就中共「網電一體戰」理論，探討海軍通資部隊之運用與發展

A Study to Probe into The Manipulation and Development of R.O.C Navy that Base on the Integrated Network Electronic Warfare Theory of PLA.

海軍上校　陳維漢

提　　要：

一、科技推動軍事革命和戰爭型態的轉變，受到1991年波斯灣戰爭的高科技武器的震撼，中共除了將新一代科技融入其建設現代化軍隊的作戰武器裝備之外，並調整軍事戰略方向，採取「質量建軍」政策，為打贏下一場「高科技條件下的局部戰爭」而準備。

二、中共瞭解未來的戰場必定會面對複雜電磁環境的嚴酷考驗，所以積極加強「聯合作戰能力」與奪取「信息主動權」相結合的演訓工作，同時將爭取「制信息權」做為用兵的基礎理念。

三、共軍的軍事轉型不僅重視中國傳統的軌道謀略，更加強運用於不對稱作戰、聯合作戰、網電一體戰，及非戰爭式動武手段。

四、本文將從中共軍備制電磁權與信息戰進展為出發點，就其發展之「網電一體戰」理論，及參考美軍網路安全與資訊作戰能量，探討海軍通資部隊運用與未來之發展，期能謀求預應對策及反制作為。

關鍵詞：不對稱作戰、網電一體戰、聯合作戰、資訊(信息)戰、電子戰、網絡戰

Abstract

1. Technology motivates the revolution in military and the war patterns, the high-tech weapons in the 1991 Gulf war shocked the world. The PLA sets the new generation technology in the troop in addition to adjust the strategy of military. Taking “quality army” policy to win the next “high-tech local war”.
2. The PLA knows that will face the harsh test of complex electromagnetic environment, so the PLA enforces on the exercise that combines “joint operations “and “information

initiative" in the same time the PLA will seek for "information dominance" as basic concept of the military.
3. The transformation of the PLA not only values the traditional Chinese strategy, but reinforces applying “asymmetric warfare”, “joint operations”,” electronic warfare”, ” network”, and “non-use of force means war style”.
4. This article will take the PLA’s “mastery of the electromagnetic” and “ information warfare progressing” as a starting point to discuss the "integrated electricity network war" theory. Refer to the network security and information warfare of the US military, this article explores the future developments of naval information forces, hoping to seek prevention and countermeasures.
Keywords: Asymmetric Warfare, Electronic Warfare, Network, Joint operations, IT (information), network warfare.

壹、緒論

目前中共軍隊正積極從事「打贏信息條件下的局部戰爭」與「軍兵種一體化聯戰能力」相結合的演訓工作，這樣的狀況可由2010年美國公佈之「中共軍力報告」中得以證實，其中表示：共軍長期目標是打造一支能夠進行和贏得「信息化條件下的局部戰爭」[1]的部隊。且共軍在未來聯合作戰模式的相關論著中，均強調「資訊攻防機先」與「制電磁權奪取」在作戰初期階段之重要性，並確保爾後戰場態勢的掌握[2]。

共軍鑑於20世紀以來，信息技術在軍事領域廣泛運用，推動機械化作戰向信息化聯合作戰轉型的發展，成為局部戰爭先進且有效的作戰型態。從世界近期所發生的局部戰爭不難瞭解：戰場信息攻防顯得格外重要，也成為作戰體系的神經中樞；而攻擊和防護戰場信息傳遞系統，更成為信息化作戰的焦點與主軸，澈底顛覆往昔以殲滅戰、消耗戰為指導的機械化聯合作戰思想。

欲進行信息化聯合作戰，將面臨指揮機制轉型、武器裝備多重發展、兵力結構重整、作戰觀念更新等挑戰。儘管如此，信息化聯合作戰，在中共有心發展下，已經不是「打不打」這麼簡單，而是如何「打的贏」、「贏的漂亮」的問題。為此，綜合運用「電子戰」和「網路戰」諸般手段，對敵電子目標和網狀化信息系統，進行的一體化偵查、攻擊與自身的防護。已成為共軍未來強化信息作戰之首要[3]。

本文將從中共制電磁權與信息戰進展為

註1：美國2010中國軍力報告，http://www.warchina.com/news/junshipinglun/2010-08-25/123336_4.html
註2：黃引珊譯，〈中共軍事戰略與準則〉，《國防譯粹》，第36卷，第7期，2009年7月，頁4。
註3：劉宜友，〈淺析中共網電一體戰〉，《國防雜誌》，第26卷，第3期，民國100年6月，頁121。

出發點，就其發展之「網電一體戰」理論，探討海軍通資部隊運用與未來之發展，期能謀求預應對策及反制作為。

貳、中共制電磁權與資訊戰之發展

一、制電磁權的發展

(一)電子戰的建設

共軍基於波灣戰爭及過去歷次作戰教訓的影響，針對其缺乏新式電子通訊、偵測、電子對抗等技術，尤其在1979年的「懲越之戰」中，更是深切瞭解光是靠著共軍的人海與勇氣，實在不是現代化科技戰具的對手，連被中共視為「小鬼」的越南軍隊，也在使用美軍留下來的老舊電子裝備輔助下，完全可以截聽共軍部隊的調動與第一線部隊狀況，對入侵的中共軍隊分批圍殲。

中共全力進行部隊通訊機組研發與更新與電戰裝備編裝定編的工作，並於1981年由共軍總參謀部頒定「電子對抗能力」為其「六大作戰能力之首」。在美國、前蘇聯、英國、以色列、義大利等國的電戰專家協助下，全面提升電戰能力，同時改進對我(臺灣)的監聽臺，使其具備電子反制與反反制等電子作戰能力。

時至今日，中共在我當面250浬範圍內的電戰單位，其密度已有凌駕我國的趨勢，且中共以相當低調的方式來增強電戰能力、全心經營現代化作戰效率、擴編軍種的電子作戰大隊(團)等動作，將嚴重影響臺海間的電戰態勢[4]。

(二)對我之電子偵測與監控能力

概估中共有50個雷達兵團、1,100餘處固定式雷達陣地，使用各型雷達2,900餘部。而其對我偵測能力則以距臺250浬範圍，近450餘處雷達為主[5]。

由於中共對於電子戰相當重視，因此除了各軍區具有當然的責任劃分外，更將大陸地區分為四大電子偵測網，分別是[5]：

1. 以遼東與膠東半島為據點，其電子偵測範圍以針對日本、韓國為主。

2. 對東北、華北、西北中俄邊界地境線為據點，其電子偵測對象為蘇聯(獨立國協北部)。此外，中共也將數架電戰機部署在華北地區，以隨時監視俄軍的電子通訊狀況。

3. 浙江、福建等為據點，偵測目標為臺灣與其周邊海空域。中共現有的「電子對抗大隊(團)」也編配在福建與廣東間的山地區域。

4. 廣東、海南島等為據點，針對東南亞地區實施電子監聽。

除了以陸基為主的電戰基地外，共軍也已經針對海上的艦艇部署，以提升整個電子戰場的作戰縱深。根據資料顯示，中共的海軍部隊是近年來投資在電戰裝備中，預算比率最大的一個軍種[5]。

