淺析中共信息戰中之網路戰

作者／周明輝 少校

提要

一、電腦開闢了人類科技新紀元，預示了信息時代的到來。信息戰已成為信息時代下的產物，而今一種全新概念的網路戰伴隨著信息戰，悄然進入到這個世界，這種戰爭不見刀槍，卻是殊死搏鬥的戰場。

二、在 1999 年的科索沃戰爭中，使神秘的網路戰從虛擬走向現實。此場戰爭已完全凸顯出網路戰是信息時代下的一種新型態作戰樣式。

三、網路戰可區分為「全球網路戰」與「戰場網路戰」兩種。而中共提出各種網路作戰模式，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。

四、新的世紀網路運用日益頻繁，網路安全防護便顯得更是重要。當前網路已被廣泛應用於軍事和經濟等領域，網路安全已直接關係著國家安全。

關鍵字：信息戰、網路戰、戰場網路戰、網軍、網路安全、國家安全

壹、前言

當前高技術條件下的局部戰爭如何打，是世界各國軍隊所探索與思考的重要課題。1991 年，第一次波斯灣戰爭之後，高技術條件下局部戰爭的課題，便完全地凸顯了出來。現在的戰爭呈現出複雜多變的特色，精確制導武器、電子戰、網路戰等，皆是高科技條件下的作戰形式，許多軍事專家以不同的角度研究和論述了高科技戰爭的特點，使共軍完全地瞭解到高技術的重要性與威脅性，以及研究與認識高技術戰爭，皆必須以科學技術對戰爭作用的角度去著眼。目前影響軍隊戰鬥力的各種科學技術中，以電子技術、電腦技術、人工智能技術等為內容的信息技術，是具有核心與關鍵性作用的高科技，它對戰爭與軍隊的影響，是歷史上其它任何一種科學技術所無法比擬的。

自 20 世紀 80 年代末 90 年代初以來，世界軍事領域興起了一場新的深刻變革，被稱之為「新軍事變革」，主要背景是因為隨著以信息技術為核心的全新技術快速發展，對武器裝備的發展、軍事思想和戰爭型態的變化，以及軍隊建設與編制體制的調整均產生重大而深遠的影響。[1]人類的戰爭已進入了信息武器時代，信息武器是軍隊武器系統的骨幹，信息系統是軍隊的神經中樞，能夠掌握信息主導權的便能打贏勝仗。因此，信息戰的概念油然而生，制信息權的問題

[1] 熊光楷，國際戰略與新軍事變革(北京：清華大學出版社，2003 年 10 月)，頁 35。

便成為一個不得不認真對待的事情。[2]

20 世紀 90 年代網路科技之

發展和全球網路的聯通，使光纖或寬頻網路連接起來的網路空間迅速成為一個嶄新的作戰空間，而網路戰也隨著風靡全球。網路戰的興起和迅速發展，帶動整個信息作戰，並向人的認識體系、思維邏輯空間、意識型態領域，以及人的心理空間拓展；不僅如此，網路戰是一場在有限作戰空間內，以進攻性地行為奪取和達成信息優勢，從而影響、破壞敵方的信息站、信息系統與電腦網路的一種作戰形式，1999 年科索沃戰爭，南聯盟使用多種電腦病毒，組織駭客實施網路攻擊，使北約軍隊的一些網站被垃圾信息阻塞，部分電腦網路系統一度癱瘓；北約則透過反擊，致使南聯盟防空系統陷於癱瘓，也由於這場戰爭，使神秘的網路戰從虛擬走向現實。網路戰這場真正的「無硝煙戰爭」將蘊含在「有硝煙的戰爭」之中，並將貫穿於未來戰爭的全過程，成為高技術條件下的一種全新作戰樣式。[3]因此，這種觀點對於我軍認識與研究高科技術戰爭的特點、建立適應高科技戰爭需要的現代化軍隊與國防體制，都具有很重大的意義。

