中共網軍發展研究

吳任傑

提要

一、中共透過網軍運作，不斷對歐、美及亞洲國家進行侵擾與攻擊，其研發的木馬和後門病毒，佔全球同類型病毒三分之一以上，已成為「網路世界的恐怖主義國家」。

二、中共網軍由解放軍(四大總部、七大軍區)及國家安全部負責攻擊、公安部負責防禦、工業和信息化部負責安全，另國家動員委員會下轄信息動員辦公室，運用科技公司及大學的科技研究力量在全國各地組建了數千支網路民兵組織，已成為中共網路作戰的主要力量。

三、中共網軍「正規部隊」已建置完成，惟其運用諸般手段隱匿其編裝、組織及部隊任務，使我無法窺探，其網軍部隊利用不定期或專案演訓，模擬戰時技術或戰術要求，採取同一時間實施不同項目、不同程度的網路模擬攻擊。

關鍵詞：網軍、網路戰、網路信息、駭客

壹、前言

中共網軍為中共網路戰部隊，其運用網路系統與敵對國家在網路空間進行戰鬥，目的是控制、破壞敵方網路系統，導致敵方網路無法正常運作，同時確保己方網路系統正常運行，網路戰在未來的戰爭中將產生決定性的影響。

近年來中共運用網軍，不斷對歐、美及亞洲國家進行滲透與攻擊，其研發的木馬和後門病毒，佔全球同類型病毒三分之一以上，已成為「網路世界的恐怖主義國家」，目前世界各國都在加強資訊安全防護，我國亦已提升相關安全作為；近期美國發生前CIA約聘技術助理史諾登（如圖一），在CIA任職期間，發現政府秘密實施代號「稜鏡計畫」的網路監控行動，於2013年6月揭發國家安全局（NSA）監控計畫，造成世界各國震驚[1]，由此可知2013年世界各國對網路監控及攻、防手段，所接受的挑戰將更趨嚴峻。

中共建構網軍目的為控制敵人、保存自己，現階段除對世界各國政府發動駭客攻擊、破壞各國電腦系統外，最常利用木馬程式大規模入侵各國政府電腦，竊取軍事、科技、商業及基礎建設等機密資訊，迄2013年，中共對美國、德國、英國、日本及我國政府與民間機構，入侵的程度與次數比往年高出許多，且有逐年增加的趨勢，並堅決否認是其所為。

貳、中共網軍概述

「中共網軍」一詞界定為中共網路部隊運用網路系統及駭客技術，入侵敵網路指揮系統，瀏覽、竊取及刪改有關數據或輸入假命令、假情報，破壞敵人自動化作戰指揮網，使其做出錯誤決策；並透過網路入侵、預先設伏、有（無）線網路傳播等途徑實施網路戰，癱瘓敵網路系統，運用病毒及駭客，攻擊敵國的金融、交通、電力、航空、廣播電視、政府等網路系統，擾亂敵國政治、經濟和社

圖一 前美國國家安全局雇員史諾登(Edward Snowden)[2]

1 中央通訊社，〈史諾登洩密案，美將修法限制監控〉，http://www.cna.com.tw/Topic/Popular/3881-1.aspx2013.8.2。

2 吳寧康(中央廣播電臺)，http://news.rti.org.tw/index_newsContent.aspx?nid=442043，2013.8.9。

會秩序，進而造成社會動盪[3]。

中共於1999年11月10日「解放軍報」首次指出，「網軍」應成為陸、海、空三軍後的新軍種，並擔負保衛網路主權及從事網路上作戰的艱巨任務。並以美國為借鏡，將網軍組成「攻擊」、「防衛」、「維護」三大部門。攻擊部隊負責滲透、監控、摧毀敵方網路系統及竊取與竄改情資；防衛部隊負責中共資安防護系統，抵禦外來網路攻擊；維護部隊負責在遭受駭客入侵後，第一時間修補網路漏洞，並追查攻擊來源。另於2002年開始即有計畫地對我國黨、政、軍、經及媒體發動網路戰，並植入木馬程式，竊取個人電腦內部檔案、文件[4]，導致我軍方機密資料外洩，影響整體國防安全。

中共網軍除研發病毒攻擊敵電腦系統與網路，並發展戰術來保護內部的電腦與網路，對許多國家的國防、政府機構已形成嚴重危害，且網路駭客近來將攻擊對象擴及重要商業機構，所造成的破壞與威脅程度相當高，甚至可藉此作為威脅條件，增加談判桌上的籌碼。中共網路戰特性如表一。

參、中共網軍組成架構及來源

中共網軍由解放軍(四大總部、七大軍區)及國家安全部負責攻擊、公安部負責防禦、工業和信息化部負責安全(如表二)，另國家動員委員會下轄信息動員辦公室，運用科技公司及大學的科技研究力量，在全國各地建立數千支網路民兵組織，且已成為中共網路作戰的主要力量。

美國紐約時報近期披露中共網路戰部隊「61398」位於上海埔東，其隸屬於中共解放

表一 網路戰特性

特 性	能 力
作戰力量多元	網路作戰包含軍隊及民間無形之網路作戰力量（區分破壞及竊取）。
作戰空間廣闊	網路作戰不侷限位置，可配置於戰略後方或敵國領土，其作戰空間廣闊，使前、後方的界線變的模糊或造成無戰線狀態。
平戰界線模糊	網路作戰存於平、戰時，在和平時期，為了進行作戰準備，在政治、經濟、軍事、心理及科技等許多領域，都會進行網路爭奪與對抗，因而造成平時與戰時的界線模糊。
智能化	網路作戰主要依賴技術與系統，其目的主在打擊敵方意志、破壞敵方決策，為高度運用智能的戰爭，因而具有智能化的特性。

資料來源：呂登明，《信息化戰爭與信息化軍隊》北京：解放軍出版社[5](本研究整理)