(三)中共的電戰部隊

由中共「解放軍報」的訊息透露，共軍各軍區均配有一個電子對抗單位，在南京軍區方面則是一個電子對抗團，所屬的第31與

註4：陳東龍，《中共軍備現況》，臺灣，黎明文化，民國88年7月，頁152。
註5：同註四，頁155-156。

第12集團軍則各配置一個電子對抗營。

部署在南京軍區第12集團軍，其下轄的各摩托化、機械化步兵師，以及坦克師、砲兵師等則編制一個電子對抗大隊，一般的步兵師則編制一個電子對抗連。全力針對我方的電戰技術實施模擬，以找出一套能反制與滲透我方電子偵測網的方法。

由以上的編裝即可研判中共對於電子戰方面的積極與重視，值得注意的是，所有的電子戰單位，均是由共軍總參謀部通信兵第四部全權負責，其重視電戰技術的動作相當值得我方警覺。

除了在部隊內所編制的電戰單位之外，中共在廣東梅花村與白雲山麓分別設有特種電子戰部隊，成員約在400至500人之間。由資料顯示，這個共軍特種電子戰部隊的任務為[6]：

1. 電子竊聽。
2. 電子干擾與反干擾。
3. 衛星電訊工程。
4. 海空軍電子戰研究。
5. 部隊電腦運用。
6. 洲際導彈電子檢測。

事實上，中共軍方近年來在教育與科技等名目下所隱藏的國防預算相當驚人，其大幅更新電戰系統以反制我方的動作也從未有鬆手的跡象，尤其是在近年總參通信研究所研製的「軍用中文保密通訊系統」、「傳真保密機」、「程控數字交換機」已全面配發到南京軍區使用，對反制我方的電子偵測已產生相當的影響[6]。

(四)指導電戰的總參三部

總參三部是共軍總參謀部第三部的簡稱，其工作性質是以高科技電子通訊(監聽)，以及對衛星情報、密碼破譯等相關之國家情報為主，與美國中央情報局所屬的特種電訊研究室，以及我國的國家安全局所屬電訊科技中心、國防部軍事情報局的大陸電訊研究

表一　中共電子對抗構成要素[7]

作戰類別	作戰功用	作戰型式	代表性武力
電子偵察	信息偵測	電子支援偵察	1. A-50E。 2. 中華神盾戰鬥系統。 3. 陸軍之「空中盾牌」的光電防空火控系統，以及外輻射目標探測與跟蹤雷達。 4. WZ-2000隱形無人偵察機。
	信息偵測	電子情報偵察	
	信息偵測	威脅警告	
	信息偵測	通信情報偵察	
	信息偵測	指揮、控制情報偵察	
電子干擾	軟殺作戰	有源干擾	1. 電戰型殲轟七戰機。 2. 052C中華神盾AN/SLQ-32相位陣列射控天線之電子戰設備。 3. 高功率微波武器、磁脈衝彈(EMPB)。
	軟殺作戰	無源干擾	
反輻射飛彈	硬殺作戰		1. FT-2000型地對空反輻射防空飛彈。 2. Kh-31P反輻射空對地或空對空飛彈。 3. X-31P反輻射飛彈。

資料來源：林宗達，《以劣勝優-中共信息戰之不對稱戰》，臺北，晶典文化，2005年5月，頁266。

註6：同註四，頁158-159。

註7：林宗達，《以劣勝優-中共信息戰之不對稱戰》，臺北，晶典文化，2005年5月，頁266。

表二　中共網軍組織架構表[9]

名稱	編制	招募對象	負責任務
駭客分隊	排	從資訊單位招募人才施訓	入侵敵人網路，藉假情報、假資訊、病毒等進行節點破壞、竄改、銷毀等攻擊。
電子戰分隊	連	通信、電子行業	對敵電子干擾和反干擾、欺騙和反欺騙、攻擊敵人電子系統。
網路戰分隊	連	相關高等院校和科研單位專業人員	設置防火牆，保護己方網路安全，製造電子垃圾阻塞對方。
信息救護分隊	連	從相關行業抽調專業人員訓練編組	網路系統軟硬體之維修和恢復工作，發揮戰時信息戰正常功能。
網路民兵分隊	營	由著名大專院校資訊科系和研究所編成	訊息救護專業，搶救維修軟、硬體系統等工作。

資料來源：黎健文，〈資訊安全國軍影響之探討〉，《海軍學術雙月刊》，第45卷，第2期，2011年4月，頁17。

室等性質相近。

由於對敵對國家的軍事情報蒐集極為不易，因此中共在進行電子監偵作業時，是採取最基本的人海戰術，也就是運用大量已退役的情報幹部，針對特定電訊進行解讀，然後才交由正職的情報軍官進行篩選。

因此在人員的編制上，中共總參三部的專業情報分析人員，一般外界的推測高達1萬8千餘人，遠超過一般西方國家的編制，其中屬於軍職身分的，估計約7,000人，其餘的一萬餘人，就是上述已退役之專業軍官，或是學有專精的學者專家，可說是世界上單一情報單位中編制最大，人數最多的一個專業組織[8]。

(五)由前述所見，制電磁權是共軍當前最重要的發展重點，其非常重視電子作戰武力與裝備，(如表一)為中共電子對抗構成要素。

二、資訊戰的發展

中共首次正式資訊戰演練於1997年10月進行，作戰想定是以某軍區集團軍遭病毒攻擊，該集團軍使用防毒軟體進行防護，以避免戰情系統癱瘓。1999年，中共「網軍」一詞首見於共軍報，網軍初期規模大概為「營級」，之後規模不斷擴充，包括有攻擊、防衛與維護三大部門，對外國進行資訊滲透、改造與破壞等工作。2002年1月1日組成「科研實驗部隊」，其中將共軍全軍規範為七大類，即陸軍、海軍、空軍、第二砲兵、科研實驗部隊、預備役部隊、武警部隊等，分別研擬訓練大綱體系。另因應軍事科技革命而組建一批新的科技型部隊，亦即所稱之「科研實驗部隊」。該部隊包括因應「資訊戰」而新成立的「電子戰部隊」、「網軍」和「心理戰部隊」，以及為搶奪立體空間「制高點」的「天軍」。中共在2005年開始將「電腦網路作戰」的攻勢作為列為演習的項目，二砲部隊於2006年還成立電子戰藍軍部隊，以攻防演練的方式大幅增進共軍網路攻擊能力。在2002年至2007年間，共軍七大軍區所

註8：同註4，頁168-169。
註9：黎健文，〈資訊安全國軍影響之探討〉，《海軍學術雙月刊》，第45卷，第2期，2011年4月，頁17。

轄之電抗團(營)，採任務編組方式或納編民間資訊產、官、學界、省屬縣市及鄉鎮之民兵共同組成，配合各項軍演實施網路作戰，陸續設置了電子戰分隊、網路戰分隊、黑客(駭客)分隊、信息救護分隊及在各個產業內設立國防訊息組織分隊(如表二)，極大地擴充了網軍的規模。