貳、本文

淺析中共信息戰中之網路戰

一、信息戰的概念與內容及網路戰的概念與範疇

信息戰的概念各國學者所下的定義皆有不同，依據美國國防大學教授林必奇(Martin Libicki)的說法，他認為目前信息戰仍未能下一個完整的定義，因為信息戰存在著幾種不同的形式，每一個形式都可歸屬於一種更大的概念範疇。林必奇認為信息戰的內容可包括指揮控制戰、情報戰、電子戰、心理戰、駭客戰、信息經濟戰與網界戰等 7 種。[4]中國大陸學者沈偉光認為，廣義地指對壘的軍事集團搶佔信息空間和爭奪信息資源的戰爭。狹義地指戰爭中交戰雙方在信息領域的對抗。[5]綜上所述，信息戰的概念可指對立雙方為爭奪對於信息的獲取權、控制權和使用權而展開鬥爭，它是各種高科技作戰運用的交互過程，其主要目的就是奪取信息優勢與制信息權。隨著各國對信息戰持續地研究，信息戰的內容也進一步豐富，如 2001 年美國陸軍出版《作戰要綱》中又增了信息保障、反宣傳、反情報等內容。日軍和印軍在其信息作戰理論中，也分別增加了電腦

[2] 張召忠，怎樣才能打贏信息化戰爭，2 版(北京：世界知識出版社，2004 年 6 月)，頁 272-273。

[3] 程漢華，張仕奇，網絡戰：沒有硝煙的戰爭，解放軍報(北京)，2002 年 4 月 24 日，版 11。

[4] Martin Libicki, “What Is Information warfare,” Strategic Forum(US: National Defense University) No. 28(1995), p.1-2

[5] 沈偉光，信息戰(杭州：浙江大學出版社，2000 年 10 月)，頁 9。

戰和駭客戰內容。[6]2003 年美國參謀聯合會議所頒布的 3-13 號《聯合信息作戰條令》(FM3-13)，將原有的信息戰 5 項內容包括電子戰、網路戰、心理戰、軍事欺騙與作戰安全，又加入了網路攻擊、網路防禦與網路開發三種核心內容，[7]顯見信息戰的作戰樣式是不斷在增加與變化的，如此更加凸顯出網路的重要性與威脅性，使網路戰在信息戰中的地位變得日益重要。

網路戰的形成是因為隨著電腦技術為核心的信息技術迅速發展，電腦網路開始向全世界各角落輻射，網路的觸角已伸向社會各階層領域，而全球信息網路的建立，超越傳統的地理空間，形成所謂的「電腦網路空間」，使得信息網路成為信息戰的重要攻擊對象；因此，網路戰的作戰樣式孕育而生。電腦網路戰是以電腦網路為主要的攻擊目標，以先進的信息技術為基礎，在整個網路空間進行各類電腦網路攻防作戰的總稱，[8]它與電子戰在根本上是有區別的，某些學者專家會將電腦網路戰與電子戰認為是相同的作戰樣式，其實兩者是不可以混為一談的。(如：表一)

表一　電子戰與網路戰兩者差異對照表

作戰名稱 / 側重內容	電子戰	網路戰
作戰目標	針對信號層次	針對信息系統
作戰重心	側重於信息傳輸環節	側重於信息處理環節
作戰形式	正面進攻，以電磁能量對抗	迂迴與正面攻擊兼具，以各種方式滲透至敵方系統；亦可採實體攻擊

(資料來源：戴清民，信息作戰概論，(北京：解放軍出版社，2001 年 10 月)，頁 15-28。)

電腦網路戰是在現今特定的時代背景下和技術條件下出現的一種全新作戰樣式，而且美國國防部也曾提出「網路中心戰」的術語，描述各種軍事行動的

[6] 陳勇，姚有志，面向信息化戰爭的軍事理論創新(北京：解放軍出版社，2004 年 11 月)，頁 161。

[7] Headquarters Department of the Army, "Information Operations:Doctrine, Tactics, Techniques, and Procedures," Field Manual(Washington, DC: Headquarters Department of the Army)No. 3-13(2003), p.14

[8] 沈偉光，中國信息戰(北京：新華出版社，2005 年 1 月)，頁 230。

實踐途徑皆可透過網際網路發揮其作戰效能，[9]當前中共軍方媒體對網路戰做了不少評論，認為網路戰區分為廣義與狹義兩種。廣義網路戰是全球網路戰，是指國家或集團運用國際電腦網路進行政治、經濟、軍事等鬥爭；狹義網路戰是戰場網路戰，是指交戰雙方運用戰場網際網路進行對抗。[10]