3 王力等，《病毒武器與網路戰爭》(北京：軍事誼文出版社，西元2001年1月)，頁21。

4 星島環球網，〈傳大陸網軍頻繁入侵，臺灣資訊戰未戰先亡〉，http://www.singtaonet.com，2007.4.16。

5 呂登明，《信息化戰爭與信息化軍隊（上、下冊）》(北京：解放軍出版社，西元2004年10月)，頁219。

軍總參謀部三部二局，部隊人數估計在數百至二千之間，至少十年前就以提供獎學金方式，招募資訊工程或英語專長的學生加入[6]，其攻擊對象87%為英語系國家（美國、加拿大及英國）[7]，故可研判其組織分工細膩，中共總參謀部三部下轄各局，已將世界各區域廣泛納入其網蒐及攻擊範圍。經研析中共網軍組成，除建制正規部隊、網路警察、網路安全員、民兵部隊及地下駭客組織等，其總數應已超過三十萬人以上，並專職負責對內監控及對外攻擊等資訊活動；以中共情資保密能力，各國掌握其網軍之資訊，恐仍將落後三至五年。

中共國防部發言人耿雁生證實中共已組成「網路藍軍」，成員約有幾十名，網路人才來自不同領域，包括現役解放軍士兵、軍官、大學生以及各種「社會人員」；該軍事單位的目的是提高共軍部隊的安全性，隸屬於廣東軍區，正式存在已有兩年時間[8]。

河北南昊科技公司自2005年起就成為軍方網路民兵組織，它由兩個小組組成，一個負責網路攻擊，一個負責網路防禦。公司所有30歲以下的員工，都屬於這個網路民兵部隊，並由當地軍方指揮，但是否進行攻擊行動未獲證實。南昊科技公司僅是中共過去10年中，從各地的網路公司和大學中建立的數千網路民兵部隊中的一支。目前中共境內負有攻擊目的的駭客越來越多，且越來越專業化和組織化，其任務包括「竊取、改變和消除敵對網站的資料」，目的是擾亂、竊取和癱瘓敵對網站[9]。

中共4所高等院校為軍隊駭客的訓練基

表二 中共網軍組成架構及具體行動

型態	負責單位	具體行動
攻擊	解放軍及國家安全部	一、解放軍七大軍區設置戰區聯合作戰指揮部，成立信息對抗中心，負責電子對抗及網路體系的防護。 二、國家安全部，下設18局，針對各國國際戰略、政經科技情報實施蒐集、研判及偵測科技器材研發，並提供網軍情蒐資訊。
防禦	公安部	下設27局，負責國內網路預防、制止和偵查違法犯罪活動，監督管理公共信息網路安全工作。
安全	工業和信息化部	負責管理通信業、指導推進信息化建設、維護國家信息安全等。

資料來源：本研究整理

6 田思怡，〈美抓駭客，揪出解放軍網戰部隊〉《聯合報》，102年2月21日，版16。

7 管淑平，〈中國網軍危駭，美嗆貿易制裁〉《自由時報》，102年2月21日，版10。

8 大紀元，〈中共首次承認網軍存在，30名專家組成「藍軍」〉，http://www.epochtimes.com/b5/11/5/28/n3269690.htm，2011.5.28。

9 吳想(希望之聲)，〈中國網軍攻防兼備國際輿論關注〉，http://big5.soundofhope.org/node/44610/，2011.10.13。

地（武漢大學、藍翔技校、交通大學、信息工程大學），重點培育中共網路人力。湖北武漢大學計算機學院「空天信息安全與可信計算教育部」重點實驗室，是中共最新網路戰術研發中心，已成功培育760名研究人員，這些人員現已進入中共軍方和政府機構，實驗室研究經費主要由中共軍事機構贊助（包括解放軍總參謀部三部）；山東藍翔高級技工學校，是大陸民間職業院校中唯一提供專業技術士官的學校；上海交通大學、河南鄭州解放軍信息工程大學則與網軍長期密切合作，研發新型網路戰術[10]。

中共網路資訊人才培育，充分運用軍事及民間力量，每年約有2萬5千名電腦程式專科畢業生可供挑選，並設立間諜學校（中共軍方洛陽外國語學院、南京國際關係學院），於2013年1月起先後在北京、上海、西安、青島、哈爾濱的民間大學，開設類似的間諜培訓學院，這些學院每年招收精心挑選的學生30至50人，為中共情報機構培訓情報員，以改造和加速中共情報機構的現代化，受過最新的數據蒐集和分析方法訓練的情報員，可納入網路攻擊使用[11]。

肆、中共網軍運用模式分析

中共網路戰有廣義與狹義之分，廣義的網路戰是敵對雙方在政治、經濟、科技領域運用網路技術，為爭奪網路信息優勢而進行的鬥爭；狹義網路戰是指敵對雙方在軍事領域，包括作戰指揮、武器控制、戰鬥保障、後勤支援、軍事訓練、情報偵察及作戰管理等方面，運用網路技術所進行的一系列網路偵察、進攻、防禦及支援行動，對軍事網路來講，只要有節點與民網相連，就可能遭敵方入侵[12]。

中共對我發動網路攻擊（竊密），從政府部門、駐外使館、中科院、電信業者、金融體系，已轉向較無防護之交通控制設備及民間基礎設施；其攻擊廣度，已從點擴增為面，並依其網路作戰規劃，擬定平、戰時攻防準據；另為突破我國防禦機制，大量利用「社交工程」手法，藉重要人士周邊關係，以迂迴方式對我機敏單位發動滲透攻擊，在獲取我單位內部網路控制權後，便進行竊取、偽造資訊及網路癱瘓等手段[13]。

中共網路戰略是試圖在網路的戰場上取

10 中央通訊社，〈美媒點名陸4高校涉及駭客行為〉，http://www.cna.com.tw/News/aCN/201305160343-1.aspx，102.5.16。

11 希望之聲，〈中共「間諜學院」曝光，培養駭客和諜報人才〉，http://big5.soundofhope.org/node/295391，2012.10.16。

