中共軍事網路作戰通訊協定發展之研析

作者簡介：

莊鎧鴻，陸軍官校正五十六期，陸軍學院八十七年班，戰研班八十八年班 ，曾任步兵排、連、營長、作戰參謀官；步兵學校校一般組教官、戰術組主任教官，現任步兵學校步兵戰術組雇員老師。

提要

1、 數位資訊的網狀化戰場一直是國軍因應未來戰場所規劃整建的目標，各軍種部隊要能獨立於廣泛複雜的資訊戰場上，獲取應有資訊，不至紊亂，就必須讓各類型戰場指管系統能有效進行網路串聯，其主要關鍵在通信協定的設定。

二、各國雖極力發展資訊化的戰場指管系統，但由於各系統所運用的技術規格不一，因此各作戰平台無法形成構聯，必須藉由最高指揮系統處理與整合方能提供各作戰單元使用，浪費時效。

三、網路作戰觀念已在各先進國家展開，平時掌握網路資源獲利及監控各網路使用者訊息；戰時才能有效監管與破壞，便是網路中通訊協定的運用了。

四、因應作法：(一)國防與民用資訊安全技術相結合；(二)建立軍事網路轉則指導單位；(三)強化單位網路管理；(四)落實單位網路軟硬體設施防護；(五)強化網路安全防護教育；(六)資訊化整體架構規劃。

關鍵詞：網路通信協定、IP 位址、網際網路作戰

前言

在國軍朝向資訊化戰場指管系統發展的階段，網路不僅是未來戰場上的主角，也是國軍轉型成功與否的關鍵。

隨著電腦資訊化運算速度及技術的發展迅速，網際網路於軍事上的運用，已於美伊二次戰爭中表露無遺，而數位化戰場是未來作戰趨勢，但目前國內對數位化步兵與戰場資訊的研究往往注重在通訊衛星、電子作戰、資訊化武器與設備或網際網路軍事運用及駭客入侵等方面研究，在各個研究領域中，不少專家學者已針對其原理及實用提出不少見解，但運用網路，不管是民間商用的網際網路（internet）或者網狀化作戰的軍事區域網路，其中都有一個極度重要的構成要素，而這個要素，卻因多數人注重在網路運用便利性與安全防範，導致極易忽略，甚至以將其可運用視為理所當然，殊不知這個要素關鍵點，卻是未來網路運用發展與控制網路使用的關鍵點。這個關鍵要素便是通訊協定。要在廣泛複雜的資訊戰場上，使各作戰、情報、後勤與戰鬥支援部門獲取應有資訊，不至紊亂，讓各類型戰場指管系統能有效進行網路串連，其主要工具就在通信協定的設定。因此藉由通信協定這部份提出個人看法，期能有利國軍未來網狀化作戰中，能有所助益。

何謂通信協定

由於網路是由多種不同的設備所連接而成，在不同的設備與軟體系統下，網路系統變成為非常複雜的不相容體系，因此必須要有一個共同的網路協定，使各系統平台與各類網路能共通使用，這就是網路的通信協定[1]。其中的IP位址，便是網際網路中重要的標識，相當於住址一樣，使每個連上網際網路的電腦皆有唯一的住址。

軍事網路運用緣起

[1]註 王正德 主編，《決勝賽柏空間-網路軍事技術及其運用》，（北京：軍事科學出版社，2003年4月），頁11

IP Address（ Internet Portocol Address）

網際網路上每部電腦都各自有一個唯一以數字為基礎的住址，稱為IP位址，IP位址由32位元構成, 分為四組(octet)各8位元, 以十進位表示,由四組 0-255 的數字字串組成，例如：123.231.132.213。伺服器採用固定IP Address, 撥接上網的電腦, 採用浮動IP Address, 由網路服務商(Internet Service Provider, ISP)隨機給定。

