復興崗學報
民 96，90 期，245-264

中共網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用

李承禹
陸軍官校政治系助理教授

摘　　要

如同資訊作戰，在網路戰的領域中，決定性因素仍然在於人的智慧與認知。因為此將界定出以何種方式及手段實施軍事現代化，以及如何提升或管制軍事科技的應用。在網路戰的概念中，人可以等同是網路系統中的脆弱節點，且阻礙科技潛能的發揮。另一方面，人也可能是網路系統中堅實的節點，網路只不過是匯聚、處理及轉換資料的途徑，離開了人，資訊系統無法做出實在而有效的選擇。本文即以此觀點為核心，探析中共解放軍網路作戰之戰略邏輯，並期望藉由資訊科技（IT）與網路概念及戰爭本質改變爭論的延伸，能夠對於網路作戰的理解上提供更多的關注和資源，找尋出網路作戰的優勢。

關鍵詞：網路戰、網路中心戰、戰略邏輯、資訊戰、電腦網路作戰

The Analysis of the Strategic Logic of Network Warfare in China's PLA: The Compartment and Application of Network and Network-Centric Warfare

Lee, Cheng-Yu
Department of Political Science, ROC Military Academy

Abstact

Similar to the information warfare, the decisive factors of networked warfare still depend on the person's intelligence and cognition, because they will define the ways and means that launch into military modernization, and promote or control the application of military technology. In the networked warfare concepts, people may be as the weak nodes of any networked system, an impediment to technology fulfilling its potential. On the other hand, people as the strong nodes of a networked system; the network merely absorbs, processes, and moves data, leaving people to do what information systems cannot make hard and responsible choices. The article is belong with this core viewpoint, analyzes the strategic logic of the networked warfare of China’s PLA, and expect through the spread of IT and networking concepts and the changing nature of warfare argue for giving more attention and resources to the cognizance of networked warfare, seeking the advantage of networked warfare.

Keywords:**network warfare, network-centric warfare, strategic logic, information warfare, computer network operations**

李承禹

壹、前言

進入二十一世紀，中共隨著經濟實力高度成長連帶也促進國家重大建設日見成就，其中尤以加快軍事現代化的進程更為明顯。其主要原因有三：第一是中共在國力上升後對區域影響力大增，軍事能力成為中共的重要後盾；縱使中共刻意壓抑軍事投資大幅成長的事實，然而仍難躲避國際間對中共軍事力量轉變的密切注意。第二，中國崛起已成事實，中共廣泛參與國際政經事務的需求也大增，因而影響原有的區域權力結構，不僅與美國經常產生權力碰撞，包含日本、印度與我國，中共都必須展現更先進的國防實力來確保其安全戰略利益。第三，中共未雨綢繆的理解到，軍事力量才是國際現實主義下的重要籌碼，無論國際外交或國際政治中，擁有具威脅的軍事能力者，才可與其他國家平起平坐。為了維持經濟持續成長與國際影響力的提升，更為了有能力爭取亞太地區的各種戰略利益，中共都需要藉著軍事現代化快速發展來滿足上述需求。

然而，在軍事現代化的進程中，中共從上一世紀末以資訊化建設（中共稱信息化）為主體的資訊基礎建設、資訊作戰、資訊戰略發展等所謂高技術條件下的軍事事務革新，至今已近十年。當國際間經歷 2001 年的「911」恐怖攻擊事件與隨後的阿富汗反恐戰爭，以及後續 2003 年美英在伊拉克所發起的「伊拉克自由」（Operation Iraqi Freedom）軍事行動，對中共的軍事現代化實為提供效仿與摹擬的絕佳機會。事實上，從中共內部大量的軍事研究報告中可證明，中共預期的軍事革新成果正是以美國為主要參考對向，再加入中共自己的風格和特色，以型塑其軍事現代化的重要面貌。[1]

此時，一個具爭議性的辯論正在產生中，即近期在台海兩岸與美國政府（尤其是敏感的軍事單位）間的網路駭客攻防，是否真為中共的「網路戰」（Network Warfare, NW）。背後的策略指導、執行部門與主要能力能否達到如資訊作戰中所定義的網路作戰效能？是否執行部門即是所謂的「網軍」？網軍的真實面目和實力為何？若不是網軍，那又是什麼？為何網路駭客攻擊或襲擾頻繁地在兩岸間進行？此為本文主要研究目的。在進行中共網軍相關分析之前，筆者認為有必要

[1] 就筆者研究所得，國際間軍事專家對於中共軍事現代化的主要內涵呈現多種揣測與辯論，焦點主要在於中共是延續舊蘇聯時期的軍事組構與科技成果，還是改採西方（尤其是美國）國家的軍事現代化模式以徹底轉型。此辯論持續至江澤民主政的後期則愈來愈明朗，中共軍委會及軍事政策研擬部門開始公開宣稱，中共軍事現代化的主要核心，是圍繞於具中國特色軍事戰略思想、環境及觀點的高技術戰爭能力的全面變革，而技術層面的學習與仿效方向是以後冷戰時期美軍數次對外軍事行動所展現的軍事科技力量的總和。

先釐清與本文有關的重要混淆：西方國家近期所發展的「網路中心戰」（Network-Centric Warfare, NCW）概念與「網路戰」有何不同？解放軍若真建置有網軍，則應與此兩概念相關連，或此兩概念可反應出以網路為戰場的積極與消極攻防思維。

貳、網路中心戰與網路戰之區隔

一、美軍網路中心戰概念

具體而言，網路中心戰是由美國海軍在 1997 年首次提出的概念，目的在於強化 21 世紀作戰組織效能的改變與轉型。從美國「國會研究服務」（Congressional Research Service, CRS）對國會提出的專案報告：《海軍網路中心戰概念：呈送國會的主要計畫與議題》（*Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress*）可理解美軍初期的網路中心戰概念。報告中指出，NCW 焦點在於藉由資訊科技（IT）的使用，而使海軍艦艇、航空器和岸置設施得以進入較高的整合型網路，充分、靈活發揮海軍各種設施之戰力。[2]美國海軍因此提出三個重要的發展計畫，以實踐 NCW 的整合效能。首先是「接戰效能整合」（cooperative engagement capability, CEC）計畫，其次是「IT-21」投入戰略，最後是「海軍-海陸內部網路」（navy-marine corps intranet, NMCI）計畫。