12 李耐國，《信息戰新論》(北京：軍事科學出版社，西元2004年1月)，頁81。

13 羅添斌，〈中國網軍攻臺、轉向癱瘓作息〉，《自由時報》，民國102年4月28日，版1 。

得絕對領先，除竊取敵國資訊情報，並企圖在第一時間摧毀他國聯絡通訊系統，打擊與摧毀敵對國家科技優勢，藉以形成嚇阻或爭取作戰勝利的契機。近期國安局說明2012年我國電腦網域遭受侵入次數高達334萬餘次[14]，可研判中共網軍對我攻擊行為，已列為每日固定模式，且採取輪班制方式，對我國網站進行持續性的資料蒐集與監控；在美伊戰爭中，中共學會利用製造不實新聞擾亂民心的方法，利用平時對敵國媒體的研究，在戰時運用媒體製造有利中共的輿論；包括竄改新聞網頁、偽造官方訊息，並對敵方人民散播假新聞。

伍、中共網軍攻擊方式及防護手段

網軍具有「攻擊端廣泛、行動隱蔽突然及作戰方式靈活」之特徵，對未來網路戰爭具有舉足輕重的作用，其作戰激烈程度不亞於現實中的戰爭，攻擊方式及防護手段概述如后。

一、攻擊方式

網軍可經由網路對政治事件運用輿論並誘導民意、透過駭客入侵我政府網站竊取機密資料或植入後門及木馬程式，平時隱藏，等待關鍵時刻再行攻擊，以取得我重要決策，以下概述四種網路攻擊方式如表三；網路駭客攻擊方式如表四；駭客運用病毒類型及運用方式如表五；網路病毒戰，病毒傳輸方式，概區分為無線、固化方式等五項如表六。

二、防護手段

由於電腦網路具有聯結形式多樣性、終端分佈不均勻性及開放性，易致使網路受駭客與惡意軟體及其他可能的惡意攻擊行為；例如資料遭竊、伺服器無法正常提供服務、

表三 中共網軍攻擊方式

攻擊方式	運用要領
網路虛擬戰	運用視訊、電子顯示、語音識別及合成等技術為基礎的新興綜合應用技術，實施攻擊。
網路駭客戰	駭客部隊，對敵實施網路攻擊或竊取敵網路資訊，通過「防火牆」後，入侵敵核心系統，奪取網路控制權，達成控制敵方之目的。
網路病毒戰	將具有大規模破壞作用之電腦病毒，利用系統漏洞，導入敵方雷達、導彈、衛星及自動化指揮中心的網路情報蒐集系統，並在關鍵時刻啟動，藉不斷傳播、感染及擴散，侵入敵系統使其癱瘓。
網路破襲戰	攜帶專用武器設備，在其軍兵種配合下，摧毀敵方網路設備，其目的為癱瘓敵指揮系統。

資料來源：李京進，「網軍－未來的第四軍種」，思維與智慧雜誌[15]（本研究整理）

14 吳明杰，〈國安局遭網攻〉，《自由時報》，民國102年3月21日，版3。

15 李京進，〈網軍－未來的第四軍種〉《思維與智慧雜誌》，2000年第9期，頁45-46。

表四 中共網軍駭客攻擊方式

攻擊方式	區分	運用要領
口令猜測或竊取	字典攻擊	駭客為竊取目標系統文件，利用自編的特殊字典，試圖破解密碼；有些駭客的字典包括了大約20萬個單詞，用來破解密碼非常成功。
	假登錄程序	駭客藉助系統上有帳號的用戶，利用程式設計出和Windows登錄一樣的畫面，以騙取受害用戶帳號、密碼。
	密碼探測	電腦系統內部保存與傳送的密碼，經過一個單向函數編碼處理，無法看出原始密碼，理論上要還原原始密碼的機率幾近於零，駭客為了探測密碼，編寫了探測密碼的軟體，反覆模擬編碼過程，直到取得系統密碼為止。
	修改系統	駭客在系統中放置木馬程式，看起來像是合法軟體，但卻隱密的記錄用戶輸入的每個口令，利用網路回傳駭客。
IP欺騙與窺探	欺騙	即駭客利用個人電腦偽裝成準備入侵的機關用電腦，而讓其他電腦誤將冒名頂替電腦作為原始機器而加以接受，誘使其他電腦向他發送數據或允許修改數據。
	窺探	利用兩臺電腦之間網路聯繫（包含網路IP位址、TCP/IP連接字號），從中攔截發送的訊息及密碼，一旦駭客擁有這些訊息，就從被動攻擊轉變為主動攻擊。

資料來源：劉由芳等，《軍事信息安全理論》北京：國防大學出版社[16]（本研究整理）

表五 駭客運用病毒類型及運用方式

類型	運用方式
後門程式（Backdoor）	允許攻擊者與受害者連線，不必經過登入授權程序。
殭屍網路（Botnet）	遭入侵的電腦系統，只受某人的指揮與控制；這些電腦經由木馬和蠕蟲等途徑傳染而遭受控制。
下載程式（Downloader）	會進行自我安裝，但殺傷力較低的惡意程式；但接續而來會下載安裝更強悍的，或者自動更新惡意程式的軟體。
鍵盤記錄程式（Keylogger）	把鍵盤上所按下的按鍵紀錄下來，並將這些資訊回傳給攻擊者。
密碼偷取程式（Password Stealer）	偷取線上特定應用程式登錄資料，是竊賊攻擊行動中相當關鍵的要素。
偽裝程式（Rootkit）	一種潛藏在系統深處的病毒，他會偽裝成作業系統的一部分，有如殭屍網路的感染途徑一樣。
木馬程式（Trojan）	在安裝和遞送惡意程式之前，會以合法檔案掩飾；等級較高的木馬程式，防毒軟體無法掃瞄（偵測），駭客可利用遠端監控程式及鍵盤側錄器監看被害人的電腦螢幕得知所需相關密碼或資訊[17]。
電腦病毒（Virus）	會感染並破壞主機，但不具自我複製的功能，病毒會被用在系統上，並植入惡意軟體，通常具有偷取資料的能力。
蠕蟲（Worm）	會自我複製的病毒，藏於系統後便能刪除或加密檔案，也能透過e-mail散佈檔案，甚至採取入侵系統獲取資料，藉由網路途徑散播。

