研究論文

中共「網軍」發展與網絡攻防：兼論我國資通安全之政策規劃

戴政龍

國防大學戰略與國際事務研究所助理教授

摘　要

1970 年代末以來，資訊通信科技的快速發展爲人類創造更爲便利的生活，尤其是電腦及網路科技裝置的普及化，更是對社會與個人生活影響深遠；虛擬的網絡世界，也形成一個新的空間領域，成爲權力競逐下的新戰場，同時也潛藏新的安全威脅。本文旨在探討中共「網軍」的發展系絡，並討論網絡空間參與者的既成結構、其導引下的「資訊權力不對稱」，以及其所引發的網絡戰爭特性。其次，列舉「網軍」運用資訊及網路科技，在網絡空間攻擊與防禦的可能方式，並指出網絡空間的「無政府狀態」，以及國家行爲者在網絡攻防時的弔詭行爲邏輯。最後，透過對政府公開文件的檢視，觀察我國資通安全的政策規劃，並提出策進意見。

關鍵字：網絡空間、網絡安全、資訊通信科技、無政府狀態、資訊權力不對稱

壹、 前言

所謂的「網軍」(cyber force),[1]並不是一個具有絕對指涉性的名詞或概念,蓋因「網軍」未必是真正的軍隊,成員也不必然是軍人,卻能具有如真實軍隊一般的攻防能力。「網軍」並不以直接造成人員傷亡或破壞各種實體設施爲主要目的,而是透過網際網路平臺,運用其結構的開放性及終端的隱匿性進行資訊(信息)戰爭(information warfare),這也是自 1970 年代末以來,資訊通信科技(information & communication technologies, ICTs)日益普及化後的負向產物,各國多視其爲國家安全的重大威脅之一。

中共關注資訊科技發展與應用源起甚早,一般皆以 1986 年的「高技術研究發展計畫(863 計畫)綱要」(簡稱「863 計畫」)爲開端,[2]而大陸軍事學者沈偉光更直言自己早在 1985 年時即曾提出「信息戰」的概念。[3]嗣後,中國大陸信息產業的研究發展,持續受到中共中央的重視與支持,各級政府機構與共軍皆投入大量資源進行研發、設置相關專責機構及培育人才;20 餘年來隨著全球資訊科技水準的普遍提昇,加上「中共崛起」蔚爲明顯的趨勢,一般咸信中共有足夠的能力及充分的意圖發展「網軍」,並運用於情報、軍事、科技、商業等領域。

以近期發生的國際事件而言,例如在 2013 年 6 月 1 日新加坡舉行的「香格里拉對話」(Shangri-La Dialogue),美國國防部長赫格爾(Chuck Hagel)在其演說中公開地指出,美國對日益增長的網路入侵表達高度關切,其中有些部分顯示與中共政府及軍方有關,美國希望中共能共同合作,建立負責任的網際行爲國際規範;[4]顯見美國官方認爲來自中國

[1] 本文認為英語的 cyber force 較能呈現「網軍」未必隸屬於軍隊或具軍事組織形貌的特性,而著重於其能力;但也常見 cyber army 的說法。

[2] 國家高技術研究發展計畫(863 計畫),〈863 計畫簡介〉,2013 年 10 月 5 日,〈http://www.863.gov.cn/1/1/index.htm〉。

[3] 沈偉光,《第三次世界大戰:全面信息戰》(北京市:新華出版社,2000 年),頁 279-282。

[4] Chuck Hagel, "Speech in International Institute for Strategic Studies (Shangri-La Dialogue)," U.S. Departmant of Defense, June 1, 2013, < http://www.defense.gov/speeches/speecg.aspx?speechid=1785>.

大陸的網路入侵行爲，已對美國造成無可忽視的威脅和損害。

在國內，政府網路遭到惡意入侵亦時有所聞，例如：2013 年 5 月 24 日行政院資通安全辦公室主動公開表示，政府的電子公文網路交換系統在月初發現遭到入侵，其攻擊手法新穎，複雜與精密程度乃屬過去罕見，是長期埋伏且有組織、有系統的非法入侵行爲。[5]這是近年來被偵測發現最嚴重的政府網路非法入侵事件，造成的損害或後遺仍難以掌控、評估。2013 年 4 月 29 日，立法院第 8 屆第 3 會期外交及國防委員會第 20 次全體委員會議，曾邀請行政院資安長、行政院資通安全辦公室、行政院國土安全辦公室、國家安全局、國防部、法務部調查局、內政部警政署刑事警察局等列席報告「我國如何因應網軍與駭客攻擊並強化資訊安全措施」，國家安全局在報告中指出該局對外網站於 2012 年間曾遭受侵擾達 334 萬餘次，其中具有惡意行爲者約 7 萬餘次，每日平均約 209 次。[6]5 月 30 日，行政院院會通過《國家安全法》部分條文修正草案，增列有關國家安全之維護範圍應包括網際網路，[7]以防止駭客（hacker）、網路間諜、「網軍」等攻擊、破壞、入侵及竊取政府重要資訊，將「國家安全」的範疇擴大到資通安全及網際空間。[8]可見藉由網路、資訊技術的隱匿性與便捷性，已對傳統的國家安全與生存利益形成巨大的挑戰，而使政府與社會不得不積極研擬有效的因應作爲。

由於現有的中文文獻對於中共「網軍」的相關主題已有不少研究與探討，[9]因此，本文對於相關文獻已論述過的部份，將盡量精簡述析，

---

[5] 謝佳珍，〈電子公文被駭，中控端重建〉，《中央通訊社》，2013 年 5 月 24 日，〈http://www.cna.com.tw/News/aIPL/201305240072-1.aspx〉。

[6] 立法院，《立法院公報》，第 102 卷第 29 期（臺北市：立法院，2013 年 5 月 17 日），頁 8。

[7] 行政院會通過由法務部、內政部及國防部會銜擬具的《國家安全法》部分條文修正草案，擬修訂該法條文第 2 條之 2，揭示國家安全的維護及於網際網路必要範圍，並函請立法院審議。參閱行政院發言人辦公室，〈行政院會通過《國家安全法》部分條文修正草案〉，行政院網站，〈http://www.ey.gov.tw/News_Content.aspx?n=F8BAEBE9491FC830&s=AE3EF6A49B7DEAD0〉。

[8] 李淑華，〈防網軍駭客　國安範圍擴及網路〉，《中央通訊社》，2013 年 5 月 30 日，〈http://www.cna.com.tw/News/aIPL/201305300139-1.aspx〉。

[9] 參閱：易承翰，〈中共網軍發展現況之研析〉，傅永茂、韓岡明、胡瑞舟、曾仲敏（編），《海軍陸戰隊論文選》（桃園八德：國防大學，2013 年），頁 223-253；林穎佑，〈大