狹義的網軍，係指共軍的正式編制，美方學界評估為營級規模，成員包括民間大學及訓練中心所訓練的民間網路專家；廣義的網軍，則由共軍、公安網路安全單位及網路管制單位整合而成，規模約數萬人。中共除了正式編組的網軍外，網軍預備役部隊亦是「網路戰」的重要部分，目前中共有150萬預備役部隊熱衷於打「網路人民戰爭」。在部分地區，共軍已經把預備役部隊編成小型「網路戰」部隊。組織上包括網路戰營、電子戰營、情報心理戰營以及技術分隊等等，可以進行電子對抗、網路攻擊和防護、雷達偵察等演練。

前國安局長蔡得勝表示，2008年中共網軍對我政府單位網站進行高達3,100多起的攻擊，目前中共至少有3萬網軍每天在對臺灣滲透。2010年1月初美國媒體引用FBI的一份機密報告中指出，中國大陸已經組建一支超過18萬人的網路部隊，其中3萬為網路特工，15萬為民間駭客。2010年4月中共中央軍委更發表了＜關於加強了新形勢下軍隊資訊安全保障工作的意見＞，意見內容強調，「加強資訊安全保障工作是資訊時代國防和軍隊現代化建設的客觀要求，提高資訊安全保障能力是做好軍事鬥爭準備的現實需要，構建資訊安全保障體系是資訊化建設的緊迫任務」，進一步增強共軍資訊安全意識，2010年7月19日共軍總參謀部成立「信息(資訊)保障基地」，除因應外軍的網路攻擊外，另對全軍資訊化建設進行集中統管，目標是2020年建立全球第一支資訊化武裝的部隊[10]。

參、中共「網電一體戰」理論與發展現況

中共軍事研究者史越東在其論述提及，當前軍隊乃至於國防系統裝備多樣性的電子設備和信息網絡，成為一個由無數信息獲取、處理節點和信息傳遞構築的龐大系統，此一方面使得這個系統具備了極強的信息獲取、傳遞和處理能力；另一方面，也使其陷入了前所未有的極度依賴信息技術和電子裝備的境地。這種巨大依賴性決定了現代戰爭系統具有相當大的脆弱性和易被攻擊性，系統中的每個節點、鏈路和環節都可能成為敵方干擾、壓制、欺騙、打擊的可選目標。

就此而言，可從以下五個面向得知：

第一，通信技術的進步使軍隊極大的增強了傳遞信息的能力，增強了控制、協調部隊活動的能力，但與此同時，也開闢了通信對抗這個信息對抗的新領域。現今由於大量的使用各種有線與無線的通信方式，如衛星通信、光纖和網絡通信等，故為敵對雙方干擾、阻塞、截獲和破譯對方通信打開了大門，使以干擾和反干擾、竊聽和反竊聽為主要

註10：黎健文，〈資訊安全國軍影響之探討〉，《海軍學術雙月刊》，第45卷，第2期，2011年4月，頁18-20。

內容的通信對抗成為一個極為敏感而激烈的信息對抗領域。

第二，雷達、聲納、紅外線等探測技術在軍事上的應用，既為軍隊獲取信息提供了有效的多樣化手段，同時也使信息對抗增加了雷達對抗、聲納對抗、紅外線對抗等豐富的內容，開闢了偵查與反偵查、隱形與反隱形的廣闊領域。雖然傳統人工信息獲取的方式依然是重要的，但依此所獲取的信息內容也有了很大的變化，不僅要蒐集對方的作戰意圖、行動計畫等傳統信息，還涉及關於敵方各種電子裝備性能和使用方式(尤其是工作頻率數據)的大量信息。

第三，各種精確制導的信息化武器廣泛應用於陸戰、海戰、空戰的各個領域，極大的提高軍隊作戰的威力，但與此同時，也將信息交戰的所有細節，令高技術作戰在實質上變成了電子戰。相較之下，傳統的直瞄式武器雖然性能較低，但卻比較穩定。

第四，計算機和網絡技術的發展及其在軍隊自動化方面的應用，對軍事信息對抗領域的進一步擴大和鬥爭的更加激化，是另一個劃時代的因素。但是，在網絡戰中，幾行計算機病毒程式成為了另一種可怕的信息武器，一個電腦玩家也可以成為信息戰士，甚至於任何一個天才的電腦駭客(Hacker)，只要有一臺計算機和一個數據機就可以對美軍信息網絡發起攻擊，乃至於接管部分美軍部隊。

第五，當前信息技術和微電子技術的飛速發展，使社會生產和生活的每個領域日益信息化、網絡化，使世界每個國家、每個單位、每個家庭、每個個人愈加容易收到各種信息，這就使得發動配合軍事行動的宣傳戰、全民心理戰、經濟戰、金融戰等愈加容易，從而使信息對抗深入到總體戰領域[11]。

以下將就中共「信息化作戰」的思想運用及其「網電一體戰」的理論進行研析。

一、中共信息化作戰思想運用

(一)運用在威懾戰方面

中共的許多戰略專家，依照信息戰的特性，發展出甚為獨特的軍事信息戰之「不戰而屈人之兵」的威懾觀。學者黃力軍即認為孫子所言的「不戰而屈人之兵」，在信息戰中可以得到全面的實現，因為信息戰的作戰目標在於控制敵方達成目的，而不在於消滅敵人的人力、物力資源。伴隨著信息技術的飛速發展，各種非致命性武器相繼出現，戰爭變得「文明」起來。這是戰爭進入了高層次的非暴力制勝時代，即以信息戰為標誌的不流血戰爭。信息戰可以在無形的信息空間中大打出手，既能懾止對手的戰略或侵略行徑，亦能從精神上摧毀敵國的意志防線，以達到「不戰而屈人之兵」之目的，獲得比武力侵略大千萬倍的效益[12]。

首倡信息戰的中共軍事戰略專家沈偉光，將信息戰與威懾之間的關聯闡述的相當透徹，其認為信息威懾是當前世界軍事戰略演變的必然。沈指出當我們沿著威懾戰略演變的軌跡進行研究時便會發現，無論是核威懾

註11：林宗達，《以劣勝優－中共信息戰之不對稱戰》，臺北，晶典文化，2005年5月，頁56-57。
註12：林宗達，《威懾屈敵－中共信息戰之威懾戰》，臺北，晶典文化，2005年5月，頁128-129。

發展到常規威懾、太空威懾，還是由單一威懾轉變為多重威懾，但從來沒有發生過世界大戰，而是一種以無形的力量「戰略」來較量或懾止各自的對手，這就是戰略的威力。時至今日，國際鬥爭的趨勢已由實物爭奪轉向信息爭奪，領土侵略轉向信息侵略，今天的戰略可以不戰而懾人之兵，一旦產生對手難以對付的戰略，切切實實的可以「不戰而屈人之兵」[13]。

沈偉光進一步從四個面向說明信息力量，對於戰略威脅的新作用，並對戰爭型態和戰爭觀產生極大的轉變。

其一是戰爭目標由領土擴張、經濟侵略轉為信息掠奪，由主要針對物質因素轉移到主要針對精神因素，爭奪制信息權，謀求「精神勝利」和不戰而勝，成為信息時代最顯著的特徵。在信息戰爭時代，全勝的戰爭思想備受推崇，戰爭將主要不表現為攻城掠地，而是實現某種控制，尋求利益平衡點，在戰略上主要是摧毀敵人發動戰爭和進行戰爭的意志；戰役層次上是打亂敵方的決策層次；戰術層次上是癱瘓敵人的力量系統。