資料來源：李正雄，資安人雜誌第51期[18]（本研究整理）

16 劉由芳、韓強，《軍事信息安全理論》(北京：國防大學出版社，西元2005年6月)，頁237-239。

17 李正雄，《資安人雜誌》，第49期，西元2008年1月，頁5。

18 李正雄，《資安人雜誌》，第51期，西元2008年4月，頁45。

表六 病毒傳輸方式

區分	病毒傳輸方式
無線方式	一、利用無線電波，對敵方網路系統的無線電接收器或設備發射病毒，使其將病毒傳輸到電腦。 二、冒充合法的無線傳輸數據，使之混合在合法的傳輸信號中進入接收器，繼而進入敵網路。
固化方式	將病毒預先存放在電腦使用的主機板、硬碟、隨身碟、螢幕、不斷電電源系統等相關資訊產品中，再出售給其他國家，當戰爭發生時，向敵對國的網路系統，發射特定無線電信號，啟動病毒，可使敵方網路系統及依靠電腦執行的武器系統產生故障。
直接方式	直接派遣間諜或買通敵方人員，直接將病毒傳輸至敵方資訊網路。
遊戲方式	如果在指管系統較高的電腦下載遊戲，則帶著病毒的遊戲軟體將可輕而易舉的進入系統。
後門攻擊	利用軟體編寫或維護人員預設，繞過正常的安全防護措施進入系統施放病毒。

資料來源：及燕麗，《軍事信息系統安全》北京：解放軍出版社[19](本研究整理)

表七 中共網軍防護手段

防護手段	運用要領
監測	實施比對檢測程序，以檢測本系統與其它系統是否不同並分析其原因，證實系統是否被入侵；還要採用類似「感測器」的被動檢測設備，以防系統被敵人惡意超載阻塞；在理想狀況下，採取監測手段，可在損害發生前瓦解敵攻擊，但因網路資訊系統攻擊速度快，且有許多攻擊型戰鬥採用欺騙手段來規避監測，容易產生防護死角[20]。
限制	透過用戶身份識別與「防火牆(Firewall)」阻隔，限制非法系統進入，以達到防護目的，防火牆建立的目的是保護網路不受外來攻擊，拒絕未經授權的用戶，並保護合法用戶使用網路資源。
防護	對關鍵資訊進行軟、硬體加密，並對安全人員進行監控，以確保管理者及使用者，遵從所有安全規則。
恢復	於遭受入侵或實體破壞時採取積極防禦方式，對關鍵網路系統實施補救，使系統儘快恢復，確保軍隊戰鬥力及快速反應能力不受損害；或開啟備份系統，以確保系統能恢復到遭受攻擊或破壞前之狀態。

資料來源：吳漢平等，《信息戰與信息安全》北京：電子工業出版社[21](本研究整理)

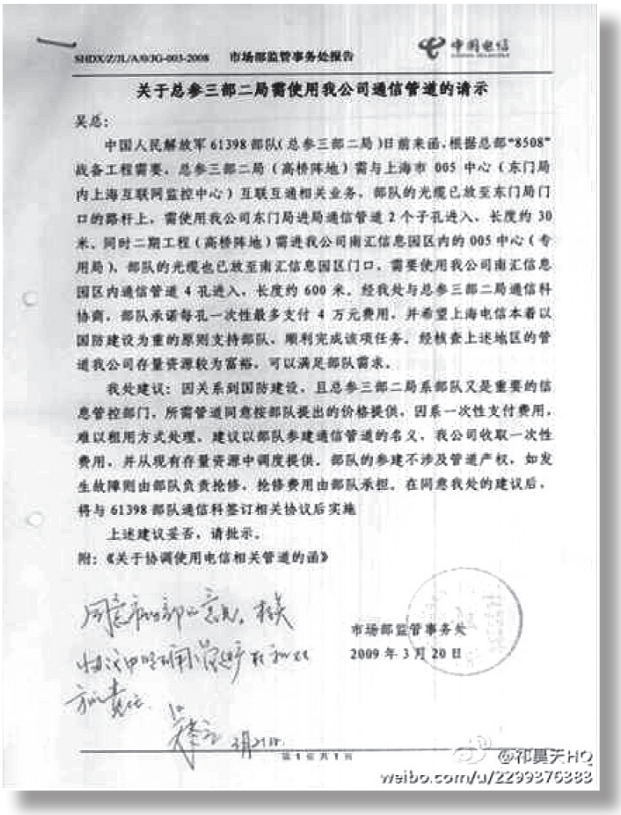
機密資訊遭竊取或洩漏等，造成的損失將無法彌補。網軍防護手段可區分為「監測、限制、防護及恢復」等四類(如表七)。

中共建構「金盾工程」（中國電訊監控工程），即一個龐大的網路監視與封鎖系統。其內容包括出入口監控、反駭客侵入、通信安全、電腦零組件加解密、電子商業安全、網路安全、防火牆、網路通訊、網路安全和管理、系統安全、病毒察覺及網路科技等，為一個多層次的封鎖和監視系統；而61398部隊與中國電信簽訂合約，要求無償使用光纖網路（如圖二），此舉意味中共網軍可以隨時監

19 及燕麗，《軍事信息系統安全》(北京：解放軍出版社，西元2004年3月)，頁69。

20 Dorothy E. Denning ，吳漢平等譯，《信息戰與信息安全》(北京：電子工業出版社，西元2003年8月)，頁53。

21 廖文中，〈中國網軍：國安、公安與解放軍〉，《全球防衛雜誌》，第271期，西元2007年3月，頁59。


关于总参三部二局需使用我公司通信管道的请示

吴总：

中国人民解放军61398部队(总参三部二局)日前来函，根据总部"8508"战备工程需要，总参三部二局（高桥阵地）需与上海市005中心（东门局内上海互联网监控中心）互联互通相关业务，部队的光缆已放至东门局门口的路杆上，需使用我公司东门局进局通信管道2个子孔进入，长度约30米，同时二期工程（高桥阵地）需进我公司南汇信息园区内的005中心（专用局），部队的光缆也已放至南汇信息园区门口，需要使用我公司南汇信息园区内通信管道4孔进入，长度约600米，经我处与总参三部二局通信科协商，部队承诺每孔一次性最多支付4万元费用，并希望上海电信本着以国防建设为重的原则支持部队，顺利完成该项任务，经核查上述地区的管道我公司存量资源较为富裕，可以满足部队需求。

