中共網路戰的發展與轉變*

林穎佑

（國立中正大學戰略暨國際事務研究所兼任助理教授）

摘要

隨著資訊科技的發展，人類對於網路的依賴日益增加。由於資訊產業的發達，中華民國在網路使用環境上相當便利，造成其成為各國黑帽駭客與網軍的目標，但也因此，我國能收集各種病毒樣本與攻擊模式做出分析。當前無論是純網路空間的情報竊取或是透過網路對硬體設備的破壞，甚至是利用網路作為不實訊息散佈的管道，都已造成我國極大的威脅。本文集中討論中共在網路空間（cyber space）的發展，特別是研究資料上，除文獻之外，也參與大量的資安人員訪談，期望以技術的層面結合軍事作戰上的認知，以及從作戰型態、組織與具體的攻擊手段分析軍改前後的影響對解放軍網軍。以其增加對解放軍研究的認識。

關鍵字：資訊安全、網軍、解放軍研究、戰略支援部隊、中共駭客

---

* 本文之完成需感謝許多資安駭客領域的好友，特別是 TDoH、LEUKOCYTE-LAB、博格資安會等國內外駭客團體對本人在資安技術上的協助，也引薦許多不願透漏姓名的駭客在”實務”上對本文的協助。

前言

隨著網際網路的發展以及數位科技的應用，網路已經進入人類社會中的每一個角落，而除了電子商務的興起所帶來的商機之外，物聯網科技的應用都讓現代社會生活相當依賴科技產品。但也讓資訊安全的問題逐漸浮上檯面。雖說資安議題在網際網路出現之時，就已經受到相當的關注，但過往資安威脅與破壞大多偏重在騷擾與宣傳以及竊取情資上，所造成的影響單純出現在虛擬的網路空間之中，但在人們逐漸加深對於網路科技的依賴，讓網路攻擊開始從虛擬走向實體，開始藉由干擾軟體的運作來破壞硬體。[1]甚至，各界也開始注意到網路在傳播以及塑造輿論上的功用，開始探討網路民眾的行為以及在虛擬空間的作為，如何影響現實世界。

2017 年中華民國蔡英文總統上台後，不但將資安列為與造艦與航太並列的三大國防產業，更多次提到「資安即國安」的戰略概念，[2]國家安全會議更在 2018 年 9 月正式頒布我國第一份資通安全戰略報告。報告中指出在便利的通訊環境之下，我國成為是許多資安威脅和惡意程式的練兵場，其

---

1 Matthew McCormack，〈資安威脅的局勢 Cyber Security Threat Landscape〉，發表於「2018 台灣資訊安全大會」研討會（台北：IThome，2018 年 3 月 14 日）。

2 李德財，〈「資安即國安」政策推動進度報告〉，發表於「2018 台灣資訊安全大會」研討會（台北：IThome，2018 年 3 月 14 日）。

中大多攻擊都是來自中國大陸。[3]

資安戰略的特性與過往傳統戰略有極大的不同，特別是在虛擬空間的環境，超越了地緣的限制與可複製的特性，甚至可以透過技術上的應用達到完全匿蹤的效果。[4]此外來自網路空間的威脅也從過去單純的騷擾到竊取情報的情報作戰，來自網路的威脅一路從虛擬走向實體，對關鍵基礎設施的攻擊可以直接影響社會民生生活；而隨著通訊軟體與社群網站的深入民眾生活，透過網路發動的不實訊息攻擊開始影響民眾的認知，期望藉此影響民眾的決策，代表網路威脅以從虛擬走向實體，甚至開始走向心理。[5]這些特性正好符合中共的戰略發展。

解放軍也知道其實力無法直接與美軍交鋒，必須以小博大、以劣勝優、以弱擊強的不對稱戰略來去取得局部優勢，

---

3 國家安全會議、國家資通安全辦公室，《國家資通安全戰略報告：資安即國安》，2018 年 9 月 14 日。，<https://www.president.gov.tw/Page/317/969/%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E6%88%B0%E7%95%A5%E5%A0%B1%E5%91%8A-%E8%B3%87%E5%AE%89%E5%8D%B3%E5%9C%8B%E5%AE%89->。

4 柯宏發，唐躍平，李雲濤，夏斌，徐勇，祝冀魯 編，《賽博空間作戰藍軍力量建設概論》（北京：國防工業出版社，2016 年 11 月），頁 3-9。

5 林穎佑，〈數位時代的新輿論戰〉，發表於「第二十屆國軍軍事社會科學學術研討會會後論文集:」（台北：國防大學，2017 年 12 月），頁 20-31。

自然網路空間會是中共嘗試與美國一較長短的戰場，這代表在虛擬空間中正在進行著一場看不見的網路大戰。

壹、軍改前解放軍對網路戰的認識與組織運作

首先須強調的是中共所稱的信息戰並不等於網路戰。信息戰是指如何利用資訊科學與資訊技術裝備來輔助軍事行動，包含剝奪、利用、破壞或摧毀對方信息系統和信息作戰能力，同時充分保護和利用己方的各種行動；[6]網路戰則是指基於信息、包含網際網路和電磁領域的新領域。[7]所謂在網路空間領域發生的衝突，可能是駭客入侵竊取資訊；也包含某國利用程式漏洞讓某國的關鍵基礎設施癱瘓；甚至是利用網路來散佈不實訊息都可算是網路戰的一部分，解放軍甚至認為網路戰的層級已經上升到了戰略網路戰的層級。[8]且隨著中國大陸經濟的發展，北京開始將網路戰結合資訊產業，以國家大戰略角度來推動網路作戰。

一、 解放軍對網路戰認識

6 解放軍國防大學出版組，《軍事變革中的新概念》（北京：解放軍出版社，2004 年），頁 172。

7 肖天亮，《戰略學》（北京：國防大學出版社，2017 年 5 月），頁 146。

8 李繼東、陳舟，＜試論戰略網絡戰＞，《中國軍事科學》，第 141 期，2017 年第 6 期，頁 47-55。

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，但無論素質和數量均遠不足規劃所需，所以才開始在民間資訊產業找尋人才，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。[9]從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，開始討論具體的網路入侵戰術。[10]

沈偉光早在 2000 年，解放軍信息戰的先驅者沈偉光便參考了美軍在波斯灣戰爭與科索沃戰爭的表現與教訓，認為信息化是未來戰爭的趨勢。固然當時認為的信息化作戰，偏重在作戰時的應用，期望透過資訊系統串聯火力，藉此發揮一體化聯合作戰的功用，除了在電子領域的「軟殺」之外，也包含了對於感測系統做出打擊的「硬殺」。網路戰雖然只是信息戰中的一部分，但其能發揮以小博大的能力，更是符合毛澤東人民戰爭思維的軍民總體戰。[11]