「消滅敵人，保存自己」的戰爭目的正在轉變為「控制敵人，保護自己」，信息戰已經使戰爭從單純的軍事領域擴大到政治、經濟、社會、文化各個領域，波及到「軍政商民」。由於這種信息攻擊是隱蔽的、無形的、和平的，人們往往容易麻痺和忽視，在信息時代，軍事威脅不僅是大軍壓境、敵人陳兵百萬，而且也是來自信息戰的突然襲擊，是國家和軍隊的「中樞神經」、「面對面」的打擊，甚至一時無法知道對手是誰，威脅來自何方，戰爭是從什麼時候開始的。

其二為信息在戰爭中的作用發生質的變化，由從屬地位上升到主導地位，戰爭的威懾屬性日益顯著，從轟轟烈烈的「血與火」的拼鬥，被靜悄悄的信息角逐所取代，信息取代人充斥於戰場上，只有信息的角逐，沒有軍隊「短兵相接」或者是「衝鋒陷陣」的空間與時間，縱然有，其作用也是微不足道的。信息時代裏，信息威懾成為新的威懾手段，在核、生、化等大規模殺傷武器仍將發揮巨大威懾作用的同時，信息戰能力、信息支援能力將以新的形式和手段，對遏制戰爭或戰爭升級產生強烈的威懾作用。

其三戰爭型態由有形演變到無形，信息戰攻擊的對象是信息邊疆，信息空間指由信息網絡和信息技術複合發展形成的看不見的空間，信息邊疆不是以地緣、海域、空間，甚至太空來劃分的，而是以信息作界碑的，這一屬性決定信息戰必定是一場無形的戰爭，戰爭可以不流血。信息邊疆的衝突主要體現在侵占、迷盲、威懾、破壞等方面，以多種手段侵入對方佔據的信息領域，掠取別人的信息為己用，欺騙迷盲的手段阻止對手的滲透和侵犯，施放威懾的信息，遏制對手的侵略，破壞對手的信息邊疆，使其有隙可乘。在網絡信息技術上領先一步的國家，依託網絡，把自己「信息疆域」擴展到許多國家，對別國的信息主權造成威脅。同時，以駭客(Hacker)非法入侵網絡為代表的「網絡破壞」事件不斷出現，對各類網絡造成了危害

註13：同註12，頁129。

和破壞。從未來的發展趨勢來看，社會信息運動的網絡性必然決定競爭對抗的網絡性，而網絡性決定了在國家安全領域的對抗，不僅僅是軍事上的信息戰，而更多是政治、經濟、外交、科技、文化、教育和意識形態等方面的總體網絡鬥爭。

其四是戰爭經歷了低層次的非暴力制勝時代、暴力制勝時代後，正在進入高層次的非暴力制勝時代，即以信息戰為標誌的不流血戰爭。科技進步能夠使人躲開戰爭的危害，客觀上，也就是說已經有這樣的技術和手段保證非暴力性戰爭的展開，無疑使戰爭非暴力性成分突顯。例如打虛擬戰爭來懾止對手的戰爭意圖，達成自己的戰略目標。在信息時代，作戰雙方的蠻動性下降，透過信息交流，雙方可以彼此瞭解對方的目的、意圖、力量和手段，作戰的透明度、戰鬥結果的可預見性提高了。在這種情況下，戰爭決策者在戰鬥之前可以有較多的選擇，談判、妥協的方式和渠道都容易找到[14]。

(二)運用在不對稱戰方面

美國的信息戰專家李比奇(Martin C. Libicki)認為以資訊(信息)科技軍備為主的作戰部隊，在與以工業科技軍備為主的作戰部隊發生衝突的時候，一般人都預料前者將會贏得這場戰爭，只是這種預期行徑未必意味著，資訊科技部隊在與前工業時代部隊作戰之際，資訊會是戰爭勝負的絕對因素，因為資訊科技對此作戰所能發揮的效果，將會比預期效用要減弱了許多[15]，這是因為依賴信息科技的武器裝備，其可發揮的效果在某些作戰領域和區域或有侷限所致。從某些作戰觀點和作戰方法而論，信息戰是具有以劣(科技層次較低者)勝優(科技層次較高者)，或者是以弱(武器裝備相對劣勢者)勝強(武器裝備相對優勢者)之特性。

自從1990年代中期之後，中共發展信息戰，已成為研究中國大陸軍事戰略的重要議題，然當前臺灣以及西方學者探究中共的信息戰，大都侷限於其信息戰之軍事作戰面向，即使或論及信息戰之非軍事面向之作戰運用，亦無法跳脫狹義軍事戰略的意涵，更難以論及不對稱戰在國家發展戰略中的運用與進行。

中共的信息戰不僅是共軍和相關武裝部隊(包含人民武警、民兵)的重要戰略，而且亦是國家發展和安全的重要戰略，亦唯有將信息戰納入國家整體發展戰略之中，才能真正符合當今信息戰發展的前衛潮流[16]。

中共的信息戰戰略是當前共軍戰略發展的主軸，更是西方國家，尤其是美國相當矚目和關注的焦點。根據蘭德(RAND)公司亞太政策中心的研究，認為中共信息戰主要特徵為：

1.屬非傳統「戰爭」武力，不是「戰場」武器。

2.屬先發制人的利器。

3.可使共軍打贏這場信息戰爭，而且是兵不血刃。

4.敵人「依賴信息」，中共則非，換言

註14：同註12，頁129-131。

註15：Martin C. Libicki，國防部史政編譯局編譯，《非傳統性的軍事衝突》，臺北，國防部史政編譯局編譯，1995年3月，頁121-122。

註16：同註11，頁45-47。

表三　中共電腦病毒戰法[20]

戰法	主要手段
前饋潛伏法	針對潛在的敵對國，戰前將病毒固化在敵方購買的電腦組件中，潛伏隱藏下來。戰時再啟動病毒，使敵方指揮系統癱瘓，飛機、坦克、潛艇等自動控制設備失靈，飛彈失去目標或提前爆炸。
臨機預置法	戰爭爆發前夕，將電腦病毒臨時置入敵指揮系統或具有電腦的武器系統中，影響敵方運作。
間接攻擊法	病毒不是直接侵入指揮系統或武器系統中的電腦主機，而是侵入其輔助系統，如電源系統、推進系統、溫度控制系統等，然後在傳染到目標系統中。
接口輸入法	利用電腦接口，輸入病毒然後從局部向全網迅速擴散蔓延，最終侵入系統核心和要害終端，使其整個網路癱瘓。
探測攻擊法	從敵方工作的電腦產生的電磁場進行偵測、探測，並對其施放病毒，或發生干擾磁場、導致電腦信息丟失、錯亂，甚至系統癱瘓。

