台灣國際研究季刊　第 12 卷　第 3 期　頁 51-68　2016 年/秋季號
Taiwan International Studies Quarterly, Vol. 12, No. 3, pp. 51-68 Autumn 2016

中國近期網路作為探討：從控制到攻擊

林穎佑
銘傳大學國際事務與外交學程兼任助理教授

摘 要

隨著資訊技術的應用，網路科技也深入至人類生活的每一角落，特別是對中國來說，電子商務的成長也逐漸的加深對於網路科技的應用，但隨著經濟發展利潤所隨之而生的便是有心人士與網路犯罪的覬覦。以及網路的匿名與自由的輿論傳遞特性也與中國對待媒體的態度有所抵觸，這都讓中國在 2000 年之後開始加強其網路監控組建中國的網路防火牆，也是日後防火長城。希望藉此控制網路的言論，以免危及政府的政權。除了對內的控制之外，中國也瞭解網路技術在軍事上的運用，已成為未來戰爭的決勝制高點。過去只有單純的與民間具有資訊專業背景的人士合作，或對懷有敵對意識的網站發動置換網頁等騷擾性的行為，但近期已演變成透過網路竊取資訊、癱瘓對方系統或是利用病毒破壞重要關鍵基礎設施都是近期中國網路作戰的模式。有鑑於網路發展的面向十分多元，難以在有限篇幅中予以討論，因此本研究集中探討於中國對內的網路控制以及其對外攻擊的手法與樣式。並嘗試融合技術面的研究以期能更加理解網路政策的內涵，而非流於政策宣傳的文字探討，方能一窺虛實。

關鍵詞：中國研究、解放軍研究、網路安全

壹、前言

隨著資訊時代的來臨，網路的應用也深入至人類生活的每一層面，特別是對中國來說，伴隨著經濟的成長以及民眾對外交流的影響，也逐漸的加深對於網路科技的應用，從最早利用數據機以及傳統電話進行撥接的上網模式，逐漸進步到新型的通訊協定甚至配合行動數位技術的進步，將網路技術與經濟發展模式加以配合，讓電子商務與行動支付結合，更加擴大了經濟效益。但隨著經濟發展利潤所隨之而生的便是有心人士的覬覦，豐厚的利潤造成了駭客集團以及網路犯罪的發展，而網路的匿名性與自由的輿論傳遞也與當前中國的政策有所抵觸，同時也有許多的網路間諜透過網路的連結來竊取相關資料，這都讓中國在 2000 年之後開始加強其網路監控，並且開始組建中國的網路防火牆，這也是日後防火長城的雛形，並且加強網路監管，希望藉此控制網路的言論，以免危及政府的政權。

除了對內的掌握之外，中國政府也從歷次的軍事衝突中，瞭解到網路技術在軍事上的運用，過去只是單純的與民間具有資訊專業背景的人士合作，對懷有敵對意識的網站發動置換網頁等騷擾性的行為，但隨著資訊技術的發展以及政府與民間對於資訊技術的依賴，不論是透過網路竊取資訊、利用分散式阻斷服務攻擊（Distributed Denial of Service attack, DDoS）癱瘓對方系統或是利用病毒嘗試破壞重要關鍵基礎設施都是近期網路作戰的模式，而中國也不例外（洪海等人，2014）。特別是在解放軍的體系中建立網軍部隊，並與大專院校合作藉此培養網路人才以供其未來運用（En, 2014）。此外也結合商業模式，與其出品的電子產品合作，建立自身的供應鏈避免受制於外國的可能，並從硬體軟體等各方式建立自身的資訊優勢，嘗試為未來的戰爭建立資訊優勢。即便是在全球化經濟的影響之下，各國處於鬥而不破的局勢，但看不見的網路戰爭卻隨時隨地的發生在虛擬空間之中，數位軍火造成的破壞可能遠已超越傳統的軍事武器。特別是我國處於特殊的國際政治環境，由於資訊條件的發達，讓台灣成為許多網路攻擊的頭號目標與駭客鍛鍊技術的「練兵場」，這些因素都讓我國必須更加重視資訊安全的相關議題，及中國對於資安的發展，增強我國國家安全。

貳、中國對內網路控制手段

最早中國政府只是單純的將網路視為媒體的一部分，一個新技術的應用，這也可從近期中國將網路輿論的應用冠上新媒體一詞可以看出。而中國政府一向將媒體視為意識型態的國家機器，從報紙、廣播、電視都在政府其掌控之下。有鑑於網際網路有許多傳統媒體所不及的特性（如匿名性以及傳播的速度），中國政府透過技術控管的方式，管理人民連外和國外連接入中國的訊息內容，達到控制的目的。甚至在近期習近平的講話中，也直接指出新媒體的輿論傳播力與引導力會是未來社會的主流，因此必須要特別關注的網路應用與新媒體的發展（新華社，2016）。