而著重在探討中共「網軍」的發展系絡，以及其他文獻相對較少檢討的面向，亦即從網絡空間參與者的既成結構，討論其所導引下的「資訊權力不對稱」，其所引發的網絡戰爭特性、攻防性能、網絡空間的「無政府狀態」，以及國家行爲者在網絡攻防時的弔詭行爲邏輯，提供宏觀的、理則性的評析。[10]最後，透過對政府公開文件的檢視，觀察我國資通安全的政策規劃，並提出策進意見。

貳、中共「網軍」發展系絡與外部觀察探索

中國大陸的駭客或「網軍」經常被各國視爲帶有不良目的、極不友善的組織性網路行爲者。從形象的認知上，究其原因可能在於中共長久以來的負面國際形象，包括「共黨中國」（Communist China）、「紅色中國」（Red China）、「中國威脅論」（the China Threat）、非西方式民主、管制民間資訊等，都促成世界各國合理懷疑：來自中國大陸的駭客可能接受中共政府及軍方的秘密指令與資助，對西方國家進行網路攻擊及竊密行動。

陸網軍與 APT 攻擊〉，《展望與探索》，第 11 卷第 3 期，2013 年，頁 95-110；黎健文，〈資訊安全對國軍影響之探討〉，《海軍學術雙月刊》，第 45 卷第 2 期，2011 年，頁 17-32；陳立函、葉怡群、陳世仁、許富皓，〈近年網路攻擊與中國駭客活動〉，《前瞻科技與管理特刊》，2010 年，頁 137-147；陳永佳，〈資訊戰發展趨勢〉，《新新季刊》，第 38 卷第 4 期，2010 年，頁 19-29；鄭大誠，〈中共網軍的發展與評估〉，《空軍學術雙月刊》，第 603 期，2008 年，頁 3-15；林宗達，〈中共信息戰之「網軍」作戰初探〉，《展望與探索》，第 5 卷第 9 期，2007 年，頁 60-84；黃俊麟，〈中共信息戰與網路戰結合未來網軍發展之研究〉，《聯合後勤季刊》，第 10 期，2007 年，頁 17-28；樊國楨、林樹國，〈網軍運作框架初探〉，《資訊安全通訊》，第 13 卷第 2 期，2007 年，頁 16-29；廖文中，〈中國網軍：網路斬首戰及公安網軍〉，《全球防衛雜誌》，第 45 卷第 4 期，2007 年，頁 58-65；廖文中，〈中國網軍：國安、公安與解放軍〉，《全球防衛雜誌》，第 45 卷第 3 期，2007 年，頁 58-65；黃筱薾，〈共軍「三戰」之戰略涵義與作戰運用解析〉，《中華戰略學刊》，冬季號，2005 年，頁 74-114；田俊儒，〈對中共未來發展「網軍」之研析〉，《空軍學術月刊》，第 548 期，2002 年，頁 20-32；張德裕，〈對中共建立「網軍作戰」之研究〉，《海軍學術月刊》，第 35 卷第 11 期，2001 年，頁 70-76。

[10] 本文將「網路」視為具有系統性及關係取向的意涵，而「網路」則視為具有實質性、技術性及工具取向的意涵。

一、共軍信息化建設的開端與戰略

中共致力發展資訊科技的開端，約可追溯自前蘇聯在 1970 年代末發軔至 1980 年代初期的「軍事技術革命」（military technical revolution）思潮的啓發。1986 年初，王大珩、王淦昌、楊嘉墀、陳芳允等 4 位科學家向鄧小平提出「關於跟蹤研究外國戰略性高技術發展的建議」，獲得中共中央高度重視；同年年底即迅速核准了「863 計畫」，選定以「生物技術、航天技術、信息技術、激光技術、自動化技術、能源技術和新材料」等 7 個高科技領域作爲研究發展的重點。[11]自此，「信息化建設」正式列入中共的國家戰略工程項目之一。

受到 1991 年各國在波灣戰爭中所展現的軍事變革與戰爭經驗的影響，共軍將這場戰爭認定爲一場「高技術局部戰爭」，而在 1993 年將「高技術局部戰爭」列爲其「新時期」軍事戰略方針，[12]並以「打贏高技術條件下局部戰爭」（winning local wars under high-tech conditions）爲軍事戰略目標。共軍認知所謂的「高技術條件下的戰爭」是指戰爭在地面、海上、空中、太空、電磁等 5 維戰場上同時進行，是一種多維化的「陸海空天電一體戰」，呈現「戰場高度信息化」、「地面作戰非線性化」、「空中作戰合同化」、「電子、火力、機動一體化」等特性，[13]並且以「信息戰、電子戰爲作戰重要的方式」；[14]而「局部戰爭」則是在局部地區使用有限武裝力量進行有限目的的戰爭，經由謀略運作，涵蓋及構連戰略、戰役與戰鬥等不同層級領域。[15]前述的「863 計畫」正是支持此時期共

---

[11] 國家高技術研究發展計畫（863 計畫），〈863 計畫簡介〉，2013 年 10 月 5 日，〈http://www.863.gov.cn/1/1/index.htm〉；〈國家 863 計畫項目：簡介和出臺背景〉，2010 年 7 月 23 日，〈http://scitech.people.com.cn/BIG5/other4204/4206/12234136.html〉；〈國家 863 計畫項目：戰略方向和總體目標〉，2010 年 7 月 23 日，〈http://scitech.people.com.cn/BIG5/other4204/4206/12234201.html〉。

[12] 張召忠，《打贏信息化戰爭》（北京市：世界知識出版社，2004 年），頁 81-82。

[13] 張銀南、趙栩，〈高技術戰爭的特點〉，國防大學科研部（編），《高技術局部戰爭與戰役戰法》（北京市：國防大學出版社，1993 年），頁 26-33。

[14] 楊毅，《高技術條件下作戰方式、方法研究與思考》（北京市：軍事科學出版社，1997 年），頁 60-62。

[15] 謝之鵬，〈高技術條件局部戰爭下中共戰役理論與指導研析〉，《空軍學術雙月刊》，第 619 期，2010 年，頁 43-44；譚傳毅，《中國人民解放軍之攻與防》（臺北市：時英，1999 年），頁 7-8。

軍軍事戰略的科研項目。

1999年科索沃戰爭及2001年阿富汗戰爭後，共軍在觀察北約（North Atlantic Treaty Organization, NATO）及以美國爲首的聯軍的作戰模式後，更加確認「信息化」是未來戰爭的必然要件與趨勢。共軍於 2002年宣示「要將建設信息化軍隊、打贏信息化戰爭，積極推動中國特色新軍事變革作爲中國軍隊的一個戰略任務」。[16]2003 年第 2 次波灣戰爭後，共軍認爲「世界新軍事變革加速發展，戰爭形態正由機械化向信息化轉變，信息化成爲提高軍隊戰鬥力的關鍵因素，體系對抗成爲戰場對抗的主要特徵，非對稱、非接觸、非線性作戰成爲重要作戰方式」，[17]以「打贏信息化條件下局部戰爭」（winning local wars under informationalized conditions）正式取代「打贏高技術條件下局部戰爭」，作爲「加緊軍事鬥爭準備」之準據。