而在將信息戰戰術戰法具體化的關鍵人物戴清民的觀點中，其更直接點出資訊作戰不是只有透過資訊系統來串連各部隊的火力，而是可以作為一個全新的作戰領域與作戰模

---

9 廖文中，楊念組編，<中共組建國家網軍進行全球資訊戰>《決戰時刻》（台北市：時英出版社，2007 年 2 月），頁 128。

10 閻雪，《中國大陸的駭客技術》（台北：松崗電腦出版社，2001 年）。

11 沈偉光主編，《信息化戰爭：前所未有的較量》（北京：新華出版社，2003 年 8 月），頁 216-223。

式，甚至在發展網路戰技術時，也能帶動中國大陸民間資訊產業的發展，這邊雖然沒有提到軍民融合，但在研究中已經出現類似的概念。當時身為解放軍總參四部（電子對抗雷達部）部長戴清民少將在著作中透露，解放軍總結「信息戰」的十大樣式聚焦於「網電一體戰」。[12]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。[13]「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。[14]在這些作戰樣式中，戴清民特別強調電子戰與網路戰的作用，特別是網路戰，對於全世界軍隊而言都是全新的領域，其具備以弱擊強、以小博大的特色，更是未來戰爭的關鍵。[15]須注意的是，當時戴清民雖然提出了網路作戰的具體戰術戰法，但解放軍在執行上仍有相當的不足，特別是在組織管理的問題上，當前的資訊作戰基本上是由總參來做主導。但網路戰與過去傳統的戰爭模式有相當的不同，是否依然適用解放軍傳統的作戰指揮體系？同時當時解放軍的軍事教育

---

12 戴清民，《直面信息戰》（北京：國防大學出版社，2002 年），頁 257-272。

13 孔亮、武心安、陳世文，〈網電空間態勢感知技術研究〉，發表於「2013 中國指揮控制大會」（北京：中國指揮控制大會，2013 年 8 月 6 日）。<http://www.c2.org.cn/uploadfile/2015/0724/20150724110746716.pdf>。

14 戴清民，《網電一體戰引論》（北京：解放軍出版社，2002 年）。

15 戴清民，《求道無形之境》（北京：解放軍出版社，2009 年），頁 66。

體系中也缺乏這類的師資。[16]這些問題雖有提及，但當時的解放軍高層並無意識到此問題的重要性，就技術現實來看，當時解放軍的技術也無法支持信息化戰爭，且對於網路戰所需的軍中人才不足，依然需要民間駭客的支援。這些問題都在當時阻礙著解放軍網路作戰的發展。

二、 解放軍網路戰的組織運作

中共與情報與國安公安組織有關的單位是最先開始應用網路技術的組織。通常一國的網路作戰單位，不會是單一組織負責，而是類似情報單位的分工擁有各自的網路作戰單位進行其任務。雖然中共情報組織各自有其任務屬性，雖號稱情報工作「全國一盤棋」，但實際上依然各自為政，甚至會出現權責不明、爭功諉過的問題，[17]類似的問題也出現在網路攻擊的作業上，最大原因在於各情報單位有部分的專業資訊技術人才從事網路攻擊，但大多各自為政缺乏統整。

當時所謂的網軍是依附在各自情報體系的少部分精通資安人士所從事的工作，也導致在網軍目標的選擇上，會與原情報單位的職能有密切的關係。這也代表在中共情報體系

---

16 朱小莉，《軍事革命問題的研究》（北京：國防大學出版社，2000 年 4 月），頁 185-191。

17 關於中共情報組織之間的矛盾可參閱：宋文《一個中國間諜的回憶》（香港：明鏡出版社，2010 年 9 月）。

中的職能分類是可以作為研究中共網軍的方向。如在中共情報體系中，國家安全部的成立晚於解放軍內的情報單位，同時兩者的任務也有所差異。國家安全部負責的是國內外情報研析，因此主要是情報竊取與反情報工作，公安部三所的任務便在於國內網路言論與網路犯罪的安全管理上，工信部則是以網路應急安全為主。[18]上述單位在任務型態上便與解放軍不同，因此雖然表面上與解放軍體系的網路部隊一樣進行網路攻擊，但其目標選擇以及在網路攻防的能力上是有相當的差異。[19]

解放軍的情報單位主要是前總參謀部底下的總參二部、總參三部、總參四部為主，其各自也有不同的職能，分別為人因情報、電子偵蒐、電子雷達對抗等。但總政治部也有專責情報的聯絡部，總裝備部也有專門負責科技情報的收集單位。這代表對中共而言，情報組織的分布相當複雜，這也影響到中共網路作戰組織的運作。[20]特別是懂駭客技術的資訊人才不一定有情報研析的概念，造成技術與情研體系上的脫節，無形之中也降低了網路攻擊的能量。[21]

---

[18] 朱志平、梁德昭，〈習近平時期美中網路安全競逐〉，《遠景基金會季刊》，第 17 卷第 2 期，2016 年 4 月，頁 19。

[19] 平可夫，《中國間諜機關內幕》（加拿大：漢和出版社，2011 年 11 月），頁 112～115。

[20] 上述單位也有網軍駭客的人才，但不一定會有確定的組織。

[21] 周哲賢，〈手把手，教你如何處理資安事件〉，發表於「2019-台灣資安大會」（台北：IThome，2019 年 3 月 19 日）。

這也促使中共在 2016 年所進行的軍事改革中，將過去散佈在各大組織的情報單位進行整合，重新組建直屬中央軍委會不屬於各大戰區的新軍種：戰略支援部隊，將航天、電子電磁、情報與網路作戰進行整合，以面對未來的戰場。[22]

貳、中共網軍作戰模式[23]

一、以騷擾為目的的網路戰

在 1990 年代，雖然網站已有基本的防禦以及伺服器防火牆的概念，但在網頁安全防護上並無安全驗證以及連線加密的防護。隨著網路普及，各國政府組織也開始架設官方網站，作為政策宣導的管道，由於其具有象徵意義，因此便成為駭客與有心人士優先打擊的目標。此外，在網站管理上，管理員登入的密碼以及頁面的系統漏洞都相當容易被駭客

---

[22] 關於戰略支援部隊可參閱：Ying Yu Lin, “The Secrets of China's Strategic Support Force” *The Diplomat* ,Augest.31.2016〈 https://thediplomat.com/2016/09/the-secrets-of-chinas-strategic-support-force/〉

[23] 關於兩岸的駭客交鋒歷史，主要是透過在駭客年會上的訪談，但因訪談對象的要求，在本文中必須隱其姓名。因早期解放軍並無網軍單位，許多網路駭客來自於與民間的合作，因此標題不使用解放軍，而是中共。

利用，有心人士可以輕易的進到網管後台取得網管權限，自然就可以置換官網資料，達到騷擾的目的。[24]

但在 1999 年網路威脅卻開始提升到了國家安全的層級，這就是 1999 年科索沃戰爭中所衍伸出來的網路攻擊事件。美國白宮以及國務院的官方網站都遭到駭客的入侵，將白宮首頁置換為播放中共「義勇兵進行曲」，並將網站放上五星旗，藉此作為「數位佔領」美國的象徵，而美國的駭客也立即反擊，將中共國務院等政府相關官網首頁置換作為報復。當然雙方都不會承認這些網路攻擊是來自於政府的授意，相反都將矛頭指向「愛國駭客」所自發的攻擊。[25]需注意的是，此時的中國網路駭客並無受到政府有組織的管理，反而是以民間社團的模式來運作。這段時期中如綠色兵團、中國紅客聯盟、中國鷹派聯盟都是知名的民間駭客團體，[26]其中綠色兵團更被稱為中國黑客的「黃埔軍校」，後來所成立的許多論壇也成為培養中國駭客的搖籃。[27]同樣在 1999 年，中華