（一）CEC 計畫

CEC 計畫是以建構能連結海軍船艦和航空部隊的整合作戰系統為主，此將可支援在 CEC 網路裡，於特定地區執行作戰任務單位，均能獲得單一或整合型式的防空網路雷達資料，獲致跨平台的即時作戰資訊。簡言之，每一個 CEC 內的作戰單位都可從其他單位得到專屬的作戰資訊，以利迅速下達決心和反應。

透過 CEC，美國海軍可自裝載有反艦飛彈的船艦上發射防空飛彈，來防衛那些沒有裝載反艦飛彈或自身雷達尚未發現目標的 CEC 船艦，也可從其他船艦導引別處船艦或戰機的防空飛彈發射。美國海軍聲稱，CEC 是網路中心戰的核心要素（central element），可以大幅度提升戰鬥群體對於空中與飛彈防衛的巨大效能。CEC 系統在 1998 年首次進行測試，2001 接續實施系統軟硬體改良並完成最終測試，目前部署於美軍各大艦隊運作中。CEC 被海軍界定為具「戰術組合網路」（tactical component network, TCN）的功能，期望能降低單一作戰系統

[2] Ronald O'Rourke, *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress* (Washington, DC: The Library of Congress, 2001), p.CRS-2.

的間隙，並分享目標獲得資訊和火力支援的需求。簡言之，此可提升海軍單一作戰系統中各作戰單元的戰場存活率，並可充分調節戰場火力以支援各作戰單位達成任務。

（二）IT-21 計畫

IT-21 是美海軍因應 21 世紀作戰需求的戰術作業平台，提供海軍在「投入戰略」（investment strategy）時，能透過桌上電腦、資料連結與網路軟體而建立一套介於海軍船艦間的戰術和行政傳輸的內部封閉網路（intranet）。較特別的是 IT-21 可以傳輸文字、資料、地圖、影像、聲音與影片檔案，故為海軍特有的多媒體戰術作業平台。IT-21 概念是由太平洋艦隊司令部在 1995-1996 年所建構，美海軍相信，IT-21 可以顯著提升海軍的作戰能力，降低人員作業的數量及時間需求，並帶來多樣化的戰術與行政機能。[3]

故 IT-21 為美國海軍特有的內部網路戰術資訊平台，可在高度資訊安全需求之環境中提供作戰單位迅速而有效率地執行戰術任務。IT-21 的成功運用，使得美陸軍單位起而效尤，分別改善其現有的戰術區域通訊系統，以更靈活有效地應用資訊科技於戰場管理。

（三）NMCI 計畫

而 NMCI 是跨越海軍與海軍陸戰隊的整合型內部網路。此近似 IT-21 的內部網路系統，提供海軍陸戰隊能充分運用各種海軍 C^4ISR 的作戰資訊，與海軍保持綿密合作。畢竟，海軍陸戰隊是美軍開往世界各地因應爭端的先鋒部隊，為主要特戰兵力之一，故 NMCI 將可大幅增進海軍與海陸的協同作戰關係。NMCI 計畫在海軍與海陸各單位內共計建置 360,000 組電腦工作站，這些分佈在美國本土、夏威夷、關島、波多黎各、古巴關塔納與冰島的 NMCI 工作站，目的在於因應 21 世紀美國海軍的重要任務和威脅。2003 年 10 月第一批 42,000 組 NMCI 建置完成，同時，美國海軍也提出 IT-21 與 NMCI 的效能合併計畫，為海軍下一個八年建立戰術整合應用的願景。

二、網路中心戰的發展

由美國海軍的網路中心戰概念可知，美軍網路中心戰的發展主要是基於對軍事需求和作戰能力的評估上。如何藉由網路中心戰的新概念來填補美軍戰略、戰術決策者與其友軍間的間隙，是最主要之目的。網路中心戰是資訊時代作戰環境裡居於領導地位的作戰行動，2004 年美國「軍事行動研究社」（military operations

[3] *Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress* , p.CRS-4.

research society, MORS）曾經從網路中心戰的物質要求、程序、方法論、模型和模擬當中，詳細定義與分析 NCW 的重要發展，並提供美軍參考。[4]

綜觀之，網路中心戰的發展是相對於平台中心戰（platform centric warfare）而來。美軍早期的平台中心戰主要考量為朝向建立全環境與全行動的作戰平台為主。探究如何強化單一作戰平台的戰鬥能力，以贏得作戰。但是，網路中心戰打破單一作戰平台的概念，而進行全網路作戰環境的建立。

根據 MORS 的分析，NCW 的原則狀態是透過穩定、強大的網路戰力（networked force）增進資訊的分享與合作，並強化資訊與意識（認知）的質與量，以增進作戰訊息的分享。而行動的基本效能（effects based operations, EBO）原則是緊密維繫於 NCW，特別是 NCW 所形成的作戰效能。因此，基於效能強化原則，美軍在 2003 年後全面建構出 NCW 概念。具體而言，NCW 關注著幾個重要面向：[5](1)堅實的網路戰力；(2)資訊分享；(3)相互合作；(4)資訊的質量；(5)分享情況的意識；(6)自我同步；(7)指揮的速度與維持。換言之，比起以往，美軍認為現今處在一個更緊密聯繫的世界裡，因此也創造出許多直接或間接的機會和挑戰，以及相對應效果。此必須藉由網路資訊科技加以連結與應用。

三、美軍網路中心戰力的轉型

在美國陸軍戰爭學院 2007 年所發表最新一期《21 世紀戰略議題表列》（*Key Strategic Issues List, KSIL*）中，明確地指出美陸軍六項與全球部署與作戰機能攸關的重要戰略議題：(1)全球反恐戰爭；(2)軍事轉型；(2)國土安全/國土防衛/民事支援；(3)國家安全戰略/軍事戰略；(4)地面戰力部署；(5)地面戰力擴增與維持；(6)領導、人員管理與文化等六項。[6]而在軍事轉型方面，美軍地面部隊相當強調兩個關係到戰場網路應用問題，一是在網路環境的領導效能；另一個是網路環境的指揮和管制（戰場指管）。[7]美軍認為，具備衝突或作戰環境中的網路攻防優勢，是 21 世紀防衛力量轉型過程必須特別重視之處。尤其在未來的作戰概念裡，如何因應各種非正規的挑戰？如何提升穩定行動（stability operations）的能力？如何適應複雜地形（complex terrain）並全然控制？如何增加戰略快速反應

[4] Dennis Baer and kirk Michealson, *Operations Analysis Support to Network Centric Operations* (McLean, Virginia: Booz Allen Hamiltion Press, 2004), p.1.