我处建议：因关系到国防建设，且总参三部二局系部队又是重要的信息管控部门，所需管道同意按部队提出的价格提供，因系一次性支付费用，难以组用方式处理，建议以部队参建通信管道的名义，我公司收取一次性费用，并从现有存量资源中调度提供，部队的参建不涉及管道产权，如发生故障则由部队负责抢修，抢修费用由部队承担。在同意我处的建议后，将与61398部队通信科签订相关协议后实施

上述建议妥否，请批示。

附：《关于协调使用电信相关管道的函》

市场部监管事务处

2009年3月20日

weibo.com/u/2299375383

圖二　中共61398部隊與中國電信簽訂合約，要求無償使用光纖網路[25]

控中國電信各種情資，並對世界各地（含中共內部）通訊網路進行滲透、監控及竊取各國網路資訊。其持續不斷強力監控網路之目的，就是不讓大陸網民得到任何有關民主、人權、自由資訊獲得管道，而中共強力封鎖網路資訊，導致許多網民利用各種網路技術繞越防火牆瀏覽外國網站[22]，如中共無法持續封鎖或防堵外國具爭議性網站（Twitter、Facebook、Youtube、Google），恐加深5億4,100萬人（截至2012年7月）網民探求真相的渴望[23]，2013年8月20日至8月31日，已有數以百計的網民因「傳播謠言」而遭逮捕[24]，此舉也間接造成中共未來將承擔輿論失控的後果。

陸、中共網軍威脅評估及防制作為

一、對我之影響

中共網軍已長年滲透我國防、外交、民生（煉油廠、水庫、發電廠）、航管及通信等關鍵系統，入侵規模及深度已構成「準戰爭程度」[26]，國安局指出，中共網軍近年竊取我方2萬6千筆資訊，且實際情形可能更嚴重[27]，歸

22　希望之聲，〈中共整頓互聯網，目的在鉗制資訊〉，http://big5.soundofhope.org/node/112478，2009.12.15。

23　大紀元，〈揭秘中共外交底線，江綿恆「金盾工程」內幕〉，http://www.epochtimes.com/b5/13/6/26/n3902536.htm，2013.6.26。

24　看中國，〈中國嚴打網路謠言〉，http://www.secretchina.com/news/13/09/07/511777.html，2013.9.7。

25　中國茉莉花行動部落，http://jasmine-action.blogspot.tw/2013/02/61398_20.html。

26　林政忠，〈駭客攻擊對象，臺灣居世界之冠〉《聯合報》，民國102年3月25日，版8。

27　曾韋禎，〈開放第一類電信需謹慎〉《自由時報》，民國101年9月28日，版2。

納中共網軍對我之影響概為四點。

(一) 竊取軍事及商業機密

中共網軍對我威脅為軍事及商業機密資料的竊取，其以「釣魚」方式植入各類型病毒，或利用各種攻擊手段，達成所望戰果；且國軍網路利用民間電信公司線路，恐有一定的風險，若加上部分人員保密習性欠佳、不遵守網路使用規定，若不慎遭中共入侵並安裝木馬或後門程式，可從電腦郵件信箱或硬碟資料庫中，獲得機密資訊。

(二) 破壞關鍵基礎設施

目前我國重要關鍵基礎設施，運作時均透過網路操作及監控，相對的也可能出現許多漏洞節點，如果關鍵基礎設施遭中共網軍入侵（臺鐵、高鐵、醫院、發電廠、股市、媒體、機場塔臺及雷達站等），其影響的層面將涵蓋軍事、經濟、社會、心理等重要層面，國家安全亦將遭受重大影響，形成人民恐慌。中共對我網路攻擊可能位置分析如表八。

(三) 非接觸先敵攻擊

中共在發動軍事突襲行動前，必定先行利用網軍對我政治、經濟、軍事、心理面採取非接觸先敵攻擊，先行破壞或控制我指管系統及傳播媒體（例如：總統府、衡指所、戰略武器、軍用雷達、發電廠、水庫及新聞媒體等），一旦成功必將對我心理影響造成打擊；中共於2013年6月24日至25日，舉行代號「聯教2013-朱日和」聯合演習，演習的戰法核心就是非接觸先敵攻擊，參演部隊包括北京軍區第38集團軍某數字化合成營、特種作戰

表八　中共對我網路攻擊（竊取）可能位置（面向）分析

區分	位置（面向）
軍事	國家、軍事戰略中心：總統府、作戰指揮中心（衡指所）、緊急應變中心等。
	偵測系統：軍用雷達。
	戰略武器系統：飛彈發射中心、中科院、中研院等。
科技	新式武器參數、效能、性能提升案
商業	國家重點培植產業、企業整併構想、智慧財產權
基礎設施	資訊基礎建設方面：大型通信、網路中心、資訊服務供應商、機房等。
	能源供應方面：臺電、發電廠及電力傳輸線路等。
	交通方面：機場、機場塔臺、雷達站、高鐵、臺鐵、捷運等大型運輸中心。
	金融方面：銀行、金融市場等。
	民生供應方面：水庫、供水廠等。

資料來源：本研究整理

營、陸軍航空兵團，第65集團軍某機械化步兵旅以及石家莊陸軍指揮學院、特種作戰學院、國防信息學院、空軍預警學院、陸軍航空兵學院、電子工程學院、空軍指揮學院和空軍石家莊飛行學院等8所院校[28]，網路攻擊運用亦有可能納入此次聯合教學性的演練項目。