---

[24] Ryan Barnett 著，許鑫城譯，《網站安全攻防秘笈：防御黑客和保護用戶的 100 條超級策略》（The Web Application Defenders Cookbook-Battling Hackers and Protecting Users）（北京：機械工業出版社，2014 年 10 月），頁 10-56。

[25] 東島，《中國輸不起的網路戰爭》（台北：湖南人民出版社，2010 年 11 月），頁 44-46。

[26] 時沖，＜1991-2016 年國內黑客研究綜述＞，《徐州工程學院學報》，第 32 卷第 3 期，2017 年 5 月，頁 91-96。

[27] 方興東、浙江傳媒學院互聯網和社會研究中心編，《黑客微百科》（北京：東方出版社，2015 年 2 月），頁 75-85。

民國總統李登輝在提出特殊國與國關係後，也引起中共的不滿，也透過置換網頁的方式對我國網站與軍事相關論壇進行騷擾。也讓我國在 1999 年的漢光 15 號演習中，開始模擬遭受解放軍網軍攻擊的想定。[28]

2000 年以前的中共網路攻擊大多偏重在於入侵主機來癱瘓對方官網，這些攻擊大多都只有騷擾的功用。但若駭客可以入侵伺服器系統並且能拿到控制權限這也代表，該電腦內部的資料是有可能拿到的，這也讓網路威脅開始邁向另一個階段。

二、 竊取資訊為主的網路戰

駭客既能入侵系統來竄改成自己想要的檔案並呈現在網際網路上，但既然能入侵系統也代表其能窺看伺服器中的所有存取資料，自然會成為有關單位獲取情報的方法。在 2000 年左右的網路世界是透過數據機來連上網際網路，當時也有不少網民透過「網路上的芳鄰」來分享資料，這些都成為駭客可以利用的漏洞。[29]且在 2000 年許多資安觀念與相關的網路監控制度都還未普及，自然給各國情報單位有相當大的發展空間。[30]

---

[28] 姜廷玉，《台灣地區五十年軍事史》（北京：解放軍出版社，2013 年），頁 164。

[29] 閻雪，《中國大陸的駭客技術》，頁 x。

[30] 關於中國網路技術的發展，請參閱：林穎佑，〈中國近期網路作為探

除了技術上的應用之外，此時期的駭客更開始使用社交工程（Social engineering）的方式來強化入侵的機會。[31]雖然駭客可以透過技術來突破各單位的資安防護網，但並非每位情報人員都有類似的資訊技術可以進行滲透。因此若是透過偽造身分的電子郵件作為惡意程式的掩護，是有可能讓受害者下載有問題的檔案，成功入侵目標電腦。在類似的手法中，社交工程最重要的目的就是希望讓受害者相信這一封信是真實而非詐騙信，因此發信者都會假藉某單位來發送信件，如系統控制中心或是官方單位，[32]期望藉此來達到誘騙的目的。這也說明在網路的世界中，能成功達成目的不一定要依賴電腦技術實力，若是配合過去情報蒐集的技巧，配合社交工程能達到的效果不一定會輸給突破技術防護的成果。[33]

此時期的網路威脅雖然開始進展到竊取機密的層級，但

討：從攻擊到控制〉，《台灣國際研究季刊》，第 12 卷第 3 期，2016 年 9 月，頁 53-62。

[31] 趨勢科技研究團隊，＜< APT 攻擊>看起來是 .PPT 附件，竟是 .SCR !!針對台灣政府單位的 RTLO 技術目標攻擊＞，《趨勢技術通報》，2014 年 5 月。https://blog.trendmicro.com.tw/?p=8334

[32] 趨勢科技研究團隊，＜APT 白皮書＞，《趨勢技術通報》，2013 年 10 月。https://esupport.trendmicro.com/zh-tw/business/topic_knowledgedownload/topic_techsupportboard/20131031.aspx

[33] 果核數位研究團隊，<只有更多沒有最多的社交工程>，《果核數位》，2019 年 6 月 04 日，<https://www.digicentre.com.tw/industry_detail.php?id=39>。

各國也在實作中發現到過往沒有注意到的問題，那就是駭客工程師與情報分析人員之間的認知矛盾。對於駭客來說駭客精神在於追求技術的突破以及入侵成功時所帶來的成就感，因此著重在於技術科技的層面，但在設計社交工程時經常會因為小破綻而功敗垂成。這也代表一個技術超群的駭客與勝任的網路情蒐駭客是有相當的差別的，駭客強調的是對資訊技術的突破，對於侵入系統有追求的熱忱，但不是每一個受到加密防護的檔案都是重要的情報。一個能進行情報收集的資訊人員，需要對於目標有所了解，同時具備基本的研析能力，才能在短時間內確認取得檔案的優先順序，避免浪費時間。[34]

如在用詞上，許多可能來自中共網軍在信件內文的用詞上都還是保留了中國大陸習慣用語而非轉換成為台灣民眾常用的詞彙，自然容易看出馬腳。[35]因此在網路戰中，在於如何取得受害者的信任進而下載含有惡意程式的檔案，此時的需求也讓網路威脅走向下一個世代：APT 攻擊（進階持續性滲透攻擊 Advanced Persistent Threat，主要透過社交工程

---

[34] 黃耀文，〈福爾摩斯兄弟性格差異：主動式 APT 之追蹤與偵測技術分享〉，發表於「2014 亞太資訊安全」論壇（台北：資安人，2014 年 3 月 20 號）。

[35] 如台灣習慣使用早安，中國習慣使用早上好；重新啟動帳號，中國經常使用激活帳號，此類的習慣用語不同，自然會被識破。Charles Li & zha0，〈APT Fail〉，發表於「2014-HITCON 第十屆台灣駭客年會」研討會（台北：台灣駭客年會，2014 年 8 月 22 日）。相關資料請至 http://hitcon.org/2014/搜尋。

的輔助配合零時漏洞對安全防禦系統進行滲透，以下簡稱 APT 攻擊）[36]。

三、 外科手術式的 APT 攻擊

APT 攻擊主要是利用帶有惡意程式的信件發動零時攻擊（0-day）[37]或檔案名稱的反向排序以及語法的更改，讓原本的惡意執行檔看起來與一般常見的附加檔案類似(惡意程式多半偽裝成 Word、PDF、Excel、RTF）藉此讓受害人放下警戒心，直接下載並執行含有惡意程式的檔案。[38]期望能藉此入侵目標的系統，進而完成目標。APT 攻擊最重要特色就是在於攻擊方對於目標的了解，會針對目標的特性而量身打造設計專屬目標的攻擊信件。[39]同時為了要讓受害者會相信信件而打開附加檔案，駭客更會偽裝為目標的常用聯絡對象夾帶目標可能感興趣的主題發出攻擊信件。雖然不一定能得到偽造單位的使用權限而直接發出信件，但是也有可能透過正式申請以帳號呈現類似的信箱名稱來混淆目標，取得信

---

[36] Tyler Wrightson, *Advanced Persistent Threat Hacking: The Art and Science of Hacking any Organization* (New York: McGraw-Hill Education, 2015), pp. 52-69.