[5] *Operations Analysis Support to Network Centric Operations*, p.6.

[6] *US Army, USA Army War College Key Strategic Issues List*（Carlisle, Pennsylvania: Strategic Studies Institute United States Army War College Press, 2007）, pp.1-13.

[7] U*SA Army War College Key Strategic Issues List*, p.6.

（strategic responsiveness）能力？如何擴張全球戰力態勢（global force posture）？如何強化戰場指揮能力（battle command）？這些美軍的轉型重點更必須在網路中心戰（network centric operations）的思維中予以建構出來。[8]

美國認為，現今的挑戰乃如何因應戰力的轉型，而此轉型必須視未來威脅與敵人加以綜合衡量。美軍最大的難題是此種衡量已超越之前的標準，所有威脅和敵人都成為潛在性而非立即性，此在戰力轉型考量上，總欠缺那一點說服力。因而，美軍提出軍事行動的分析程序，認為軍事行動必須由上而下地採取一致性的評估：[9]首先是問題的構成，此包含有利措施探討；再來是人力（組織）因素；方案（細節）；工具（可由既有資料獲得）；風險與不確定因素。最後產生評估報告。

網路中心戰則必須掌握四個關鍵領域：(1)物質領域（physical domain）；(2)資訊領域(information domain)；(3)認知領域(cognitive domain)；(4)社會的領域(social domain)。網路中心戰的物質領域所指的是橫跨不同環境的攻擊、防禦與演習。資訊領域是指建立、操作與分享資訊。認知領域則是檢視、意識、信念和價值所在，以及觀點的形成與決策的產生等。[10]由此得知，網路中心戰並非僅是戰術上的區隔或作戰行動之劃分，而是戰略層級的整合運用，且關乎非戰爭性之民間資訊資源的整合。類似之處，尚有 C^4ISR 之整合環境建構，此乃提供美軍新一代軍事思維的科技基礎，並據此引導出美軍軍事事務革命的具體作為。此亦為軍事轉型之重點。

網路中心戰的另一個重要轉變是由美國國防大學的一份戰場智慧與網路戰專題研究（*Battle-Wise Seeking Time-Information Superiority in Networked Warfare*）所描述。戰場的決勝因素始終在變化當中，隨著科技日新月異，戰場關鍵因素從人力到火力，又從火力著重到資訊力，現今又回到人力，只不過並非人數多寡，而是敵對雙方的腦力對決。此即研究中所訴說的：「從戰場火力到資訊力再到腦力」（From Firepower to Information Power to Brainpower）。[11]其強調現代戰爭的網路中心戰需求，也強調建構網路優勢以打敗網路敵人。所謂網路優勢主要在於軍事行動中的洞察與推理的整合，其次是將技術性的網路力量轉化為辨識力。目的在於超越軍事侷限的突破，建構戰場智慧戰力。此非狹隘的網路戰或駭客戰，

---

[8] *USA Army War College Key Strategic Issues List*, pp.6-7.

[9] *Operations Analysis Support to Network Centric Operations*, p.12.

[10] *Operations Analysis Support to Network Centric Operations*, p.13.

[11] David C. Gompert, Irving Lachow, and Justin Perkins, *Seeking Time-Information Superiority in Networked Warfare*（Washington, D.C: Center for Technology and National Security Policy by National Defense University Press, 2006）,pp.3-12.

而是將網路等同於整合性資訊的流動虛擬平台，此平台並不受限制，端視戰場需求與投入部隊或支援部隊多寡而定，更無距離與隸屬的刻板關係。

四、網路戰的定位

由對網路中心戰的認知再進入網路戰的層次，就較為清晰許多。網路戰乃屬資訊戰概念底下的一種攻防型態。1995 年美國國防大學 Martin C. Libicki 教授即已為資訊戰做出清楚界定，此界定並受到往後的研究者大量引用。Libicki 界定資訊戰區分了包含網路戰等 7 種資訊戰類型:[12]指揮管制戰（command-and-control warfare, C2W）、情資戰（intelligence-based warfare, IBW）、電子戰（electronic warfare, EW）、心理戰（psychological operations, PSYOPS）、駭客戰（hackerwar, software-based attacks on information systems）、經濟資訊戰（information economic warfare, IEW）、網際戰（cyberwar）。

基此，所謂網路戰是指敵對雙方針對戰爭可利用的資訊和網路環境，進行制資訊權的爭奪。通過電腦網路確保己方資訊和網路系統的安全，並蓄意擾亂、破壞與威脅對方的資訊和網路系統。本質上，網路戰是資訊戰的特殊形式，乃在網路空間進行一系列的襲擾、竄改、竊取、監視與破壞的作戰行動。與傳統戰爭相比，網路戰具有突然性、隱蔽性、不對稱性和代價低、參與性強等特點。

與資訊戰相同，網路戰也陷入似戰非戰的困境。資訊戰應是一種作戰概念的統稱，而並非是作戰行動本身；是在於描述軍事作為（應用）與資訊科技（介面）的整合效能，非實際對敵展開的武裝行動。亦即，武裝行動的本身，縱使大量採用資訊戰概念與技術，也不宜稱其為資訊戰行動；事實上應仍以作戰行動之目的賦予適當稱號（如伊拉克自由行動）。然而，網路戰出於資訊戰之概念，網路戰是否為一實際的作戰行動？此實與資訊戰相同，仍是藉由網路載台的攻勢或守勢概念，縱使有所損耗或破壞，仍無法界定為作戰行動。

因此，若因為駭客的蓄意破壞、阻礙、監視或盜取即稱之為網路戰，又稱其為網軍，在《武裝衝突法》等《戰爭法》之法理上難以被認可。[13]當然，如果所定義的網軍並非正式軍隊組織，而僅是類似軍隊般的暴力或恐怖份子，則就另當別論。故而，本文所強調與分析之重點並非在於實施網路攻擊的黑手是否具有官

---

[12] Martin C. Libicki, “What Is Information Warfare?” *Strategic Forum* (NDU INSS Press, Number 28, May 1995), pp.2-3.。論述資訊戰具多種作戰方式之文獻可參考：George Stein, “Information War-Cyberwar-Netwar,” Air War College, 1993; John Arquilla and David Ronfelt, “Cyberwar Is Coming!” *Comparative Strategy*, Dec 1993, pp.141-165.