共軍對於信息化戰爭的認知，是指交戰雙方或一方使用信息化武器裝備，並與相適應的作戰方法所進行的戰爭，其作戰樣式包括：非對稱、非接觸、非線性作戰、快速決定性作戰、網絡中心戰、精確作戰、陸海空天電一體化聯合作戰、信息戰、太空戰等，進而使戰場空間透明化、作戰行動及時化、打擊目標精確化、力量運用高效化，並認爲以網絡爲中心的信息化戰爭，將是信息化條件下局部戰爭的新樣式。[18]而這些軍事作戰的戰爭理念與理論，不但用於共軍的軍事建設與對戰場空間的模擬，同時也平行移轉到網絡空間，建立組織化的資訊通信科技專業單位，並運用於軍事及非軍事目的，成爲兼具國家戰略布局、戰術規劃、戰鬥執行的導引方略。

二、外界對中共「網軍」的調查研析

研究指出，早在 1999 年，共軍內部即啓用「網軍」一詞；「網軍」的任務旨在進行電腦網路的攻擊和防禦，其建軍方向以陸、海、空、天、

[16] 張召忠，《打贏信息化戰爭》，前引書，頁 82。

[17] 中華人民共和國國務院新聞辦公室，《2004 年中國的國防》，2004 年 12 月，〈http://www.gov.cn/zwgk/2005-05/27/content_1540.htm〉。

[18] 王文榮，《戰略學》（北京市：國防大學出版社，2003 年），頁 348-349；謝之鵬，〈高技術條件局部戰爭下中共戰役理論與指導研析〉，前引文，頁 46。

網一體化發展爲目標，並朝成爲共軍陸、海、空軍與二砲之外的「第 5 軍種」來建置。[19]換言之，即將網絡空間視爲地面、水面（下）、空中及太空之外的戰爭空間，並將其作爲整合及構連不同空間的平臺與關鍵力量。

有關中共「網軍」的界定，狹義的對象是指共軍編制內的網路作戰部隊，主要成員由軍方及大量的民間大學、學院及訓練中心所訓練的民間專家組成；廣義的對象則包括共軍、網路管制單位、公安網路安全單位，總人數約 30 餘萬人；2001 年至 2003 年間，共軍分別在濟南軍區（鄭州、濟南）設置「信息戰模擬研究中心」及「信息戰保密研究中心」，北京軍區（北京）設置「信息戰作戰研究中心」，南京軍區（南京）設置「信息戰情報研究中心」、蘭州軍區（西安）設置「信息戰裝備發展中心」，並且網羅北京大學、清華大學、交通大學、復旦大學等學界、民間產業界之資訊人才、民間駭客，以及整合官方機構（如：國務院信息化工作辦公室與信息安全組、國家電腦網絡應急處理協調中心、中國信息安全產品測評認證中心），納編從事「網軍」之相關工作。[20]由上觀察，中共對於「網軍」的建置，從垂直整合到水平分化，包括政策規劃、機構設置與分工、人才培育及進用、資源配置、目標設定到獲取成果，均已常規化並有明確之戰略引導。

各國政府、媒體、研究者等對於中共的電腦網絡戰（computer network operations, CNOs）、信息戰等相關調查研究可說從未間斷。例如，美國國防部每年定期向國會提報的年度《中國軍力報告》（*The Military Power of the People's Republic of China*），[21]自 2005 年起迄今，每年的報告書均對中共 CNOs 發展與應用提出研析與警訊，[22]是間接觀察中共「網軍」發展之重要參據。

---

[19] 曾章瑞，〈數位國防〉，曾章瑞、馮震宇、宋餘俠、詹中原、吳秀光、項靖（編），《數位化政府》（新北市蘆洲：國立空中大學，2008 年），頁 124。

[20] 曾章瑞，〈數位國防〉，前引文，頁 129-131。

[21] 該報告自 2010 年起改為《中國軍事與安全發展報告》（*Military and Security Developments Involving the People's Republic of China*）。

[22] 本文檢閱美國國防部 2002 年至 2009 年《中國軍力報告》及 2010 至 2013 年《中國軍事與安全發展報告》。各年度報告參閱美國國防部網站 http://www.defense.gov/。

新近對中共「網軍」進行長期性大規模研究者，莫過於 2013 年 2 月 19 日，由美國麥迪安網路安全公司（Mandiant Corporation）情報中心（Mandiant Intelligence Center, MIC）公布一份名爲《APT1：揭發中國大陸某支網路間諜單位》（暫譯：*APT1: Exposing One of China's Cyber Espionage Units*）的報告，這份厚達 74 頁的報告直指共軍涉及全球網路攻擊，並附加一份超過三千餘筆的技術資料證明來自中國大陸、代號爲 APT1（Advanced Persistent Threat 1）的攻擊行動，以及一部可即時線上收視的說明影片。[23]此爲近年來對中共運用網路進行攻擊、竊密行爲最具體詳盡的非官方研究調查資料。

MIC 的報告指出，APT1 行動擁有完整架構、指揮統禦系統、展開行動的詳細程序與方法；MIC 是偶然發現其中有 3 個疑似網路攻擊者，登錄名稱爲 UglyGorilla、DOTA 和 SuperHard，這些網攻者可能爲了貪圖方便，沒有繞過防火牆登錄外國網站，而直接使用攻擊端所在的伺服器來登錄社群網站，導致行蹤曝光而被發現。[24]APT1 行動至少從 2006 年起即長期或定期侵入受害機構的網路，廣泛竊取智慧財產、技術藍圖、製造規程、實驗結果、商業計畫、議價文件、聯盟協議及電郵名單；曾遭到 APT1 行動入侵的 141 個受害機構中，87%爲英語系國家的機構總部，這些產業符合中共第 12 次 5 年（十二五）計畫中 7 大策略性成長產業中的 4 項；APT1 行動透過大量電子郵件 GETMAIL 和 MAPIGET 軟體，全年性地入侵受害機構和人士的電子郵件，最長期間達 4 年 10 個月；報告中研判，這些透過網路進行偵蒐攻擊，負責執行 APT1 行動的機構，應該是共軍代號「61398 部隊」（Unit 61398），其任務與 APT1 行動長期進行的網路攻擊行動極爲相似，兩者位置都在上海浦東新區

[23] Mandiant Intelligence Center, Mandiant Intelligence Center Report (2013), < http://intelreport.mandiant.com/>; Mandiant Intelligence Center, *APT1: Exposing One of China's Cyber Espionage Units*, February 19, 2013,< http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf >.

