家安全＞《國防雜誌》，第17卷第6期，民國90年12月1日，頁50。

國防力量，是國家安全的基石；但是穩定的心防和周全的民防作為，更是敵人不敢輕啟戰端的關鍵。不可諱言，台澎防衛作戰正是具有「同島一命」的特質，戰爭一旦發生，就沒有前方、後方的分野，必須軍民一體、寸土必爭，大家共同保衛我們的家園。所以建軍備戰尤須以「全民防衛的觀點」，將全國的人力，物力、財力、科技等，從事長遠整體的規劃，才能「化民力為我力，融我力於戰力」，成為確保國家安全的堅強後盾。

鄉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「資訊通信暨傳播委員會」，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[15]。而今中共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。

繭全面詳細評估資訊戰之損害：

成立專責機構，全面展開評估，中共若對我實施資訊戰攻擊，對我軍事、經融、交通、心理之殺傷效應，並積極謀求解決之道，以降低損害。

關提高保防警覺，維護系統安全：

自從解嚴以來，中共對我之滲透簡直易如反掌，其滲透之途徑現已多元化，如偷渡、探親、假結婚、依親來台設籍就學、服役、就業、受邀來台訪問等，依統計每天約有四萬多人在台活動，深信其中部份人員應具有特殊任務，故我們平時應養成恪遵各項保密規定的習慣，時時提高保防警覺,以防敵滲透人員直接將電腦病毒散播在電腦網路上；或將帶有電腦病毒的滑鼠、列表機還是其它電腦配件安裝在我方網路上,俾經由某配件在網路上傳播病毒,而影響我電腦網路系統之運作。

賽培養資訊人才，提升資訊戰力：

中共解放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，在軍事院校納編學有專精師資，針對部隊需求廣招

[15]《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。

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。

滭加強人員審查，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[16]。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。

輸重視安全措施，強化網路安全：

依據美國國防情報局之估計，在所有入侵件數中，被察覺者僅係少數，因此電腦遭入侵之確切次數，尚不得而知。該國國防部之電腦系統在1995年間可能有25萬件試圖入侵之案例，且入侵之件數亦持續增加中。此外，依據美國國防情報局對該國國防部之電腦系統所作之入侵實驗資料顯示，在38000次實驗中，約有65%入侵成功，且於所有之成功入侵案例中，僅4%被國防部之電腦系統偵測出來[17]。故應重視網路安全防護措施，阻抗駭客之入侵，以維資訊安全。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（可檢查進出者生理或行為之特徵，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。

顙綿密情資蒐整，開發防毒軟體：

目前市面上銷售最好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。

嫚儲存備份資料，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，故我們平常應完成兩份以上之備份作業資料，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。

寰結合民間科技，增強資訊戰力：

[16]《青年日報》（台北），民國87年11月24日。

[17]＜1996年5月之審計報告＞《美國審計總署》。

捍衛國防固為國軍的天職，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，資訊戰事涉國家整體戰略，資訊作戰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。

滫組建數位化部隊，強化傳輸能力：

虧充實數位化裝備：

數位化裝備發展迅速，應充分運用商用技術及商規設備應急以增加資訊網路連接及降低投資成本，並研製模組化、易擴充功能之制式裝備，以整合武器系統，使軟、硬結合戰力相乘。

豐提升傳輸效能：

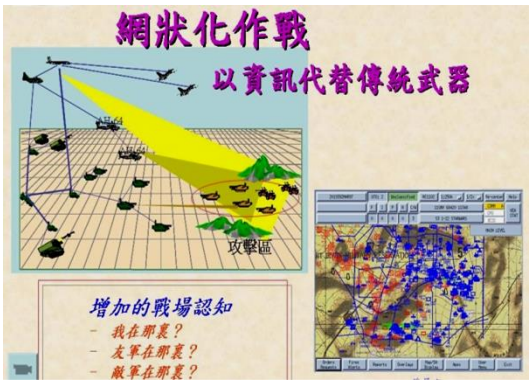
利用光纖固網建立營區區域網路，野戰則利用藍芽技術建立無線區域網路，減少布線的困難並增加其機動性。

鄳持續準則修編：

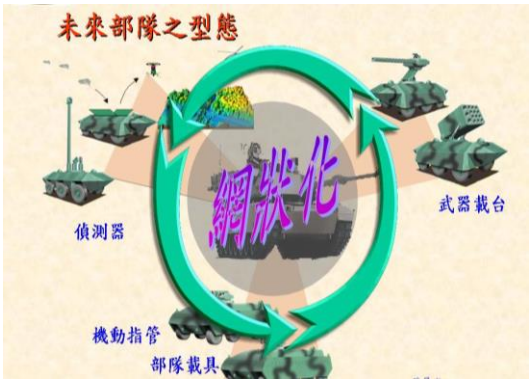
隨著「數位化戰場」來臨，新式武器、裝備將與通資系統平台整合，故戰技、戰術、戰法將相應改變，且將隨者科技或環境的變化而有所不同，準則必須持續的研發與修編，以配合時需，因而必須建立相當程度的研發能量，以及將課程、課目、單元有系統的「分合」，藉著共同的經驗參與及創新累積智慧，以滿足不同需求。達到模組化的功能。