[13] 劉正，〈網路戰的國際法應對〉，《山東社會科學》，No.3, 2006 年。

方或軍隊的身份，更非否認網路戰或網路攻擊的不存在，而是在於如何以較清楚的觀點來區分與看待網路戰，如此方能獲得正確的回應態度、方式及手段。

總之，資訊戰是資訊化戰爭的核心。網路戰是資訊戰的特殊形式，屬於資訊戰範疇。網絡中心戰是機械化戰爭形態向資訊化戰爭形態過渡的產物，是因為資訊網路的發展為工業時代機械化部隊注入活力而帶來作戰形態的更新。因此，無論是資訊戰還是網路戰和網絡中心戰，都離不開資訊技術的迅速發展，也離不開網路技術的應用與普及。[14]

參、中共國防現代化中的網軍虛實

一、中共網軍虛實

在 2003 年的 9 月 3 日，行政院資通安全會報宣布，在過去一個月內，國內發生多起電腦病毒惡意破壞事件。先是「疾風病毒」A 型入侵，接著變種 B 型、C 型、D 型，最後是 Sobig「老大」病毒接踵而來。據資通安全的觀察顯示，駭客已善於植入木馬程式並完成網路傳輸通路之建置，另被駭客當跳板主機除與國內各廠商（單位）通連外，同時與國外主機包括美國、英國、加拿大、日本、德國等 31 個國家通連。依照行政院說法：「此極可能是中共籌備中的「網軍」實施駭客資訊作戰的模擬演練，顯現中共的確有積極成立網軍的計畫。」[15]

另外，2003 年 9 月 15 日，我國行政院宣稱政府機關及企業數月來遭到中國大陸駭客組織有計畫的入侵，包括國防部、中選會等 88 家政府機關及企業內植入了「木馬程式」，企圖竊取重要資訊。隨即透過國內著名防毒軟體公司（趨勢）進行研析，確認此次駭客密集攻擊是中共網軍所使用的木馬與後門程式，總體歸納為三隻主要病毒變種，代號分別為 BKDR_NETBFX.A（網軍一號病毒）、BKDR_KOTN.A（網軍二號病毒）、TROJ_CONEDRPR.A（網軍三號病毒）。其中網軍一號與二號病毒為後門程式，網軍三號為木馬程式，而這些病毒工具就是我國刑事警察局偵九隊所公佈的「中國網軍」攻台所使用的主要駭客工具。[16]

上述兩例，均顯現出來自中共的網路破壞、攻擊的事實，也凸顯出我們刻意將其描繪成一種准軍事衝突的草率。網軍是否存在實仍待驗證，至少在共軍編裝

[14] 錢逢水，〈解讀資訊戰、網路戰、網絡中心戰〉，新華網，2004 年 7 月 22 日。http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/mil/2004-07/22/content_1626118.htm

[15] 行政院 國家資通安全會報，〈成功遏止駭客團體企圖大規模癱瘓我國電腦系統案〉，《資安論壇》，92 年 9 月 32 日。http://forum.icst.org.tw/phpBB2/viewtopic.php?t=1513

[16] 陽宜珊，〈對抗中國「網軍」防毒公司加入戰線〉，《東森新聞報》，2003 年 9 月 15 日。

與公開訊息上並無網軍蹤跡。職是之故，文本強調，看待中共的網路攻擊應回復到以技術面之研擬對策和控管為主，不應以空洞之網軍詞彙掩飾技術或必要軟硬體應變之不足。

簡言之，以現代資訊科技而言，網路為平台的攻防無時不在進行中。然而，資訊攻防的最大效果乃在於整合應用資訊及網路科技後的整體軍事力量提昇，如美軍的網路中心戰概念；而非僅見著網路內流通的病毒、攻擊程式或依此而單面作為而取代如網路中心戰的大型戰術系統的研製。資訊能力其實已成為另一種霸權競逐的環境，特別是應用於軍事力量上，更凸顯現今軍事霸權的主要特徵：全面、彈性而迅速的整合及反應軍事力量，以嚇阻、制壓敵人並主導戰場。美軍的網路戰並非僅是駭客攻防，而具體的網路中心戰更非僅是抽象的網路戰，這是在 1980 年代的早期資訓戰發展時期，就已經確認的差異及重點，實值得我軍事資訊部門參考。

二、美國的「網軍」？

2006 年 3 月 11 日，美國空軍部長 Michael W. Wynne 公佈，最遲在 2008 年即將成立「空軍網際司令部」（Air Force Cyberspace Command），美國空軍目前是以第 8 指揮部為臨時司令部，計畫將承擔有關培訓和裝備任務，目的是使美軍能夠在網際網路上或通過網際網路開展全球性行動（主要為對抗網路恐怖主義），有效掌控網路和太空資源，以保護軍用及民用網際網路的安全。[17]然而，中共媒體一致宣稱此為美空軍新成立的網軍部隊，將對中共及如伊朗、北韓等敵意國家或基地組織進行網路監控與破壞攻擊。實情為何？目前不得而知，然而，此既然為美國空軍第一個專門從事電腦網防衛的主要機構，而攻防作為均屬相同技術性範疇，中共提出嚴厲質疑其實是可理解的。

技術純熟的網路駭客能利用電腦網路的弱點，竊取或改變電腦裡的資料，以電腦病毒癱瘓電腦網路，或是以大量資料灌爆電腦。愛沙尼亞網路在 2007 年 5 月間就曾遭到大規模的攻擊，政府網站、銀行、學校以及其他機構被迫關閉。此為國際駭客所為？還是某國網軍所為？即便美國軍方已坦承，自 1990 年代後期以來，曾潛在地實施電腦網路作戰，如北大西洋公約組織在柯索伏戰爭時，曾對南斯拉夫發動電子攻擊。然而，網軍存在嗎？

如同中共近年不斷提升資訊網路攻防能力，蓋達恐怖組織也經常利用網際網

[17] Robert Lemos, “Air Force establishing cyberspace command,” *SecurityFocus*, 2006.11.03. http://www. securityfocus.com/brief/346

路招募信眾並密謀攻擊，美國近年來也不斷擴大本身的網路作戰能力。前駐中東美軍指揮官，目前已經退休的阿必塞德將軍表示：「我們得在虛擬空間裡競爭」。他指出：「在拿破崙時代，戰爭限於陸地與海上，現在我們不僅得在陸地、海洋、空中與太空裡作戰，我們也必須了解，虛擬領域是需要我們持續注意與警惕的作戰領域，僅僅留意是不夠的。」

質言之，網路攻防實隨著資訊與網路科技的普及運用而生，全世界皆然。此真實困境應如美軍般以實際行動展現出對抗的決心，以優勢科技水準與人才確保資訊網路的安全，並隨時給予還擊。