（四）資安人力及財政負荷

國安局預判中共網軍編制已有十餘萬人，其中六千到一萬人是招攬民間的年輕駭客，年度網路作戰經費高達八千多萬美元[29]。我國目前負責資電作戰有三個中隊，兵力概約三千餘員，為因應現今網路攻、防作戰之趨勢，準備擴編為四個中隊[30]，人力及財政之負荷，應儘早完成配套措施及長遠規劃，以因應未來網路作戰型態。世界各國提升網路安全作為如表九。

二、國軍防制作為

在現今複雜多變的網路戰場對抗環境，國軍必須確保中共網軍無法入侵軍事網路，並持續研發先進的網路安全技術，才能保障

表九 世界各國提升網路安全作為

國家	提升網路安全作為
美國	將網路攻擊列為全球首要安全威脅，推動訊息安全分享機制、強化基礎網路設施維護、減少貿易機密遭竊等相關政策應對；立法限制政府採購中國網通產品；並將網路攻擊部隊人力由500名提升至4,500名，預算由2012年39億增加至2013年47億美元，以強化網路攻防能量。
英國	近將成立「反網路威脅中心」，延攬通訊總部（GCHQ）及軍情五處（MI5）網路專家專責保護網路安全。計劃於2010至2014年間投資6億5,000萬英鎊，執行國家安全防護專案。
德國	憲保局（BfV）為因應社群時代通聯模式與攻擊目標變化，將加強網路早期預警能量；聯情局（BND）亦於2013年4月建立「網路戰爭處」，招募相關網安人才，應對愈趨嚴峻之國際網路威脅；國防部已成立約六千人的網路部隊至阿富汗執行網路監控任務。
日本	防衛省2013年將編列100億日圓成立「網際空間防衛隊」，警察廳4月起於13個道府縣警局成立「網路特搜隊」防止網路駭客攻擊。
南韓	2013年將制定針對北韓網路攻擊的軍事應對方案，且將增加網路戰人力，發展美韓聯合司令部網路戰體系，並於今年增撥167萬美元，由民間產業招聘「白帽駭客」戰力。

資料來源：羅添斌，（英美德日韓強化網路攻防），自由時報2版，102.4.28[31]（本研究整理）

28 多維新聞，〈解放軍數字化合成營將首次公開亮相〉，http://china.dwnews.com/big5/news/2013-05-29/59198850.html，2013.5.29。

29 自由時報電子報，〈國軍將成立第四支電戰部隊〉，http://www.libertytimes.com.tw/2013/new/apr/30/today-p6.htm，2013.4.30。

30 王炯華，〈國安局遇襲300萬次〉《蘋果日報》，民國102年4月30日，版8。

31 羅添斌，〈英美德日韓強化網路攻防〉《自由時報》，民國102年4月28日，版2。

戰場網路安全。現行採取防制措施說明如后。

(一) 全面更新系統

國軍為確保戰時各項網路設施及能量遭敵攻擊時能將傷害減至最輕，已全面換裝資訊作業系統，運用網路磁碟集中管控資料，並持續要求軍、民網路實體隔離[32]。

(二) 落實網路防護

國軍已落實檔案加密、封閉光碟機、USB接頭及隨身碟管制作法，並嚴禁公務家辦，在接收軍、民網郵件時，應確認郵件內容及寄件人身分，避免遭中共網軍植入木馬且開啟後門程式，導致軍事或職務機密外洩，肇生無法彌補的後果。

(三) 強化演訓深度

於漢光演習或不定期資安攻防演訓時機，除加強與民間機構進行仿真演練，模擬作戰真實場景，針對可能影響我指揮、管制及通聯之民間機構及外部可能滲透之節點進行最大限度攻擊演練，實際瞭解防護漏洞，否則單一演訓科目作為之成效恐有限。

(四) 建構境外網軍

網路作戰最重要的是集中效能，而非集中兵力，為避免中共第一擊時以導彈或電磁脈衝等武器，破壞和擊潰國軍網路戰力，應於採購新設備時，評估其抵抗電磁脈衝的防護能力，且我方網軍攻擊能量應予保存戰力，防範國軍網路系統及備援系統遭癱瘓時，能透過境外網路，對中共網軍戰力予以反擊[33]。

柒、國軍資訊作戰能力與限制

一、國軍資訊作戰能力

國軍資訊作戰部隊，目前資電作戰指揮部現有3個中隊，國軍內部負責資訊安全兵力約有三千餘員，網路作戰投資預算也會提升，因國軍資訊安全部隊多為資安防護，攻擊能量正逐漸建立。資電作戰中隊（老虎小組），已具備網路攻擊能力，更曾多次與中共網軍交手，十年前就已自行研發上百種電腦病毒並曾癱瘓過對岸網路系統[34]。

近期國防立委視察資電部網路戰大隊，下轄包括網路防護、網路情蒐及電戰三個中隊，編制約三百餘員，並於七月份成立第四支網路部隊，以強化國軍網路作戰能量，目前軍中網路防火牆等技術，應沒有被中共網軍攻破的疑慮，而未來網路部隊人才招募，在待遇與制度應更具彈性，才能吸引民間網路高手投入國軍網路部隊[35]；國軍於漢光廿九號

32 許博淳，〈國軍全面換裝電腦系統，確維資安〉《青年日報》，民國102年1月8日，版3。

33 行政院國家資通安全會報-資安論壇，〈境外網軍最後防線與反擊能量〉，http://forum.icst.org.tw/，2007.10.31。

34 吳明杰，〈已掌握監控中國網軍部隊〉《自由時報》，民國102年4月30日，版6。

35 吳明杰，〈立委籲招募網路高手〉《自由時報》，民國102年5月31日，版2。

演習，模擬臺電遭駭客攻擊，導致供電無法正常運作，並由資電作戰部隊立即投入救援，協助搶救與管控[36]，而此類型演習應將列為爾後重點訓練項目。

行政院資通安全辦公室將持續研修「國家資通安全通報應變作業綱要」，提升通報應變能力，行政院國家資通安全會報技術服務中心除彙整及關聯分析政府機關資安防護資訊，掌握對我資安攻擊的全貌外，並將能量運用於協調處理跨部會的重大資安事件；國安局為能擴大網軍及駭客威脅情資掌握範圍，除持續增進自身資通安全防護力度外，亦將持續統合「網情蒐集」體系各單位內部作業能量，並與其他行政部門進行橫向聯繫，建立網際空間作戰攻擊、防禦及情蒐等應變能力[37]。