早在 1996 年，中國就頒佈了「中華人民共和國計算機信息網絡國際聯網管理暫行規定」，以及「計算機信息網絡國際聯網出入口通道管理辦法」（中國網路空間研究院，2015）。其中對於個人、法人和其他組織（用戶），若要使用國際網路，必須調相關單位辦理申請登記，其餘需要連到國際聯網的用戶，必須使用郵電部國家公用電信網所提供的通道，任何單位或個人不得自行建立或使用其他通道進行國際聯網。2000 年 10 月則進一步對於網路服務，內容的法案「互連網信息服務管理辦法」與「互連網電子公告服務管理辦法」其中明訂欲從事資訊服務，需向主管機關申請，核准後方能實行經營性資訊服務，而非經營性資訊服務則也需要備案後方能實行。而對於電子公告（BBS）部分亦規定：未經專項批准或專項備案手續，任何單位或個人不得擅自開展電子公告服務（黃柏翰，2005：49）。而在 2000 年 11 月，更特別針對網路新聞的管制發佈了「互連網站從事登載新聞業務暫行規定」，為全球第一個針對網路上登載 新聞業務加以規範的國家法令。在法令之下，中國也利用國家的力量來對網路進行控管，最有名的就是俗稱「防火長城」的系統，其名稱來自於學者 Charles R. Smith 在 2002 年所發表的一份有關中國網路審查的文章，其認為中國的網路審查透過了技術上的支援，將具有敏感詞彙的字詞，加以遮蔽，其功能與過去抵擋北方游牧民族入侵的長城有異曲同工之妙，因此取名為 Great Firewall，一般網路都稱為 GFW（Bu, 2014）。

特別是在 1999 年科索沃戰爭，便有中國駭客利用入侵北約網路系統以及透過電子郵件夾帶惡意程式、入侵官方網站來對北約轟炸表達抗議。隨後，美軍誤炸位於南斯拉夫的中國大使館後，意外帶出美中兩國熱血網民主動發起網路攻擊（東鳥，2010：45）。雖然在當時的技術限制之下，兩國大多是利用網頁的設計漏洞入侵，並且主要是透過更換網頁的方式達到宣傳以及騷擾的目的。但這些攻擊已經敲響中國政府的警鐘，開始思考未來如果再發生類似的事件，中國的網路安全防護系統是否有可能會遭到破壞而崩解？今日來自外國的駭客可以輕鬆的置換網頁，是否也代表其可以輕易的竊取電腦上的機密資料？而中國網民雖然號稱愛國駭客，但若是這些人無法被政府控制的話，是否有可能會在某日對政府發動網路攻擊？在這些考量之下，都讓中國政府認為必須加強網路監管，已確保在資訊上的掌控確保政權與國家的安全。

在防火長城的運作之下，透過通訊協定的設定以及對於關鍵字的鎖定，許多中國政府不想看到出現的網路上的資訊，都會遭到技術性的屏蔽。如六四天安門事件一直是中國政府的大忌，自然不會出現在中國的搜尋引擎中，其他涉及「敏感」的字句，如台獨、藏獨、疆獨、法輪功等都是中國網站上嚴加看管的文字。此外可以自由讓民眾接觸到不同言論的社交平台（如 Facebook），或是自由散播各種影音資訊的平台（如 Youtube），其標榜自由的精神自然不容於中國政府，因此都是封鎖的對象。甚至是提供電子郵件服務的系統商，中國也要求必須提供網管權限以及配合中國政府可以進行調閱記錄，這些都讓許多電子系統商重新思考中國市場的利與弊。美商 Google 由於不願意配合中國的網管政策，因此在 2010 年宣布退出中國市場，而在中國自然也無法使用其 G-mail 收發信件。許多知名的通訊軟體也有類似的狀況發生，如目前市佔率相當高的 LINE，若是安裝在美商 APPLE 的 IOS 系統上，便會遭到中國防火長城的阻攔，但是若使用者選擇的是 Android 系統則完全無此問題，這可能與 IOS 的加密語法有相當的關係。APPLE 並無提供其解密金鑰給外界，甚至是連美國的聯邦調查局（Federal Bureau of Investigation, FBI），若在無外界的支援之下，也無法憑一己之力破解其加密演算法（林亞慧，2016）。在無法完全掌握的情況

之下，最好的方式就是施加干擾使其無法正常運作，這就是中國政府的網路政策。

值得注意的是，雖然中國政府有計畫的屏蔽部分網站，但這些網站都有中國所自行研發的類似功能的系統可以作為替代品。如在中國無法使用 Google 搜尋，但百度的出現適當的彌補此不足，而在影音平台上，中國也有土豆網、優酷網等類似的網站。而在通訊平台上，在中國最多人使用的系統從早期的 QQ 到近期的 WeChat，都是由中國廠商一手打造的，這些軟體在中國政府有計畫的推廣之下，也可能會有資料備份以及監控的作用。雖說如此，但在中國其憑藉著龐大的市佔率，讓外國人只要有意願與中國朋友聯繫，很難不使用其系統，這也在無形之間將這些人納入其監控之中。而中國政府為了達成監控國內網路的目的，也設計了三種不同的系統來對網路做出監控。其中「防火長城」是由宣傳系統所掌握；「金盾系統」則是中國公安部門來監管；而「綠壩」則是由工信部所掌握（劉文斌、孔德瑞，2010：33）。而這些監控單位不只是解放軍內部保衛部門與國安體系，也與公安部有業務情報上的合作（王官德，2008：185）。