[37] 零時攻擊主要是指系統的漏洞在廠商修補前，已遭駭客利用。

[38] 邱銘彰，〈揭露網路威脅秘辛 40 分鐘搞懂 APT〉，發表於「換個腦袋作資安」資安趨勢論壇（台北：資安人，2011 年 12 月 6 日）。

[39] 程三軍、王宇，〈APT 攻擊原理及防護技術分析〉，《信息網絡安全》，第 16 卷第 9 期，2016 年 9 月，頁 118-123。

任。[40]

APT 攻擊最大的特色在於攻擊方從信件釣魚轉變成為「魚叉式攻擊」。魚叉式攻擊是由駭客鎖定目標，並且在發動攻擊前會有詳細的情報，深度了解目標的喜好、生活習性、交友關係、使用系統來規劃 APT 攻擊時的內文以及檔案模式。針對目標進行精準打擊，這就是魚叉式攻擊最大的特色。

APT 攻擊也會依據目標近期的行程來規劃，如會特別選擇目標在國外出差或是近期有可能招開的會議議程，特別發出邀請函來給目標，企圖騙取目標的密碼以及個人資料。如我國曾有某立委在當選前，便收到某偽造成政府機關訓練單位的邀請函，邀請撰寫相關分析稿件並前往該訓練中心發表相關文章。目標欣然同意後，也為了日後經費核銷提供了個人相關資料，但在表定會議當日前往該會場，卻沒有任何會議舉行，事後發現該訓練單位根本沒有發出邀請通知，但根據受害者所出示的電子信件，內容的單位與連絡人都是真實存在的。[41]類似的案件經常出現在於學者間，經常會有單位假藉研究案或是研討會的名義發出邀請函，若目標未經過

[40] 如在電腦中零 0 與英文的 o 有極高的相似度。

[41] 〈「鬼電郵」邀演講 黃國昌慘遭欺騙〉，《蘋果即時新聞》，2014 年 11 月 7 日，〈 http://www.appledaily.com.tw/realtimenews/article/new/20141107/501987/〉。

電話再次確認，經常會遭到欺騙。[42]

APT 攻擊在 2005 年之後，成為網路攻擊的主流，更是各國網軍經常使用的方式。[43]如： 2010 年攻擊 Google 的「極光行動」（Operation Aurora）[44]以及在 2011 年 McAfee 資安公司發表的一份報告中便指出由中共網軍主導的「夜龍行動」 (Night Dragon)，[45]其針對 10 多家能源企業進行 APT 攻擊，從外網主機 web 伺服器進攻使用 SQL 注入攻擊，[46]之後再利用外網作跳板，對內網突破，再利用遠端存取工具（Remote Access Tool ,RAT）傳回大量重要資料（WORD、PPT、PDF）。[47]最後再利用社交工程將郵件破壞力發揮到最

---

42 作者本人便多次接到類似的信件，其中有許多被假冒的都是政府單位、學術團體、新聞媒體。

43 關於網路戰的案例與歷史可參考: Bruce Middleton, *A History of Cyber Security Attacks* (UK: Taylor& Francis Group, 2017). Paulo Shakarian, Jana Shakarian, Andrew Ruef 著，吳奕俊譯，《網路戰：信息空間攻防歷史案例與未來》（Introduction to Cyber-Warfare: A Multidisciplinary Approach）（北京：金城出版社，2016 年 9 月）。

44 Xecure-Lab 研究團隊，〈三起 APT 事件攻擊手法解析〉，《資安人》，2011 年 12 月 6 日，〈 https://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=6768&pages=3〉。

45 Professional Services and McAfee Lab,"Global Energy Cyberattacks: Night Dragon,", 2018/4/7, < https://kc.mcafee.com/corporate/index?page=content&id=KB71150&locale=zh_TW >。

46 關於中國對於 SQL 的應用可參考：李鑫、張維緯、隋子暢、鄭力新，〈新型 SQL 注入及其防禦技術研究與分析〉，《信息網絡安全》，第 16 卷第 2 期，2016 年 2 月，頁 66-73。

47 郭璇、肖治庭，《現代網絡戰》（北京：國防大學出版社，2016 年），

大。而 2011 年 8 月同公司又發佈了一項資安報告，其中指出一項由「國家單位」所指導的網路入侵行動，代號為「暗鼠行動」（Operation Shady RAT）。此名稱與英文「遠端存取工具」（RAT）有關；而 Rat 也代表了潛伏在黑暗之中的老鼠，無時無刻的都在嘗試破壞或是偷取有價值物品，與目前駭客以及所使用的入侵方式不謀而合。[48]其中：端口掃描、程式漏洞（bug）、殭屍網路（botnet）、DDoS、緩衝區溢出（buffer overflow）、木馬（Trojan horse）、Rootkit、Worm、SQL injection 都是中國駭客常見的攻擊手法。[49]

這些攻擊非一般的駭客可以發動的，因為其仰賴的不是只有技術的層面，能夠擁有完整的行蹤紀錄、個人資料與交友關係的絕非一般資訊駭客可以完成，同時對駭客而言一般入侵的目的是在鑽研更高的技術或是自我的突破；若為黑帽駭客多半是為了獲取利潤而入侵，但這些學術資料相較於銀行個人資料以及其他財經資料，在黑市利潤價值有限，很有可能呈現「有價無市」的狀況，畢竟特殊領域的相關資料，除非特定國安單位有特別的需求，不然不會有太高的價值。如中共網軍入侵洛克希德馬丁（Lockheed Martin）取得其研

頁 168-172。

[48] Xecure Lab，〈APT 時代的縱深防禦〉，發表於「TWNIC 2013 網際網路趨勢」研討會（台北：台灣網路資訊中心，2013 年 3 月 27 日）。

[49] 時沖《黑客：網絡社會的流浪者》（上海：復旦大學出版社，2017 年），頁 14-16。

製的 F-35 匿蹤戰機資料，[50]此類資料在黑市中客戶群相當有限，若非國家網軍一般不會耗費太多的成本（時間與研發的漏洞）在此類攻擊上。

雖然當前北京從未承認運用對他國關鍵基礎設施進行網路攻擊，但在其部份研究中，有提及到若在兩國衝突時，用網路攻擊是可造成對方相當大的破壞。[51]雖然在 1999 年的超限戰中有提及類似概念，但大多集中在恐怖份子如何透過此種方式來對美攻擊，部分研究雖有提到解放軍應該借鏡這些攻擊，但在文章的討論中多半還只是集中在介紹這些作為，對於具體的作法並無特別的討論。[52]

解放軍在進攻他國關鍵基礎設施時，依然需要先滲透進入系統，這邊仍然離不開 APT 攻擊，以及利用系統的 0-day 漏洞將病毒與惡意程式潛伏在目標的系統中。當北京與他國發生軍事衝突時中共可以利用安裝在敵國關鍵基礎設施的病毒，癱瘓敵國的社會運作。[53]如在部份的研究

---

[50] Clarke and Knake, *Cyber War* (New York: HarperCollins, 2011), pp. 233-235.