國家高速網路與計算中心已啟用「惡意程式知識庫」，並開放民眾免費下載使用，此系統可監測上網瀏覽網頁是否有惡意程式潛伏，並可針對惡意程式實施監測及分析[38]；另從2005年開始由民間駭客社群主動召集，開辦「臺灣駭客年會」（HITCON，Hacks In Taiwan Conference），目前已成為我國資安界一年一度的盛事，且已成為國際性規模會議；而2013年年會主題，演講者除深入解析中共網軍的駭客手法，同時也關注政府、軍方與社會應如何培育下一代駭客級資訊戰人才，此會議參加者除了駭客，更有國防部、國安局、調查局等政府單位參加，相信必定能吸收多元知識並強化國軍資訊作戰能力[39]。

行政院、國安局及國家研究機構已針對資安政策、統合網路作業能量及分析監控惡意程式等項目，逐步構建資安防護網，國軍應積極參與上述機構之整合，以提升網路作戰能力。

二、國軍資訊作戰限制

(一) 資訊設備及產業開放

中共投入網路攻擊係以全國力量，包含各軍事院校及民間學校人力培訓，公、民營資訊（通信）產業研發設備（例如華為、中興、聯想等），因兩岸經貿往來密切，以中共資金投入我國相關資訊網路產業之管道將更加多元，而國軍資訊作戰成敗，與國家政策息息相關；以近期「海峽兩岸服務貿易協議」討論開放第一類[40]及第二類[41]電信業，其牽涉範圍廣泛，如未能設立法案予以規範，並嚴訂

36 同註30。

37 自由時報電子報，〈國安局籲電信業者 強化骨幹網路安全〉，http://www.libertytimes.com.tw/2013/new/apr/28/today-fo1-3.htm，2013.4.28。

38 李宗祐，〈臺灣成為國際駭客戰場〉《中國時報》，民國102年8月30日，版8。

39 呂紹玉，〈無聲的世界網戰正在開打〉，http://techorange.com/2013/07/16/2013-hitcon/，2013.7.16。

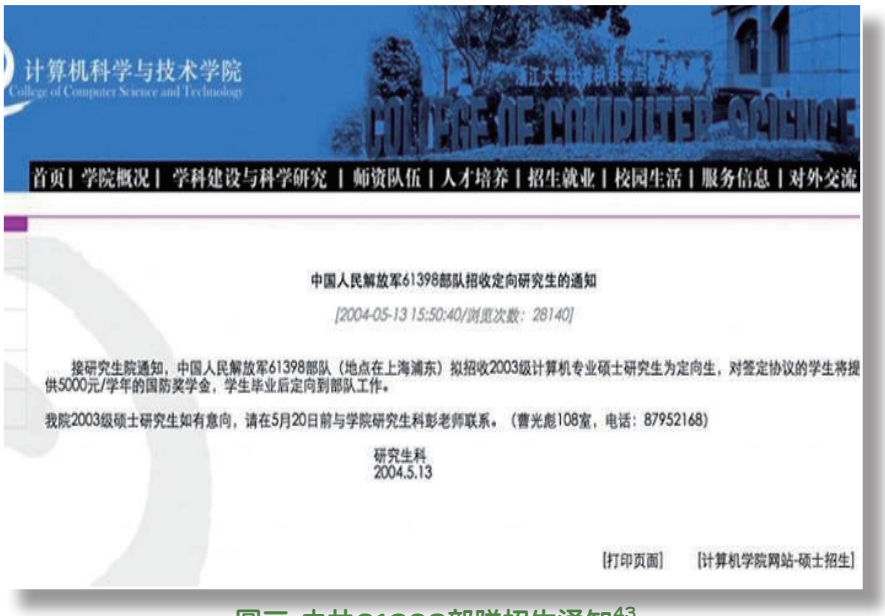
40 曾韋禎，〈若開放可在臺發動攻擊〉《自由時報》，民國101年9月28日，版2。

41 陳璟民，〈歐美國家嚴格審查〉《自由時報》，民國102年9月10日，版9。

機制，則網路資訊安全稍有不慎將功虧一簣，開放品項如表十。

（二）軍事院校培育人力不足

2012年國防大學理工學院資訊工程學系招生23員、管理學院資訊管理學系招生19員[42]，陸軍專科學校電腦與通信工程招生97員，每年招收學生人數是否可滿足網路作戰人力需求，應重新檢討網路作戰思維，適度增加招生員額及重新律定網路戰授課課程，以符合未來網路作戰需要。



圖三 中共61398部隊招生通知[43]

（三）對民間大學資訊專長學生徵才無規劃

中共資助資訊專長學生畢業後有興趣至軍中服務的學生獎學金（如圖三），再律定服役年限，以網羅優秀人才；而國軍應與民間大學畢業相關資訊工程人才至軍中服務完成配套措施，或與民間科技學校簽訂相關計畫，以補強國軍網路專長需求。

（四）未規劃招募民間網路駭客

近期我國與菲律賓之間，因廣大興28號漁船事件，所引發的網路攻防，我國民間駭客運用DDoS（Distributed Denial of Service）

表十 兩岸服貿協議第一類及第二類電信業預劃開放品項

類別	開放品項
第一類	電信基線設備、行動基地臺、ADSL、光纖等電信、網路服務。
第二類	存轉網路服務、存取網路服務、數據交換通信服務。

資料來源：本研究整理。

42 國防大學網站，http://www.ndu.edu.tw/releaseRedirect.do?unitID=183&pageID=3215。

43 大中華民國復興會，〈中共國防部否認攻擊，共軍61398部隊招生通知曝光〉，http://greatroc.tw/thread-13264-1-1.html，2013.2.23。

