中共網路（絡）戰發展對我防衛作戰影響之研析

陸戰隊上校 寧大強

提　要

一、隨著科技的高度發展，「資訊戰」儼然已成爲21世紀之戰爭主流。資訊戰力整備中之「資訊網路攻擊戰術戰法」運用，因其可達兵不血刃而千里屈人之兵的效果，已形成極度重要之課題。

二、軍事系統的現代化已和電腦系統密不可分。電腦網路的廣泛運用，一方面爲增強軍事作戰效能提供了潛力；另一方面增加了資訊系統遭受攻擊的危險。因此，國防資訊安全防禦措施，往往較發展資訊攻擊武器更重要。

三、中共網路（絡）戰是屬於信息戰之範疇，其體認到由於信息技術、網路（絡）技術等發展的非均衡性，未來戰爭中的網路（絡）戰，同樣可能出現非對稱局面。

四、一次波灣戰爭後，中共即調整建軍方針，加強對外學習要求以「質量建軍、科技強軍」爲原則，爲「打贏高技術條件下的局部戰爭」展開一系列準備。從大力培養「懂資訊專業技術又懂作戰指揮的複合型人才」，到逐漸形成之建立「網軍」等作爲，已充分展現了共軍爲獲得全面「資訊優勢」做準備的決心。

五、中共近期提出各種數位網路攻擊模式，期以新型態之「網軍」達到「損小、效高、快打、速決」的戰略指導原則，將對我國防思維及現有優勢造成重大衝擊，須密切注意其發展，並研擬因應之道，以確保我國家安全。

壹、前　　言

中共網路（絡）戰是屬於信息戰之範疇，說到網絡戰應先從中共之信息戰說起，1991年一次波灣戰爭後，興起了中共軍事事務革命，深刻體認到高技術條件下局部戰爭中，「制網絡權」是定勝敗的要素，由於信息技術、網路（絡）技術等發展的非均衡性，未來戰爭中的網路（絡）戰，同樣可能出現非對稱局面。網路（絡）空間是繼陸海空天之後的第五維作戰空間。從戰場的勢能來看，這些作戰空間按照出現的時間順序依次遞增，海上勢能大於陸上勢能；空中勢能大於海上勢能、陸上勢能；天宇勢能大於前三者；新出現的網路（絡）的勢能則處於最高位勢。制海權、制空權都曾成爲某一特定歷史時期戰爭的主導權；在未來高技術條件下局部戰爭中，制網路（絡）權將成爲決定戰爭勝

敗的重要因素。網路（絡）日益成爲軍事作戰系統的「CPU」，網路（絡）時空日益成爲關注的焦點。

貳、網路戰之定義及特性

一、網路戰之定義

㈠美軍

「任何阻絕、利用、篡改或破壞敵軍網路與網路功能，防護我軍免於遭受敵軍加諸於我之類似傷害，並利用友軍網路戰功能的行動」；「採取之行動除可影響敵之資訊、資訊處理、資訊系統及電腦網路，以取得資訊優勢外，亦同時防護我之資訊、資訊處理、資訊系統與電腦網路安全」[註一]。

㈡中共

中共所謂的「信息戰」即爲我方所稱的資訊戰，此類戰爭方式之定義爲：「在電腦網路空間的戰爭，包括使用邏輯炸彈、病毒及其他以電腦爲基礎的方式，對敵人電腦及傳輸系統發動電子攻擊，以癱瘓、摧毀、中斷或操控對方國防或經濟資料」[註二]。其網路戰係屬信息戰之範疇，泛指運用程式控制、病毒、駭客、心理戰、訊息等攻擊方式，使敵方之系統無法正常運作。

㈢國軍

資訊戰係透過指管程序，藉情報戰、心理戰、實體破壞、資訊攻擊、電子戰及傳統武力攻擊等手段，對敵方任何資訊與系統，加以遲滯、干擾、癱瘓摧毀，並獲取敵方資訊供我軍運用；同時藉由軍事欺騙、安全措施、資訊防護等方法，確保我方資訊與系統之完整、防止洩漏、瓦解或遭受破壞，以支援並維持我軍事決策指揮作戰[註三]。