目前全球使用的網際網路其前身緣起於美國國防部為了不受戰爭或其他因素影響，運用電腦實施網路傳送電子信息及文件，發展出分散式強韌網路系統ARANET，後又在美國國家科學基金會（NSF）規劃下發展NSFNET正式取代ARANET成為Internet的骨幹（backbone），並於1991年3月開放商業用途使用，逐漸形成全球所使用的資訊網路。

隨著網路科技的迅速發展，在軍事上利用網路與資訊科技迅速處理大筆戰場上複雜資料與傳遞資訊，以提高作戰效率，已是必然趨勢。從波灣第一次戰爭，美軍將各軍後勤指揮中心資訊化後，與設在美國本土的「全球指揮控制中心」形成網路連結，完成一個從美國本土到中東作戰地區的巨大網路連結，也使「戰場資訊高速公路」的觀念逐漸形成；在二次波灣美對伊的自由戰爭前後，以網路結合各個作戰部隊及數位化步兵第4師的運用一再顯示未來戰場上網路作戰的重要性。尤其為因應未來戰爭，美國正建構軍事專屬的「全球資訊網路」（Global Information Grid，GIG），將有線、光纖、無線電、衛星通訊、視訊及多媒體服務等通訊服務加以統合，以改變現行戰場指管系統縱向垂直連結的特性，讓全球間任意兩個點或多點之間可進行資訊交流。以全球性的接收及使用為目標，運用封包交換技術在網際網路中傳輸資料，提供共同使用者整合的資訊架構[2]。以結合武器系統、全球情報資料與作戰兵力形成一「網路中心戰」，其目標是將所有戰場上敵軍與我、友軍的動態影像提供給美國部隊指揮官及部隊，使每個軍隊成員在戰場上都能擁有戰場及時影像及擷取想獲悉的戰場資訊[3]。

軍事網路運用瓶頸

但目前各式的戰場指管系統架構仍有瓶頸難以突破，主要是各軍種都會擁有自行獨力發展的戰場指揮管制系統，常因技術規格不一，作戰平台無法行平行構聯。以美軍為例，目前美軍的監測單位及戰鬥單位間的連接仍相當分歧，例如空中預警機獲得的戰場資訊必需先傳至航管或戰管中心，然後才能透過網路傳輸連結線或或無線電將狀況

[2]註黃偉傑、陳國銘、舒孝煌，〈軍事事務革新的試金石—2003精實國防站立科技研討會〉《全球防衛雜誌》（台北：），民國93年1月14日http//www.diic.com.tw/comment/930114-1.htm

[3]註 魏國金，〈美打造上帝之眼，迎接未來戰爭〉《自由時報》（台北），民國93年11月14日，版6。

或任務命令傳送至在戰區待命的戰鬥部隊。且目前戰場指揮管制系統的環境限制，包括頻寬限制導致的安全控制點和相容性問題；網路多為垂直整合，缺乏水平的整合；基礎架構太過分歧，也太過複雜。由上到下從各軍種聯合作戰到單一軍種協同作戰，網路通訊架構太過複雜，彼此互不統屬。另外前線戰鬥部隊不論是人員攜行或車載裝備使用的電腦，要能與戰場管理資訊系統相連結以獲取及時資訊及命令，便需使用與網路做連結，但受限於通信協定與網址分配不足問題，便難以實行[4]。