除了禁止可能散播不利訊息的網站之外，為了善用網路此一新媒體的宣傳能量，中國也出現所謂的「五毛黨」與「網路水軍」的名詞。網路水軍此一名詞最早出現在行銷學之中，其基本定義為：特定組織雇用網路公關公司，為他人針對特定產品或是特定議題發表文章或是回應他人文章，期望藉此打響自身的知名度（林叢晞，2012：139-40）。特別是在網路的討論中，當多數社群成員的發言有特定傾向，贊同的人會有正面的反應，反對的人則保持沉默。即使有人會分享其他貼文，但這些轉載文章也多是經過立場篩選。這將會導致社群成員更增強其原有的觀點，缺乏不同論點的對照與思考。此外，許多以議題為主的討論區雖鼓勵發表多元論點，卻由於網路的特性造成言論內容淺薄或流於情緒的批判，缺乏了理性對話或評論的機會，類似的效果正是網路水軍所追求的目的（黃國鴻，2015：86-87）。而另一個類似的名詞，則是五毛黨，五毛黨基本上與網路水軍十分類似，但這些網民基本上就是中國政府的代言人，在網路上透過大量吹捧或是以積極正面的網路發言來對中國的行為做出宣傳。甚至會主動前往

其他國家的網路論壇，或是新聞媒體的官方網站大量留言，創造出主流民意支持中國政府作為的假象。而也在主要的網路管理站協助之下建立「網管員」（網路管理員）負責監控網站言論，該等網管員具有三種以上的作用：發現負面反政府言論就通知網管站加以刪除；主導網路論壇，引導輿論方向，協助政府導正網民觀念；發表或製造親政府輿論，協助政府達成政治控制的目的，如在中國主流的社交平台微信與微博上，都有類似的網管人員協助監控，來防堵系統監控的漏洞（Wright, 2010: 6）。

為了有效達到控制網路的目的，中國政府在網路使用上也採取了「實名制」，政府可以透過 IP 追蹤的方式確定每一位上網者的身份與位置，如其言論或是言行真有涉及中國國家安全之虞，司法體制是可以循線進行追蹤，即便是在公共網路，也必須要有證件出示身份才能使用網路，主要就是為了確保網路用戶的真實身份。但道高一尺、魔高一丈，許多的民眾也透過網路技術不斷的嘗試突破中國政府的封鎖，從關鍵字的修改（如代號、或是發音相近的字句）到 IP 位置的跳版（潘月紅，2006：67），以及直接利用 VPN（Virtual Private Network）跳板來達到翻牆的目的，或是直接利用實作匿名通訊的軟體（The Onion Routing, Tor；中文俗稱為洋蔥）搭配公共網路，來進行溝通與交易，這都是為了因應網路審查下所出現的特殊狀況（Dingledine, et al., 2014）。

而中國的網路環境也造成了匿名假帳號以及網路詐欺的橫行。由於網路審查的原因，讓許多具有專業網路技術的駭客，為了追尋隱私與自由開始利用自身的技術來逃避中國的網管，這些盜取身份以及販賣個人資料的行為，搭配豐厚的電子商務利潤，造就了中國特有的網路地下經濟，也就是俗稱的「黑色產業鏈」（騰訊安全實驗室：2015）。無論是透過竊取的假身份，或是利用木馬程式植入被害人的電腦，將其成為殭屍網路的一環，作為日後發動攻擊的跳版，都是利用科技避開網路審查的方法（畢裕，2014）。而近期興起的行動支付、數位產品以及物聯網的普及，更是成為網路詐騙犯罪集團最好的工具，其利用網路的超地緣特性以及殭屍網路的匿名性，避開司法單位的追蹤（馬克．古德曼，2016：307-20）。這也是近期中國在國際資安會議上多次遭到其他國家抨擊的原因，中國的網路犯

罪已經成為國際上的問題，成為當今重要跨境犯罪問題。這也突顯出中國的網路管制依然存在許多的漏洞，以及其雖能限制網民的言論，但是只能收到表面的效果，而非從根本杜絕其問題，甚至會演變出更加難以掌握的黑色產業鏈，這都是中國在進行內部網路控管時，並無想到的問題。

近期這些封鎖系統更為進化，封鎖所採用的資訊技術手段已不限於阻止網民獲取資訊，而是已經轉為握網路意識形態（網權與制網權）、資訊技術話語權的對決，主因是金融與經濟等資料，現在都已成為電子數位資料的形式在全球流通，而其中資訊加密與解密的戰爭，甚至會波及關鍵基礎設施的運作（如密碼被竊取，以及遭到電腦蠕蟲的破壞而癱瘓）。過去的防火長城也在不斷的進化後變成所謂的中國加農砲（Great Cannon）藉由攔截大量網路流量，對特定目標網站發動 DDoS 攻擊來癱瘓敵對網站。如之前對中國政府抱持著質疑態度的香港媒體，以及線上原始碼儲存網站 GitHub、監控防火長城封鎖現況的 GreatFire 網站，都遭到了攻擊，這次攻擊採用了「旁觀者攻擊」（man-on-the-side attack）的新技術，並配合 DDoS 方式癱瘓這些網站使其失去效能（Marczak, et al.: 2015），並讓這些監控與攻擊都有可能隨著中國軟體而擴散至世界。讓被害者的網站系統完全癱瘓。