資料來源：林中斌，《點穴戰爭：中共研發下世紀的戰略武力》，臺北，學生書局，1999年5月，頁7-9。

之，掌握信息戰爭的優勢，即掌握敵人的弱點，而中共本身並沒有這個弱點[17]。

中共期望以不對稱作戰戰略達到以低規格和相對劣勢的武器裝備戰勝諸如美國這種擁有高規格和優質科技作戰武力的國家。中共在1991年波斯灣戰爭時，即已經瞭解到信息戰的重要性，並大力發展之。長期以來中共即以美國的高科技作戰為模擬對抗中的主要參考目標，並將信息作戰準則，做為現今「軍事革新」的主軸。而此一趨勢，亦正隨著目前中共的經濟逐漸壯大而受到加強。而且，共軍已經將發展信息戰之「不對稱作戰」之武器裝備，做為是中共與美國對抗中，其打贏這場高科技戰的重要方式[18]。

集中全力進行重點打擊，是中共不對稱作戰戰略的主要核心，故中共在軍事作戰上相當關注此一重點之發揮，而「電子網絡戰」正是中共可以將此運用於不對稱戰之重點打擊的最佳戰略論證基礎[19]。

林中斌博士則將上述信息戰的作戰重點打擊方式稱為「點穴戰」，現代戰爭中的C4ISR系統(指揮、管制、通信、電腦、監視、偵查)如果能有完善的組織系統，自然可以比對方擁有更強的競爭優勢，就好比武術上功夫的強弱，能夠判斷決鬥生死的情形。在現代戰爭當中運用電腦病毒，將對方的電腦破壞，就可以使敵人之C4ISR系統失靈，如果電腦病毒造成電腦當機，再先進的武器也將如同廢鐵一般，要打仗也不能打仗。中共的電腦病毒戰法(如表三)。

「點穴戰爭」的武器大致可以分為兩種，硬殺傷和軟殺傷。前者主要包含精確制導武器(Precision Guided Weapons)如巡弋飛彈、反輻射飛彈、制導飛彈、制導砲彈、制導魚雷和遙感武器，如遙感地雷、遙感水雷、遙感引信和遙感砲彈等。這些武器相當先進，但大體來說比較傳統。至於軟殺傷武器和以往武器大不相同，他作戰的效果不是破

註17：同註11，頁47

註18：林宗達，〈中共信息戰略武力之發展〉，《中國事務》，第7期，新境界文教基金會，2002年1月，頁105-108。

註19：同註11，頁254。

註20：林中斌，《點穴戰爭：中共研發下世紀的戰略武力》，臺北，學生書局，1999年5月，頁7-9。

壞敵人武器或設備的硬體，而是破壞其功能，軟殺武器是「點穴戰爭」或「不對稱戰爭」或「信息戰爭」的最大特點[21]。

二、中共「網電一體戰」理論探討

「網電一體戰」一詞，首見於美國防部「2008年中共軍力報告」，宣稱：「針對中共民用和軍事網絡的攻擊能力，正是共軍發展不對稱戰法的『非接觸作戰』重要組成部分」。後在其「2009年中共軍力報告」之定義為：「利用電子戰、電腦網路作戰、動態殺傷等方式，以阻斷支持敵方作戰與投射武力的戰場網路資訊系統」；又「2010年中共軍事與安全年度報告」則為：「運用電子戰、電腦網路作戰和主動攻擊，來擾亂戰場上支援對手作戰和力量投射能力的資訊系統」。以信息化專家諮詢委員主任戴清民少將之論著，「網電一體戰」：「係指在信息戰場上，將「電子戰」與「網絡戰」兩種手段綜合運用，為破壞敵方戰場網絡化信息系統，並保證己方戰場網絡化信息系統之正常運行，而採取之一體化攻擊行動」。就其目的則是在奪取戰場電磁和網路空間的主導權。

「網電一體戰」已不是簡單的把「電子戰」與「網絡戰」相疊加乘的粗淺認知，而是要求這兩種手段的互相彌補不足之處。它著眼於對戰場的信息獲取、傳遞、處理和運用全過程的削弱與破壞，進而通過「電子戰」來干擾對方的信息取得，並以「網絡戰」來癱瘓對方的信息處理和運用，並藉兩者綜合運用形成整體戰力，達到全面破壞敵方的指管系統及信息傳遞管道。

鑑此，在現代信息化的戰場上，唯有取得電磁和網絡兩個領域的優勢，方能掌握現代戰爭的主動權，致「網電一體戰」成為共軍信息作戰的主要形式[22]。

「網電一體戰」的核心為一體化作戰，其戰鬥效能之發揮，為建立信息交換正常運作機制之上，而其一體性之主要表現，則在於指揮、力量、目標和行動等方面之集注。所謂指揮上的一體化，乃是對「電子戰」和「網絡戰」實施籌劃、組織、協調和控制。而力量上的一體化，就是將「電子戰」和「網絡戰」諸般手段結合運用，並互為補充。目標上的一體化，即是使「電子戰」和「網絡戰」的作戰效能，同時應用於戰場C4ISR系統關鍵與要害。再者，行動上的一體化，則是對「電子戰」和「網絡戰」作為能密切配合，形成合力[23]。

所以，「網電一體戰」是戰場電子信息目標網絡化的客觀需要，是促進「電子戰」和「網絡戰」融合互補，實現體系對抗的必然要求。從軍事理論發展的規律來看，戰爭實踐就是不斷催促作戰新的思維變革，「網電一體戰」其實是「一體化聯合作戰」之表現，為使有效對抗敵方指管作為，共軍自創全新的信息作戰構想，未來信息化戰場所屬各作戰要素，可藉其掌握運用，削弱對方政治、軍事、經濟等多方面的綜合戰爭潛力，

註21：譚傳毅，〈不對稱戰略的思考：間接施放病毒理論〉，2000年國家安全戰略情勢評估：不對稱戰略思考與作為學術研討會，臺灣，第7期，淡江大學國際事務與戰略研究所，2000年，頁9。

註22：同註3，頁123-124。

註23：同註3，頁123-124。

進而影響敵全面性的作戰效能[24]。

「網電一體戰」緊緊抓住未來信息化戰場特徵和信息作戰的特點，無論從力量構成、戰術技術和指揮控制等方面，將「電子戰」和「網絡戰」融為一體，使其分布在戰場上各個不同空間的電子信息系統設備，藉由計算機網絡的介接，形成一個完整的系統，產生一個巨大的結構效益，提高作戰系統的整體化與集成化程度，即時對敵信息傳送機制進行全維打擊[25]，針對敵網絡中心的各作戰體系信息實施攻防，破壞其信息獲取、傳遞、處理和截取所要資訊，達到擊敵要害與關節癱瘓之效果[26]。

「電子戰」和「網絡戰」的一體化運用，突破了原先僅能在武器射程的傳統侷限，作戰空間將更加抽象和廣闊，全縱深一體化、非接觸性及非線性作戰等方式，將充斥在信息化戰場的整個作戰進程中，使其比現有的任一作戰方式，都具有更廣大的空間[27]。