肆、中共網路作戰之戰略邏輯

就美國所掌握的訊息顯示，在過去十年中，中共戰略部門經常耗費大量心力與資源以精確觀察美國的國家戰略與軍事轉型的本質，且著手因應中。在 2003 年美國的「解放伊拉克行動」（Operation Iraqi Freedom）之後，解放軍戰略專家強烈建議中共政府不僅要緊隨美軍的「軍事事務革命」，更要加快進程追上美國。在 2006 年 RAND 的一篇《中共對美國軍事轉型的反應及對美國國防部的隱示》（*Chinese Responses to US Military Transformation and Implications for the Department of Defense*）中推論出，中共面對美國軍事轉型時，最可能的因應選項之一，即是進行網路作戰（一種近似網路中心戰的應用，並非僅是駭客攻擊）。其主要是依循著幾個重要變項的推論而來。[18]

一、中共網路作戰的國家安全考量

根據 RAND 的分析，中共回應美國軍事轉型第一要考量的是重要的國家安全目標。十六大後中共安全目標被明確地界定在政治穩定、國家團結和諧、廣泛的國家力量表徵、快速的經濟發展。但由於政治和經濟目標的糾葛，中共被迫在主要的政治、社會、經濟和國際等眾多挑戰間，分配其財政與和科技資源以因應美國的軍事轉型。[19]而國防現代化又會與重要的預算及經濟資源成長形成競爭。

---

[18] James C. Mulvenon, Murray Scot Tanner, Michael S. Chase, David Frelinger, David C. Gompert, Martin C. Libicki, Kevin L. Pollpeter, *Chinese Responses to US Military Transformation and Implications for the Department of Defense*(Santa Monica, CA.: PAND Corporation Press, 2006), pp.5-10.

[19] *Chinese Responses to US Military Transformation and Implications for the Department of Defense*, p.Xi.

因為自 1990 年代後期開始，國營企業無力償還高額借貸而導致政府銀行壞帳擴張，上升的社會不安也加添「國家安全」資源的競爭。[20]況且，為了使影響國防現代化成敗的較高教育和下層結構能獲得改善，財物募集壓力更為吃重。結果是，無論提升解放軍戰力的本質策略為何？回應的選擇則是被限定在具有較佳的政治利益上，被迫降低預算需求與執行成本，且受限於現有的科技層級並必須服膺於像是內部安定與政權鞏固的其他國家安全目標。

依據 RAND 的長久觀察，中共對美國軍事轉型的因應作為必須均衡於四個基本的國家安全目標：[21](1)政治上，確保中共的政權及維持內部穩定與國家統一；(2)經濟上，持續高幅度的經濟成長，特別是人民的就業保障和機會創造，提升收入水平，促進國際貿易與投資，加速科技現代化；(3)兩岸間，阻止台灣從中國長久（合法）分離，期望達成最終統一；(4)國際上，增加中國廣泛的國家力量，此國力概念不僅包括中共軍力的擴張，還包含經濟、外交、政治與「軟實力」的增強。此四點是中共各時期領導者難以反對的國家安全目標。

然而，當中共成功地追求國家安全目標過程中，某種程度也製造出一些障礙。例如，北京政府清楚地瞭解，若人民擁有較高的生活標準與教育水平，將可增加政府的合法性，但是其他發展中國家的經驗清楚地指出這些「人類資本」（human capital）的改善也會製造出更多難以控制的自我主義者及難以駕馭的平民。就 PLA 的觀點，這些人類資本的進步可以產生大量的尖端科技人才，同時也需要仰賴一系列的軍事現代化策略，但此也亦將逐漸擴大非職業軍人的招募與維持高技術資質士兵的成本和困難。

從中共國家安全目標可發現，當中共回應美國軍事轉型時，其主要的回應對向是美國，而台灣因素僅是其回應時的考慮變項之一。簡言之，台海情勢會影響中共國家安全狀況，也影響對美國軍事力量的回應方式和戰略。

二、中共網路作戰概念

中共 2002 年 11 月第四版的《國防白皮書》中除一貫地透過安全形勢分析，強調美國與台灣是未來必須因應的兩大長期和持續的安全威脅外，中共數次提出將以資訊戰（information warfare）和資訊作戰（information operations）來進行

[20] *Chinese Responses to US Military Transformation and Implications for the Department of Defense*, p.Xii.

[21] *Chinese Responses to US Military Transformation and Implications for the Department of Defense*, p.6.

其軍事戰略革新。[22]此引起美國與台灣高度關注，到底中共資訊戰的真實能力為何？隨後，美國國防部在 2002 年的《中共軍力報告》（*The Military Power of The People's Republic of China*）中也明確地顯示出對中共解放軍資訊戰力的擔憂。[23]有趣的是，接續在 2004 年的中共《國防白皮書》裡，異常地找不到資訊戰字眼，但「軍事事務革命」與「資訊化」卻出現超過 20 次之多。[24]無論如何，2002 年的中共國防白皮書顯現出解放軍對資訊科技的仰賴已朝向建設「多維戰場空間」（陸、海、空、天、電）邁進的企圖。[25]中共國防建設的資訊導向是非常的清楚的，在 2002 年國防白皮書中，中共明確將高技術的應用列入解放軍的首要建設，而 20,000 公里長的大西部光纖資訊網路也在 2002 年完成，據信中共全國光纖網路已全部建置完畢。

中共透過資訊化基礎建設的成果來提升軍事效能，尤其是資訊作戰與網路作戰能力，是值得高度關切的。在 2000 年 10 月，中共總參首次在北京近郊實施電腦網路與電子對抗演練，而自 2001 年開始，多數的解放軍部隊也正式將網路電子戰（network-electronic warfare）整合概念融入平日訓練中。中共解放軍到底會以何種資訊作戰或網路戰概念，應用在現在或未來的衝突同和作戰時空中，此不僅台灣至感困惑，就連美國也同樣關切。

中共軍事科學院在 2002 年向總參謀部提出專報，說明解放軍研究與發展網路電子戰概念的效能與急迫性。軍科院指出，整合網路電子戰應針對幾個重要關鍵著手：(1)資訊戰的矛盾處；(2)敵人的資訊戰重心；(3)網路最脆弱地方；(4)重要的資訊科技訓練；(5)達成資訊優勢；(6)界定資訊作戰及其他相關作為均保有中國特色。[26]基此可知，中共對於網路電子戰的整合運用正如火如荼展開。而值得關切的是，中共網路攻防會在何時啟動（此處非指駭客攻擊，因為駭客攻擊無所不在）？對手是誰？又為何採取網路攻擊？此實與其戰略邏輯有關。

三、中共網路作戰之戰略邏輯

從前析得知，美軍新一代軍事轉型是以網路中心戰取代舊有的平台中心戰。

---

[22] 中共國務院新聞辦公室，《2002 年中國的國防》白皮書，北京，2002 年 11 月

[23] Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2002*, Washington, DC.2002.