軍事網路連結關鍵點

在軍事網路上運用不僅止於文件或信息的傳達接收而已，而是要能將各種軍事網路（含太空、天空及地面）架構進行垂直與平行構聯，使戰場資訊能直接用於作戰為各層級作戰部隊及單位使用。其中要使網路完成構聯的主要關鍵便在於通信協定上，目前網路的通行標準之一是網際網路位址協定（Internet Protocol，IP），作為網路節點定址（Add
ressing）與路由功能。目前通行的是 IPv4 版，基本原理是比對封包目的位址 IP 的網路前置碼，若網路節點離開原網路漫遊至其他網路，因網路前置碼不同而無法路由至正確地點。由於手提電腦及行動上網日益普遍，網際網路標準組織（IETF）開始制訂 Mobile IP 的協定及相關技術，IPv6 版則在制訂中，直接整合行動 IP 技術。Mobile IP 和無線網路技術將是未來的趨勢，此技術應用在軍事上，解決目前軍用 C4ISR 雜亂無章的現象。建構軍用的行動隨意網路（Mobile Ad hoc Network，MANET），未來的軍用無線網路，並無實體的網路架構，每一個前線單位均配有自己的 IP，透過手持或配備在船艦、飛機上，可以傳輸數據資料，具有與網路連接能力的三軍通用戰術無線電（JTRS），可以隨意連上區域網路，如果該單位移動到其他區域網路時，不需再重新登入，可以在機動的同時仍保持和網路連線，因此未來資訊不再有延遲的問題，也不會有機動的限制[5]。

中共 IPv6 與 IPv9 網路發展建置

中共認為，不管從政治、軍事或經濟角度來看，全世界掌控網際網路的核心一直是在美國手中，由於不管是網際網路的基礎位址

[4]註 王正德，《解讀網路中心戰》，（北京：國防工業出版社，2004 年 5 月），頁 4

[5]註黃偉傑、陳國銘、舒孝煌，〈軍事事務革新的試金石—2003 精實國防站立科技研討會〉《全球防衛雜誌》（台北：），民國 93 年 1 月 14 日 http//www.diic.com.tw/comment/930114-1.ht

（IP）或網域名稱（Domain Name）[6]的申請都必須經由美國商務部授權「網際網路網址名稱及位址管理組織」(The Internet Corporation for Assigned Names and Numbers, ICANN)管理網址，ICANN是全球網址名稱的總管單位，負責全球網路位址空間的分配，再授權給其他的公司行號，接受各界的申請。且網際網路（Internet）採用網址系統（Domain Name System, DNS）將網址解析為IP地址。而這些伺服器目前都在美方或親美方國家的手中，從申請註冊的被控制到網址域名解析的被控制，對所謂中共網路及資訊安全構成極大威脅，因此中共除消極抵制美國中文網址的

註冊權，另一方面極力研發通訊協定中所謂「中文網址域名系統」期能掌握網際網路的優勢，並轄其未來經濟，強迫亞洲及華人世界使用其中文域名系統，如此不僅可與美國分庭抗禮，更可自然取得未來戰略上的優勢[7]。

由於網際網路及通訊科技的蓬勃發展，全球網路使用人口迅速增加，目前32位元的IP(IPv4)的資源已不敷使用，預計所有的IP位址，將於近幾年耗盡。全世界40億網路IP位址美國便佔74%，而

[6]註網域名稱

網域名稱(Domain Name)是一連串的文字，對應到網路上的實際位址(IP Address)。 Internet，之所以稱為網路，代表其由上億台電腦互相連結而成，然而，在沒有網域名稱之前，電腦電腦之間互通則需記憶彼此的IP位址，這樣複雜的記憶不利於網路的推廣，因此在1981年由 Jon Postel 設計出網域名稱，並在1984年左右，Wisconsin 大學定義出網域名稱轉換機制及網域名稱伺服器 (Domain Name Server: DNS)，如此一來，用戶不必再背誦一長串無意義的數字字串，只要記得該公司的網域名稱，即可順利地找到該網站，而這就構成當今網際網路的運作基礎。

[7]註劉台平，《島計畫-2008中共發動對台割喉戰》（台北：時代出版社，民國93年1月14日），頁38

中華人民共和國僅有3,000萬多個位址，根本不夠中共發展網際網路使用。更因中共對IPv4位址分配並不具備發言權，因此為抓住網際網路的基礎核心，中共認知到必須積極投入研發更寬廣且具有與美方抗衡的中文系統的通信協定，因此積極與日、韓聯合研發IPv6，除希望藉由日、韓的技術奠定中、日、韓於亞洲網路的主導權[8]。