除了技術的進步之外中國也積極經營網域空間，嘗試成為能與美國分庭抗禮的網路大國。這些企圖都可從其對資訊產業的投資中可看出，近期中國製造的資訊產品已經逐漸進入國際市場，特別是其低廉的成本更是吸引許多民眾的青睞[1]。此外，中國也透過召開國際性的世界互聯網大會、電子商務、甚至資訊安全大會，除吸引外資，也期望形塑出中國已是資訊大國，符合近期中共在許多國際重要場合的表現，企圖以新型大國關係的姿態經營其國際地位（張裕亮，2016：19-22）。如在 2016 年與俄羅斯莫斯科舉辦的中俄網路空間發展與安全論壇中，除了探討技術合作之外，打擊網路犯罪、通信與網路安全以及網路治理，中國網信辦主任魯煒更是在開幕式上暢言其對於網域空間的理念，認為同為網路大國的中俄，應如何發展與治理網路空間，並應負起大國應有的責任與擔當（中新社，2016）。

1 如華為、中芯、小米、安全衛士 360 等中國廠商。

特別是隨著習近平的上台後，中國成立「中共中央網絡安全與信息化領導小組」、「中華人民共和國國家互聯網信息辦公室」這些單位都是由習近平親自主導與整合網路發展與網路控制的國家單位。其積極朝總體佈局統籌各方創新發展，努力建設成為網路強國為主要方向，並在多次的談話中都有提到必須維持網路安全，才能確保國家安全，可見其已將網路安全列為國家安全中的重要一環（新華網，2014）。其中更是將網路技術的發展作為產業信息化的火車頭，配合未來中國製造 2025 以及物聯網+的應用，發揮知識經濟的效用。但隨著網路技術的發展，對於網民的管控以及引導輿論的作用便更加重要，這些訊息都透露出習近平對網域空間治理的態度（新華社，2016）。

叁、中國網路對外攻擊方式

在網路空間的攻防上，硬體設備的好壞並不是決定勝負的關鍵，這也讓許多國家發現此一能與大國一決勝負的新領域。網際網路的普及是在 1990 年後所發展的新科技，而個人電腦以及數位行動裝置的普及，也讓硬體科技的門檻下降不少。這也促成在進行網路攻擊時，並不需要過於先進的裝備，反而是駭客自身的技巧才是網路空間一決勝負的關鍵（李倫銓，2015）。過去在傳統軍事作戰中，科技經常主導戰場上的勝負，特別是從軍事事務革命的角度來看，科技的優勢可以適當的彌補數量的不足，甚至達到主宰戰場的目的（Farrell & Terriff, 2005: 299-301）。

因此在網路戰場中，科技所佔的因素卻無傳統軍事作戰一般的高。電腦的進步只會影響到運算速度，同時在全球化的影響之下，一般國家對於資訊科技的落差並無過大，甚至在軍方也有部分系統是與民間相同，與傳統軍事武器相較，資訊設備在軍民之間的差距較小，也代表各國在資訊科技上的差距是有限的，反而對資訊依賴程度較高的先進大國其在資安防禦上更容易出現漏洞（Clarke, et al.: 2010: 144-46）。因此擁有駭客技術的人才只要有適當的電腦設備，可連結至網際網路，就有可能入侵系統。不論是透過攻擊關鍵基礎設施或是竊取重要情資，小國都有利用網路攻擊戰勝

強國的機會。

此外，在資安攻防的領域上，發現漏洞永遠會比修補程式來的快速與容易。過去傳統軍事上遭受實體攻擊時，可能還可透過地理位置的方式分散風險，但在網域中除了實體隔離外，一旦資安防禦網遭攻破，入侵者可以藉由控制權限以及內部網路達到擴散的目的。因此，即便最先侵入的電腦可能與最終目標無關，但若員工缺乏資安意識以及內網的連結，最終還是可以達到攻擊方目的。又在雲端科技的加持下，只要有一端遭到入侵，可能整個資料庫便全面失守。而在 10 個漏洞中，即便防守方找到 9 個，只要有一個被攻擊方發現並成功入侵，前面防守方的努力便白費（Hotz, 2015）。因此在網路的領域中，並無明顯的防禦縱深，這都是在資安領域中先天對防守方不利的原因（Denning, 2003: 45-48）。

中國很早就體認到網路在戰場上的效益，早在 1999 年開始解放軍就已經展開組建「信息戰士」的任務。當時解放軍的規劃「信息士兵」僅限於解放軍內部人員，無論素質和數量均遠不足規劃所需，所以才開始在各地發掘與資訊產業相關行業中找尋人才，組建全國性的「信息戰民兵」組織，平時負責研究、訓練和演習，戰時執行軍事任務。從一些文獻來看許多近期的網軍攻擊技術其實早在 2000 年左右就已經大致成形了（閻雪，2000）。特別是在網路空間的作戰並不需要前往特別的演習地，只要可以連上網路，就可立刻上戰場發動攻擊，超越了地域性以及時間性的限制（呂兆祥，2015：12-14）。