簡言之，網路戰爲破壞敵方資訊系統的使用效能和保障己方資訊系統正常發揮效能而採取的綜合性行動。廣義的網路戰是敵對雙方在政治、經濟、軍事、科技領域運用網路技術，爲爭奪資訊優勢而進行的鬥爭。狹義網路戰是指敵對雙方在作戰指揮、武器控制、戰鬥遂行、後勤技援、軍事訓練、情報偵察、作戰管理等方面，運用網路技術所進行的一系列網路偵察、網路進攻、網路防禦和網路支援行動。

網路戰正在成爲高技術戰爭的一種日益重要的作戰樣式，其著眼是可以兵不血刃地破壞敵方的指揮控制、情報信息和防空等軍用網絡系統，甚至可以悄無聲息地破壞、癱瘓、控制敵方的商務、政務等民用網絡系統，不戰而屈人之兵。網路戰是爲干擾、破壞敵方網路資訊系統，並保證己方資訊系統的正常運行，而採取的一系列網路攻防行動，網路戰分兩大類：一類是戰略網路戰；另一類是戰場網路戰。

二、網路戰之特性

㈠具全民戰爭特性

資訊技術是軍、民共通性的。因此，只要具有網路攻擊能力的都可運

註一「美軍資訊作戰野戰教範」(臺北，國防部總政治作戰部譯印，民國87年3月)。
註二「要目簡介」，國防譯粹(臺北)，民國90年6月，頁1，。
註三 柴惠珍，「E-國軍」，資訊傳眞周刊 No.15，2000年12月6日。

用。未來的網路作戰並非是單靠軍人利用網路對敵軍事資訊系統進行攻擊，而是運用「所有具備網路攻擊能力的人」，對敵交通、金融、貿易、軍事等各個領域的全面攻擊，以達到遏止戰爭的目的。

㈡戰場透明度高，資訊共享

透過網路傳輸將偵察衛星、戰場雷達、熱成像儀、戰場視訊等第一線獲取的情報資料，即時呈現到指揮所的螢幕上，極大地拓展了偵察和監視的視野。通過網路快速傳輸資訊，使戰場上之情資透明化，並能即時掌握及共享。

㈢戰場空間無遠弗界

高科技武器的遠投及快打性能，加上數位資訊的推波助瀾，使得戰場指揮、管制、通信、情蒐等不再受地域限制。所以戰場空間，均朝向大縱深、高高度及立體化發展，過去以有限距離考量威脅的思維已不適用。

㈣網、電一體化

由於網路戰的出現，使得電子戰已不能完全涵蓋所有高技術的「軟殺」手段，從而導致資訊戰概念的提出和資訊戰理論的迅速發展，形成網路戰與電子戰一體化的資訊戰，更將網、電作戰緊密結合在一起。

㈤戰場破壞力大增

數位科技的精確性使武器在投射精準及爆炸時效均大幅提高，整體作戰效能呈倍數提升。

㈥戰場非對稱性擴大

以電磁脈衝(EMP)等武器來癱瘓敵對國家數位資訊網路系統，達成小兵立大功的非傳統作戰非對稱性運用的可能性大增。

㈦戰場奇襲突發性大增

由於破壞數位資訊系統結構而癱瘓政府及軍事作戰機制之效益奇高；因此，數位化奇襲作戰的突發性大增。

參、中共網路(絡)戰之發展

一次波灣戰爭後，中共即調整建軍方針，加強對外學習要求以「質量建軍、科技強軍」爲原則，爲「打贏高技術條件下的局部戰爭」展開一系列準備。從大力培養「懂資訊專業技術又懂作戰指揮的複合型人才」，到逐漸形成之建立「網軍」等作爲，已充分展現了共軍爲獲得全面「資訊優勢」做準備的決心。中共認爲未來高科技作戰，信息技術是致勝的關鍵，故早於「九五計畫」(1996-2000年)期間，即每年投資約90億美元（相當其公布的年度國防預算），建立戰備通信電訊網路，以太空衛星爲主體，結合地面活動衛星接收站、數位化微波系統、電腦系統等，組成資訊傳輸系統，以接近科技先進國家的資訊水準[註四]。爲發展信息技術，於1995年，就成立「國防科技信息中心」，負責資訊、軟體科學研究及服務；1996年成立「信息安全研究室」，從事電腦病毒、駭客攻擊、反攻擊的「軟件組織的對抗」，於「總參二部（軍事情報部）」設「科學裝備局」，發展電腦病毒、電磁脈衝等技術與試驗，研製戰術性「非殺傷