[51] 趙旭東、陳志龍、龔華棟、郭東軍，〈關鍵基礎設施網路體系易損性定量評估〉，《解放軍理工大學學報》，第 17 卷第 3 期，2016 年 6 月，頁 241-245。

[52] 崔國平、唐德卿、王玉鬥，《國防資訊安全戰略》（北京：金城出版社，2000 年 4 月），頁 298-304。

[53] 劉楊鉞　張旭，〈網路空間武器化的發展態勢以及對戰略穩定的影響〉，《資訊安全與通信保密》，2019 年 9 月，頁 8-10。

中，都有提到俄羅斯網軍攻擊烏克蘭電廠的停電案例，[54]以及美國與以色列合作攻擊伊朗核電廠的震網病毒案例，這些文章都有提到對於利用網路攻擊關鍵基礎設施是未來作戰的新型態。特別是對於能源系統與軍隊後勤運輸的攻擊，是可以發揮以小博大、以弱擊強的功能。[55]其中如何將偵查（使用者習慣與系統）、攻擊（癱瘓或毀損）、偽裝（避免被對方的防毒軟體察覺）整合在入侵程式中是這幾年中共數位軍火發展的方向。[56]

參、軍改後中共網軍的新作為

一、軍改後中共網軍在戰術上的改變

在攻擊方面，中共網軍在經過軍改之後，其戰力大幅提升，但提升的關鍵不是在於網軍的技術實力，而是在於組織整合後的表現。過去的中共網軍散佈在各大軍區以及總參謀部與總政治部都有負責網路作戰的單位，但經常會碰到疊床

---

[54] 郭慶來、辛蜀駿、王劍輝、孫宏斌，〈由烏克蘭停電事件看資訊能源系統綜合安全評估〉，《電力系統自動化》，第 40 卷第 5 期，2016 年 3 月，頁 145-147。

[55] 楊承軍，〈關注軍事物流網絡戰〉，《中國物流與採購》，2015 年 1 月，頁 30-31。董翔英、鄒饒邦彥、呂亞飛，〈對軍事物流資訊系統基礎安全問題的認識〉，《物流科技》，2015 年 3 月，頁 108-110。

[56] 王源、張博，〈賽博武器的現狀與發展〉，《中國電子科學研究院學報》，2011 年 3 月，頁 221-225。

架屋與資源重複的問題。[57]軍改之後大部分的網軍單位都列入戰略支援部隊，也將網軍重組，配合情報分析以及整合後的任務分配，讓現今的中共網軍更是如虎添翼。

在 2015 年至 2018 年之間，中共網軍有較為沉寂。資安公司長期觀察的 8 個中共網軍駭客組織，在 2015 年至 2018 年各別皆有將近一年至二年停止行動的跡象。在這期間，這 8 個駭客組織暫停行動的步調有所不同，但在 2018 年下半年，這些組織已經全數展開新的網路攻擊行動，其使用的攻擊工具、方法與目標對象，有部分與過往不同。到了 2018 年第三季，8 個駭客組織全部都恢復行動，而且其中還有一個是從 2015 年至 2018 年皆未有活動的駭客組織，卻在 2018 年第三季復出，重新展開行動。這個稱之為 Group A 的駭客組織，與 2013 年資安公司 Mandiant（Fireeye 於 2013 年購併）所揭發，隸屬於解放軍總參謀部三部二局 61398 部隊的網軍組織 APT 1，都採用相同的 WARP 惡意程式。

這些都代表解放軍網軍的重組，更值得注意的是過去特定區域的網軍有自己的任務目標，但在近期與國外交流所收到的網軍惡意程式樣本可以看到，彼此之間的交流是相當密切的，合理懷疑是現今的中共網軍在經過整合後，會由中央統一指揮攻擊目標，同時在網路空間中是不會有地緣戰略的因素存在，只要能連線上網路就可以發動攻擊，這些都代表

[57] 李繼斌，《聯合戰役網絡空間作戰指揮問題研究》（北京：國防大學出版社，2016 年），頁 77-79。

過去依地緣屬性所作的目標分工無實質的效果,反而由中央統籌規劃更能發揮攻擊的效益。

近期中共對台網軍主要分成兩個族群：Waterbear 和利用 Taidoor 變種的 Huipi。Waterbear 在年初曾經攻擊過台北市政府與新北市政府，[58]主要利用政府常用的管理或資安軟體進行滲透，這也代表中共網軍可能有掌握新的零時漏洞。而 Huipi 則是以交通物流為目標，其特色為植入常見 VPN 程式(Softether)以利日後橫向攻擊，且許多防毒軟體並不會對 VPN 程式有反應，之後橫向攻擊透過 LOL（Living off the Land，LoL）BIN 的指令來發動攻擊。[59]其中在其複雜的攻擊鏈當中完完全全只使用一般電腦系統會使用的系統工具，使防毒軟體偵測難上加難。這些都是當前中共網軍常用的手法。

二、中共成立專屬網軍（戰略支援部隊）的意義

2016 年的中共網軍攻擊下降最大的原因應該是與中共軍改有直接的關係，解放軍在 2016 年的軍改直接將過去的

---

[58] 趨勢科技研究團隊，＜主要鎖定台灣,專偷機密技術的 BlackTech 網路間諜集團＞，《趨勢技術通報》，2017 年 07 月。https://blog.trendmicro.com.tw/?p=50684

[59] 〈微軟警告竊密程式 Astaroth 來襲，攻擊過程完全使用合法工具〉，《IThome》，2019 年 07 月 09 日〈https://www.ithome.com.tw/news/131742〉。

網軍單位全部打散，重新整合至戰略支援部隊。[60]最明顯的便是總參二部與總參三部的網路作戰單位皆轉移至戰略支援部隊的麾下。總參謀部技術偵查部部長鄭俊傑少將(前解放軍資訊工程大學校長)出任網絡系統部司令，其後在 2019 年出任戰略支援部隊副司令兼參謀長，也代表解放軍對網路作戰的重視。新整併的信息工程大學是由解放軍信息工程大學以及外國語大學整併而成。[61]原隸屬總參二部的信息工程大學和總參三部的解放軍外國語學院如今歸屬在戰略支援部隊，這也間接證實總參二部部份單位與三部已整併至戰略支援部隊。[62]

1. 情報與數位科技的結合

解放軍網軍在進行網路情蒐時，依然是採用 APT 攻擊（進階持續性滲透攻擊 Advanced Persistent Threat, APT）藉此竊取情報。[63]軍改後的解放軍網軍跟過去最明顯的差異點

---

[60] John Costello,「Strategic Support Force: A Force for a New Era」PLA Reform, Part Deux 2017 International Conference on PLA Affairs.(Taipei: CAPS-CSS-NDU-RAND November 17-18,2017).

[61] 武千妍，〈軍校巡禮｜第二十一站：解放軍資訊工程大學〉(2017 年 6 月 13 日)，《中國軍網》，<http://www.81.cn/jwgz/2017-06/13/content_7636741.htm>。

[62] 林穎佑，〈中共戰略支援部隊的任務與規模〉，《展望與探索》，第 15 卷第 10 期，2017 年 10 月，頁 114-115。

[63] Tyler Wrightson, *Advanced Persistent Threat Hacking: The Art and Science of Hacking any Organization*, pp.52～69.