而在 2002 年，當時身為解放軍總參四部（電子對抗雷達部）部長戴清民少將在一份內部報告中透露，解放軍總結「信息戰」的十大樣式聚焦於「網電一體戰」（林勤經，2002：439）。美國國防部於《2008 年解放軍軍力報告書》中便宣稱：「針對中國民用和軍用網路的攻擊能力，正是解放軍發展不對稱戰法的非接觸作戰中的重要組成」（劉宜友，2011：121）。解放軍認為在戰役初期掌握電磁優勢，是確保戰場勝利的首要任務。「網電一體戰」便是形容利用電子戰、電腦網路作戰、動態殺傷等方式以阻斷支持敵方作戰與投射武力的戰場網路資訊系統，並將「網電一體戰」視為「一體化聯合作戰」的基本形式之一。

從 2005 年起，中國便有許多針對美國不同目標產業的網路攻擊行動，如針對 Google 發動的極光行動（Aurora Operation）、能源產業的夜龍行動（Night Dragon）、國防產業與智庫的驟雨行動（Titan Rain）、而後更有攻擊更為細密的暗鼠行動（Operation Shady RAT）（Bodme, et al.: 2014: 2-22）。在上述的攻擊中，大多都是利用 APT 攻擊（Advanced Persistent Threat, APT），對美國重要單位進行網路入侵。APT 攻擊首見於美國空軍在 2006 年所提出的報告，其特性為高針對性、潛伏期長、高威脅性。也因為此，除了具有特殊資訊專長背景的人有可能在短時間內發現異狀之外，一般人員根本不會注意到大量數位資料已經外洩（黃浩倫，2016）。APT 攻擊所重視的是攻擊者的資料來對攻擊目標量身打造設計專屬的社交工程（social engineering）策略，配合魚叉式攻擊（spear-phishing）藉此突破目標的資安防護（Wrightson, 2015: 164-67）。隨著資安防護意識的增強，中國網軍的 APT 攻擊也開始由對目標進行社交工程，開始改為針對特殊的網路設備進行攻擊，將目標鎖定特殊設備（如網路路由器）的韌體發動網路攻擊，特別是這些機器很可能本來就是中國廠牌，在未來物聯網的環境下，類似的攻擊手法發生的機會只會更為升高。

如中國網軍在 2011 年竊取美國航太公司洛克希德馬丁所研製的 F-35 戰機資料。其攻擊的流程，便是先以洛馬所採用的動態密碼供應商 RSA 公司為目標，將惡意程式偽裝成 Excel 檔並以人員應徵的名義寄送至 RSA 員工信箱，取得帳號密碼竊取動態密碼的演算法相關資料，攻破最後目標（洛馬）的資安防線，竊取重要的戰機資料（Clarke & Knake: 233-35）。其中的關鍵便在於利用 Adobe Flash 的漏洞 CVE-2011-0609 從中植入木馬取得動態密碼（SecureID）的參數，這便是「零時攻擊」（zero-day attack）的作用。零時攻擊是指程式漏洞被駭客發現，但官方還未提供修補程式的安全漏洞（此種漏洞稱為零時漏洞），而在資訊大廠根本無法得知的情形之下，自然無法推出修正程式，造成選用該產品的廠商根本無法採取任何防禦措施，最終釀成災情（王清，2011：2-5）。

在分析國家網軍的行動與目標時，除了單純的技術分析之外，若能結合情報學的觀點，甚至是該國情報體系的特色，或許更能發揮事半功倍之

效。如中國網軍的組織普遍認為是專職電子情報的總參三部（中國人民解放軍總參謀部技術偵察部）與總參四部（中國人民解放軍總參謀部電子對抗與雷達兵部）是負責網軍的主要單位（Stokes, et al.: 2011）。從技術層面分析，此觀點並無錯誤，特別是在許多資安報告上都明確的指出 61398、61486 都是隸屬於總參三部底下的部隊。但今天在網軍主要運用的 APT 攻擊上，重視的是攻擊者的基本資料、工作執掌、交友狀況、研究喜好、生活特徵、作業系統，並藉由這些情資的收集，來對攻擊目標量身打造設計專屬的社交工程策略，藉此突破目標的資安防護，這些資料都是負責情報彙整的總參二部（中國人民解放軍總參謀部情報部）的職責，而二部也相當重視網路的功用（尼科拉斯，1998：117）。

另一值得注意的角度在於，網軍是屬於國家指揮的網路作戰部隊，但不同的部門也會有各自的網軍單位，這又與該國的情報蒐集體系有所關連。如中國負責情報的單位除了隸屬軍方的總參謀部體系與總政治部的聯絡部外，還有隸屬國務院的國家安全部，以及司法公安單位。這些組織理應都有所屬的網路作戰單位，只是其所負責的領域各有不同。根據中國情報體系的分工，主要對外情搜主要由總參體系負責（包括政軍經心各類），而國安部以反情報以及針對反對勢力組織（如藏獨、疆獨、法輪功）為主，公安體系底下是以治安事件為主，反情報為輔（但中國國安部成員也自稱警官，因此真實身份外人不易瞭解）。不同的職能也反應到網路部隊的任務之上，如國安體系會針對境內管控，網路封鎖為主，並且針對海外反對勢力進行網路攻擊（除竊取資料之外、近年也開始利用 DDoS 技術嘗試癱瘓境外主機）；隸屬解放軍體系的網軍則是配合部隊需求竊取相關資料。因此在分析資安事件時，若能先透過資產鑑別，瞭解自身單位的屬性，並配合對中國情報組織的瞭解，在輔以數位鑑識（log 檔的紀錄），應能對攻擊來源作進一步的確認。