[24] 中共國務院新聞辦公室，《2004 年中國的國防》白皮書，北京，2004 年 12 月。

[25] Timothy L. Thomas, "Chinese and American Network Warfare," *Joint Force Quarterly*, Issue 38, 2003, pp.76-83.

[26] 戴清明，〈論整合型網路電子戰〉，《中國軍事科學》（北京：軍科院，2002），頁 112-117。

美軍透過網路與資訊高科技的使用，將作戰資訊整合於跨越時空的網路中心戰系統中。此轉型將使美軍戰力更向前躍進，相對地將阻礙中共晉升區域霸權的期望，且更加威脅中共軍事現代化的成果。

（一）網路作戰的戰略背景

中共對美國軍事轉型的反應主要基於國家安全目標的維護，並據以考量適當的回應策略與戰術。解放軍認為就傳統戰力而言，要與具有高科技戰力敵人對抗是必須步步為營，謹慎評估。根據解放軍《戰役學》的區分，中共將武裝衝突分成「戰爭」、「戰役」和「戰鬥」三類，戰爭是由數個決定性的戰役所組成，其戰略的本質乃直接關連到國家的政治、經濟和外交政策等。換言之，戰役是在有限的地域中進行與國家政治、經濟、外交需求有關的武裝行動。而戰鬥則是達成戰役目標的戰術行動。[27]自 1980 年代開始，特別是在美國「沙漠風暴」（Operation Desert Storm）行動結束之後，中共認為解放軍下一次面臨的戰爭絕非是總體戰爭（total war），而較可能是持續時間較短，地境與目標受限的有限戰爭。

此外，下一個衝突將包括強烈的使用尖端科技。此尖端科技顯現於偵察能力的改善和超越地平線投射能力的精準武器之上，以及能夠快速處理的情報流通能力，最後能達成區域優勢與對敵人的精準打擊。中共將這類型的現代戰爭概念化為集中在高科技條件下的區域戰爭。[28]

基此分析，現代戰爭侷限於較小的作戰地域與有限目標，必須具備高機動性與快速投射能力，故而比起總體戰，中共僅可能同時進行兩至三場戰役。為達戰勝目的，解放軍必須在短時間內做出決定，如同中共分析家所言：「在一個有限的高技術戰爭（high-tech war）中，行動的步伐是快速的，而時間短暫，一場戰役通常呈現打打停停的特徵。非常清楚地，戰鬥時的速度與決心要求，在此戰爭中將極為重要。」[29]

此種未來戰爭的特徵造成解放軍的戰略應用困境。解放軍承認要擊潰像美軍一樣的高科技對手是困難的。的確，中共軍事專家也認為，在可預知的未來，無論再怎樣提昇傳統武器系統性能，與美軍相較，解放軍的武器系統仍屬劣質品。[30]如《戰役學》中的說明：「這最顯著的真實情況是解放軍所面對的未來戰役，實際上是使用低等的武器與擁有高級武器的敵人較量。」[31]

（二）網路作戰的戰略構想：先制攻擊與積極防禦

---

[27] 葉徵編，《陸軍戰役學教程》（北京：軍事科學出版社，2001），頁 239。
[28] 《陸軍戰役學教程》，頁 239-240。
[29] 魯林祺，〈高技術有限戰爭中，先制打擊是具決定性的〉，《解放軍報》，1996 年 2 月 7 日。
[30] 彭光謙，《戰略學》（北京：軍事科學出版社，2001），頁 466-467。
[31] 王厚卿、張興業編，《戰役學》（北京：國防大學出版社，2000），第三章。

但是否此為中共一種延續自毛澤東思想的刻意示弱表象，實不得而知。縱使近年來中共加速國防現代化與新穎武器系統的建構，仍然未能明確證實中共的國防武力已逐漸趕上或可以與美國並駕齊驅。由於較低劣的軍事科技，中共被迫發展出一種「以劣勝優」的戰略思想。此種思想轉換為實際行動即是發展出避免與強敵正式接觸的不對稱作戰，而解放軍此類戰略構想最重要的支撐是奪取戰略及戰術主動權（seizing the initiative）。

由於高技術區域戰爭的勝敗決定在戰役初期能否掌握主動與反應速度是否快速。如一種可確信的主張指出：主動權可讓軍事行動保持自由，若喪失主動權，軍事行動必受影響；[32]對弱者而言，若待高科技敵人完全部署好後才開啟攻擊，則注定失敗。中共曾以 1992 年伊拉克在波灣戰爭的失敗提出建言，伊拉克如果能在聯軍戰力集結完成之前對聯軍展開攻擊，伊拉克應該能打敗當時的美軍與其他支援部隊。[33]由此可引伸至解放軍對台海衝突的戰略思維，在奪取主動權的概念下，中共勢必在軍事行動發起前，對台灣物質與心理戰力率先進行破壞，而也將對美國的干預與馳援行動實施干擾，至少是使美軍失去「先制」優勢，此般手段仍是在避免與美軍正面軍事交鋒的原則下進行。

如前析所見，奪取主動權是中共因應強敵的致勝關鍵，而此重要概念解放軍又將其界定成「積極防禦」，以符合中共的軍事思想及戰爭觀點。中共受中國傳統兵略的「慎戰」思維影響，認為軍事上的防禦作為才適合央央大國的慎戰與仁民愛物哲理。如孫子兵法的「兵者，國之大事，死生之地，存亡之道，不可不察也。」[34]又如「故上兵伐謀，其次伐交，其次伐兵，其下攻城。攻城之法為不得已。」[35]中國古老的軍事思想明顯地強調只有當領土首先受到攻擊時才予以還擊，但積極防禦的軍事行動是朝向掌握主動權的操作。因此，中共界定的積極防禦是戰略上採取守勢，而戰術行動上改採取攻勢。

（三）網路作戰的戰略目標

解放軍奪取主動的積極防禦概念的方法之一，是「確保對第一擊的支配」。[36]解放軍相信保有強烈的攻勢心理是積極防禦的必要條件，因此必須持續在奪取主動權上採取攻勢作為或尋求戰場致勝方法。而兩個重要方向是解放軍獲得支配

---

[32] 葉徵編，《陸軍戰役學教程》，頁 150。

[33] 魯林祺，〈高技術有限戰爭中，先制打擊是具決定性的〉，《解放軍報》，2003 年 9 月 16 日。

[34]《孫子兵法》始計篇。

[35]《孫子兵法》謀攻篇。

[36] James C. Mulvenon, Murray Scot Tanner, Michael S. Chase, David Frelinger, David C. Gompert, Martin C. Libicki, Kevin L. Pollpeter, *Chinese Responses to US Military Transformation and Implications for the Department of Defense*(Santa Monica, CA.: PAND Corporation Press, 2006), p.49.