「分散式阻斷服務攻擊[44]」，對菲律賓官方網站開戰，我國駭客主要攻擊包括菲國海岸防衛隊等30個網站[45]；其實我國有為數眾多的民間網路人才，為強化我國網軍實力及與民間人才交流，應訂定規範以吸引優秀電腦高手為軍中久用。

（五）未能參與國與國軍事防駭演習

我國擁有為數龐大的高科技優秀人才，若能妥善規劃，極力爭取國際軍事聯合防駭演習，藉由我國科技產業與網路建設的成就，在國際上加強與其他國家的軍事資訊交流合作，並結合高科技廠商加入國防行列，不僅有利於我國軍事安全的保障，更能深入參與區域的多邊安全機制，形成對我國安全有利的外部環境，進而由內而外建立整體的國防安全體系，利用本身科技優勢提升與盟友的關係，使國軍在未來高科技戰爭中能維持局部優勢，建構一支質量併重的網路戰專業部隊。

捌、結論與建議

自2000年開始因無法證實中共「網軍」的正式編制，而對其存在有所懷疑，然中共國防部發言人耿雁生已證實，中共確已建置「網軍部隊」，人員來自不同領域；中共認為現階段網路作戰已成為各國軍事鬥爭的重點項目，網路攻防在這個時代已經不是什麼新鮮事，憑什麼其他國家可以有網軍，中共不可以有，中共不但會理直氣壯地建立網軍，而且對於曾經遭受的外來駭客攻擊，也將及時、充分、針鋒相對地公布和揭露。

中共網軍利用不定期演訓或專案演訓，模擬網路戰技術與戰術，採取同一時間對不同項目、不同程度的網路模擬攻擊，並嚴格要求攻擊成效，而非只是例行性的訓練，必須有針對性、目標性，且通過測驗者，逐級提升訓練難度，面臨戰端可即刻投入網路戰場；而國軍網路攻、防訓練是為了作戰，未來的網路戰跟誰打、兵就盯著誰練，仗在什麼環境下打、兵就在什麼環境下練，中共對我威脅與日遽增，身為國軍應有認知，絕不能因為兩岸經貿、旅遊往來頻繁，而有所鬆懈。所以部隊必須適應現代化網路戰爭，並以高估對手能力、提升訓練質量及模擬真實環境等條件下，從難從嚴訓練，這樣才能跳脫窠臼。針對中共網軍崛起，謹提出下列四點建議。

一、資安單位整合支援

行政院資通安全辦公室、國安局、國防部、國家資訊相關研究機構、電信業及資訊

44 維基百科，分散式阻斷服務攻擊：亦稱洪水攻擊。顧名思義，即是利用網路上已被攻陷的電腦作為「殭屍」，向某一特定的目標電腦發動密集式的「拒絕服務」式攻擊，藉以把目標電腦的網路資源及系統資源耗盡，使之無法向真正正常請求的使用者提供服務， http://zh.wikipedia.org/zh-tw/（分散式阻斷服務攻擊）。

45 蕭承訓，〈攻菲「鍵盤開戰」兩岸齊發〉《中國時報》，民國102年5月13日，版AA3。

安全產業等相關資安維護機構，應由政府部門實施整合，建構國家未來5至10年網路發展及人力需求規劃，確立國家資訊安全政策，避免因各自發展造成資源分散、權責不清；完成垂直整合後可使各部門共享資源，並針對職掌分工律定完成時間及進度，相關資訊設備統由國內自行研發生產，建構一套適合我國的資安防護網，以降低軍事及商業機密外洩風險。

二、培育網戰專業學子

網路作戰能力之養成極為不易，需完成數年理論課程，才逐漸執行實際演練；軍事院校教育課程、教學內容、方式及招收人數是否需重新檢討，有待商榷，建議應針對現代網路戰環境，審慎評估授課課程之適切性，避免浪費教育資源，而訓練出無效人力；另應與國內各專業技職大學及資安廠商合作，針對國軍網路作戰特性，開辦專業課程實施授課，或以獎學金方式，鼓勵有志報國學子加入國軍。

三、妥善運用民間人才

中共上海交通大學學者，與對美國政府機關及企業發動攻擊的「61398部隊」研究員，已有多年合作關係，且該校信息安全工程學院、計算機科學與工程系為中共網軍部隊提供資源，並相互研究合作[46]；兩岸高科技競爭已從軍事拓展到民間，臺灣擁有不少的高科技優秀人才、民間駭客及科技院校，若就他們的專業能力妥善規劃，鼓勵民間高科技廠商、應屆科技學校畢業生及民間駭客加入國防行列，或簽訂相關合作條款，除可化解人才荒，亦可使國軍未來在高科技網路戰爭中能維持一定優勢。

四、強化攻勢作戰能力

美國國家安全局，為反制駭客攻擊，將於2015年成立40個網路部隊，其中13個將在美國遭受網路攻擊時回擊（屬攻擊性部隊）[47]；而我國更應審慎正視中共網軍發展的威脅，不能只採取被動、消極的守勢作為，應積極強化網路攻勢作戰能力及建構適質適量之網路作戰部隊；另可結合國家資訊相關研究機構成立電腦病毒戰情中心，並編成數個網路攻擊小組，由外部網路節點，針對可能影響我指揮、管制、通信、情報及監偵設施，採無預警模擬駭客手段攻擊，以瞭解內部網路節點可能漏洞，期能有效遏止未具名的網路攻擊。

作者簡介

吳任傑中校，中正理工學院84年班，陸軍後勤學校正規班92年班，陸院正規班97年班，現任職於陸軍後勤學校人勤組主任教官。

46 張沛元，〈上海交大，遭爆與解放軍駭客部隊合作〉《自由時報》，民國102年3月25日，版12。

47 賴昭穎，〈2015年前，美將組40支網路部隊〉《聯合報》，民國102年3月25日，版8。