網路戰的作戰樣式隨著電腦日趨普及與網路不斷延伸，一些意外事件與犯罪活動所造成的嚴重危害，已經使人們意識到，即使有意或無意的對公共電腦網路破壞，也可輕而易舉使電腦網路普及的國家難以招架。電影「終極警探 4.0」的內容情景，可充分表達出電腦網路的可怕性。又例如 1991 年，美國一位農夫在掩埋死牛時，挖斷一條光纖電纜，導致美國聯邦航空管理局所屬 30 個主要空中交通控制中心其中 4 個關閉長達 5 小時，可見電腦網路對日常生活影響甚劇。由此可見，由於網路技術迅速發展，使整個世界正在發生一場極為巨大的變革，這種網路化的趨勢已然對政治、經濟、文化和等各領域產生重要影響，從而使各國在相關方面發展競爭中展開激烈角逐。目前，世界各軍事強國為了能在未來網路化社會的爭奪中佔據主動，皆已紛紛採取措施，努力加緊網路化建設，以便逐鹿網路戰場，力佔先機。[11]

二、網路戰的特點與作戰手段

網路戰是特定時代背景與技術條件下出現的一種全新作戰樣式。與其他作戰樣式相比具備下特點：

(一)作戰力量廣泛

信息技術的軍民通用性和電腦網路相互關聯性，使作戰力量廣泛化，無論是國家、地區、組織、集團或個人，不管是軍人或百姓，只要具備電腦知識，掌握一定的網路攻擊手段，都有可能介入其中。作戰力量日益廣泛化，使網路戰發生可能性增加，而且使網路戰變得異常複雜，由於在網路空間難以確定攻擊者發起攻擊的時間，以及真正企圖與實力，甚至受誰攻擊還毫無察覺。

(二)知識性作戰手段

網路戰與傳統作戰操縱的武器不同，其操縱工具是鍵盤、滑鼠，利用豐富的電腦專業知識，尤其是入侵電腦網路與傳播電腦病毒等方面的技能來作戰。此為網路戰手段有別於傳統作戰，且具有高智能性。少數智能高的人，以電腦工作站與數據機就能危及他人生命，並給經濟、交通、金融或其他基礎設施造

[9] 劉鵬，王立華，走向軍事網格時代 (北京：解放軍出版社，2005 年 5 月)，頁 100。

[10] 新華網，美軍網路部隊作戰能力超強，努力打造駭客部隊，2007 年 6 月 21 日，http://blog.xuite.net/nisaa.guardian/nisaa/12210758

[11] 祝利，軍事強國逐鹿網絡戰場，解放軍報(北京)，2002 年 5 月 22 日，版 11。

成巨大的破壞，知識的重要性不亞於武器與戰術，此說明這種知識的作戰手段所具有的巨大威力。

(三)作戰空間廣闊

網路戰是不受地域約制的，只要是網路空間能到達之處，都是網路作戰可及的範圍，都是其作戰空間。因此，網路戰將更加抽象與廣闊，使傳統作戰概念變得不適用，作戰界線越來越模糊。如國家的地理界線將失去作用，很難界定網路攻擊來自何處？也因為國家的地理界線、距離失去作用，所以網路系統所能到達的地方都是其戰場，無論本土目標與戰場目標都一樣易受攻擊。

(四)作戰時間連續

網路戰不受任何外界自然條件的干擾，沒有天候因素的限制，沒有地理環境的影響，沒有黑夜與白天的區分，其作戰時間是具有連續性，亦可說是全天候、全時程的連續作戰。因此，網路戰已淡化戰前、戰後等時間概念。

(五)作戰過程短暫

網路戰不同於傳統的雙方物質、力量、智力的競賽，而是具實質意義上的知識力競賽。攻擊效果不受時間與距離的影響，而具有光速傳輸、瞬時到達的特性。當一方對另一方實施網路攻擊時，就會對其政治、經濟、科技、文化、軍事系統造成影響與破壞，使整個戰略態勢發生急遽變化。因此，網路戰的過程會在很短的時間內完成，也許幾十分鐘、幾分鐘甚至幾秒鐘而已。[12]