而隨著解放軍在 2015 年底開始的一系列軍事改革，中國網軍的編組也有了相當的變化，其中最大的改變便是在戰略支援部隊的成立。過去解放軍的對外情報作為主要是由負責人因情報的總參二部、負責電子情報與網路作戰的總參三部、四部，總政聯絡部、甚至總裝也有負責科技情報的情

搜單位（平可夫，2011：143-44），現以全部調至戰略支援部隊，這也代表解放軍情報部門的重整。特別是在總參二部與三部的整合上，過去解放軍網軍大多歸屬於總參三部的麾下，但其多半偏重於技術領域的駭客，現今若與總參二部的人事情報與分析能力進行整合，勢必會讓中國網軍的實力如虎添翼，對其他國家的攻擊更為猖獗。而在大軍區改組為戰區之時，戰略支援部隊並無隸屬在戰區的指揮，可見過去在總參體系下散落至各大軍區各司其職的網軍部隊，現以透過軍改進行整合由中央統一指揮網軍作戰，而非由過去散落各地的網軍自行選擇目標，畢竟網域空間唯一超越地緣的新戰場。

而除了原有的解放軍成員之外，中國也積極與民間駭客合作，從早期的紅客聯盟到近期的烏雲安全網，這些成員都是中國政府密切合作的對象，除了善用其在網路技術上的天分之外，也可以利用民間駭客並無政府身份，可以進行更多處於灰色地帶的任務。中國積極與民間社團合作，甚至在 2016 年成立了中國網際網路安全協會，作為與民間接觸以及進行國際交流的平台，更是規範中國資訊安全產業的重要組織。這些都是習近平所提出的網路強國戰略中的一環。（中國網信網，2016）

肆、結論

現今中國對於網路安全的議題日益重視，如在 2014 年成立中央網路安全和信息化領導小組，由習近平擔任小組長，顯示中國已將網路安全及發展，提升為國家安全戰略一環。並統合軟體、硬體、人才與指揮，以確保網路安全。

而中國也積極利用其龐大的市場作為經濟誘因，吸引過去因為不服從網路政策而離開的企業。如 2015 年習近平訪問美國時，先前往西雅圖舉辦美中網路產業論壇中可看出。會議由中國政府主導，微軟（Microsoft）協辦，美國各大科技廠商無一缺席，探討網路合作以及資訊產業在中國發展的前景。未來美國企業是否會為了商業利益與中國有更多的合作或妥協，而中國在開放市場時是否會持續維持資訊管控，都是未來觀察的焦點。

而網路作戰是解放軍近期積極經營的戰場，而為了避免引發戰爭以及牽涉到國際法規，各國在發動網路作戰時，經常會與民間駭客組織合作，以雇用「網路傭兵」的方式進行攻擊。這些中國駭客組織其與政府有不少的合作關係，除了給與報酬之外，也在不影響國家安全以及符合官方利益目標的前提之下，默許其遊走於灰色地帶的網路作為（劉得民，2014：26）。甚至直接與民間大學合作，作為未來網軍的人才庫。並透過中國國家網際網路應急中心贊助的烏雲安全網，作為中國資訊安全性漏洞資料庫的回報平台（劍心，2014），並積極透過資訊大廠舉辦中國的資訊安全大賽（如百度盃）期望藉此籌備未來的資訊人才。但這些都違背所稱所謂的駭客信念[2]，日後是否有可能出現中國版的史諾登事件，也是外界可注意之處。

相對於中國的成長，我國在資訊技術上有一定的水準，甚至在駭客人才的素質上，民間自行組成的駭客隊伍，屢次在國際駭客競賽中創下佳績，許多資安公司也受到國際大廠的青睞以高價併購，甚至在駭客攻防的技術上，都是其他國家取經的對象，這都表示我國資安技術的實力絕對可與其他國家一較長短（陳文政，2015）。

2015 年民進黨所提出的國防願景藍皮書中，針對未來的網路威脅，提出了相當多的看法，也預計將資安列入航天、造船等國防產業的行列，並提出在執政後籌組資電軍的計畫。上述的國防規劃也有出現在 2016 年蔡英文總統就職後的諸多對外講話內容。值得注意的是在其藍皮書中的規劃裡，資電軍並不是只有網軍，網路作戰只是其一部份，其主要的作為是在於支援聯合作戰所必須具備的 C4ISR 能力，是以資電整合作為技術前提而形塑出的作戰部隊，網路空間的競逐只是其中的一環，而非全貌。同時在網路安全的領域裡，一般軍方的網路部隊不可避免的會與情報單位有所關聯[3]，這也造成軍方並不適合做為主導全國網路安全的單位，這也會導致在進行國際交流時的障礙。因此較可行的作為應該是在行政院的體系下建立