第一擊的可能作為：一是奇襲，一是先制攻擊。[37]事實上，此兩種方法誠屬一體兩面，此莫非在強調解放軍軍事行動的致勝原則。奇襲為解放軍的行動態勢；先制攻擊為解放軍的行動時機。當然，行動速度、攻其要點（破機重心、重點打擊、攻擊節點、點穴）與攻其心理，是解放軍面對優勢敵人的不二法門，亦是所謂的不對稱作戰概念。[38]

中共在戰略避免直接與美國交戰而以攻擊美國軍民的弱點來替代之，此乃能達到爭奪主動的目標。依照此戰略，解放軍可能選定正確的資訊系統與平台實施集中式攻擊。美軍評估，較之地面設施，解放軍此一戰略目標較可能針對美軍的空中、飛彈與海上設施進行資訊與網路攻擊，尤其是較可能被忽略的特戰部隊，則是中共特別針對的對向。其理由至明，近十年來特戰戰力是美軍介入國際爭端的首要部隊，扮演開路先鋒角色，且更多是唯一角色。美軍認為此戰略亦為中共侵犯台灣時，為傳統兩棲進犯行動所鋪設的高技術作戰方式。

綜論之，就中共戰略中的傳統戰力觀察，中共若要攻擊美軍就必須先掌握以下幾個優勢。首先是發揮精銳武器效能，中共已具備龐大的傳統戰力可立即因應衝突，包括少數先進的武器平台，如蘇凱-27（Su-27s）、蘇凱-30（Su-30s）與基洛級(Kilo-class)潛艦；這些少數的精銳武器可被用來創造美軍或台灣的相對弱點，以彌補大量落後的武器系統對前述主動權和先制優勢等的失能。其次，是廣泛的使用科技，美軍確信經過多年努力，中共已具備部分重要科技優勢，只欠缺整合性運用和實戰測試。第三，在台海衝突或一些偶發的邊境糾紛案例中，基於戰力是運用在國土之內，故可除去與同盟間的信任要求；此也代表解放軍必須建立較大的防禦縱深，並將戰力分佈至較廣的地區。而此地理因素可能會限制空軍攻擊的效能，造成美軍必須危險地穿越敵人領空對散佈在廣大區域的重要目標進行攻擊。

質言之，中共清楚地瞭解到必須使用傳統的行動與高技術的網路作戰來合併進行重點打擊，但仍然欠缺在全規模的高技術戰爭中有效壓制美國的裝備和能力。儘管如此，解放軍仍建構出兩個可影響美軍轉型與面對台海爭端時的重要方法：第一，透過相關手段針對美國海、空軍設施，特別是航母運輸戰鬥群（aircraft carrier battle group, CVBGs）進行破壞，或是促使這些設施能拉大投射距離，迫使美軍必須實施遠距操作，加大部隊投射風險。第二，透過對美國太空設施的攻

[37] *Chinese Responses to US Military Transformation and Implications for the Department of Defense*, pp.49-48.

[38] *Chinese Responses to US Military Transformation and Implications for the Department of Defense*, pp.53-54.

擊，摧毀或降低這些目標的重要通訊連結，以阻斷美國必要之指管情資或中斷美軍的全球地位系統（Global Positioning System, GPS）。

四、中共網路作戰的戰略手段

如上分析，中共的回應必須在確保國家安全目標的條件下進行，故不得衝擊中共政權及不利國家統一；不得損及經濟成長與人民工作；不得促成台灣獨立；不得降低綜合國力。因而，中共提出幾點可能的選項以回應美國軍事轉型和軍事力量的挑戰。RAND 的評估指出，有四個可能的選項是中共未來的軍事現代重點：(1)增加傳統武力的現代化，包括：從人民戰爭到高技術條件下的區域戰爭變革，爭奪先制權，攻擊美國重心；(2)顛覆、破壞與資訊作戰；(3)飛彈中心戰略；(4)網路作戰等。其中，筆者必須以網路作戰為主要論述重點。中共特別強調其獨特的 NCW 戰略，此乃顯現自中共特有的科技、文化與組織脈絡。那到底中共網路作戰的真實面貌為何？

而飛彈中心戰是較激烈卻有效的手段，其秉持的仍是優異的衛星制導科技與飛彈載體和彈頭技術，此又間接與資訊及網路科技有關。惟使用飛彈中心戰就是選擇與美國正面交鋒，後果不堪設想。中共戰略家關注著該如何影響美國軍事部署，以回應美軍的軍力威脅時，中共遭遇當前傳統戰力的限制，即是缺少足夠能力來阻止美國向日本或其他地區（關島）實施軍力部署。傳統武器對美國而言其實並不具威脅，而核子武器的選項也僅具理論上的能力，儘管如此，在面臨衝突初期，核子武器仍不具使用價值。彈道飛彈系統則可混用傳統或核子彈頭，能用來攻擊日本或關島的美軍，但無論使用何種傳統彈頭都不確定能達到核子彈頭的類似效果。然而，光憑彈道飛彈有能力裝載核子彈頭且中共具有精確發射及制導能力，就足以名列有效的威懾性武器。[39]

根據對中共阻斷敵重心的戰略思維檢證，確信使用電腦網路作戰（computer network operations, CNO）來對台、美實施攻擊是可行的。第一是中共的資訊作戰部門相信，CNO 可以發揮難以想像的心理作用，尤其是對基礎設置與經濟活動的攻擊，更具削弱台灣人民意志的效果。第二是中共資訊戰單位判斷 CNO 可以有效地制止美國對台海衝突的介入，且在美軍抵達前，台灣可能因為基礎設

[39] Gerald P. Krueger and Louis E. Banderet, "Implications for Studying Team Cognition and Team Performance in Network-Centric Warfare Paradigms," *Aviation, Space, and Environmental Medicine*, Volume 78, Supplement 1, May 2007 , pp. B58-B62(1)