網路戰的地位與作用已不容小覷，以網路為平台來實施的作戰樣式，已造就網路戰的絕對優勢，網路戰的出現已是一種不爭的事實，其已成為一種對未來戰爭勝負具有全新影響的作戰手段，網路戰進攻的目標除指向敵方軍隊與軍事設施外，尚包括關係國家經濟命脈的政治、經濟、金融、商業及軍事網路相連接的公共網路系統等非關係軍事潛力發揮的軍事目標。[13]綜觀這些年來世界各國對網路戰的研究與實戰情況，網路攻擊主要體現在以下幾個方面：第一、駭客攻擊；第二、病毒傳播；第三、通道干擾；第四、節點破壞；第五、邏輯炸彈；第六、飽和攻擊；第七、弱點攻擊等，[14]現針對網路作戰手段分述如下：

(一)電腦病毒傳播

電腦病毒係指能夠竄改正常運行的電腦程式，破壞這些程式的有效功能，

[12] 李顯堯，周碧松，信息戰爭(北京：解放軍出版社，1998 年)，頁 151。

[13] 張俊勇，劉恩亮與康永升，「戰爭新空間：從科索沃戰爭看國際互聯網對未來作戰的影響」，現代軍事月刊，(香港：中國國防科技資訊中心)，第 10 期，1999 年 10 月，頁 28。

[14] 梁華傑，「網路戰資訊安全探討與省思」，國防雜誌，(桃園：國防雜誌社)，第 23 卷，第 2 期，2008 年 4 月，頁 111。

並且能複製與侵入其他程式中，使周圍的電腦程式亦遭到破壞。[15]程式遭到破壞，工作就受到影響，電腦病毒實際上就是專門用來破壞電腦正常工作時的特殊程式，其破壞的方法有：傳染性、潛伏性、隱蔽性、破壞性病毒等。

軍事領域最容易感染電腦病毒或受病毒破壞的武器裝備可區分：第一、各種軍用指管系統。如：C^4I系統、電腦網路、雷達系統，以及各式感測器等。第二、由電腦控制的各種高科技武器系統。如：現代化的飛機、艦艇、坦克、導彈等裝備的自動駕駛、火控、導航系統等。電腦病毒之所以危害是因為信息共享、信息交流與網路開放性。電腦網路彼此互聯相通，就有可能發生病毒感染和入侵與攻擊，尤其是軍事信息系統的核心設備與信息武器裝備的關鍵裝置，都將成為病毒進攻的主要目標。根據網路防毒專業公司趨勢科技分析，中共的「網軍」可能使用的木馬與後門程式可歸納為 3 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)與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。[16]

(二)網路駭客

駭客原泛指那些熟悉掌握電腦知識與技能的電腦迷，現在則是指非法使用電腦系統進行犯罪活動者。目前駭客入侵網路的方式令人防不勝防與膽顫心驚，而中共網路戰部隊就會成為駭客侵入敵方指揮網路系統，隨意瀏覽、竊取與刪改有關資料或輸入假命令與假情報，破壞敵方整體作戰自動化指揮系統，使其做出錯誤的決策，此種駭客的手段對網路必定會造成一定程度的影響，甚至嚴重的損失。網路駭客使用的技巧，的確是未來網路作戰所必須具備的，在客觀需要上，提高網路安全性亦是網路戰重點所在。

駭客進入網路的方式可區分：第一、強行進入。即利用掌握的電腦技術，透過技術手段進入敵方的網路系統，也是目前駭客最常用的方法。第二、利用擄獲器材進入。指在戰場上直接通過俘虜隨身攜帶的通信器材進入敵方的網路系統，此將隨著部隊的數位化越來越有可能。當前中共駭客分成數群不同的聯盟，包括國際駭客聯盟、歲月聯盟、駭客基地等，約有 250 個駭客團體，中共當局容忍甚至鼓勵其進入與干擾外國電腦網路。[17]由此觀之，中共駭客撰寫惡意程式來攻擊他人網站或電腦的能力已經越來越強。

---

[15] 朱幼文，馮毅與徐德池，高技術條件下的信息戰，2 版(北京：軍事科學出版社，1997 年)，頁 311。

[16] 楊曉欣，中共網軍對我資訊安全威脅之探討，2008 年 1 月 14 日，www.tcivs.tc.edu.tw/public/tcivsdata/20081144249438.doc

[17] 自由時報，美國國會警告：中國精密網路戰威脅大增，2008 年 11 月 22 日，http://www.taiwanus.net/news/news/2008/200811212144301144.htm