2 所謂駭客信念：不要損壞（包括崩潰）你所侵入的電腦系統、不要更改那些系統中的訊息（除了修改日誌掩蓋自己的蹤跡）、分享所獲得的訊息（Dreyfus & Assange, 2012: 475-79）。

3 如美國網站司令部的指揮官一般也身兼美國國家安全局（NSA）局長。

專屬的資訊安全單位，作為民間資安的管控組織以及對外交流的窗口，未來的資安防禦更需要的是情資的分享以及攻擊手法的通報分析交流，這也是近年各國逐漸重視網路安全聯合演習、以資訊安全情資交流的主要原因。

在特殊的政治環境影響之下，我國經常成為中國網軍駭客的頭號目標或是測試病毒的練兵場，卻也因此擁有大量的電腦病毒樣本，這些分析能力都是我國發展資安產業的基礎。此外，我國對於解放軍研究以及中國問題的觀點往往能突破西方學者的盲點，而有創見，這些都是我國可以在國際上發揮的本錢。因此，若是能有效整合我國資安實力以及長期對解放軍研究累積的能量，以技術配合情報與軍事的科技整合，或許是未來研究的新途徑。

參考文獻

中國網信辦，2016。〈中國網路空間安全協會成立〉《中國新聞網》3 月 26 號（http://big5.chinanews.com/gn/2016/03-26/7812399.shtml）（2016/06/20）。

中國網路空間研究院，2015。《中國網際網路 20 年發展報告》12 月 16 日（http://big5.china.com.cn/news/world/2015-12/16/content_37328346.htm）（2016/6/18）。

中新社，2016。〈首屆中俄網路空間發展與安全論壇在莫斯科舉行〉《中國新聞網》4 月 28 日（http://big5.chinanews.com/gn/2016/04-28/7851880.shtml）（2016/06/19）。

王官德，2008。《中國共產黨對解放軍的控制》。台北：知書房。

王清，2011。《0day 安全：軟件漏洞分析技術》。中國北京：電子工業出版社。

尼柯拉斯（李豔譯），1998。《中國情報系統》。台北：明鏡出版社。

平可夫，2011。《中國間諜機關內幕》。Richmond Hill, Ont.：漢和出版社。

呂兆祥，2015。〈共軍網路作戰對我資電作戰之影響〉《國防雜誌》30 卷 6 期，頁 1-27。

李倫銓，2015。〈失衡的數位軍火發展〉發表於「CLOUDSEC 2015」。台北：企業資安高峰論壇。8 月 13 日。

東鳥，2010。《中國輸不起的網路戰爭》。中國長沙：湖南人民出版社。

林亞慧，2016。〈FBI：破解槍擊案犯人的手機方法只適用於 iPhone 5c〉《科技新報》4 月 8 日（http://technews.tw/2016/04/08/fbi-cracking-iphone-method-only-apply-to-iphone-5c/）（2016/05/08）。

林勤經，2002。〈中共網軍建設與未來發展〉收於林中斌（編）《廟算台海》頁 431-67。台北：學生書局。

林叢晞，2012。〈從傳播視角探析 “網絡水軍” 現象〉《中國傳媒科技》12 期，頁 139-40。

洪海、曹志華、鮑旭華，2014。《DDoS 分散式阻斷服務攻擊深度解析》。台北：碁峰出版社。

馬克·古德曼（Marc Goodman，林俊宏譯），2016。《未來的犯罪》（*Future Crimes*）。台北：木馬文化事業。

張裕亮，2016。〈第二屆世界互聯網大會評析〉《展望與探索》14 卷 1 期，頁 18-24。

畢裕，2014。〈寄生在騰訊業務下的黑色產業〉發表於「2014-HITCON 第十屆台灣駭客年會」。台北：台灣駭客年會。8 月 20 日。

陳文政，2015。〈國防產業不能有顏色〉《蘋果電子報》10 月 15 日（http://www.appledaily.com.tw/realtimenews/article/new/20151015/711363/）（2016/5/8）。

無作者，2015。〈2014 年騰訊雷霆行動 網路黑色產業鏈年度報告〉《環球網》〈http://tech.huanqiu.com/it/2015-01/5452665.html〉（2016/5/4）。

黃柏翰，2005。〈中國大陸網際網路檢查政策概況〉《應用倫理研究通訊》35 期，頁 47-52。

黃浩倫，2016。〈被攻擊的那五年：APT Operation 運作模式大解析〉發表於「2016 台灣資訊安全大會研討會」。台北：IThome。3 月 8 日。

黃國鴻，2015。〈網路資訊傳播與大學生的社會參與〉《台灣教育評論月刊》4 卷 1 期，頁 86-87。

新華社，2014。〈中央網路安全和資訊化領導小組第一次會議召開 習近平發表重要講話〉《新華網》2 月 27 號（http://www.cac.gov.cn/2014-02/27/c_133148354.htm）（2016/06/19）。