施的損壞與信心崩潰而放棄抵抗。[40]

在戰略階層，一般戰略分析家認為 IO 與 CNO 是中共用來彌補傳統戰力的空缺，且是具效力的（轉弱為強）不對稱選擇。就中共而言，電腦網路作戰是最具以弱擊強的效能，而 CNO 則是使用 CNA（電腦網路攻擊）進行點穴式的阻絕。[41]CNA 強調一種潛在的功能，如中共戰略制訂者所言，「我們必須透過電腦網路攻擊傳達給敵人一個訊息，以壓制敵人放棄戰鬥。」[42]對解放軍而言，CNA 擁有特別的吸引力，因為比起傳統武力，CNA 有較持久的投射能力。它讓解放軍能從較遠的距離與美國維持接觸和對抗。具中共戰略分析家的描述，「長距離的監視和精確、強力的長距離網路攻擊是我們軍隊目前能做到的。」[43]然而，美軍也認為中共 CNA 擁有可確信的高度阻斷與隱藏能力，足以供應解放軍的戰略應用。例如某些情報來源聲明：「針對中共來說，資訊戰爭是廉價的手段，敵國會因為資訊攻擊而麻痺指揮效能，終端設備透過資訊網路的接收，將難以分明是孩童的惡作劇還是來自敵人的攻擊。」[44]

需要重視的是中共的 CNA 準則乃要求解放軍瓦解和癱瘓目標，但卻不摧毀它。從心理與歷史角度觀察，CNA 戰略實接近毛澤東的「持久戰」理論，他主張：「我們必須盡可能地遮蔽敵人的眼睛和耳朵，使他們變得又瞎又聾，並且我們要盡可能地混淆其指揮官的心智，使他猶豫不決，最後贏得我們的勝利。」[45]解放軍內部訊息透露，「以電腦網路攻擊敵人武器系統核心和癱瘓 C^4I 系統，可對敵造成致命打擊。」再者，中共戰略分析家認為，利用此種攻擊方式還可嚇阻敵人或升高衝突成本到不可負荷的地步。尤其是將 CNA 使用在非軍事目標上，則能夠動搖決心，摧毀敵人戰爭潛力，是贏得戰爭的較高明的手段，最後達到崩潰對方民眾參與軍事對抗的意志。

伍、結語

研究中共的網路戰時，必先確認此並非是美軍所謂的網路中心戰；而美軍的網路戰效能也與中共的網路戰或狹隘的駭客攻擊大不相同。質言之，中共網路作戰能力正處於美軍資訊作戰中的網路戰與駭客攻擊中的過渡階段。就戰略而言，

---

[40] 樊國麗，朱蕊蘋，〈網路中心戰及其脆弱性分析〉，《火力與指揮控制》，Vol.32, No.1, 2007 年 1 月。
[41] *Campaign Studies*, pp. 173–174.
[42] 鈕利、李江中，〈資訊戰略的初探〉，《軍事科學》，Vol. 13, No.2, 2000 年 4 月。
[43] Campaign Studies, p. 170.
[44] 韋景成，〈人民戰爭新形式〉，《解放軍報》，1996 年 6 月 25 日, 版 6.
[45] 毛澤東，〈論持久戰〉，《毛澤東選集》，第二集（北京：外語學院出版，1961），頁 83。

尚無法整合運用於資訊攻擊的軟硬殺上，但戰術上實已具有單一系統的部分軟殺能力。此能力侷限在網路系統的資料竊取、竄改、監視與中斷，至於癱瘓、損毀及跨系統的重大破壞能力，據信中共尚在努力發展中。

另外，在台海局勢中，中共網路作戰具有兩種針對性的作戰目標，主要目標在於與美國軍事轉型對抗，並制止或遲滯美軍對台海爭端的反應；次要目標為心理戰術的應用，是針對台灣對抗意志的威脅，此為中共網路戰的附加價值。崛起後的中共，隨著經濟實力快速累積和成長，國家相關建設均朝向「寧大勿小」進行，在不影響政權穩定條件下凡事與國際接軌，唯一不接的是人權價值與政府統治的合法性。尤其是中共國防現代化，十多年來國防預算始終佔據國內 GDP 在 2.4%～5.5%的高比例之間，我們必須瞭解這些預算除了更新有形的軍事裝備外，更多隱藏在我們所無法察覺的資訊戰和網路作戰上。

其次，1991 年第一次波灣戰爭之後，中共確立以美軍軍事變革為師，極力效法美軍的資訊戰力建構。然而，短期內中共仍無法達到 91 年時的美軍水平，但解放軍朝向整合式資訊戰與網路作戰的努力是明確的。尤其現今美軍正進行高技術條件的網路中心戰，將原有平台中心概念轉換為網路中心概念。此種轉變，中共一方面想要制止、阻撓；另一方面，中共更想要學習仿效。據判斷，當中共軍事能力提升到一定水準時，網路中心戰將是其新的選項。

再者，網路作戰不僅是駭客襲擾，還具有資訊戰的軟硬體與資訊系統破壞能力。自 2001 年迄今，中共對美國及台灣的網路作戰練兵從不間斷，雖多數察覺的是一些來路不明的惡意程式，但相信中共已日漸具備網路攻防效能，而未發覺的網路破口可能也不在少數，此為我們應警覺與高度關注之處。如同漢和評論平可夫所言，網路戰爭是一場別具意義的「民間戰爭」，沒有固定的疆界、沒有前線後方、也沒有正式意義上的宣戰或停戰。但的確是一種衝突行為，因為這種行為可能招致巨大的損失。[46]

總而言之，戰略上，中共仍以國家安全目標為最主要考量，避免在刀口上與美交鋒，然而戰術上，卻不排除使用傳統武器，尤其是彈道飛彈（巡曳飛彈）威嚇台灣。此證明其戰略守勢、戰術攻勢的積極防禦信念。而在攻守勢之間，資訊戰及網路電子戰實是解放軍從無間斷的嚇阻手段，目的在於瓦解對手的意志，並尋找其戰力間隙。此重要發展值得我戰略與國防事務研究者密切關注，並謀求反制之道。

[46] 平可夫，〈中美網絡戰新人民戰爭〉，《大紀元》，2001 年 5 月 9 日。http://www.epochtimes.com/b5/1/5/9/n86540.htm

（投稿日期：96 年 9 月 18 日；採用日期：96 年 11 月 21 日）