[24] Mandiant Intelligence Center, *APT1: Exposing One of China's Cyber Espionage Units*, *op. cit.*;〈共軍網路駭客　總參三部二局〉，《中央通訊社》，2013 年 2 月 20 日，〈http://www.cna.com.tw/News/aIT/201302200334-1.aspx〉；廖漢原，〈美報告點名解放軍　依指示網攻〉，《中央通訊社》，2013 年 2 月 19 日，〈http://www.cna.com.tw/News/aOPL/201302200008-1.aspx〉。

（Pudong New Area），並且可能由中共政府部門和軍方直接支持。[25]

MIC 報告中指出「61398 部隊」隸屬於共軍總參謀部技術偵察部第 2 局（簡稱：總參 3 部 2 局），[26]位於上海埔東新區高橋鎮大同路一棟 12 層高的建築；其成員約在數百人到 2 千人之間，並直接從大學甄選具電腦和英語專長的人才，專責進行網路行動。[27]「61398 部隊」的滲透入侵方式，通常經由「魚叉刺魚」的攻擊方式進入目標電腦網路，讓受害機構（公司）成員收到僞裝或假冒的電子郵件，而誤啓連結或附加檔案，成爲入侵者的後門；其最優先的目標通常是資訊科技產業，其次是航太產業，從竊取或轉移資料；其行動使用時間通常平均不到一年。[28]

我國國家安全局亦在 2013 年 4 月 29 日向立法院報告有關中共「網軍」組建情形，報告內容指出：「共軍自 2002 年起擴充網路戰能量，發展初期雖遠落後各先進國家，然近年來蓄積相當能量，且業務分工廣布總參四大總部、七大軍區、國防科研機關與各級院校等，任務包括戰時網路攻擊，以及平時網路竊密、網路滲透遂行諜報活動等；另國防動員委員會亦將信息民兵納入編組，整體軍事機關網軍組織架構基本成形，預判其正式編制內人力約 10 餘萬人，2013 年投資經費推估已超過 8,000 餘萬美元。」[29]顯見當前中共「網軍」的規模與能力持續擴大，對我國及各國資訊通信安全的威脅實不容輕忽。

---

[25] Mandiant Intelligence Center, *APT1: Exposing One of China's Cyber Espionage Units*, *op. cit.*; 廖漢原，〈美報告點名解放軍　依指示網攻〉，前引文。

[26] 該報告指出，中國電信集團公司曾就光纖通訊基礎建設和「61398 部隊」訂有契約，內容呈現出該部隊對高寬頻的需求；契約書上稱「61398 部隊」隸屬於共軍總參謀部 3 部 2 局；此外，中國電信集團基於支持「國防建設」的考量，同意接受軍方提出的較低價格交易服務。參閱 Mandiant Intelligence Center, *APT1: Exposing One of China's Cyber Espionage Units*, *op. cit.*;〈共軍網路駭客　總參三部二局〉，前引文。

[27] 2003 年曾在中國大陸的網路貼文發現到，61398 部隊提供獎學金給浙江大學計算機科學與技術學院的碩士班研究生，條件是畢業後到該部隊工作。參閱 Mandiant Intelligence Center, *APT1: Exposing One of China's Cyber Espionage Units*, *op. cit.*;〈共軍網路駭客　總參三部二局〉，前引文。

[28] Mandiant Intelligence Center, *APT1: Exposing One of China's Cyber Espionage Units*, *op. cit.*;〈共軍網路駭客　總參三部二局〉，前引文；廖漢原，〈美報告點名解放軍　依指示網攻〉，前引文。

[29] 立法院，《立法院公報》，前引書，頁 6。

綜上論之，中共「網軍」的建置乃充分運用「信息化局部戰爭」的理念，並已具備系統性、常規性之規模與攻防自若的能力，其目標亦已不僅止於純軍事領域的範疇，而包括科技、商業等領域。若以喬良、王湘穗所描繪的「超限戰」來看，[30]中共「網軍」的建置與運用，可以視爲對「超限戰」理念的落實和體現。

參、「網軍」之攻防性能與追求資訊權力的弔詭

回顧 20 世紀初的工業社會時代，英國學者麥金德（Halford John Mackinder）在 1904 年提出著名的「心臟地帶論」：誰控制東歐，誰就統治了心臟地帶；誰控制心臟地帶，誰就統治了世界島；誰控制世界島，誰就統治了世界！同一時期，美國學者馬漢（Alfred Thayer Mahan）提出「制海權」的觀念，他認爲海洋的航線可以帶來巨大的利益，因此國家必須保有強大的艦隊與足量的商船來獲取之。義大利學者杜黑（Giulio Douhet）則在 1921 年發表了「制空論」，認爲以飛機飛離地面獲取優勢空間，並以轟炸來使陸上和海上的敵人屈服，掌握空權就能獲得勝利。陸權論、海權論與空權論三者的論述或許各有偏重，也都主導過 20 世紀若干戰爭攻防的原則，但麥金德的理論中，鐵路是擴張陸權最重要的渠道和載臺，馬漢看重的航線與船艦也是擴張海權的渠道和載臺，杜黑重視的空中立體空間及轟炸機，亦是確保空權的渠道和載臺！時至當前的資訊社會時代，上個世紀 3 位傑出戰略家的理論同樣具有其適用性，亦即：掌握資訊網絡的渠道與載臺，相對也就控制了世界的主宰權！

一、網絡空間有利「網軍」活動之結構特性

由當代資訊通信科技所聚合而成的系絡，在使用者終端具有即時性、友善性、隱匿性、共享性、虛擬性、聚合性、脆弱性、易被滲透性、去疆界性等特性，但在網絡的管理與維護端卻具有控制性、透視性、追蹤性、維安必要性、技術性等權限與專業要求，而軟、硬體的建置端上又有一定程度的專業知識與技術門檻，形成「使用者—管理者—設計製

[30] 參閱喬良、王湘穗，《超限戰：兩個空軍大校對全球化時代戰爭與戰法的想定》（北京市：解放軍文藝出版社，1999 年）。

造者」3 端的「資訊權力不對稱」（information power asymmetry）的既成結構。「網軍」、駭客或網路間諜等非法入侵者，因而可以擁有許多攻擊、破壞、竊取、竄改等危害網絡安全行動的自由空間，且非常容易利用網路的開放性和隱匿性而不被發現。

當資訊成爲一種資源，網絡空間成爲一種新的戰場空間，則資訊的利用、爭奪、傳輸、保護，便成爲一場無時無刻都處於接戰狀態的戰爭。這種戰爭與傳統的戰爭不同之處在於：

（一）參與者之間未必一定有零和式的敵意；

（二）沒有宣戰的過程，從事戰鬥的人員也未必是軍人；

（三）完全看不見敵人，亦難以發現真正的敵人；

（四）戰爭不以殲滅敵人有生力量爲目標；

（五）非對稱、非接觸、非線性的戰鬥的形式；

（六）成功攻擊的成本，遠低於成功防禦的成本。

二、攻擊方可採取的行動

（一） 入侵：透過各式網絡（有線、無線），入侵標的者或具安全弱點者的電腦或伺服器，進行瀏覽、蒐集、竄改、盜用、毀損、干擾、攻擊、破解安全防護、開啓後門或建立爲己方所用的跳板等行動。

（二） 破壞：阻斷服務（denial of service, DoS），導致網路正常服務中斷。

（三） 攔截：在網絡的節點或以搭線技術，窺視、監聽、擷取、干擾或阻攔標的者發出的電磁資訊，或改變已知網站的 DNS（domain name service），轉移至所望之網址。