(三)節點破壞

連接在網路上的每一個電腦設備都稱為網路節點，它可能是人們常使用的個人電腦、工作站與伺服器等電腦在網路上的電腦，也可能是用來管理網路的路由器，上述網路節點都是網路戰可能攻擊的對象，一旦節點被破壞將無法接收與傳輸任何資訊。

(四)通道干擾

通道(Tunner)技術是指在 A、B 兩個網路之間建立一個網路連線，A 網路裡的封包經過一連串的封裝，將原本的資料封包以另一種方式(另一種通訊協定)包在另一串資料流中，接著才透過這個網路連線送到 B，等封包送到 B 網路後再將其解開，恢復成原來的樣子。透過對通道的干擾將造成網路上資料無法有效的傳送。

(五)邏輯炸彈

為一種任務導向的惡意程式，可被設計成獨立運作而不需與原攻擊方聯繫。一旦資訊系統及電腦被植入邏輯炸彈，可於特定的時間或條件下，自動發作而破壞資訊系統及電腦。

(六)飽和攻擊

使被攻擊之目標產生大量的垃圾資訊，以消耗其網路寬頻或系統資源，讓其減低或喪失功能。

(七)弱點攻擊

利用被攻目標的系統弱點或電腦弱點所進行的攻擊，使其系統發生錯誤，造成被入侵或是當機。

三、中共網路戰部隊的發展趨勢

從上述網路戰的概念、內容、特性與作戰手段，可以清楚地瞭解到網路戰的影響性與嚴重性，而中共網路戰的攻擊，所依靠的就是其所成立的網路戰部隊，即所謂的「網軍」。「網軍」一詞最早是在1999年中國軍方「解放軍報」的一篇報導中，該報當時呼籲，應該在陸、海、空軍之外，另外再新增一個軍種，來負責網路防衛與攻擊的任務。目前中共的「網軍」隸屬於1985年成立的「國家信息安全工作領導小組」之下，有嚴密指揮系統，組織相當龐大，「網軍」為展現效率，會採取輪班方式攻擊，在深夜時也有專責攻擊西方國家的小組在運作，「網軍」的分工是細密的，這批「駭客部隊」主要負責打「不見血的戰爭」。[18]雖然中共「網軍」是其軍方系統培育的網路駭客；然而，這些駭客

[18] 大紀元，中共網軍主打不見血戰爭，2007 年 11 月 10 日，http://www.epochtimes.com/b5/7/11/10/n1896729.htm

仍不算正規解放軍成員。直至2002年開始，中共「網軍部隊」(Net Force)由解放軍與國動委託民間IT、產、官、學界的信息民兵共同組成。[19]

當前中共對於「網軍」的訓練主要分為兩個階段。第一階段由共軍的軍事院校培訓；第二階段則具體藉由演習把知識轉化為實際操作能力。美國國會的「美『中』經濟與安全檢討委員會」(U.S.-China Economic and Security Review Commission, USCC)，認為中共「網軍」的「網路戰」作為已由「防禦性」轉變為「攻擊性」。在2007年的《中共軍力報告》當中，美國國防部更是以相當篇幅說明了中共「電腦網路作戰」。報告當中說：「中共的『電腦網路作戰』概念」包括電腦網路攻擊、電腦網路防衛，以及其它電腦網路的使用。雖然共軍目前似乎沒有正式有關『電腦網路作戰』的準則，但顯然共軍已經將『電腦網路作戰』當作獲取早期戰爭當中『電磁優勢』(electromagnetic dominance)的重要手段。2005年，共軍已經將『電腦網路作戰』融入了演訓當中，特別是發展攻擊敵人網路的第一擊能力之上」。[20]上述的內容中已表明，美國對中共網路戰的持續發展現狀已感到憂心。

中共除了有正式編組的「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，有些已具有相當規模，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，可以進行網路攻擊與防護、雷達偵察等演練。中共亦曾規劃「四大電戰網」，其中「華東」電戰網專司對付台灣。通常來說，預備役部隊能夠進行「網路戰」訓練的地區，就是能匯集大量高科技人才與相關硬體設施的地區，如屬於經濟特區的廈門就被視為對台進行「網路戰」的重點地區。[21]