便是在進行 APT 攻擊時更融合了更進一步的情報分析手法，讓網軍在進行社交工程時所撰寫的詐騙信件更具有說服力。過去 APT 攻擊便是一個針對目標量身打造的病毒信，其對於目標的喜好、興趣、基本資料、電腦作業系統以及人際關係都有一定程度的了解，再根據上述資料，設計出專屬的攻擊策略，期望藉此騙取目標的信任，進而突破其資安防護網。過去中共網軍大多歸屬於總參三部麾下，[64]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整合，勢必會讓中共網軍的實力如虎添翼，對其他國家的攻擊更為猖獗。

2. 提昇網軍的士氣

對於駭客而言，最常碰到的問題就是其無法融入公務組織的作息。特別是過去許多駭客團體的高層管理人員，由於其歷練與年資的問題，對於網路技術與資安的了解相當有限，自然會對隸屬在網路作戰部門的網路戰士採取一般部隊的管理模式，這對資訊工作者而言造成相當大的不便。此外，則是在績效評估上，若缺乏對於網路作戰的認識，管理階層便無法了解網路駭客所從事的任務價值，自然會採取過去傳

64 Mark A Stokes, Jenny Lin and L.C. Russell Hsiao ,***The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*** (Washington D C:Project2049,November 11,2011).<https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf >.

統的評比方式來對駭客進行考核與績效評估，這對資訊工作者而言並不公平。也造成不少在解放軍服務的駭客在服務一段時間後，會選擇離職加入民間的資安公司，或是會將這些技術應用於網路犯罪，而不會選擇在解放軍長期發展。畢竟在考量經濟壓力、未來升遷與高層對網路作戰的重視程度後，離開軍隊發展會有更大的發展空間。在與駭客的合作上，解放軍除了最直接的金錢補助之外，也會給予這些願意合作的駭客部分的特權與其在從事灰色地帶的網路活動時，可以給予法律上的豁免權。這會讓原本遊走在法律邊緣的中共駭客有更多與政府合作的動力

而在軍改後所成立的戰略支援部隊，其中的網絡系統部整合了過去散落在各單位的網軍部隊之外，戰略支援部隊網絡系統部司令員，從首任的鄭俊傑（現任戰略支援部隊中將副司令兼參謀長，過去信息工程大學校長）或是現任的巨乾生都有過去在總參三部的資歷，由了解網路作戰特性的將領作為統領網軍部隊的主官，對於內部管理或許較其他野戰部隊空降來的長官，更能發揮網路作戰的特色，而非出現外行領導內行的狀況。這些都可能是解放軍成立戰略支援部隊後，中共網軍更具威脅的原因。

3. 數位三戰

在前述的網路戰發展中，我們可以發現到網路入侵的效益已經日益擴大，但隨著社交平台與通訊軟體的發達，資訊分享的同時，有時也成了不實訊息傳遞的管道。特別是結合

過去宣傳戰的手法，並利用網路作為收集資訊的管道，針對特別的族群設計專屬的不實訊息，企圖激化目標內部的分裂。上述的攻擊雖然沒有任何的資訊技術成分，但是透過數位途徑卻可以輕易地達成效果。特別是在進行網路輿論戰或網路心理戰時，最重要的就是熟知目標的使用習性、議題愛好、意識形態、以及政黨立場，這些個人資料都是日後設計病毒或是進行輿論操作時的最好樣本。

現行最普遍的數位輿論戰便是利用大量的內容農場（Content Farm，指以取得網路流量為主要目標，圖謀網路廣告等商業利益的網站或網路公司）與操控的帳號進行文章發送，並利用網路水軍進行自我宣傳，並透過通訊軟體大量發送給民眾，許多的民眾並未仔細閱讀便直接轉發，成為擴散不實訊息的幫兇。雖然部分不實訊息的內容是經不起查證的，但是在大量傳播的情形之下，此種真假相參的不實訊息最容易吸引大眾的關注，並得到民眾的信任。近期類似的作為，也提升到修改照片，配合圖說散發不實訊息來汙衊軍方或重要政治人物，類似的訊息結合時事以及通訊軟體快速地流傳，來達到詆毀目標的目的。亦會利用國內不同政治支持者之間的對立，刻意反串不同立場者發表較為偏激的言論，企圖嫁禍對方激起更高的矛盾。最後在關鍵的時間點（如選舉）時，大量放出不實訊息，造成輿論影響民心，甚至在適當時刻配合 DDoS 攻擊癱瘓官方網站，使民眾無法得到正確資訊，甚至誤信不實訊息或在煽動之下採取激進抗爭手段

進而引發恐慌。[65]

中共一向重視網路輿情的變化，甚至也有許多專門的研究。[66]解放軍也在 2014 年提出「制腦權」的概念，其中認為經歷陸、海、空權以及制網權的較量後，透過媒體與宣傳的制腦權會是未來重要的戰場，更是兵家必爭之地。[67]而想要在此一新戰場中獲得先機，資訊的輔助會是致勝的關鍵，未來的網軍作戰不會只限於情報的竊取以及系統漏洞的滲透，結合資訊技術的新輿論戰，更是讓網路戰爭步向新的階段，而制腦權也是在過去所謂制海權、制天權、制電磁權之外，全新的戰場。[68]

肆、 結語

軍隊的改革大致可以分為：「理論、科技、組織、人才」四個階段。早在 1998 年在熊光楷的推動下，開始針對美軍

---

[65] <資訊戰研究：中國網軍攻台模式以內容農場、在地協力最嚴重>，《中央社》，2020 年 10 月 29 日，<https://www.cna.com.tw/news/firstnews/202010240196.aspx>。可參考：民主實驗是的相關著作：https://medium.com/@doublethinklab

[66] 可參閱：網絡輿情研究與對應》（北京：電子工業出版社，2014 年）。

[67] 蘭舟達、馬建光，〈制腦權視野下的新型網路戰——以顏色革命為例〉，《國防科技》，2015 年 2 期，頁 57-62。

[68] 可參閱：曾華鋒、石海明，《制腦權：全球媒體時代的戰爭法則和國家安全戰略》（北京：解放軍出版社，2014 年）。

信息戰的相關理論著作，進行大量的翻譯與論述研究，也陸續提出信息戰、一體化聯合作戰的理論概念。[69]但在當時受限於資訊技術不足，無法發揮信息戰之效，這也讓解放軍了解必須在資訊科技上有所突破才能進行現代戰爭。直到2010年後信息化的系統陸續就位，這才讓解放軍開始從「機械化」步向「信息化」。

2015 年底的軍改對解放軍網軍而言，最大的改變在於組織體系上的變化。對網路作戰而言，最重要的並不是硬體設備或軟體撰寫，而是在資安人才的確保上。許多具有資訊天分的天才是可遇不可求，對於中共而言如何發掘或培養「網路戰士」是其近期研究重點。雖然中國大陸有與民間大學合作或是有隸屬軍方的學校作為培養網軍的組織(如隸屬戰略支援部隊的信息工程大學)，[70]但是許多具有資安天分的人才不一定會願意加入具制度與規律生活的公務體系，因此不少資訊高手仍然藏於民間。這也是中國大陸近年多次舉辦網路駭客競賽的原因之一，並且過去也在政府的贊助下，成立了中國大陸民間組成的網路漏洞回報平台：烏雲安全網。[71]都是期望能藉此吸引網路高手來為國所用。