三、中共「網電一體戰」發展狀況

共軍認為「網電一體戰」，係集中體現高技術戰爭本質特點和規律的作戰方式。1995年12月，共軍於石家莊陸軍學院召開「迎接世界軍事革命的挑戰」研討會，會中通過以資訊技術為核心的軍事革命浪潮，發展具「中國特色的資訊戰法」，總結出10種作戰方式，正式著手進行因應資訊作戰的工作，經過3年由下至上、由部隊至機關院校，逐級討論，並於總參謀部第二部(人力情報、研究和分析)下設「科學技術蒐集局」，翌年，共軍在「聯合九六」、「機動二號」、「中南九六」等聯合作戰演習中，都將電子戰納入演訓科目之中，突顯出為因應未來戰場的複雜電磁環境，已將電子戰廣泛運用於年度重大演訓中。

表四　科索沃戰爭信息作戰經驗[28]

科索沃戰爭信息作戰經驗	北約為奪取資訊優勢，分別從高中低三個層次，採取綜合電子戰行動。然南聯在北約強大電磁壓制下仍另闢蹊徑，在全球發動對北約的網路攻擊，曾使白宮網站一整天無法工作，另「尼米茲」號航空母艦的指揮控制系統，竟也被迫停止運行3個多小時。

資料來源：劉宜友，「淺析中共網電一體戰」，《國防雜誌》，第26卷，第3期，民國100年6月，頁127。

1997年中共成立由國家主席親自領導的「國家信息安全工作領導小組」，召開全國信息化工作會議，藉整合軍、情、公安與信息產業等各相關部門，進行網路安全保障與網路攻防能力的整體建置，其中總參擔任對敵方軍事與政治單位進行網路情蒐及攻擊，並組建信息民兵負責信息安全保障。

中共國務院於1998年成立「信息產業部」，對全國各相關部門進行分工；1999年6月，總參總結科索沃戰爭經驗(如表四)，將原信息工程學院、測繪學院與電子技術學院整併組建為信息工程大學，並將原資訊戰10種作戰方式精簡為6種，借鑑小國面對優勢軍事強國實施電磁作戰時，亦能憑其有限之資訊戰力遂行反制作為。

2000年起，共軍積極推動軍事自動化指

註24：同註3，頁125-126。
註25：同註3，頁125-126。
註26：同註3，頁125-126。
註27：同註3，頁125-126。
註28：同註3，頁127-128。

揮環境的構建，將情報蒐集、資訊傳遞、定位導航、精確打擊、海洋監視、戰場控制及作戰指揮等能力進行提升與整合。2002年，由時任共軍總參四部部長戴清民少將規劃全國性國家戰略級的資訊戰分工，明定軍委階層負責「電子戰」和「網絡戰」－即「網電一體戰」，並由總參四部負責規劃成軍，完成全軍指揮自動化網路，使其具備聯合作戰所需指揮與通信能力；而負責網路安全、心理戰、情報戰等防禦性作為，另有不同部門分主其事。經多年努力，如其引以為傲的「華東電戰網」為例，係整合共軍各軍種在浙閩境內的電子對抗部隊，專司對臺灣方面電子作戰，於2007年優先完成東南沿海一帶的區域綜合電子信息系統，藉以有效整合戰區內指揮管制、情報偵蒐、預警偵察、通信與電子作戰等系統，建構完成其所謂「三級聯戰機制」(中央軍委－地方作戰集團－實際參戰部隊)，藉此提升部隊戰時應變能力，進而奪取電子戰場的主控權[29]。

四、中共「網電一體戰」能力研析

2009年4月，美智庫「國家亞洲研究局」和陸軍戰院的戰略研究所聯合出版《Beyond the Strait：PLA Missions other than Taiwan》專書，其中一篇題為＜PLA Computer Network Operations：Scenarios, Doctrine, Organizations, and Capability＞研究報告，針對共軍發展「網電一體戰」的能力虛實，提出深入剖析：

目前中共可運用的「網電一體戰」工具包括：駭客、電腦程式病毒、硬體設備破壞、內部滲透攻擊，以及電磁脈衝攻擊等。至於執行任務的平台則包括：電腦、全球網路連線，以及具操作能力的作戰人員。對於軍事科學院及國防大學而言，其當前的重要任務之一，就是要訓練出能夠成功執行任務的「網電一體戰」軍官[30]。而其執行「網電一體戰」任務的主要機構(如表五)。

而共軍發展「網電一體戰」的作戰能量

表五　共軍「網電一體戰」任務的主要機構

機構	任務
總參三部通信局	負責國防信息化保障任務，並執行戰場網路情報蒐集。
總參四部電子雷達對抗部	負責電腦網路運作及電子反制能量的組建。
軍事科學院及國防大學	負責研發各項「網電一體戰」的作戰指導與準則，並積極培育訓練各類執行任務的軍官與士兵。
戰區聯合作戰指揮部	在七大軍區設置戰區聯合作戰指揮部，並成立信息對抗中心，負責電子對抗及網絡信息體系的防護。

資料來源：本研究整理。

表六　共軍「網電一體戰」作戰能量的主要項目

項次	作戰能量
一	透過電腦網路攻擊來完成長距離的攻擊破壞任務。
二	運用電腦網路攻擊癱瘓對手的重要經濟活動能力，達到警告嚇阻的效果。
三	運用電腦網路瓦解敵方C4ISR系統。
四	運用電腦網路攻擊，發揮「先發制人」的戰略威懾效果。
五	結合電腦網路和電子戰特種部隊的奇襲能量，達到心理威懾的戰略目標，並迫使臺灣接受政治談判的條件。
六	運用電腦網路攻擊破壞美軍的後勤補給系統。
七	運用電腦網路攻擊破壞臺灣的電力運輸和通訊系統

資料來源：本研究整理。

註29：同註3，頁127-128。
註30：同註3，頁128-129。

主要項目(如表六)。

共軍戰略規劃圈的主流意見認為，應積極發展「電腦網絡作戰」能力，並建立「非對稱性戰略優勢」的重要環節，而其中的內涵包括「制信息權」和「制電磁權」，並以「電子對抗」、「通信對抗」，以及「網絡對抗」為主要的作戰形式。此外，透過整體的「電腦網絡作戰」能量，隱藏在非官方的民間公司組織中，並藉由電腦網路的連結，可以在世界上各個角落，直接或間接的對攻擊目標，進行「網路戰」而不易被察覺。這種「巧戰而屈人之兵」的作戰型態，儼然已對我政軍重要機構之電腦網路系統，造成相當程度的威脅[31]。

肆、美軍網路安全與資訊作戰能量概述

美國國防部網路安全係由華府的「全球網路作戰聯合特遣部隊」(Joint Task Force for Global Network Operations)主導，此部隊隸屬美國戰略司令部。美空軍成立「網域全球打擊暨網路作戰指揮部」(Cyberspace，Global Strike and Network Operations Command)，具備遂行攻擊任務的能力，毋須投擲炸彈即可阻止敵軍事行動或政府運作。美國在2005年4月在國防部戰略指揮部(USSTRATCOM)中，成立了「網路戰聯合司令部」(Joint Functional Component Command for Network Warfare, JFCC-NW)，負責具體為美國進行攻擊性的網路戰。美國戰略司令部係美國戰略部隊之統一作戰司令部，負責管制軍隊太空作戰、資訊戰、戰略預警和情報評估、規劃全球戰略作戰，並全權負責電腦網路作戰。美國戰略司令部下轄太空與全球打擊、情監偵、網路作戰、整合飛彈防禦，以及打擊大規模毀滅性武器等數個聯合作戰指揮部。