中共網路戰的發展已不可同日而語，其網路戰力持續增長已嚴重威脅到美國。根據英國媒體報導，美國國會「美『中』經濟與安全檢討委員會」表示，中共網路戰能力不斷提高，可以利用網路戰能力打亂美軍的全球部署計畫。該委員會還表示，中共的網路戰能力，可能使中共得以在局部戰爭中取得優勢。據該委員會發布的報告指出，美國政府、國防企業與商業部門頻頻遭到來自中共電腦的遠端攻擊。這種遠端網路戰能力可以讓中共「隨時對世界上任何地點發動網路攻擊」。報告中透露，2007年美國共有五百萬台電腦遭到攻擊，美國

[19] 廖文中，中國網軍：國安、公安與解放軍，全球防衛雜誌(台北：全球防衛雜誌社)，第 271 期，2007 年 3 月，頁 2。

[20] 鄭大誠，中共網軍的發展與評估，2008 年 4 月 27 日，http://tw.mybolg.yahoo.com/jw!0RhCSD.LHwIcZmpXnmtWD_6tdQ--/article?mid=319

[21] 同前註。

網路共遭受到四萬三千八百八十起大規模網路攻擊，攻擊總數量比2006年增加了三分之一。此外，該報告也警告說，中共發動網路戰的能力「非常嫻熟」，美國可能無力阻止甚至無從察覺(網路間諜活動)。[22]

中共在網路上的間諜活動儼然已成為未來的一個主要戰場，而許多被攻擊的商業網站甚至渾然不知。2002年以來，中共的網路間諜活動不斷增加，美國的國防部與政府部門的電腦網路也遭受過持續性的攻擊；不僅如此，近幾年來各國的政府與商業網站也有曾遭到中共網路攻擊的經驗，所遭受攻擊的國家包括澳洲、南韓、英國、法國、德國等。可見中共在網路戰上的實力已今非昔比。以下是近幾年各國政府與商業網站曾遭駭客攻擊事件，依年代日期先後所整理的一覽表(如：表二)

表二　各國政府與商業網站遭駭客攻擊事件一覽表

報導媒體	年代日期	事件
澳洲 《Fairfax 報》	2008/2/10	中國電腦黑客對澳洲政府機密電腦網路發動攻擊。中共當局據說是在蒐集澳洲的軍事秘密、澳洲公司對媒炭和鐵礦等資源的要價。
南韓 「聯合新聞通訊社」	2008/1/1	南韓軍方透露，被懷疑有可能是中國人的第三國駭客，透過向南韓官兵個人電子信箱發送含病毒的郵件，並盜取和瀏覽儲存在南韓軍方電腦的軍事情報資料。報導指出，中共當局於 2000 年設立了一支專門進行網路攻擊和擾亂情報等規模練的「Net force」戰隊，目前中國約有 100 萬名被稱為「紅客」(red hacker)的駭客組織。
香港 「明報新聞網」	2007/12/1	英國軍情處五處總處長埃文斯向英國各大銀行、會計師皮律師樓共 300 名商界領袖及保安首長發出密函，指中國黑客正入侵英國各大銀行和金融公司電腦系統，竊取商業情報。這是英國官員首次直接批評中國電腦間諜活動。
《紐西蘭報》 THE DOMINION POST	2007/9/11	紐西蘭安全調查局主管 Truker 對外宣布，政府的電腦系統被黑客襲擊，並被安裝了難以檢測的木馬程序，導致信息外洩。Truker 說他有證據顯示這次襲擊來自一個國外的政府，但目前他不想討論是哪個政府所為，不過據加拿大安全機構指出，這是中共間諜所為。