---

[69] 林中斌，《以智取勝》(台北：全球防衛雜誌出版社，2005 年 1 月)，頁 25-35。

[70] 武千妍，〈(軍校巡禮 | 第二十一站：解放軍資訊工程大學〉，《中國軍網》，2017 年 6 月 13 日，〈http://www.81.cn/jwgz/2017-06/13/content_7636741.htm〉。

[71] 劍心（本名：方小頓），〈烏雲這幾年運作的心得及優缺點〉，發表於

但與民間人士的合作是否會為未來政府埋下洩密的未爆彈？前述的烏雲安全網在 2016 年 7 月突然停止運作，甚至連負責人方小頓也無法聯繫，據稱可能與該網站紕漏了政府網站的漏洞有關，[72]這都說明了民間合作依然會有相當的變數。[73]但在公認的駭客精神裡便包含了創業精神與對社會的挑戰，[74]這也促使駭客團體中大多都有許多不成文規範，[75]如發揚自由的精神，以及不能向公權力屈服的反叛精神。[76]這些理念都與當前北京的網路管理有相當大的差異，中共對於駭客人才管理是相當嚴密的，但這樣的管理模式，是否會讓更多的人有所反彈甚至出現中共版的「史諾登事件」，這些都是中共成為網路強國背後的隱憂。

「2014-HITCON 第十屆台灣駭客年會」研討會（台北：台灣駭客年會，2014 年 8 月 20 日）。

[72] <烏雲平臺"升級"無法訪問 或受"白帽子"被捕影響>，《人民網》，2016 年 07 月 21 日<http://media.people.com.cn/BIG5/n1/2016/0721/c40606-28571270.html>。

[73] 黃彥棻，<從烏雲升級事件看中國政府對網路的箝制>，《IThome》，2016 年 08 月 12 日<https://www.ithome.com.tw/news/107478>。

[74] 海莫能 著，劉瓊云 譯，《駭客倫理與資訊時代精神》（台北：大塊文化，2002 年 5 月），頁 39。

[75] 中國黑客守則 13 條可參閱：時沖，《黑客：網絡社會的流浪者》（上海：復旦大學出版社，2017 年），頁 224-225。

[76] 如維基解密創始人，朱利安・亞桑傑(Julian Assange)描述了他心目中的駭客法則：「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。」這也成為後來成立維基解密的核心價值。Sulette Dreyfus、Julian Assange，《維基解密創辦人帶你揭開駭客手法》（Underground）（台北：國際漢宇，2012 年 3 月），頁 475-479。

參考文獻

專書

方興東、浙江傳媒學院互聯網和社會研究中心編，2015 年。《黑客微百科》。北京：東方出版社。

平可夫，2011 年。《中國間諜機關內幕》。加拿大：漢和出版社。

朱小莉，2000 年。《軍事革命問題的研究》。北京：國防大學出版社。

宋文，2010 年。《一個中國間諜的回憶》。香港：明鏡出版社。

李繼斌，2016 年。《聯合戰役網絡空間作戰指揮問題研究》。北京：國防大學出版社。

沈偉光主編，2003 年。《信息化戰爭：前所未有的較量》。北京：新華出版社。

肖天亮，2017 年。《戰略學》。北京：國防大學出版社。

東島，2010 年。《中國輸不起的網路戰爭》。台北：湖南人民出版社。

林中斌，2005 年。《以智取勝》。台北：全球防衛雜誌出版社。

姜廷玉，2013 年。《台灣地區五十年軍事史》。北京：解放軍出版社。

柯宏發，唐躍平，李雲濤，夏斌，徐勇，祝冀魯 編，2016 年。《賽博空間作戰藍軍力量建設概論》。北京：國防工業出版社。

時沖，2017 年。《黑客：網絡社會的流浪者》。上海：復旦大學出版社。

崔國平、唐德卿、王玉鬥，2000 年。《國防資訊安全戰略》。北京：金城出版社。

郭璇、肖治庭，2016 年。《現代網絡戰》。北京：國防大學出版社。

曾華鋒、石海明，2014 年。《制腦權：全球媒體時代的戰爭法則和國家安全戰略》。北京：解放軍出版社。

程工，2014 年。《網絡輿情研究與對應》。北京：電子工業出版社。

解放軍國防大學，2004 年。《軍事變革中的新概念》。北京：解放軍出版社。

閻雪，2001 年。《中國大陸的駭客技術》。台北：松崗電腦出版社。

戴清民，2002 年。《直面信息戰》。北京：國防大學出版社。

戴清民，2002 年。《網電一體戰引論》。北京：解放軍出版社。

戴清民，2009 年。《求道無形之境》。北京：解放軍出版社。

專書譯著

Paulo Shakarian, Jana Shakarian, Andrew Ruef 著，吳奕俊譯，2016 年。《網路戰：信息空間攻防歷史案例與未來》（Introduction to Cyber-Warfare: A Multidisciplinary Approach）。北京：金城出版社。

Ryan Barnett 著，許鑫城譯，2014 年。《網站安全攻防秘笈：

防御黑客和保護用戶的 100 條超級策略》(The Web Application Defenders Cookbook-Battling Hackers and Protecting Users)。北京：機械工業出版社。