除了「網路戰聯合司令部」外，美各軍種也分別組建自己的網路戰部隊。美國陸軍成立「陸軍電腦緊急反應隊」(Army Computer Emergency Response Team, ACERT)，負責陸軍各基地的電腦網路防衛(Computer Network Defense，CND)行動，必要時也可發起網路攻擊，侵入他國的軍事網路。海軍主要的「資訊戰」計畫稱為「海軍資訊戰活動」(The Naval Information Warfare Activity, NIWA)，與「艦隊資訊戰中心」(Fleet Information Warfare Center, FIWC)共同研擬與規劃海軍資訊戰的相關事宜。「艦隊資訊戰中心」還在諾福克(Norfolk)成立了「海軍電腦事件反應隊」(Navy Computer Incident Response Team, NAVCIRT)。「海軍網路防衛作戰指揮部」(Navy Cyber Defense Operations Command)，位於維吉尼亞州的諾克該指揮部約有170名成員遂行「24小時監測」。監測包括海軍與陸戰隊的內部網路和戰術網路，計有位於16國的300個基地76萬14名用戶。目前的美海軍網路防衛作戰指揮部，其前身是「艦隊資訊戰中心」(FIWC)於1995年成立的處級單位，2003年成立獨立的指揮部，即「海軍資電立即反應小組」(Navy Computer

註31：同註3，頁129。

Instant Response Team)，美海軍網路防衛作戰指揮部負責網路防衛和網路管理，由位於諾福克的指揮部人員與所有業務的系統經管人員密切合作執行這兩項工作。美國空軍則直接在第八航空隊(8th Air Force)的基礎上，在2006年轉化為「空軍網路戰指揮部」(Air Force Cyber Command，AFCC)，以擴大整備因應網域戰爭。該指揮部位於路易斯安那州的巴克斯岱爾(Barksdale)空軍基地，將籌設成為美空軍第一個主要從事網路作戰的司令部，專職部隊訓練與配備，並透過網域與航太作戰充分整合，以逐行持續性全球網路作戰。「空軍網路戰指揮部」共有2萬5千人在此工作，負責防衛網路、基礎建設系統保安和監察工作。國防部長蓋茲2009年6月23日正式下令組建網路司令部，以統一協調保障美軍網路安全和開展網路戰等與電腦網路有關的軍事行動，美軍的網路戰部隊將於2030年全面組建完畢[32]。

伍、海軍通資部隊未來運用與發展之研析

一、國軍「通資電」不對稱戰力發展之SWOT策略分析

依國防大學管理學院林明武上校民國100年8月於「國軍應用通資電科技於不對稱戰力之研究」文中論述：國軍「通資電」不對稱戰力之範疇，包括通資電支援及資電作戰等兩部分，就是以聯合C4ISR為基礎，運用電腦網路戰 (Computer Network Operations,CNO)、電子戰(Electronic Warfare,EW)、心理戰、(Psychological Operations,PSYOP)、軍事欺敵(Military Deception,MILDEC)及作戰安全(Operations Security,OPSEC)等核心能力，去影響、中斷、破壞或奪取敵方之決策指揮機制，同時防護我方之決策指揮機制，以創造通資電優勢。林上校之研究應用SWOT邏輯方法論，依國軍內部的優勢(S)、劣勢(W)與外部的機會(O)和威脅(T)實施「通資電」不對稱戰力發展之策略分析，其結果歸納(如表七)所示[33]。

二、海軍通資部隊現況

(一)任務特性

各地區通資部隊負責基地內有、無線電通信勤務及資安、資訊網路管理及通信載具、裝備維管等工作。

(二)勤務特性

1.無線電通信傳報與機動通信載具之部署。

2.有線電通信網路維管、巡檢、查修與架設。

3.衛星通信系統網管、監控與分析。

4.大成指管系統網管與檢試。

5.超視距鏈路系統(迅安系統)中繼站維管。

6.基地資訊流管理介面之安全防護與監控。

7.基地通信交換主機、光纖傳輸系統、發射站台遙控自動化等專案保修維管。

(三)海軍通資部隊就其當前任務角色，

註32：同註9，頁22-23。

註33：林明武，〈國軍應用通資電科技於不對稱戰力之研究〉，《國防雜誌》，第26卷，第4期，民國100年8月，頁88-89。

表七　國軍「通資電」不對稱戰力發展之SWOT策略分析

優勢（Strength）	劣勢（Weakness）
1. 國軍遵照總統馬英九先生「固若磐石」的指導，發展「通資電」不對稱戰力，平時建構之C4ISR可支援作戰指管；另災害發生或作戰時，可支援災害防救或發揮通資電優勢，對敵實施反制作為，完全符合國家安全及利益。 2. 考量周邊區域安全、敵我戰略態勢及未來兵力結構調整等因素，國軍應積極建立以「通資電」為中心之制衡戰力，能運用「有效嚇阻」之資電作戰手段，達成「防衛固守」之目的，可有效支持國軍軍事戰略構想。 3. 基於達成「為用而訓、訓用合一」之目的。國軍已推行「作戰任務連結聯戰任務行動要項」之聯戰訓練機制，將來運用通資電支援措施籌建分散互動式模擬仿真系統及設施以結合聯戰訓練，能對有限訓練資源做合理分配與運用，全面提升聯戰戰力。	1. 「全民防衛動員法」對通資電高科技人力與設施之動員法令欠完備，應藉由演訓納入操練課目，讓國軍平時保有最小限「資電作戰」核心能力，戰時才能迅速動員轉換戰力。 2. 目前維持總員額27萬5千員的兵力規模，未來兵力目標呈遞減之勢，惟有發展「通資電」建構不對稱戰力，一方面可減化行政負荷；另一方面能強化並保有一支量適、質精、戰力強的武裝力量。 3. 國軍現階段C4ISR之建置已初具成效，將來仍需配合戰、技術程序的轉換與內化為聯戰戰力(含災害防救)，並持續檢討評估，以建構完整C4ISR之能力。 4. 國軍「資電作戰」大多僅限於電腦網路戰與電子戰之運用，面對共軍信息戰的威脅，將來如何整合心理戰、軍事欺敵及作戰安全等核心能力，去影響、中斷、破壞或奪取敵方之決策指揮機制，同時防護我方之決策指揮機制，以創造通資電優勢。 5. 國軍各層級電腦輔助指揮所演習應用之軟體，彼此間較不具關聯性，無法上下相互指導與支持。通資電應形塑共通作業環境運用網路，建置「聯合實兵一虛擬一兵棋」訓練環境，有效鏈結實兵一虛擬一兵棋為合成化戰場，不須將參演單位之作業兵力集中於聯演中心，卻可達成聯戰演訓效能之總和。
機會（Opportunity）	**威脅（Threat）**
1. 資訊科技開啟人類第三波文明的鎖鑰，緊接著全球資訊革命產生了資訊時代，現在網路革命產生知識雲，也就是21世紀的新概念雲端運算(Cloud Computing)。正如培根所說：「知識就是力量」，發展不對稱戰力一「通資電」，不僅掌控了戰場致勝的關鍵知識，更符合世界潮流與趨勢。 2. 中華民國資訊產業實力傲視全球，世界經濟論壇(World Economic Forum, WE)2008-2009年網路整備評比：我國排名全球第13、亞太第4；另依據英國經濟學人資訊中心(Economist Intelligence Unit ,EIU)2009年全球66個國家(Information Technology ,IT)產業競爭力評比報告，我國排名全球第15，在亞太排名第4，在在顯示民間資訊產業有實力與資源支持發展「通資電」不對稱戰力。 3. 隨著知識經濟時代的來臨，通資電科技產業是21世紀強化國家競爭力的重要因素。而財團法人資訊工業策進會(Institute for Information Industry, III)及工研技術研究院(Industrial Technology Research Institute,ITRI)皆屬國際級的科研單位，可提供國防通資電科技技術與情報，甚而延聘為專業顧問「融民力為我力」，以達全民國防之實效。	1. 面對中共軍事武力的強大威脅，國軍應以敵為師，運用智慧發展可恃戰力一「通資電」以小博大。 2. 依中共2010年軍事與安全發展報告，文中明白揭示「建構一支能打贏信息條件下局部戰爭的部隊。」為共軍改革的長期目標。簡言之，控制並支配現代戰場整個資訊頻譜是中共反介入／拒止戰略的重要因素，亦即共軍所謂「信息封鎖」或「資訊主宰」，在戰爭初期階段掌握主動權並獲得資訊優勢，進而掌握空中和海上優勢。 3. 中共軍方強調「網電一體戰」，就是為實現「信息封鎖」或「資訊主宰」。在戰場上運用電子對抗與計算機網絡作戰來攻擊、影響對手指揮與管制能力的資訊系統，並主導電磁頻譜。 4. 早在1999年，前總統李登輝發表兩岸「特殊國與國關係」論點，引起大陸駭客攻擊臺灣政府、大學與商業網站，此後幾乎年年發生大陸駭客攻擊臺灣政府或企業。另2009年3月，加拿大研究人員發現了一個電子間諜網絡，而且這一網絡很顯然是以中國大陸為基地。據稱，該網絡曾向包括印度在內的世界各國政府網站滲透。103個國家的1,300臺電腦曾被入侵。