[22] 共軍網路戰力破壞美軍全球部署，青年日報(台北)，2008 年 11 月 26 日，版 4。

法國 《世界報》	2007/9/8	法國國防秘書長德隆說，法國政府的電腦網路曾遭中國黑客入侵。黑客入侵在法國總統薩爾科齊當選後開始，而黑客的「來源地」和入其他國家的黑客一樣。
英國 《泰晤士報》	2007/9/6	一名政府消息人士告訴《泰晤士報》:「中共正從事有敵意的情報活動，他們集中於電子手段以獲取英國國防部和外交部的機密。他們在科技上相當先進，並且擅於此道。」
英國 《金融時報》	2007/9/3	美國國防部五角大廈 6 月份曾遭受到網路黑客嚴重攻擊，致使國防部隊蓋茲辦公室的部分電腦系統關閉一週。一位熟悉此一事件人事表示，「有非常高的把握，幾乎達百分之百肯定」，中共軍方應為此事件負責，來自中國不同地點的駭客。一名前美國國防部官員說，中共軍方也滲透進入美國軍火公司與智庫的電腦網路。
德國 《明鏡》周刊	2007/8/26	《明鏡》周刊以「黃色間諜」為封面故事，引述德國情報單位「聯邦憲法保護局」的報告說，2007 年 5 月起，德國聯邦總理府、梅克爾總理辦公室、外交部、經濟部、學術研究部等政府部門的電腦內，發現來自中國蘭州、廣東和北京的木馬程式，夾帶來 Word 和 Power point 的檔案，意圖竊取機密，幕後黑手指向中共人民解放軍的情報單位。

(資料來源：陳祐欣，現代版木馬屠城，中共以網路向全球開戰，看雜誌雙週刊，(台北：華人希望文化事業，第 9 期，2008 年 4 月)，頁 3-4。)

四、面對中共網路戰我之因應作為

(一)確立網路安全防護觀念與強化網路系統管理機制

在中共「網軍」日趨密集的攻擊下，我國一般民眾卻缺乏憂患意識。當前在網路建設與管理中，人們的傳統觀念上普遍存在「重建設、輕防護，重使用、輕管理」的模糊認識，這種錯誤觀念很容易對國家安全帶來嚴重威脅，一些政府單位人員還因為擔心發生重大資訊問題後需要檢討，因而要求內部保密。不得對外張揚，欺瞞的結果往往擴大了中共對我「網路戰」攻擊的威脅性，這樣的逃避態度是非常不正面的。因此，要做好網路安全應從提高網路安全意識與強化網路保密觀念開始做起，確立網路安全管理人人有責的觀念。[23]

[23] 閻慶森，劉偉，聚焦網絡安全管理，解放軍報(北京)，2002 年 1 月 16 日，版 11。

為有效防制中共網路戰，加強網路系統防護就成為確保我軍網路系統的基本目標。中共的網路戰會滲透到各項網路操作系統與數據庫系統等，都有可能針對網路系統的安全漏洞與脆弱性，進行網路攻擊，造成我軍在網路系統方面受創。因此，我軍在網路系統的漏洞上應該具備一整套安全防護措施與管理體系，方能抵制中共網路戰攻勢。目前我國行政院已建立「國家資通安全會報」，並著手進行相關資通安全防護工作，國軍各級單位也已建立「CERT」防護機制，使強化資訊安全的管理。網路安全系統的預防工作是不嫌多的，當前我軍仍可持續強化網路安全管理，如監偵與反偵蒐全軍節點能力，預防指揮管制機能遭到破壞，提升各項資訊系統的安全防護網，並建置安全的通資作業環境，以及研發不易破解之加密技術，以確保資料安全等。

(二)培訓網路戰專業人才

人才素質與能力的培養不只是口號，必須要去付諸實行。首先，必須建立培養網路戰人才的新思維。我軍既然決心追求「全募兵制」的兵力結構，鄉網路戰區塊的部隊組建與結構性，就必須要培養與編成真正「網路戰精英」，將網路人才素質作為網路戰戰力的評鑑標準；再者，我軍必須致力於留住現有軍中的網路戰人才，應採取充分尊重專業的作為，提供軍中發展的利基，避免產生網路戰人才流失的不良後果，如此，方能確保網路戰精英能夠立即投入「網路作戰」的行列，使網路戰得以真正成為全民國防的一環，化為新世代國防的堅實戰力。[24]當前在推動「全募兵制」的同時，應在各行各業吸收網路人才，對於現役志願役軍人中有網路專業者，可增訂特別法或修訂現行任職條例，使其延長軍中服役時間，成為具備領導能力的網路專業幹部，甚至進一步改進動員制度，建立產、官、學界合作機制，廣泛吸收編組「非常規網路戰隊伍」，在社會乃至全球範圍內擴充，蓄積網路戰能量。[25]