新華社，2016。〈習近平：堅持正確方向創新方法手段 提高新聞輿論傳播力引導力〉《新華網》2 月 19 號（http://www.cac.gov.cn/2016-02/19/c_1118102596.htm）（2016/06/19）。

新華社，2016。〈習近平總書記在網路安全和資訊化工作座談會上的講話〉《新華網》4 月 25 日（http://www.cac.gov.cn/2016-04/25/c_1118731366.htm）（2016/06/18）。

劉文斌、孔德瑞，2010。〈中共網際網路控制作為研析〉《展望與探索》8 卷 10 期，頁 24-49。

劉宜友，2011。〈淺析中共網電一體戰〉《國防雜誌》26 卷 3 期，頁 120-34。

劉得民，2014。〈中國大陸網軍外圍組織現況研究〉發表於「中國大陸在網路空間戰略的競逐學術論壇會議」。台北：中共研究雜誌社。7 月 7 日。

劍心，2014。〈烏雲這幾年運作的心得及優缺點〉發表於「2014-HITCON 第十屆台灣駭客年會」。台北：台灣駭客年會。8 月 20 日。

潘月紅，2006。〈淺談網路安全技術〉《應用技術》7 期，頁 67-68。

閻雪，2000。《中國大陸的駭客技術》。台北：松岡電腦圖書。

Bu, Ruiwei. 2015. “The Great Firewall of China.” (http://campus.murraystate.edu/academic/faculty/wlyle/540/2013/Bu.pdf) (2016/4/29)

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War*. New York: Harper Collins.

Denning, Dorothy E.（戴清民、吳漢平譯），2003。《信息戰與信息安全》（*Information Warfare and Security*）。中國北京：電子工業出版社。

Dingledine, Roger, Nick Mathewson, and Paul Syverson. 2014. “Tor: The Second-Generation Onion Router.” (http://www.onion-router.net/Publications/tor-design.pdf) (2016/5/5)。

Dreyfus, Sulette, and Julian Assange（王蕎、李現芳、葉曉紅譯），2012。《維基解密創辦人帶你揭開駭客手法》（*Underground*）。台北：國際漢宇。

En, Austin，2014。〈分析台、中、韓三國駭客養成文化，專訪世界級駭客團隊 HITCON 總召蔡松廷〉《有物報告》（https://yowureport.com/14137/）（2016/5/7）。

Farrell, Theo, and Terry Terriff（國防部譯），2005。《軍事變革之根源：文化政治與科技》（*The Sources of Military Change: Culture, Politics, Technology*）。台北：國防部。

Hotz, George. 2015. （Why Are Our Tool So Terrible?）發表於「2015- HITCON 第十一屆台灣駭客年會」。台北：台灣駭客年會。8 月 26 日。

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fiflield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, Vern Paxson. 2015. "China Great Cannon." (https://citizenlab.org/wp-content/uploads/2009/10/ChinasGreatCannon.pdf) (2015/4/16)

Sean Bodmer, Max Kilger, Gregory Carpenter, and Jade Jones（Archer Swordlea 譯），2014。《請君入甕：APT 攻防指南之兵不厭詐》（*Reverse Deception: Organized Cyber Threat Counter-Exploitation*）。中國北京：人民郵電出版社。

Stokes, Mark, Jenny Lin, and L. C. Russell Hsiao. 2011. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." (http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf) (2016/5/2)

Wright, Austin（李柏彥譯），2010。〈無形的網路戰爭〉《國防譯粹》37 卷 5 期，頁 4-9。

Wrightson, Tyler. 2015. *Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization*. New York: McGraw-Hill Education.

Discussion of Recent China Cyber Operations: From Control to Attack

Ying Yu Lin
Adjunct Assistant Professor, International Affairs and Diplomacy Program, Ming Chuan University, Taipei, TAIWAN

Abstract

With the application of the information technology, network technology also goes deep into every corner of human life, especially for China, the growth of e-commerce has gradually deepened for the application of network technology; however, with the profit of economic development, which causes the greediness of the interested parties and Internet crimes. Moreover, the characteristics of anonymous using and free public opinions transmission in Internet, which are inconsistent in the attitude that China towards the media. All above mentioned are the reasons that China began to strengthen its network monitoring ability and build up Internet firewall since 2000, and it's also the Great Firewall of China in order to enhance the network monitoring, hope to control public speech in Internet, and make it not to jeopardize the government's regime. In addition to internal controls, China also understands the use of Internet technology in the military will become the commanding heights of winning future wars. In the past, they had only simple cooperation with folk personnel who has IT professional background, or launched some harassing activities such as the replacing web pages of those websites which had hostile awareness, but recently, the pattern of China network operations has evolved into a theft of information through the Internet, the paralysis of other systems or the use of virus to damage important key infrastructure. Whereas the development of network-oriented is multiple, it's very difficult to be covered in a limited page, therefore, this study focuses on China's internal network control and its external attack technique and type. F urther, this study also tries to integrate the researches of technology perspective in order to be able to have better understanding in the contents of network policy, rather than the discussion of text from the government policy advocacy, that will be the way to glimpse of the actual situation.

Keywords: China Studies, PLA Studies, Cyber security