（四） 追蹤：跟隨標的者的資訊發送路徑，追蹤標的者的通訊目的地，加以標註、記錄或設置陷阱。

（五） 僞裝：透過電子郵件發送僞裝訊息或誘騙附件、僞裝已知網站、綁架網站等方式，設置假身分、僞 IP、木馬程式（Trojan Horse）或進行社交工程（social engineering），作爲入侵、攔截、追蹤等行動之前置行動。

（六） 散佈：散佈電腦病毒，例如：木馬程式、蠕蟲（worms）、邏輯炸彈（logic bombs virus）、定時炸彈（time bombs virus）、巨集病毒（macro virus）等，並感染標的者關係網絡中的其他電腦，同樣爲入侵、攔截、追蹤等行動之前置行動。

（七） 滲透：利用標的者周邊的人際網絡進行滲透，獲取關鍵的身分資訊或安全資訊；透過軟、硬體的設計製造，預設後門或寫入韌體，以利後續之入侵、攔截、追蹤等行動。

（八） 操縱：透過網路散播有關標的者的謠言、毀謗言詞、不實廣告，影響公眾認知或操縱市場，進而獲取實質利益。

（九） 公開：將已獲取之資源性資訊（如：國防機密、政府機密、財務性秘密、專利、程式碼等）或隱私性資訊公開，造成標的者的實質損害。

（十） 仿製：將已獲取之資源性資訊（如：製造機密、智慧財產、商業機密等）加以仿製，使標的者蒙受損失。

三、防禦方可採取的行動

（一） 阻攔：建立實體性與程序性的防護設施與措施，例如：登入者身分管制、安裝防毒程式、防火牆（fire wall）、機敏網路與終端設施的實體隔離、強化電子閘門（gateway）的安全過濾功能、主動及被動式的偵測程序與措施、人員、設施、工作程序的安全管制等。

（二） 加密、隱匿與屏蔽：建立軟、硬體之加密措施，以增加破解之難度；利用涓流技術或分割技術，降低資訊遭竊風險；將重要資訊隱藏於一般檔案程式碼之中，而不易於傳輸過程被發現；

建構有效之電磁屏蔽設施及裝置，防範物理性破壞。

（三） 鑑別：建立有效之使用者身分鑑別機制（如：密碼、生物特徵、數位簽章、金鑰等）。

（四） 監控：確立授權機制、主動偵測過濾器、持續性與常規性監控網路進出流量，建立時態分析模型。

（五） 漏洞防補：建立系統與程式之弱點與漏洞偵測機制，即時進行修補工程。

（六） 備份與備援：建立即時、獨立、多元的備份與備援機制，防範大規模損害。

（七） 軟、硬體安全能量：建立可靠之系統、程式與硬體設計、製造與修護能量，防止人為滲透。

（八） 掌控原始碼：掌握操作、傳輸、儲存機敏資訊之系統與程式原始碼（source code），避免為特定對象（廠商）掌控。

（九） 教育訓練：對資訊管理、操作與維護人員實施資訊安全教育訓練，確保工作紀律與相關安全程序。

四、網絡攻防的對比與政策成本

在軍事理論中，攻擊與防禦是作戰的一體兩面，在網絡空間中亦有相似的原則，且更為直接的技術對應，即：攻擊方必須瞭解防禦的策略與技術性能，方可能突破防禦工事；同樣地，防禦方也必須瞭解攻擊的策略與技術性能，方足以盡可能防範各種攻勢。

從前述網絡攻防的可能行動可以得知，以網絡空間作為戰場的戰爭，對戰爭的參與者而言，具有結構性的「資訊權力不對稱」；因此，網絡空間的戰爭，明顯有「易攻難守」的特性。採取網絡攻勢者，可以採取集中、奇襲等戰術，輕易獲得價廉效高的戰果，無論是國家、政府、軍隊或其他尋求特定目的有心者，很難排除這種現實的誘惑；而網絡防禦者則正好相反，必須盡量投入更多的資源，採取全面、周延、滴水不

漏的各種防範及控制措施，因而可能降低整體運作效率，也無法確保絕對的、滴水不漏的成效，故難以立竿見影，也相對未必獲得主政者、政策參與者與其關係人的支持。這種特性在政策規劃與執行時，又造成決策時的「偏好不對稱」（preference asymmetry），形成結構上的「雙重不對稱」（double asymmetry）效果，而使網絡的攻勢行爲得到直接的鼓勵。

然而，從規範層面論之，無論利用網路進行何種攻勢行動，都是違反隱私權、國際法規範與各國國內法的非法行爲，甚至是被認定爲「網路恐怖主義」（cyberterrorism）的行徑，有著極高的「倫理風險」（ethical hazard）。即便是純軍事行動上的網路攻勢行爲，也都可能引發或加劇實體的國際衝突，或遭致以牙還牙的報復。

五、網路空間的「無政府狀態」與其弔詭

從國際關係現實主義（realism）的觀點來看，虛擬的網絡空間之「無政府狀態」（anarchy）相較於實存的國際體系實有過之而無不及。在現實主義的典範下，國家必須擴大自身權力，以確保國家利益、生存與安全。因此，將國際關係現實主義帶入上述之「雙重不對稱」結構中可知：各種國家及非國家行爲者成立類似「網軍」的機制或組織，從事網絡的攻擊、防禦、維護及開發等有特定目標、有組織、有系統、計畫縝密的網絡活動，便成爲一種默示的決策方案，以保證「無政府狀態」下的「相對獲益」（relative gains），鞏固國家安全與利益。

弔詭的是，因「網軍」行動的不道德性與違法性，幾乎不會有任何國家或政府會公開承認運用「網軍」對其他國家、組織或個人進行網路攻擊、滲透及間諜行爲，至多只會宣稱採取必要的防護行動，以維護網絡的安全；其合作或參與計畫的企業、組織或個人更不會輕易承認參與「網軍」的計畫與行動。換言之，「無政府狀態」下的網絡空間，追求權力的各種行爲者會藉由「網軍」行動，擴大自身的資訊權力，掌握相對大於敵對者或競爭者的資訊權力，以確保安全的狀態。

2013 年 6 月 8 日，美國總統歐巴馬與中共國家主席習近平在加州陽光莊園（Sunnylands）舉行非正式高峰會中，網路安全問題成爲雙方會談的焦點之一，但中共卻表明本身也是網路安全的受害者，也希望積