(三)透過通資電兵監學校與各軍事院校強化網路戰專業教育

目前陸軍通信電子資訊學校的軍官分科班、士官高級班與正規班教育，國防大學陸軍指參學院、戰爭學院等基礎與深造教育班隊皆有教授相關通資電課程。然而，囿於受訓時間的限制、其他教育課程時數的安排，以及T評制度的影響，可能會造成學員在學習網路專業上不夠專心，若能建立專門的網路戰專業教官培訓班隊，對國軍各單位網路人才進行戰術戰法教育、技術訓練與戰技融合教育，使其能發展出更具組織與系統的網路戰，而國防大學方面可開設網路

[24] 梁華傑，培訓網路戰人才應有之新思維，青年日報(台北)，2008 年 12 月 7 日，版 5。

[25] 新華網，透視台軍網路戰的新戰略思想，2008 年 8 月 26 日，http://big5.huaxia.com/gate/big5/blog.huaxia.com/html/02/8402_1198.html

戰精英深造班或由國防大學與民間大學策略聯盟，選拔人才進行培訓與留用，使其成為具備領導網路戰部隊的網路戰精英。[26]

(四)編組網路戰專業部隊與建立病毒資料庫

面對中共「網軍」病毒攻擊，基本反制作為即透過防毒軟體與及時掃描進行基本防護，這也是最有效的防範病毒方式，使用電腦時應注意勿隨意開啟來路不明的執行檔案，以免被植入木馬程式並開啟後門程式，導致機密外洩。若電腦感染後門或木馬程式時，國家資安單位應協助支援，深入過濾與追蹤病毒來源，若發現是中共「網軍」所為，可思考進行反情報並且利用為散佈謀略情報的管道。[27]此外，欲解除「網軍」威脅不能只是被動，我軍應該可以考慮仿效其它各國，由精通網路戰的軍人與專家組織一支網路專業部隊，保障國家與軍隊的網路安全，反擊他國的資訊入侵，防止他國的網路犯罪活動，並且能夠及時補救網路上所發生的事故，以確保網路上的安全。另外，國防部也可在行政院之下成立一個專門的病毒資料庫，蒐集各式可能造成社會不安的重大性病毒，同時配合各大學術機構研究的成果，把各種病毒的特性與功能做一個詳細的分類與管理。如此，國軍能在最快的時間反應，找出威脅國家與軍隊的病毒類型，並且予以解除。

參、結論

中共網路戰的發展已具規模，但一些專業人士卻認為，雖然中共「網軍」發動的網路攻擊的頻率很高，但從網路技術來看，入侵的手段多只是一些加密的網頁上動手腳，或者造成該網站「擁堵」(jamming)，致使他人難以連上特定網站(特別是美國與我國的國防部)，但是並沒有真正地侵入重要網站的內部機密，尤其難以進入國防部以及其他軍事機構的加密系統之內；況且，軍用網路與民用網路是分開的，如果不從軍隊內部，而由一般網際網路來攻擊軍網，通常是不大可能成功入侵的。因此，就整體而言，中共「網軍」還難以造成真正的實質性破壞；此外，因為中共沒有自己的電腦作業系統與硬體製造技術，所以中共在發展「網軍」上仍然面臨了不少實際困難。[28]

儘管如此，就國家安全層面，網路攻擊依然是一種強大的軍事武器，當我方電腦遭到攻擊，整個作戰系統就會癱瘓，敵方可以在戰前就先癱瘓我方的通

[26] 同前註。

[27] 沈明室，反制中共網軍應建構網路專業部隊，青年日報(台北)，2007 年 9 月 17 日，版 4。

[28] 錢程燦，中國網路戰系統有致命漏洞，戰時可能失去控制權，2008 年 3 月 17 日，http://big5.ce.cn/xwzx/mil/uunmore/200803/17/t20080317_14864842.shtml

訊、運輸、交通等能力，就像是孫子兵法說的「不戰而屈人之兵」，這會對國家安全帶來重大威脅。舉例來說，網路攻擊手法運用在金融機構上，若敵方駭客將國內銀行的所有資金轉移到國外的銀行，那勢必造成經濟的中斷與混亂；若攻擊公共控制系統(如用遙控方式去控制某些裝置)，不但會影響他人的生命財產與安全，更會引發社會大眾的恐慌，這對國家安全而言絕對是一個非常大的隱憂。因此，在未來中共對我軍可能採取網路戰攻擊的威脅下，我軍仍應妥善做好防範未然的準備。