由於現行的網際網路通信協定（IPv4）與新一代的網際網路通信協定（IPv6）在位址長度與封包格式上有顯著的差異。因此兩者主機是無法直接溝通的。IPv4要轉換為IPv6受位址的長度與標頭格式及標頭訊息處理方式改變影響，無法直接轉換，目前各國轉換計畫大多朝向漸進式相容，因此IPv4與 IPv6並存到完全轉換仍會持續一段時日，預估2040年前IPv4才會完全消失。但不管是IPv4或是IPv6其關鍵點的網路域名及分散式網址服務系統中的頂級網址伺服器等上層管理單位，仍是美國控制為主，其安全保密算法均控制在外國手中，因此中共仍無法擺脫可能遭監控與被入侵或遭惡意切斷網路通信的的恐懼，因此中共為強行抵制世界網際網路網址認證及網際網路網域名稱的美商維聖公司（VeriSing）的認證權，並積極投入開發「中文網域名稱註冊系統」，期能藉為與美抗衡。

2001年10 月，中共信息產業部在上海宣布成立了「國家十進制網絡標準工作組」，由上海通用化工研究所負責全國十進制網絡標準

[8]註劉台平，《島計畫-2008中共發動對台割喉戰》（台北：時代出版社，民國93年1月14日），頁37

制訂與推廣應用。並於11月向外宣布中文數字域名（數字功能變數名稱《數字網域名稱》）系統IPv9研發成功[9]。在IPv9協議中不同於IPv4與 IPv6的十六進位制算法的方式，是採用十進位制，並採用全數字碼於撥接上網的電腦上由網路服務者隨機提供網址，整個網路

系統主要由IPv9地址協議、IPv9報導協議、IPv9過渡期

協議、數字域名規範等協議和標準構成，能兼容現有網際網路協議（IPv4與 IPv6），又可實現邏輯隔離，達到安全可控。目前數字域名系統已在三十多個國家和地區申請專利，專門書籍《數字域名和數字化地球；數字域名總體方案》也做了版權的登記，不僅在經濟、政治上可打破美方獨大的態勢，也使非英語國家對資訊發展與建設不再受限於英文域名，可結合各國自行語言發展資訊相關科技，降低網路使用門檻，加快全球數位化進程。

最重要的，中共將數字域名系統的網路中心設於中國大陸，不僅可藉大陸未來經濟發展性掌控未來網路市場，更迫使網際網路世界形成兩大集團，更甚的以網址的使用性，更可能取代Internet。因此中共以全球戰略角度擬訂計畫，除在上海成立研發中心，開發與推廣數字域名應用服務系統與終端設備於大陸地區使用，更於香港建立與網際網路交換平台和實際運作點，進行數字域名的應用試

[9]註摩托羅拉工程學院無線論壇，＜IPV9技術簡介＞，http://www.chinatelecom.com.cn

行。加快與非英語系各國大型網路服務提供者（ISP）與電信設備製造商家快編列數字域名產品與國家標準，實施域名的分配、註冊、收費、服務與管理，充分運用版權和專利產生的新資源，與目前網際網路分庭抗禮[10]。

中共中文數位網域名稱系統通訊協定運用研析

中共全力發展中文數位網域名稱系統（Digital domain name system ），其目的在使自己擁有如同美國「網際網路網址名稱及位址管理組織」（The Internet Corporation for Assigned names and Numbers ,ICANN ）一樣可管理全球網址申請、分配與協定參數的配置。現行網址都以英文為主，非英語系國家使用上仍有語言上的隔閡，目前國際上中文網址系統實際運作的有多國語文網址系統（VeriSign）、國際化域名系統公司（i-DNS）、台灣網路資訊中心（TWNIC）/中國互聯網絡信息中心（CNNIC）三套，但以美方 ICANN 支持的 VeriSign 為主，中共因此強行抵制美國中文網址註冊權，宣告中文是中國的。當中國擁有自己的上層網址便可同網際網路（Internet）一樣採用分散式網路系統（DNS）將中文數字域名系統解析為 IP 位址，去管理各國所申請的根伺服器與網址所有人的網址伺服器[11]。