註四 通信電子資訊學術半年刊(中壢)，第93期，民國89年2月16日，頁47。

性武器」。另自美輸入超級電腦，電腦輔助設計軟體等技術，近期並已於東南沿海，鋪設長達3萬7千餘公里的光纖通訊網路，將沿岸設置導航臺聯網，用全球衛星定位作遠程航海精確導航，並加強指、管、通、情抗干擾能量，重要軟體加裝防火牆，軍事演訓更加入電腦病毒植入科目，由此可知中共對網路之重視。中共著手進行因應資訊作戰建設工作，一方面於1992年間完成共軍「情報自動化指揮系統」之連線工程，另一方面亦針對運用電腦網路竊取、竄改資料、散佈謠言及散播病毒程式等犯罪行爲加以監控防制。

一、中共網路（絡）戰發展概況

目前共軍在資訊作戰之建設作爲方面，係著重於軍隊「指管功能」之提升，對資訊戰爭的領域而言，屬於著重守勢防禦性作爲，其發展概況如后：

㈠自動化指揮系統之建立

共軍自1978年起，即已著手籌辦「全軍自動化指揮系統」之建設工作，迄今已開發成功「野戰自動化指揮系統」、「野戰自動化指揮車」、「砲兵自動化指揮系統」、「長河二號」艦艇遠程導航系統、「雷情二號」空防管制系統等裝備，並已展開全面部署。

㈡鋪設光纖網路

光纖通訊方面，迄2003年已完成總長3萬7千公里之22條跨省區光纖通訊網路之工程，並以數位化電腦交換機爲主要中繼設備，達成「信息高速公路」計畫之建設目標。

㈢資訊作戰普及化與相關專業訓練

中共陸軍成立培訓資訊及指揮通信專業人員之「信息工程學院」，各軍事院校亦加強電腦資訊教育，並增設相關資訊作戰技術之教學課程，另針對新配備之光纖通訊、數位通訊、衛星通訊、微波通訊等裝備，實施專業人才培訓，並將新型裝備運用於戰役通信演練及電子戰對抗演練。

㈣電腦數位化科技提升部隊戰力

共軍於1996年底，公開宣稱其電腦之使用已普及全軍、師、旅、團級部隊，新換裝之武器裝備亦實現電腦化。各集團軍技術兵種運用電腦之普及率達三分之一，現正積極建設作戰部隊專用之電腦網路及數位化軍事資料庫，以達成作戰、訓練、指揮全面自動化之目的。中共軍隊亦開始演練電腦病毒作戰，1997年10月10日瀋陽軍區兩個師指揮所相互以電腦病毒進行攻防，同年11月中旬一個摩步化步兵師進行「信息戰條件下，實兵實彈戰術演習」，其中包括駭客人侵、電子戰、反精確制導等項。[註五]1999年北京軍區演訓項目包括兩軍電腦對抗、2000年成都軍區將網際網路納入演訓項目。此外，共軍於2001年模擬對臺戰爭中，係以資訊網路攻擊爲開端。

㈤開發各式模擬訓練裝備

共軍應用電腦數位化科技，已完成多種戰機、火砲、坦克、飛彈等武器裝備之模擬訓練系統，並開發各類戰役模擬之電腦兵棋軟、硬體，由聯訓基地

註五 趙介一，「中共信息戰發展及我因應之道」，陸軍學術月刊(桃園)，民國89年1月，頁39。

所屬戰役訓練模擬中心或軍事院校進行電腦模擬對抗戰役之測試，並將其結果運用於戰術、戰法之研究與精進。

㈥培養訊息幹部

1999年4月28日中共解放軍通信指揮學院以其跨學科組織專家教授完成的「信息作戰指揮控制學」和「信息作戰技術學」專著爲理論體系，首創信息戰指揮控制這門新興學科，爲其數位化部隊建設提供了理論基礎。迄2003年該院先後爲共軍培養了四批300多名信息作戰的人才，使中共信息戰幹部大量增加；並組織專家到總部機關、部隊和院校巡迴講課；出版製作有關信息戰刊物和多媒體教學軟體。