Sulette Dreyfus、Julian Assange，2012 年。《維基解密創辦人帶你揭開駭客手法》(Underground)。台北：國際漢宇。

海莫能 著，劉瓊云譯，2002 年。《駭客倫理與資訊時代精神》。台北：大塊文化。

專書論文

林穎佑，2017 年。〈數位時代的新輿論戰〉,《第二十屆國軍軍事社會科學學術研討會會後論文集》。台北：國防大學，頁 20-31。

廖文中，2007 年。〈中共組建國家網軍進行全球資訊戰〉，楊念組編,《決戰時刻》。台北市：時英出版社，2007 年 2 月)，頁 128。

期刊論文

王源、張博，2011/03。〈賽博武器的現狀與發展〉,《中國電子科學研究院學報》，頁 221-225。

朱志平、梁德昭,2016/04。〈習近平時期美中網路安全競逐〉,《遠景基金會季刊》，第 17 卷第 2 期，頁 19。

李繼東、陳舟，2017/12。＜試論戰略網絡戰＞,《中國軍事科學》，第 141 期，頁 47-55。

李鑫、張維緯、隋子暢、鄭力新，2016/02。〈新型 SQL 注入及其防禦技術研究與分析〉,《信息網絡安全》，第 16 卷

第 2 期，頁 66-73。
林穎佑，2016/09。〈中國近期網路作為探討：從攻擊到控制〉，《台灣國際研究季刊》，第 12 卷第 3 期，頁 53-62。
林穎佑，2017/10。〈中共戰略支援部隊的任務與規模〉，《展望與探索》，第 15 卷第 10 期，頁 114-115。
時沖，2017/05。〈1991-2016 年國內黑客研究綜述〉，《徐州工程學院學報》，第 32 卷第 3 期，頁 91-96。
郭慶來、辛蜀駿、王劍輝、孫宏斌，2016/03。〈由烏克蘭停電事件看資訊能源系統綜合安全評估〉，《電力系統自動化》，第 40 卷第 5 期，頁 145-147。
程三軍、王宇，2016/09。〈APT 攻擊原理及防護技術分析〉，《信息網絡安全》，第 16 卷第 9 期，頁 118-123。
楊承軍，〈關注軍事物流網絡戰〉，《中國物流與採購》，2015 年 1 月，頁 30-31。
董翔英、鄒饒邦彥、呂亞飛，2015/03。〈對軍事物流資訊系統基礎安全問題的認識〉，《物流科技》，頁 108-110。
趙旭東、陳志龍、龔華棟、郭東軍，2016/06。〈關鍵基礎設施網路體系易損性定量評估〉，《解放軍理工大學學報》，第 17 卷第 3 期，頁 241-245。
劉楊鉞、張旭，2019/09。〈網路空間武器化的發展態勢以及對戰略穩定的影響〉，《資訊安全與通信保密》，頁 8-10。
蘭舟達、馬建光，2015/02。〈制腦權視野下的新型網路戰——以顏色革命為例〉，《國防科技》，頁 57-62。
研討會論文
邱銘彰，2011/12/06。〈揭露網路威脅秘辛 40 分鐘搞懂 APT〉，

「換個腦袋作資安」資安趨勢論壇。台北：資安人。

Xecure Lab，2013/03/27。〈APT 時代的縱深防禦〉，「TWNIC 2013 網際網路趨勢」研討會。台北：台灣網路資訊中心。

孔亮、武心安、陳世文，2013/08/06。〈網電空間態勢感知技術研究〉，「2013 中國指揮控制大會」。北京：中國指揮控制大會。

黃耀文，2014/03/20。〈福爾摩斯兄弟性格差異：主動式 APT 之追蹤與偵測技術分享〉，「2014 亞太資訊安全」論壇。台北：資安人。

劍心（本名：方小頓），2014/08/20。〈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」研討會。台北：台灣駭客年會。

Charles Li & zha0，2014/08/22。〈APT Fail〉，「2014-HITCON 第十屆台灣駭客年會」研討會。台北：台灣駭客年會。

Matthew McCormack，2018/03/14。〈資安威脅的局勢 Cyber Security Threat Landscape〉，「2018 台灣資訊安全大會」研討會。台北：IThome。

李德財，2018/03/14。〈「資安即國安」政策推動進度報告〉，「2018 台灣資訊安全大會」研討會。台北：IThome。

周哲賢，2019/03/19。〈手把手，教你如何處理資安事件〉，「2019-台灣資安大會」。台北：IThome。

政府報告

國家安全會議、國家資通安全辦公室，2018/09/14。《國家資通安全戰略報告：資安即國安》，

<https://www.president.gov.tw/Page/317/969/%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E6%88%B0%E7%95%A5%E5%A0%B1%E5%91%8A-%E8%B3%87%E5%AE%89%E5%8D%B3%E5%9C%8B%E5%AE%89->。

網際網路

2014/11/07。〈「鬼電郵」邀演講 黃國昌慘遭欺騙〉,《蘋果即時新聞》,〈http://www.appledaily.com.tw/realtimenews/article/new/20141107/501987/〉。

2016/07/21。<烏雲平臺"升級"無法訪問 或受"白帽子"被捕影響>,《人民網》,<http://media.people.com.cn/BIG5/n1/2016/0721/c40606-28571270.html>。

2019/07/09。〈微軟警告竊密程式 Astaroth 來襲,攻擊過程完全使用合法工具〉,《IThome》,〈https://www.ithome.com.tw/news/131742〉。

Xecure-Lab 研究團隊,2011/12/06。〈三起 APT 事件攻擊手法解析〉,《資安人》〈https://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=6768&pages=3〉。

果核數位研究團隊,2019/06/04。<只有更多沒有最多的社交工程>,《果核數位》,2019 年 6 月 04 日,<https://www.digicentre.com.tw/industry_detail.php?id=39

>。

武千妍，2017/06/13。〈軍校巡禮 | 第二十一站：解放軍資訊工程大學」〉，《中國軍網》，<http://www.81.cn/jwgz/2017-06/13/content_7636741.htm>。

黃彥棻，2016/08/12。<從烏雲升級事件看中國政府對網路的箝制>，《IThome》，<https://www.ithome.com.tw/news/107478>。

趨勢科技研究團隊，2013/10。＜APT 白皮書＞，《趨勢技術通報》，<https://esupport.trendmicro.com/zhtw/business/topic_knowledgedownload/topic_techsupportboard/20131031.aspx>>。

趨勢科技研究團隊，2014/05。<<APT 攻擊>看起來是 .PPT 附件,竟是 .SCR !!針對台灣政府單位的 RTLO 技術目標攻擊>，《趨勢技術通報》，<https://blog.trendmicro.com.tw/?p=8334>。

趨勢科技研究團隊，2017/07。＜主要鎖定台灣,專偷機密技術的 BlackTech 網路間諜集團＞，《趨勢技術通報》，<https://blog.trendmicro.com.tw/?p=50684>。

外文資料

Book

Knake Clarke ,2011. *Cyber War* .New York: HarperCollins.

Middleton Bruce, 2017. *A History of Cyber Security Attacks* .UK: Taylor& Francis Group.

Stokes Mark A, Lin Jenny and Hsiao L.C. Russell, 2011/11. The

Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure. Washington D C:Project 2049.

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

Conference

Costello John, 2017/11/17-18.「Strategic Support Force: A Force for a New Era」PLA Reform, Part Deux 2017 International Conference on PLA Affairs. Taipei: CAPS-CSS-NDU-RAND.

Web Materials

Lin ,Ying Yu, 2016/08/31."The Secrets of China's Strategic Support Force" *The Diplomat*, 〈 https://thediplomat.com/2016/09/the-secrets-of-chinas-strategic-support-force/〉.

Professional Services and McAfee Lab, 2018/04/07."Global Energy Cyberattacks: Night Dragon", < https://kc.mcafee.com/corporate/index?page=content&id=KB71150&locale=zh_TW >.

The Development and Transformation of PLA Cyber Warfare *

Ying-Yu Lin

(Adjunct Assistant Professor,

Institute of Strategy and International Affairs

National Chung Cheng University)

Abstract

With the development of information technology, people have become increasingly dependent on the Internet. Because of its highly-developed information industry, Republic of China (ROC) boasts a convenient environment for use of the Internet, which, however, also makes it become a target for black-hat hackers and cyber forces around the world. Chinese cyber forces usually take ROC as a testing ground for cyber attacks, conducting cyber-enabled theft of intelligence or causing

* As writing this paper, I was indebted to many friends in the information security field and hacker circle for their advice on information security technology. They included TDoH, LEUKOCYTE-LAB, Borg, and other local and foreign groups. They also introduced me to other hackers, who, speaking on condition of anonymity, offered me much advice on hacking practices.

damage to hardware via the Internet. They even use the Internet as a means to spread misinformation. All this has greatly threatened the security of ROC. This paper focused on cyberspace-related threats. It started off with an interpretation of cyber warfare as defined by China before analyzing and probing into China's threats to Taiwan's cyber security.

Keywords: Cyber Security, PLA Strategic Support Force, China Hacker