極解決此類問題。[31]然而，美國《華盛頓郵報》（*Washington Post*）卻在此期間報導指稱美國多個大型電腦、資訊公司涉及美國政府的「稜鏡」（PRISM）計畫，將使用者的隱私提供政府情報機構使用；美國國家安全局（National Security Agency）與聯邦調查局（Federal Bureau of Investigation）能夠直接進入這些企業的伺服器，搜尋使用者的語音、影片、照片、電子郵件與上網記錄，並追蹤其在網路上的行蹤；[32]無獨有偶，英國《衛報》（*The Guardian*）也在同一期間披露：在歐巴馬總統發布的政策指令（Presidential Policy Directive）第 20 號機密文件，指出「攻勢網絡效果行動」（Offensive Cyber Effects Operations）可以提供美國獨特及非傳統的能力，在全球選定所需的攻擊目標。[33]此一事件不但造成美國民眾極大的疑慮與抗議，後續更引發一連串的國際糾紛。後續發現洩密者爲美國中央情報局（Central Intelligence Agency）前雇員史諾登（Edward J. Snowden），美國政府發布通緝並嚴厲譴責洩密者嚴重傷害國家安全利益，要求各國協助遣返史諾登返美受審。從美國對中共從事網路竊密的指控，到史諾登洩露美國政府侵犯個人隱私及從事網路攻擊情事，再到美國譴責史諾登傷害美國國際形象與利益的一連串事件，清楚呈現了在「無政府狀態」下的網絡空間與實際的國際體系中，各國「說一套、做一套」的弔詭。

---

[31] 〈習近平答美媒：陸也受網路攻擊〉，《中央通訊社》，2013 年 6 月 8 日，〈http://www.cna.com.tw/News/aCN/201306080151-1.aspx〉；〈網路安全　歐習共盼解決問題〉，《中央通訊社》，2013 年 6 月 8 日，〈http://www.cna.com.tw/News/aOPL/201306080101-1.aspx〉；林淑媛，〈談網路安全　習：大陸也受害〉，《中央通訊社》，2013 年 6 月 8 日，〈http://www.cna.com.tw/News/aOPL/201306080154-1.aspx〉。

[32] Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington Post*, June 7, 2013, < http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html >;〈美科技大咖否認助華府情蒐〉,《中央通訊社》，2013 年 6 月 7 日，〈http://www.cna.com.tw/News/aOPL/201306070066-1.aspx http://www.cna.com.tw/News/aOPL/201306070066-1.aspx〉。

[33] Glenn Greenwald and Ewen MacAskill, "Obama Orders US to Draw up Overseas Target List for Cyber-attacks," *The Guardian*, June 7, 2013, < http://www.guardian.co.uk/world/2013/jun/07/obama-china-targets-cyber-overseas >；黃貞貞，〈衛報：歐巴馬下令設定網攻目標〉，《中央通訊社》，2013 年 6 月 8 日，〈http://www.cna.com.tw/News/aOPL/201306080025-1.aspx〉。

肆、當前「網軍」之威脅與我國資通安全政策規劃之應對

前述，在網絡空間的無政府狀態下，各國都可能進行程度不一的網絡攻防行爲。在兩岸複雜的政治與經濟關係中，中共運用「網軍」對我國進行各種網路攻勢、情蒐、竊密等行動，已爲我政府相關部門證實，政府也對此實存的威脅採取若干的因應對策。

一、中共「網軍」對我國之攻擊方式

根據我國家安全局的研判，當前中共「網軍」爲突破我國資通安全之防禦機制，大量利用「社交工程」手法，藉機敏機關或重要人士周邊關係，以「由近而遠」或「由疏而密」等迂迴方式對我發動突穿、滲透等駭侵攻擊，在獲取我遭駭單位內部網路最大控制權限後，大肆進行盜竊、僞造資訊或癱瘓網路通聯等；另中共爲全面掌握我國防、政治、外交、兩岸等發展動態，其網路攻擊竊密對象，已由政府機關、駐外館處，轉向民間智庫、電信業者、委外廠商等，並轉變思維攻擊我較疏於防護的網路節點設施，或車輛交通號誌儀控設備、寬頻路由器、工業微電腦控制器、網路儲存系統等崁入式系統裝備，預判未來恐將擴及我國關鍵基礎設施與個人，並逐步蒐集民間政黨規劃、經貿分析、學術著作，以及電信網路、關鍵基礎設施系統等隱性資訊，或是透由網路攻擊癱瘓我國運作。[34]從上述研判來看，中共「網軍」對我國資通安全已形成極大威脅，也突顯其攻擊目標並不僅局限於軍事目標，而是全面性地情蒐、滲透、掌控。

就網路應用的實務而言，「社交工程」式的網路攻擊的確是當前最常見、也最難防範的攻擊形式。在受攻擊者瀏覽或開啓附加檔案後，即同時被安裝惡意程式，接著就可能遭到遠端入侵、攔截、追蹤、監聽或成爲另一個攻擊行動的跳板。當這種社交工程尋找到適當的關鍵者，便潛伏並進一步釐清其人際網絡與可資運用的弱點或機會，進而找到漏洞加以突破，接著便可發動更進一步的攻擊行動，或突破原本難以破解的資通安全防護機制。由於「社交工程」的對象難以捉摸，因此，舉凡政

[34] 立法院，《立法院公報》，前引書，頁 6-7。

治（如：選舉計票作業）、金融（如：財金中心所屬網路）、科技（如：精密科技研發）、商業（如：企業營運、專利設計）、通訊（如：各大網路服務供應商）、工業（如：生產製造）、國防（軍事安全）等各領域，以至個人隱私，都有可能暴露在「網軍」攻擊的範圍之中，其影響是全面的，而且損害難以掌控、評估。

二、政府對資通安全防護之政策規劃

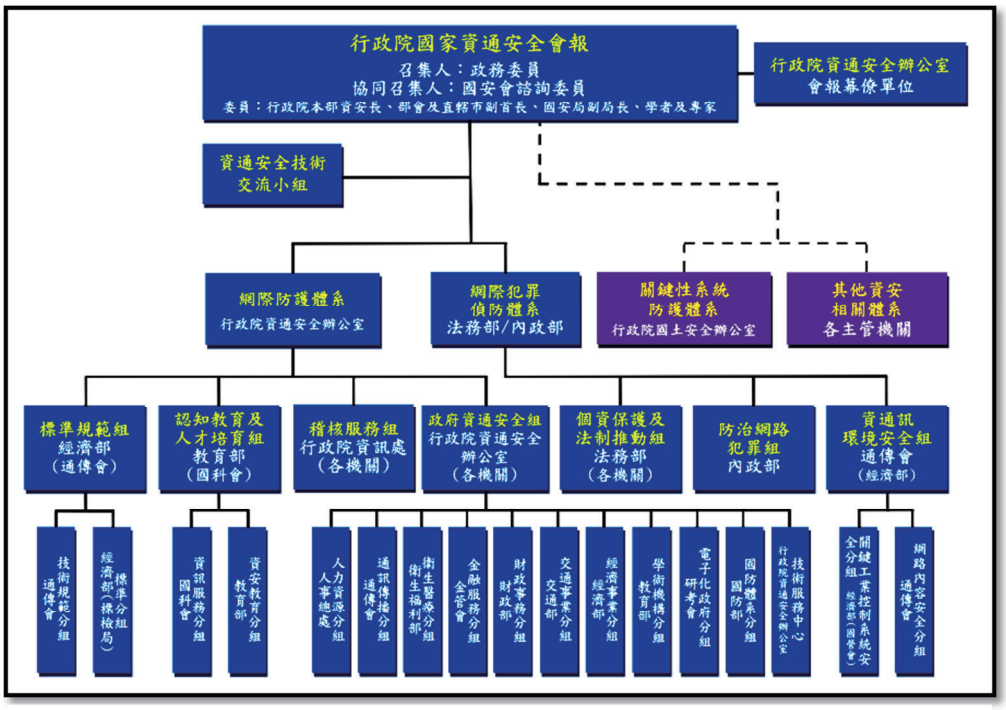
面對「網軍」與各種資訊通信領域中的潛在威脅，我國政府對資訊通信安全議題的具體回應，始於 2000 年 5 月國家安全會議研提「建立我國通信資訊基礎建設安全機制」的建議書，經總統核定後轉送行政院規劃。次年初，行政院以「會報」形式，統整相關工作；10 年後，再成立以國家安全會議爲系統的「指導小組」，共同參與資通安全之政策規劃。