㈦網路象徵國家主權

1999年11月10日「解放軍軍報」發表文章指出，網路（絡）秩序現已成爲各國經濟運作和發展的重要指標，網路（絡）空間受到侵犯，就是國家主權受到侵犯，其嚴重性不亞於領土、領海和領空受到侵犯。2000年2月10日「解放軍報」又發表文章指出，信息殖民現象將成爲未來戰爭的重要原因。不能確立信息的獨立自主權，就沒有眞正獨立的國家主權。沒有信息安全就沒有國家在政治、經濟、軍事等方面的安全。

㈧成立數位化部隊

中共軍委會命令「解放軍」須在2000年前後建立數位化部隊；北京軍區第38集團軍遂在國防大學和解放軍通信指揮學院之協助下，開始訓練未來數位部隊人員。[註六]

二、中共網路戰戰法

㈠資訊網路戰攻擊

以干擾、摧毀、破壞與迷惑敵人資訊系統爲目標。分析其運用挖眼、斷道、掏心、擾宿等手段：

1.挖眼：即消除信號源。運用方式如后：

⑴「察」：偵查信號源之位置。

⑵「擾」：干擾信號源。

⑶「毀」：摧毀破壞信號源。

2.斷道：即切斷敵人資訊通道。運用方式如后：

⑴「光電干擾」。

⑵「網路破壞」。

3.掏心：利用植入電腦病毒或兵、火力等干擾、破壞與摧毀敵人資訊戰指揮中心（即資訊處理中心）。運用方式如后：

⑴電子偵聽。

⑵特攻破壞。

㈢火力摧毀。

⑷電磁脈衝彈(EMP)。

⑸病毒奇襲。

4.擾宿：即干擾敵之信宿。運用方式如后：

⑴欺騙。

⑵威懾。

⑶激光致盲。

中共在網路戰攻擊方面是以癱瘓敵指管通情系統爲主要目標，其攻擊是以網路超載、施放病毒、阻斷節點爲主要手段，研究具體成果爲「網路制敵五法」（斷電、精確打擊、超載廢網、散

註六 吳啓昌博士，中共進行「資訊戰」之意圖及能力評估座談會會議記錄談話內容。

播病毒、駭客滲透)[註七]、「信息網路對抗五法」(網路刺探法、網路破節法、網路動截法、網路攻程法、網路癱瘓法)[註八],顯示中共已規劃網路戰攻擊戰法雛型及實施方式。

㈡資訊網路戰防禦

爲抗擊敵人資訊進攻,所採取之基本戰法有以下幾種:

1.護眼開源:藉由以下方式達到保護資訊偵蒐系統,擴大軍事資訊來源目標。運用方式如后:

⑴隱形求存。

⑵動中求生。

⑶以假護眞。

2.護道暢流:透過以下方式及堅守樞紐等方式,保證各種軍事資訊暢通無阻之目標。運用方式如后:

⑴廣拓信道。

⑵確保幹道。

3.護機保心:置重點於確保電腦之安全,以維持資訊中心之運作。運用方式如后:

⑴防敵偵察。

⑵防敵病毒入侵。

⑶防敵摧毀。

4.多法抗擾:綜合運用多種資訊傳遞方式,提高信宿系統抗干擾能力,並使用多種資訊反干擾及反摧毀等手段,以達到抗擾、抗毀之目標。運用方式如后:

⑴多種方式傳遞信息。

⑵以多種技術提升抗干擾能力。

中共在防制駭客方面著重以實體區隔、安全防護、欺騙誘敵,並參酌外國駭客攻擊方式,提出反駭客侵襲戰法,其主要防制方法有變更隔離、眞僞鑑別、靈活組網、防洩保護、隱匿規避、誘敵欺騙及干擾摧毀等七種方法。

㈢電腦病毒攻擊

中共電腦病毒攻擊戰法強調先期將電腦病毒預植於敵電腦系統,並在特定時間啓動病毒程式,主要以破壞性、複製性與擴散性病毒癱瘓敵網路系統爲主,其戰法有前潰潛伏、臨機預置、間接攻擊、接口輸入、探測攻擊等五種方式[註九]。

肆、中共網路戰未來發展趨勢

從中共近年來有計畫地發展信息戰攻防戰略,並將其列爲軍事演訓項目之企圖心來研判,中共可能已將我鎖定爲資訊戰及網路戰之目標,並且可能已有計畫、有組織、有目的地研發資訊戰、網路戰之攻防戰術,俾竊取我國家機密、破壞重要網路、散播謠言、影響我經濟民生及動搖民心、以遂行其政治及軍事目的。研判中共網路戰未來發展趨勢如后:

一、網軍建立趨勢

電腦網路已經越來越顯示與領土、領海、領空權所具有的同等經濟、政治

註七 李章瑞,解放軍報(北京,2000年5月9日),版6。

註八 解放軍報(北京,1999年6月5日),版6。

註九 陳兆海,解放軍報(北京,1998年7月7日),版6。

和軍事意義。從發展的前景，「網軍」極有可能成爲繼陸軍、空軍、海軍之後的又一新軍種。中共近期提出各種數位網路攻擊模式，期以新型態之「網軍」達到「損小、效高、快打、速決」[註十]的戰略指導原則，將對我國防思維及現有優勢造成重大衝擊，須密切注意其發展，並提出因應之道，以確保我國家安全。中共認爲網路戰是不對稱作戰方式之一，更是未來主要作戰型態，正積極展開網路建設，以利網路戰遂行。綜觀中共網路戰準備，以建設光纜、研發指揮自動化系統、研製電腦病毒及培養資訊工程人才爲主，並配合網路戰作戰型態，組建網路戰部隊，以及在南京、廣州等軍區實施演訓，驗證網路戰戰術戰法理論與研究。中共目前尚未有正式的編制和命名，就其未來可能編制與任務以及部隊型態預判如后：

㈠廣泛編組屬於陸、海、空等各軍種直屬部隊，擔負著各類部隊和戰略級、戰役級、戰術級電腦系統及電腦網路的使用安全[註十一]，包括電腦安全防火、防盜、防電擊、防靜電和防電磁輻射等「有形作戰」任務，以及電腦安全的偵察、防護、反間和消防病毒等廣泛的「無形作戰」任務。

㈡部隊型態：網軍依其擔負不同的任務，區分四種部隊型態：

1.防竊部隊

主要擔負防止電腦信息洩漏的任務。由於電腦是靠高頻電磁脈衝工作，其無屏障的電纜不斷向周圍空間輻射電波信號；因此確保電腦安全的首要任務，即對電腦的信息輻射採取防範措施並加以抑制。對此電腦防竊部隊採取主要措施有距離防護、屏障防護、設備防護和附加干擾防護等。

2.防毀部隊

主要任務是負責防護電腦免遭武器的軟、硬體殺傷。爲對付敵人的「硬體殺傷」，中共電腦防毀部隊主要增加預警力量，對電腦關鍵設備要進行疏散配置、僞裝，並強固工事和採取多種欺騙措施。對付敵人的「軟體殺傷」，主要採取電子欺騙、壓制敵信息系統，開發光電技術、數字技術和低頻率截獲技術等，增強抗毀和再生能力。[註十二]

3.防毒部隊

負責防護電腦免遭病毒襲擊的工作。主要有下列幾種方法[註十三]：

⑴測病毒：防止「病從口入」，確保電腦安全，對電子設備的生產、進口和使用，進行嚴格測試、鑑定和管理。

⑵消病毒：監督電腦管理和使用，要求電腦用户安裝防毒軟體和病毒防護程式，禁止使用任何未經病毒檢測的軟體，杜絕病毒傳染途徑，採用指令、身分識別、程序控制等方法或對數

註十 鍾堅，「共軍犯臺能力與作戰方式之研究」，陸軍89年度第一次軍事學術研討會，民國88年11月2日，頁40。
註十一 「計算機防護兵正向我們走來」，89年軍事史林2-3期，頁52。
註十二 同註八，頁54。
註十三 同註九。

據採取加密、多層級加密和「防火牆」等措施，防止非法闖入者的竊取和破壞。

⑶抗病毒：研製「病毒」疫苗，增強電腦自身抵抗能力。目前世界上已研製出許多行之有效防毒軟體，他們不僅能檢測、消除病毒，有的防毒軟體，還能確保電腦在帶病毒的情況下正常、安全工作。

4.對抗部隊

主要擔負電腦對抗的部分任務。其職責是採取各種手段破壞敵方電腦軟體、硬體，從而破壞敵人作戰指揮系統和智能化武器系統，另肩負特定病毒對抗任務。

二、駭客網站能力增強、數量增多

目前中共相當活躍網站有「中國鷹派」、「網路紅軍」、「紅色聯盟」及「黑狐網路」等；駭客工作群更深入網路攻擊程式庫，研究並整合現有的攻擊程式，從而創造新的攻擊程式；過去幾年來，由中共發動已知的網路攻擊，便可見端倪。