[10]註 同註 7，頁 55

[11]註 The Internet Corporation for Assigned Names and NumbersList of Accredited and Accreditation-Qualified Registrars(ICANN 認可之登錄網址公司)，<IP Addres>, http://www.icann.org/registrars/accredited-list.html

而網路域名的管理不僅止於政治、經濟上的利益，在軍事上其用途隨著資訊進步也越來越多樣化，除了可連結各軍事網路或軍事作戰系統讓戰場情資更透明化外，藉由資訊產業發展在網路通信、電話無線電手機邁向3G以能即時取得語言、文字、視訊、個人網站等傳輸設備是日益受重用，但相對的其軍事國防上的保密與監管就愈顯重要

。而中共這套IPV9利用IPV4 和IPV6相容於IPV9的理論，利用既有設備，卻無法偵測它的存在，因此可鎖定特定號碼與位址進行偵控與攻擊，而未來更可藉由對行動網址的掌控，對各型導引武器、飛彈進行空中破壞或誤導。

研判中共運用此一發展於軍事上用途如下：

1、 運用網路通訊系統，滲入台灣掌控電信

中共對電信各區號碼管控甚嚴，惟近期常可發現對台不僅實施公開發售，更給予優惠，以此滲入台灣電信業，將造成我國內各電訊通話為其掌控，幾無秘密可言[12]。

2、 構建自主的軍事作戰指揮網路體系

因為技術決定未來作戰模式與作為，中共極力擺脫國際間通用的網際網路必須受限於美方的技術，若研發成功，將與美國分庭抗禮於世界，更甚獨霸於華語世界，對其未來網狀化作戰下

[12]註　同註8，頁156。

的通資技術有莫大助益。[13]

國軍網路運用現況與因應作為

國軍目前對網路之運用，除國防部為遵循行政院「便民服務」及配合「電子化—網路化政府推動計畫」政策，完成「國防部全球資訊網系統」適時提供各項國防訊息與申辦事項，供民眾查詢，以滿足民眾知的需求，提昇國家競爭力，建立全民國防共識外。國防部亦積極推動網路運用，期能提高國軍各單位平、戰時作業效率並有效掌握世界各國軍事情勢與中共各項資料，提供國軍建軍備戰參考
，提升國軍戰力。

電腦網路在軍中之運用已蓬勃發展中，然基於安全考量，國軍現行運作之「國軍資訊傳輸網路」（MINET）及各軍總單位架設之區域性網路系統基於安全考量大多採封閉系統，故坊間時有所聞電腦犯罪尚未對國軍構成嚴重影響
；惟長遠考量國軍網路系統朝開放的網路系統應是必然的走向，故如何加強國軍各單位網路安全觀念，採取有效的網路安全防護作為，以保障安全機密等級極高的軍事資料避免為外界入侵，將是國軍面對未來資訊網路作戰時的重大挑戰。僅就個人淺見，提出幾點因應作法，俾供有關單位參考。

一、國防與民用資訊安全技術相結合

[13]註王正德，《解讀網路中心戰》，（北京：國防工業出版社，2004年5月），頁326

除了國軍針對軍事網路運用的安全防護必須不斷研發外，由於藉由民網為軍事所用是不可避免趨勢，如何能用其利，避其害，必須結合現行民間資訊技術，對各民間的資訊安全技術加以整合，已獲取管理網路安全關鍵技術，奠定國軍未來網路運用的安全防護研發能力。目前國軍部分軍事院校已加入台灣學術網路，藉以進行招生及學術交流等資訊傳輸，如能針對各學術單位正進行的資訊安全防護技術相互交流，及運用國內民間知名掃毒網路公司，可發揮分工合作累積安全防護能量。

二、建立軍事網路專責指導單位

網路運用雖便利，但對網路的安全防護應借重軍方資訊長才與民間具備網路安全專業知識人才，針對網路可能遭受到的攻擊、破壞滲透等實施有效防護措施的指導與執行，平時指導國軍各單位從事網路安全之整備與建立國家網路安全防護研發，戰時可運用來實施網路各式作戰。