資料來源：林明武，〈國軍應用通資電科技於不對稱戰力之研究〉，《國防雜誌》，第26卷，第4期，民國100年8月，頁89。

工作主軸偏重於服務基地內有、無線電及軍用資訊網路之用戶，其工作特點類同於海軍的「中華電信公司」。

(四)而就作業能量而言，遵國防部政策不建立電子戰、資訊戰能量外，餘有無線電通信、光纖網管、資安防護等功能架構，均與國防部資電部類同。

三、海軍通資部隊未來發展與運用

就本文蒐整之相關文獻資料可知中共軍隊正積極從事「打贏信息條件下的局部戰爭」與「軍兵種一體化聯戰能力」相結合的演訓工作，這樣的狀況可由2010年美國公佈之「中共軍力報告」中得以證實，其中表示：共軍長期目標是打造一支能夠進行和贏得「信息化條件下的局部戰爭」。且共軍在未來聯合作戰模式的相關論著中，均強調「資訊攻防機先」與「制電磁權奪取」在作戰初期階段之重要性，並確保爾後戰場態勢的掌握；而美海軍軍令部更已於2006年增設「通信網路署」負責發展與整合通信、資訊及網路系統，以確保美海軍具備資訊優勢與網狀化能力。

就中共與美軍通、資、電組織架構及其發展趨勢研析，通資部隊的特性均具備攻擊與防禦能量，人力、裝備編制均極為完整，且於通信、資訊作戰技能之研發與資源之分配上，亦均採事權統一、整合統籌架構運作，不但於平時可迅速支援急難救助外，戰時更可於最短時間依令啟動反應機制。

爰前所述，未來海軍通資部隊之發展與運用建議如后：

(一)就資源整合與基地核心通資防禦作為上

1. 考量當前敵情與通資組織架構發展趨勢，將海軍通資部隊轉型，除擔負原有通信、資安管控任務外，亦結合雲端服務建置，成為「地區資料中心」，將基地內網路管理、資安防護、機房、資訊系統、資料庫共構整合，俾達「管控集中化」、「作業標準化」目標，提供資訊、通信系統高效能、高效率且安全、便利之服務。

2. 整編海軍各單位獨立資訊編制，以統籌整合資訊作業能量、嚴整通信、資訊人員經管，並完整通資作業編組架構。

(二)就通資作戰能量發展上

1. 目前國防部政策規範軍種不具備資訊戰研發、作戰能量，相關作戰能量分別建立於國防部參謀本部資電作戰指揮部之「網路戰大隊」，而海軍通資部隊僅對內部執行資訊安全管控任務。

2. 然若海軍通資組織架構及人力完成整編、轉型之後，可運用整編之專業資訊人力，輔以人員計畫性專業培育、訓練，可適才、適所整合編組建立通資戰術戰法研析、鑑識作業能量。

陸、結語

科技的發展推動了軍事革命和戰爭型態的轉變，當前決戰制勝的關鍵，不再以兵力的多寡、火力的強弱為主要因素。「作戰靠指揮、指揮靠通信」，交戰雙方誰能掌握通資優勢，破壞敵方戰場通資系統，並保證己方戰場通資系統之正常運行，在作戰初期即已勝負分明。

本文從中共發展之「網電一體戰」理論，及參考美軍網路安全與資訊作戰能量，探討海軍通資部隊未來之發展與運用，芻議當務之急即為進行通資組織架構、人力及任務轉型，未來之海軍通資部隊，除擔負通信、資訊服務與安全管控任務外，亦將具備通資作戰與反制之能量。 ⚓

作者簡介：

陳維漢上校，國防大學管理學院資訊管理系85年班，管理資訊正規班93年班，國防資訊研究所95年班資訊管理碩士，現服務於海軍通信系統指揮部。

老軍艦的故事

美堅軍艦 LSM-349

美堅艦為一中型登陸艦，是美國芝加哥FAIRBANXS MORES CO.造船廠所建造，公元1944年3月1日完工下水成軍，原編號為LSM-76，服勤於太平洋海域。二次大戰美國以剩餘物資之名義將該艦售予我國國營招商局，成為一商用貨輪，其船名改「華字210號」。民國41年5月該艦奉令移交海軍，海軍派遣許江興少校於淡水接收。由於接收時該艦之機器裝備均已損壞，不堪使用，經過接艦官兵三個多月克難整修，於8月中始將部份故障修復而將該艦駛至左營基地，繼續進行整修工程，並加裝武器裝備及補充人員。

該艦服勤時曾參加過「重慶」、「莒光」、「雲飛」及「復國」等演習，成效良好。另該艦在金門砲戰期間曾參與震驚中外之九二料羅灣海戰，寫下光榮史頁。美堅艦在我海軍服勤18年後，由於機器裝備均已老舊，維修困難，乃奉令於民國59年1月1日功成降旗除役。(取材自老軍艦的故事)