（一）組織設計與任務

「行政院國家資通安全會報」於 2001 年 1 月設立，負責推動我國資通安全基礎建設工作，綜理國家資通安全各項政策與事務；2011 年 3 月 7 日，再成立「行政院資通安全辦公室」，以統籌規劃國家資通安全政策、通報應變、重大計畫推動與管考及辦理相關會議。[35]（「行政院國家資通安全會報」現行組織架構，如圖 1）

[35] 行政院國家資通安全會報，〈緣起背景〉，〈http://www.nicst.ey.gov.tw/cp.aspx?n=2C3EAFE096F5A753〉；行政院國家資通安全會報，〈行政院資通安全辦公室設置要點〉，〈http://www.nicst.ey.gov.tw/cp.aspx?n=78869EB6335CF18C&s=F1D4DE53057005AE〉。

圖 6　行政院國家資通安全會報組織架構



資料來源：行政院國家資通安全會報，「行政院國家資通安全會報組織架構圖」，《國家資通安全通報應變作業綱要》（臺北市：行政院國家資通安全會報，2013 年 9 月 9 日），頁 3。

「行政院國家資通安全會報」的任務是負責國家資訊通信安全政策、通報應變機制與重大計畫之諮詢審議、跨部會資通安全事務之協調及督導。[36]會報設有召集人 1 人，由行政院院長指派之政務委員兼任；協同召集人 1 人，由國家安全會議諮詢委員兼任；會報下設「網際防護」及「網際犯罪偵防」2 個體系：[37]

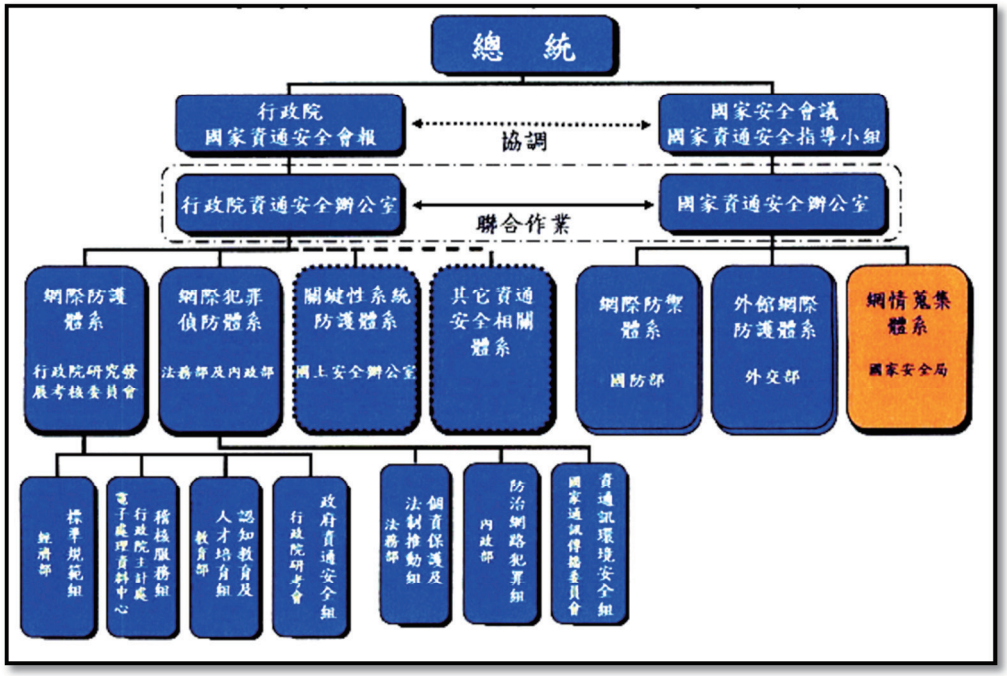
1. 網際防護體系：由行政院資通安全辦公室主辦，下設「標準規範組（經濟部）」、「稽核服務組（行政院資訊處）」、「認知教育及人才培育組（教育部）」、「政府資通安全組（行政院資通安全辦公室）」，負責整合資安防護資源，推動資安相關政策。

[36] 參閱「行政院國家資通安全會報設置要點」第 2 點。
[37] 參閱「行政院國家資通安全會報設置要點」第 3 點、第 5 點。

2. 網際犯罪偵防體系：由法務部及內政部共同主辦，下設「個資保護及法制推動組（法務部）」、「防治網路犯罪組（內政部）」、「資通訊環境安全組（國家通訊傳播委員會）」，負責防範網路犯罪、維護民眾隱私、建立資通訊基礎建設安全等工作。

2011 年 4 月 6 日，國家安全會議訂定發布「國家資通安全指導小組設置要點」，在國家安全會議設置「國家資通安全指導小組」、成立「國家資通安全辦公室」，並設置「網際防禦（國防部）」、「外館防禦（外交部）」及「網情蒐集（國家安全局）」等 3 個體系，[38]與行政院「國家資通安全會報」及「資通安全辦公室」進行協調與聯合作業，並同時受到總統指揮（我國整體資通安全機制組織架構，如圖 2）。

圖 7　我國整體資通安全機制組織架構



資料來源：立法院，《立法院公報》，第 102 卷第 29 期（臺北市：立法院，2013 年 5 月 17 日），頁 7。

[38] 立法院，《立法院公報》，前引書，頁 7。

（二）政策規劃與執行

我國自 2001 年開始，陸續展開 3 個階段，各爲期 4 年之重大資通安全計畫：第 1 期機制計畫（2001 年到 2004 年），旨在建構政府重要機關資安防護體系，包括機關分類分級鑑別、關鍵基礎設施實施資安管理方案、推廣資安認知及教育訓練等爲政策目標；第 2 期機制計畫（2005 年到 2008 年），旨在健全資安防護能力，包含政府機關資訊安全長（Chief Information Security Officer, CISO）責任制度、國家資通安全防護管理平臺（National Security Operation Center, NSOC）、強化資安稽核、強化資安責任等級分級作業與機密資訊保護、建構資安關鍵指標等爲主要政策；第 3 期爲國家資通訊安全發展方案（2009 年到 2012 年），以「強化整體回應能力」、「提供可信賴的資訊服務」、「優質化企業競爭力」及「建構資安文化發展環境」爲 4 大政策目標，透過「需求端」與「供應端」規劃，符合政府、關鍵基礎建設及企業需要的 5 項資安措施、共 20 個行動方案；在「環境面」強化法制建設、認知宣導、創新合作及衡量指標等利於形塑資安文化的 4 項措施、共 10 個行動方案。[39]