三、大量培育網路人才

網路戰是一種新的作戰型態，近年來中共積極研究此一作戰相關課題，加速培養網路戰人才。自1997年起，成立「光纖通信技術培訓中心」負責培養光纖通信技術人才，以滿足未來網路建設需求，另於1999年合併通信工程學院、工程兵工程學院、空軍氣象學院及總參所屬63個研究所，組建「解放軍理工大學」，專研資訊戰，該校成立「全軍網路技術研究中心」，全力研發資訊戰關鍵技術，並在北京和清華等民間大學招收「大專儲備軍官」，特別著重電子資訊等相關科目的專才，顯示中共刻正加強網路戰之準備。西方國家的高科技公司爲中共培訓爲數眾多的網路人才，如IBM、CISCO、MOTOROLA等網路通訊大公司在過去數年間，與「中國」的大學合作開辦數以百計的網路技術學院，已培訓超過上萬的網路人才。[註十四]

四、結合衛星、偵照科技

目前中共數位資訊戰力之優勢主要爲衛星通信、偵察技巧及無核輻射污染低當量的戰術性電磁脈衝武器(EMP)。且積極持續發展以數位資訊系統支撐的攻擊戰力，依照我國防部評估，將可在2005年左右對我國構成實際威脅[註十五]。

五、軍隊資訊化、數位化發展

中共爲執行資訊戰，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，已構建完成中央與各軍區司令部的系統鏈路連線，未來將可透過圖像螢幕掌握戰區戰略態勢。另外中共在數位資訊國防的發展上，是以國家層次來推動，並且充分包含了「戰略、戰術、戰技、戰鬥」各層次。此外，中共建置高技術作戰能力之時，也不斷調整其軍事思想，目前已納入「不對稱戰」、「不接觸戰」及「超限戰」等理念。其中「超限戰」，基本理論是中共按照游擊戰的思維，以窮國對富國，藉

註十四 吳啓昌博士，中共進行「資訊戰」之意圖及能力評估座談會會議記錄談話內容。
註十五 前國防部長唐飛先生，「國防部施政報告」，民國88年11月1日，頁9。

城市游擊戰、恐怖主義及電腦病毒等……超限思維，追求超越傳統戰爭模式，打破一切限制、一切手段，結合非軍事手段，從各層次領域及對象來打破世界軍事大國；超限戰包含以數位資訊手段執行的電子戰、網路戰及媒體戰等；理論上各種戰法必須組合運用，才期達到最高作戰效能。共軍依據其所可能採用之戰法，成立各種相應部隊型態，除現有之電子對抗部隊、數位偵察部隊外，近期亦成立心戰特攻部隊、電腦模擬部隊及網路安全單位等，將可創造出對未來作戰優勢的乘數效果，吾人絕不可小覷。

六、研製電腦病毒

中共於1997年初成立「軍區電腦網路攻防小組」，進行各項驗證，並於同年先後在南京軍區實施演訓，實際模擬電腦病毒攻擊，以及10月中共北京軍區某集團軍進行「以電腦病毒癱瘓廣播與指揮系統」爲想定，實施師指揮所電腦網路病毒對抗演練。近年來，亦於瀋陽、南京、廣州等軍區實施反電腦病毒攻擊課目演練及光纖通訊網路測試與「防火牆」效能驗證。另美國國家安全專家發現已有三家美國及日本防毒軟體公司，向中共提供300多種破壞性電腦病毒及竊聽軟體，認爲是中共利用這些公司代其蒐集病毒軟體，做爲研究網路施放病毒的研發參考，同時加強其網路防毒防衛作戰能力[註十六]，顯示中共在電腦病毒研發及網路防衛能力上大幅提升。

伍、中共網路戰發展對我影響

依據中共網路戰之發展趨勢研判，若對我實施網路攻擊，其影響如后：

一、系統功能癱瘓

國軍研擬整合通信及資訊以建立指管通資情監偵(C^4ISR)系統、推動國防管理資訊系統以及在國家資訊基礎建設(NII)上發展國防資訊基礎建設(DII)等等作爲，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的「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。此項國防發展策略有效遂行，皆植基於資訊網路之安全，故一旦戰時遭受敵之網路攻擊，將對國防通信、資訊整合系統之功能，形成癱瘓。