三、強化單位網路管理

國軍各單位在國軍網路化的架構下，紛紛建立所屬單位網站，而網路的建構並非難事，其管理與維持網路正常運作才是單位必須重視與注意的。而網站管理除專人專責外，必須隨時掌握網路現況與單位成員運用情形，預防網路外圍人員不當入侵與竊取破壞，對不正常的流量與封包進出能有效管制監控，能隨時主動察覺便可減低

傷害到最小。

四、落實單位網路軟硬體設施防護

除了積極研發經濟有效的監控與防護系統，對各類型防護技術必須常常檢視，落實各種防護技術，如防火牆、網路安全監控軟體、防毒軟體、系統密碼保護、網路實體隔離等手段，以維護單位網路系統不為有心分子入侵，確保各單位在使用資訊網路及網路運用上的安全。

五、強化網路安全防護教育

使用人員一直是網路安全管制的最重環節，除了教育官兵妥善運用網路資訊外，對網路可能遭受的危害及影響必須不斷透過教育，讓其瞭解網路雖便利，但其危害的嚴重性非同小可。因此網路運用安全必須靠使用者運用複雜的密碼、傳送的加密、不明程式的注意不好奇等，來做好第一道防線工作，雖然繁雜但卻是安全首要。因應電腦及網路犯罪日益嚴重，立法院已於86年9月25日三讀通過相關電腦洩密、竊取、破壞及經濟等犯罪之刑法增修條文，並於於86年10月8日公布實施，國防部總政戰部特研析整理「使用電腦及網際網路作業特應注意事項及常犯違規情事」，各單位應逐級加強宣教提示要求，俾使所屬對電腦及網路連線作業有正確之體認，並知法守法。

六、資訊化整體架構規劃

軍事通訊與各類武器、裝備傳導網路化已是國軍邁入未來作戰趨

勢，因此研提未來本軍資訊化整體架構規劃，從通信網路架構之建立、資訊作業環境之配置、應用系統架構之規劃、以及資訊化整體架構完成後，全軍依其業務導向、任務導向規劃完整之資訊流程架構等，都必須有前瞻性。對於現行無線網路運用與研發要能結合戰術區域通訊網路與民間基地台網路，達成有、無線電網路多重通連系統，以供全軍資訊自動化之傳輸運用。

而資訊網路作戰中身擔重任的是能快速解算戰情資訊、整理數量龐大的後勤資訊以及儲存全軍各類彙整資料庫之主官決策支援系統主機的建置。另亦需廣泛建置以工作站或軍事專屬網路伺服器為主以處理全軍各項業務資訊系統，當全軍整個通信網路架構以及資訊作業環境均能夠完全涵蓋全軍各單位後，未來整個應用系統之架構，將朝向以網際網路型態的作業方式，架構起全軍的應用系統骨幹，以管理資訊及行政業務系統為血管，透過各作戰單位為手腳，以期能使本軍之打擊戰力充分發揮。

結論

陸軍要邁入網狀化作戰，不可避免的就必須與各個指揮管制與勤務支援的資訊指管作戰系統相結合，而目前網路作戰大部分雖處於紙上談兵階段，但要讓資訊化戰場成立就必須作戰各個單位與單元間能連結，面對未來資訊化戰場，中共已成編「網軍」，美軍於伊拉克網路作戰的運用，類式的網路攻擊、防禦作戰已然形成，隨著時代

的演變，網路作戰已被視為一種正式的作戰方式，就如同網路犯罪已逐漸被視為一種正式的犯罪方式一樣。但如果等到台海正式的網路戰爭開打之時，才開始網路戰爭的準備與研究

，那就為時已晚，唯有以前瞻的理念，瞭解欲進入數位化戰場，就必須瞭解戰場變化中網路運用的關鍵趨勢，及早防範與準備，才能在未來戰場取得先機。