三、面對「網軍」威脅下資安政策規劃之檢視與精進

我國國家安全局於 2013 年 4 月在立法院的報告中，對於如何因應網軍與駭客攻擊並強化資訊安全措施，提出 2 項策進建議方向：[40]

（一）加深我國總體防禦縱深，強化電信關鍵基礎設施防護：

我國爲高度資訊化社會，電腦、手機等資通訊產品應用普及，然各類通訊均需透由骨幹網路進行通訊傳輸，故面對日益嚴峻的資安威脅與挑戰，除加強個人資安防護觀念與作爲外，更需結合國內電信業者力量，前進部署防護措施至電信骨幹網絡，共同組建多層次防禦縱深機制，故籲請國內各家電信業者不能僅考量自身商業利益，更應配合國家整體政策需求，強化並落實基礎骨幹網路安全。

---

[39] 行政院國家資通安全會報，〈我國重大資安政策進程〉，〈http://www.nicst.ey.gov.tw/News_Content3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF&s=1ACE1B808B9444DF〉。

[40] 立法院，《立法院公報》，前引書，頁 8。

（二）整合政府機關相關資源，拓增國家安全局網情蒐集來源管道：

近年由於美國、愛沙尼亞、拉脫維亞、南韓等國民生關鍵基礎設施遭受網路攻擊事件頻傳，且攻擊模式由阻斷服務攻擊轉爲直接毀癱攻擊，世界各國均已編列大量經費，組建網路戰部隊進行防禦攻勢。鑒此，爲能擴大「網軍」及駭客威脅情資掌握範圍，國家安全局除持續增進自身資通安全防護力度外，亦將賡續統合「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，強化政府網路安全。

由國家安全局的建議來看，可以從兩方面加以解讀：一是對個人、電信產業及國家基礎骨幹網路建設的正面期待；二是期待立法機關早日通過《國家安全法》部分條文修正案，將網際網路增列爲國家安全維護之範圍，並擴增該局能量與資源，提升其網路攻防及情蒐能力。由此，正好可以藉以檢視我國資通安全的政策規劃所面臨的若干問題。

首先，我國的資訊通信安全機制分由「行政院國家資通安全會報」與「國家安全會議國家資通安全指導小組」雙線式掌理並相互「協調」，再分別下設「行政院資通安全辦公室」、「國家資通安全辦公室」進行「聯合作業」，各自擁有由不同機關組成的「網際防護體系」（見圖 2）。此一設計，應是基於《國家安全會議組織法》第 2 條有關總統決定「國防、外交、兩岸關係」國家安全大政方針定義之延伸，因而形成行政院與國家安全會議在資通安全機制上的雙線體系。實際運作上，因雙線體系的頂端是總統，故 2 個機關應能相互尊重協調；惟資通安全維護應採一貫的、全面的、整合的戰略與政策，方可確保技術層次的一致性與可預期性。因此，現有機制組織結構的順暢運作，必須有更多的溝通、更多的相互確認，當然也就需要更多的時間。

其次，無論是「行政院國家資通安全會報」或「國家安全會議國家資通安全指導小組」的體系，包括「行政院資通安全辦公室」、「國家資通安全辦公室」均屬「任務編組」性質，其專業能力、整合能力、常規化運作能力、資源等，相較於各國紛紛成立專責機構、招聘專業人力、挹注大量資源等積極作爲，現有的組織體系可發揮的成效相對偏低。

再者，從我國自 2001 年起的 3 個資通安全計畫方案中可知，我國的資通安全政策規劃是以結合國內社會趨勢、經濟發展、民生需求爲政策主軸；換言之，也就是以滿足內部需求爲最優先的順位。因此，對於網絡攻防的建設上，偏向採用被動的、防禦/防護的策略導向。建議未來可朝建立外部需求（如設定網絡空間的假想敵），調整增加主動的策略思考，以創造有利的戰略優勢。畢竟，在無政府狀態下的網絡空間中，攻擊仍是最好的防禦。

伍、結論

中共「網軍」的建立，是從「打贏高技術條件下局部戰爭」到「打贏信息化條件下局部戰爭」軍事戰略演進下的必然產物。伴隨中國大陸綜合國力的上升，中共有足夠的資源大量挹注於信息化建設，「網軍」在過去 20 年間已快速具備系統性、常規性、隱匿性之規模與攻防自若的有效能力，其目標亦已超越純軍事領域的範疇，而以獲取全面性國家利益爲目標。

網絡空間的開放性與隱匿性，加上當代資訊通信科技的環境，造成「使用者—管理者—設計製造者」3 端的資訊權力不對稱結構，而使各類非法入侵者有危害網絡安全的極佳機會與空間；從攻防雙方的成本來看，以網絡空間爲戰場的戰爭，明顯有易攻難守的特性。對各國或有特定目的組織及個人而言，在現實利益的考量之下，網路攻擊確實是一種價廉效高的行動。

網絡空間沒有國界。包括我國在內，世界各國已注意到網絡安全問題是國家安全新戰場。或許「網軍」只是一個代名詞，提醒政府、企業、組織與每一個應用資訊通信科技的人們注意在資訊權力不對稱之下，網路「不安全」的隱憂將如影隨形地跟隨。國家安全的規劃者與從業者，必須從底層的戰技（ICTs 操作技術）、戰鬥（ICTs 技術應用）開始理解「安全」的變化，方能擬定適切的高層戰術（ICTs 發展策略）與戰略（國家安全與利益取徑），有效對付來自四面八方的「網軍」危安攻勢。

（本文為作者個人意見，不代表本部政策立場）

The Development and Network Offensive/Defensive of PRC's Cyber Force and ROC's Policy Formulation to Information/Communication Security

Cheng-lung Tai

Assistant Professor
Graduate Institute of Strategic Studies and International Affairs
National Defense University

Abstract

From the 1970s, the rapid development of information and communication technologies has created many advantages for human beings. The influence of computer and Internet popularization on individuals and communities is even greater. In the meantime, the virtual cyberspace also becomes a new sphere of power struggles and poses potential threats. This article tries to analyze the PRC cyber force's context and development, raise the issues of participator's structure, and information power asymmetry and cyber war characteristics. Moreover, based on cyber force's capabilities in information and communication technologies, this article tries to predict possible offensive/defensive scenarios, point out anarchy in cyberspace, and analyze logical paradox of state actors in cyber O/D action. In the end, this article comments on ROC's policy formulation to information/communication security by surveying the government public records.

Keywords: cyber space; cyber security; information and communication technologies; anarchy; information power asymmetry