襖持續推動戰力整合，提升作戰效能：

近年來，我已採購、研發各類新式武器，現較欠缺的為各類武器戰力之整合。系統整合工作不是各搞各的，是要以作戰的立場思考問題，將 C^4ISR 系統與武器系統、戰備戰力整合在一起，各作戰區戰力整合應以指、管、通、情為基礎，依據作戰任務與戰備需求，運用既有的裝備設施，明確律定各級部隊縱向指管及橫向通聯體系，使各級部隊均能納入作戰區的統一管制，並就現有裝備功能不足之處，或連結構制不完整之處，隨時提出需求及建議，共同研究檢討解決問題，以達到戰力整合的功能，在作戰時才能選擇「經濟、快速、有效」的武器殲滅敵人，發揮「一加一大於二的效能」(如圖十三、十四)。



圖十三　建構網狀化作戰使指揮官能透明戰場
資料來源：步校發展室參數資料庫



圖十四　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

翰強化電磁脈衝防護，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，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。總而言之，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。

蔡強化軍民心理建設教育：

虧強化國軍心理建設教育：

唐加強心戰專業人員培養：

雖當前政戰編制縮減，但心戰仍不可或缺，且心戰人員也不是三五天訓練一蹴可成，故應成立心戰專業人員訓練班，訓練專門人才，俾因應當前局勢，強化國軍心戰及反心戰能力。

書精進幹部心戰訓練：

基層部隊心戰，若只靠連隊輔導長是不夠的，況且現連隊輔導長多為預官，軍官養成教育的刻苦耐勞性不足，所以抗壓性也較不足，故應強化部隊所有幹部之心戰訓練。目前因國軍課程基準變動，各兵科學校已無心戰相關課程，建議未來應恢復此課程，並納入戰鬥教練實作，以發揮精神戰力與物質戰力之相乘效果。

㈡強化戰場心理訓練：

戰場官兵通常處於疲勞困頓、危疑不安中，在持續緊張狀態下，心理情緒很容易失衡，平時訓練應特重戰場心理訓練，以鑄造堅強之心理盾牌，強固我軍之心理防線。

㈢落實精神動員：

除平日運用各種集會加強愛國教育，使官兵了解「為誰而戰、為何而戰」，堅定五大訓練外，戰時更須落實精神動員，藉任務研討、立功宣誓、慶功（追悼）會等活動，激發官兵同仇敵愾之殺敵決心。

㈣防敵謠言、耳語等心理破壞：

妥善運用忠貞份子，對情緒失衡及品德頑劣的重點人員進行監控，防其與外勾連，散布謠言、耳語影響軍心，並演練追謠、破謠等反制措施，防敵之心理破壞。

㈤強化國人心理建設教育：

民國 85 年台海飛彈危機與民國 88 年 7 月 9 日李前總統論述兩岸為「特殊國與國」關係期間，中共當時積極對我展開文攻武嚇，不少對國家沒有信心的人便急忙出脫手上所持有之股票，造成股票市場下跌，經濟混亂；更有人買飛機票到國外避難；有些甚至舉家移民，社會上瀰漫著些許悲觀氣氛。這情況與我們所知道以色列要跟鄰近國家打仗時的狀況大不相同，如果能效法以色列人的精神，敵人想在『45 分鐘』解決戰事，是不可能的[18]。因此，我們應強化國人心理建設教育，不要去相信香港部分中共傳聲筒所釋放出的假消息，應堅定民眾與土地共存亡的決心，才能匯集全民力量與中共相抗衡，確保國家安全。

柒、結語：

隨著時空環境的變遷，戰爭型態亦隨之改變，未來戰爭之趨勢在於資訊的對抗。在這一場戰爭中，擁有資訊優勢的國家將比其他國家更易達成作戰使命。面對中共將擁有成熟的資訊作戰能力，我地面部隊亦應積極進行資訊化的建構與整合工作;另一方面應有效遏制敵方對我進行資訊侵入、破壞，進而癱瘓重要設施（尤其是 C^4ISR），唯有如此，才能克敵制勝。

[18]《青年日報》（台北），民國 88 年 11 月 2 日。