二、網路傳輸受阻

國防各種資訊應用之操作，在戰場透明化與各種情資共享的迫切需求下，勢將採取開放式網路架構與通信系統整合之規劃，方能建立全軍共用的共通作業環境與共享資料庫。而各種情資在網路上之傳輸與交換，一旦遭敵之資訊網路攻擊，如網路實體破壞或阻斷式服務攻擊等等，將造成通資系統網路傳輸受阻，使得大量的戰場資訊分送、更新與管理困難，致各單位無法即時反應戰情、有效予以反制。

三、網路安全威脅大

中共爲獲取「制網路權」，積極網羅具網路資訊專業人士研究網路戰戰術戰法，以及打擊網路戰具，據美國智庫

註十六 中央日報(臺北，民國90年4月8日)，版9。

專家以美國、加拿大等地法輪功網站及日本因否認「南京大屠殺」後，電腦網路遭駭客攻擊等事件，顯示中共在網路戰之研究成效，以及在網攻技術方面大幅提升。因此，電腦網路安全之威脅，隨共軍網攻技術提升而遽增。軍事情資均有著高度的機密性與敏感性，在對電子資訊的依賴日益加深的情況下，一旦通資系統所建構的資訊傳輸網路遭受資訊網路攻擊，如以網站入侵竊取資料，或截取傳輸中之資料封包，極易造成軍事情資之洩漏，導致戰局形勢之丕變。

四、指管判斷不實

戰場情資蒐集往往是決定戰爭勝負的關鍵所在，戰場指揮官莫不以各種手段來獲取情報。確保戰場情資的正確性與有效性，即是通資系統整合環境下務須考量之重點。若敵對我實施網路攻擊，如僞造資料封包或進行資料篡改等等，則經由通資整合系統分散式環境之各個偵測端末辛苦蒐整得來的情資，不管是友軍、敵軍，均攸關指揮官決心下達的是否適當，亦將對指揮、管制、判斷造成嚴重之影響，阻礙作戰任務之遂行。

陸、因應之道

在邁向21世紀，國軍新一代兵力的整建之際，「網路戰」，將是21世紀世界舞臺上的主角；網路戰乃爲資訊戰之重要一環，在電腦與通訊網路不斷發展的現在，開放式觀念及主從式架構成了現在網路應用的趨勢，國軍各單位使用者充分運用現有網路上各項資訊技術，有效提升作業層級、增進作業效率，已是必然之趨勢。由於我國資訊產業之發展較中共爲進步，人民日常生活、工商產業以及國軍業務處理上，對資訊網路的依存性也會與日俱增，所以我們在網路戰這個課題上，如何保護我國不會受到網路攻擊的傷害，較如何使用網路戰來攻擊中共更爲重要；且中共發展「信息戰」不遺餘力，國軍必須採取積極之作爲，以有效遂行未來資訊作戰。

一、落實網路安全防護機制

由於電腦網路具有開放性、互連性等特徵，易受到電腦駭客、電腦病毒和其他非法攻擊，網路安全已成爲重要問題。爲確保國軍網路安全，首先軍用網路須與網際網路完全隔離，使駭客無法透過網際網路進行攻擊。其次在軍用網路上傳輸和處理軍事機密資料，須採多層級、多功能加密措施。再其次是建立一套完善入侵檢測系統，對可能危害網路安全事件進行掃瞄，分析網路中各個封包內容，以確定所傳輸內容是否經過授權，對入侵資訊發出警告，並採取隔開網路連接、跟蹤攻擊源、記錄攻擊過程等措施。

㈠資訊安全機制：從密碼防護機制、電腦病毒防禦機制等方面去強化。

㈡網路安全機制：設置網路防火牆、虛擬私有網路(VPN)等技術方面去防護。

㈢系統安全機制：可從弱點掃描、入侵偵測損害預防等機制之建立建構防護。

二、有效整合通信網路

傳輸平臺之建設爲爭取「資訊優勢」之關鍵要素；國防部指管通情及資訊傳輸系統之整合，係以建立三軍通用戰術聯戰網路爲目標，結合國軍有、無線電通訊系統及民間通訊資源，形成軍民共用多重節點、複式網路的通聯手段，以充分有效運用整體國家資源，提升通資戰力，有效支援作戰。

三、建立優勢資訊戰力

資訊戰首重「安全」，國軍基於當前戰略構想，且考量資訊安全應置網路防護爲優先，故目前資訊戰的重點乃在網路安全防護，且以全方位思考與創意運用爲原則；在發展安全防護機制與系統裝備之外，更朝向構建自動化、系統化以及資訊化之安全防護系統目標邁進。由被動性的防護進而建立主動性的監、偵能量及反制作爲，同時結合產、官、學、研界能量，構建國防自主能量，俾確保國軍在資訊戰場的優勢，以剋制中共犯臺企圖。

四、加強國軍幹部資訊教育

資訊教育以強化電腦運用、提升資訊系統管理運用能力爲目標。各軍事院校規劃資訊學程，要求能上網路與運用相關軟體爲重點；指參、戰略教育則以網路安全、資訊戰、指、管、通、資、情、監、偵等課程爲重點。[註七]

五、強化網路保防工作

㈠立即反應，隔離處理

針對電腦病毒戰的攻擊，除迅速對症下藥，清除病毒外，並應以「防火牆」機制，事先劃分若干個封閉「隔離箱」的整個電腦系統立即分塊隔離，避免整個系統染上病毒。

㈡貫徹預防，多管齊下

運用各種防禦手段包括通過對電腦加密防止敵方（或駭客）進行電腦滲透來竊取電腦情報，對核心系統和重要用户的密碼和口令，要嚴格控制知曉範圍，嚴守機密，使「駭客」無計可施；通過加強管理、監督、檢測、維護等各種技術手段，對敵方實施電磁欺騙和干擾，減少電磁信號，也可利用一定功率的干擾釋放假信號，擾亂對方的微波探測，誘惑其上當或直接干擾敵探測設備的正常工作，以達到屏蔽己方的資訊源，保護系統正常工作的目的。

㈢科技整合，系統防護

我國現行所有與資訊相關的單位，如雷達站強網、情報、資訊中心、資料中心的作業中，有數量龐大的商購裝備與系統是外購的，放在系統整合上應有保防的考慮，嚴密的對商購系統做安全查核，並在系統的整個作業流程、作業系統及資料鏈的保護上要有保防的觀念。

六、結合民間科技，研發國軍網路安全關鍵技術

網路安全防護之技術除由國軍自力研發外，尚應結合全國在資訊安全防護領域之研究單位，例如：中正理工學院、國防管理學院及民間大學如交通大學、臺灣大學及元智大學等，先就資訊安全方面正進行之研究資源進行整合。

註七 中華民國九十一年國防報告書第六篇第四章第三節，頁266。

再針對各單位之研究特性，選定不同研究領域或重點項目，以充分發揮分工合作之效益；期由對某些網路安全之關鍵技術獲得，逐漸累積整合研究之成果，以奠定國軍網路安全防護科技自行研發之基礎。

柒、結　　語

中共近來極熱中於信息戰的發展，在面對中共的威脅下，如何維護我方指管通情系統的完整，應是軍事戰略上的優先考量。除了本身對於信息戰應建立基本正確的觀念，更急迫的是應於平時即養成通資保密與網路安全之概念。我們從近來各資訊網路遭到入侵的相關資訊，可以了解到駭客技術已從早期的偷窺、毀壞資料，進步到分散式阻絕服務攻擊以圍剿目標網站；電腦病毒的佈放，更從個人檔案的傳遞感染，演變成附加在電子郵件的寄發以擴增影響範圍。此正顯示出資訊戰中最鮮明的一項特質：「科技的進步加速了資訊網路攻擊戰術戰法運用之不斷革新」。網際網路的便利，提供了駭客與病毒入侵之管道，新的犯罪型態及資訊恐怖主義勢必會威脅到正常的網路用户。尤其國防資訊系統是敵方駭客最欲遂行網路攻擊及侵入的目標，國軍各單位應積極研擬有效之資訊網路攻擊及防護之戰術戰法，於癱瘓敵軍指管通資網路系統之同時，亦能阻絕使用網路攻擊之敵軍，以充分達到通資支援作戰，確保國家安全之目的。

收件：93年12月07日
修正：94年03月30日
接受：94年05月05日

作者簡介

寧大強上校，海軍官校71年班、海院81年班、陸院戰研班83年班；現任職於國防大學軍事學院海軍學部教官。