大陸網軍與APT攻擊

PLA Cyber Army and Advanced Persistent Threat

林穎佑（Lin, Ying-Yu）
淡江大學國際事務與戰略研究所博士候選人

壹、前言

本文先探討網路戰的定義以及概念上的差異，再探討資訊安全的發展歷程。特別是2008年開始，駭客攻擊手法便不斷更新，中共亦藉由組織民間駭客，有系統的規劃網軍部隊利用「ＡＰＴ攻擊」手段輔以「社交工程」，針對特定關鍵人士做出網路攻擊，藉此竊取重要情資。有鑑於網路空間並無時間，地理限制，隨時可以運用具有連線功能的相關設備進行網路攻擊，形成真正的「全民皆兵」。

“資訊安全是一個過程 不是產品”
“數學是合乎邏輯的,但是現實是主觀的”
By Bruce Schneier[1]

近年來，在媒體與政府的宣導之下社會大眾對網路戰與資訊安全相關議題並不陌生。美國更在2010年正式成立網軍司令部，正式將網路戰公諸於世，更在2011年5月由白宮提出國際網路安全策略。[2]但軍隊早在20世紀末期便開始利用網路技術的輔助來進行戰爭，隨著資訊化戰爭時代的到來，第一次波斯灣

[1] Bruce Schneier 著，吳蔓玲譯，**秘密與謊言**（臺北：商周出版，2001年9月），頁I。
[2] White House , 「International strategy for cyberspace」(2011年5月16日)，2012年1月8日 download，《***The White House***》，http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf。

戰爭是一場一盎司矽晶，比一噸鈾還重要的戰爭。[3]新軍事事務革新的重點便在於，如何有效利用高科技的輔助來加強作戰的效果。但近年來在用語與概念分析不清的狀態之下，也導致網路戰一詞常與其他名詞產生誤解。

貳、網路戰的定義與相關名詞解釋

資訊戰、網狀化作戰、網路戰這3個名詞是一般最常誤用的概念，事實上這些名詞都有其特別的意涵與不同的定義，過度的延伸與用詞的不精確只會凸顯專業上的不足。

一、資訊戰與網狀化作戰

資訊戰(Information War)是一種藉由干擾敵方資訊、資訊流程、資訊系統、電腦網路並保全我方資訊、資訊流程、資訊系統、電腦網絡、以確保我方資訊優勢的行動。因此，對於資訊戰而言，如何利用資訊科技來輔助戰爭進行，都可以算是資訊戰的範疇。[4]無論是在決策、指揮、作戰上面，技術的進步都對戰爭的發展帶來革命性的發展。

資訊戰應是一種作戰概念的統稱，而非是作戰行動本身；注重於描述軍事作為（應用）與資訊科技（介面）的整合效能，非實際對敵展開的武裝行動。[5]共軍所稱的「信息化作戰」主要便是利用高科技進行輔助的戰爭，包含了所有運用電腦科技技術的戰術戰法。[6]其中各作戰單位形成網絡化、一體化，並將打擊對方指揮控制系統視為主要作戰關鍵。[7]

而網狀化作戰（大陸又稱做網路中心戰Net Center War,NCW ）則是利用資訊優勢，讓各軍種可以在最短時間內達到資訊分享，進行聯合作戰，在短時間內發揮最大火力擊潰敵人，[8]其主要關鍵在於能否達到資訊整合以及指揮作戰一體化。特別是在預算有限的情形之下，如何有效結合各軍種的力量，透過C4ISR，發揮火力，便是網狀化作戰。

---

3 艾文 托佛勒著，傅凌譯，**新戰爭論**（臺北：時報文化出版社，1994年），頁90。
4 陳文政、蘇紫雲，**不完美戰場**（臺北：時英出版社，2001年5月），頁19。
5 李承禹，「中共網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用」，**復興崗學報**（臺北），第90期，（2007），頁245-264。
6 徐小岩，**信息作戰學**（北京：解放軍出版社，2002年7月），頁5。
7 國防大學科研部，**軍事變革中的新概念**（北京：解放軍出版社，2004年4月），頁18-21。
8 許秀影、劉豐豪、張瑞勇，**前瞻國軍對次世代網路之應用**（臺北：國防大學管理學院，2010年11月），頁238-243。

二、網路戰的定義與特色

相對之下，網路戰(Cyber War)的定義，便較單純也比較容易定義。網路戰是指利用網際網路作為攻擊的媒介，是資訊戰概念底下的一種攻防型態，是資訊戰的一種特殊發揮形式。其特色在於，網路空間完全不受時間、地理區隔、天候的影響，讓傳統疆界變得模糊不清，而網路戰的低廉成本更使威脅的範圍與機會大增。[9]同時對管理人員而言，雖然可以透過IP追蹤的方式來搜尋使用者，但如何證明使用者登記的網路地址與真實的使用者是同一個人，目前在技術上仍有實證的困難。因此，雖然在網際網路的發達之下，國家、企業、個人，都因網際網路而串連在一起，但背後的真相卻是彼此根本不能確定對方，在網際網路中的使用者可以隱藏自己的真實身分，沒有人知道使用者的身分，這都增加維護資訊安全與有關單位進行追蹤的難度。[10]究竟入侵系統是駭客單方面的個人犯罪行為，還是由敵對團體甚至敵國政府所授意下的軍事行動？就算確定攻擊對象的來源，如何明確界定這是屬於警政體系的社會安全問題，還是關係到國土安全的國際問題？這都增加事後採取報復行為以及反擊行動的困難。

網路戰另一個特色在於，受害者不知道電腦已經被入侵，電子資料的存取與實體物體不一樣，人們對於錢包、手錶、護照的保管或遺失會立刻發覺，但是對竊取電子資料而言，只是一個單純的複製下載的動作。因此除非網管或是IT部門有特別監控，一般人並不會察覺。一個冷戰時期的間諜能偷走的資料有限，透過照相機或是膠捲的輔助以及冒著生命危險的潛入，都增加失敗的風險。但在網路世界中，駭客可以坐在遙遠的椅子上，透過網路的傳輸，便可輕鬆的下載資料。被害人在發現時，往往已有大批機敏資料已經遭到竊取。不易察覺問題這也是網路戰的一大特點。

早期網路攻擊只是單純駭客個人的行為，但近年來逐漸發現，有國家或是其他相關單位有系統的組織駭客，利用國家的組織動員力量成立專屬的網路攻擊部隊（以下簡稱網軍），針對特殊的目標量身打造專門的入侵戰略。有別於過去釋放病毒或後門程式，網軍經常化被動為積極，主動入侵目標的電腦，或是透過APT式攻擊以及社交工程，來嘗試突破目標的資訊安全防護網，從一臺電腦的突破進而擴散到全機構系統。一旦發生資安事件，各單位都會立即受到

9 鈕先鍾，**21世紀的戰略前瞻**（臺北：麥田出版社，2001年8月），頁148。
10 Andrew L. Shapiro, "The Internet", ***Foreign Policy*** (Washington), Issue. ll5 (Summer, l999), p. 17-19.

影響；只要有一處資安漏洞，就會危及全軍。[11]雖然目前作業軟體的漏洞，並不是一般人可以解決的問題，必須由熟識電腦程式語言的專業人員進行作業。但對資訊安全的認知以及平時的防護是每個人的責任。

由於電子商務的興起以及社會對網路系統的依賴，各政府或民間企業甚至個人對於資訊安全都有一定程度的認識或防護，但資訊安全是一個過程，並不是產品。資安不是單純的購買防毒軟體，以及設立防火牆便可解決。近年來網路攻擊其效應已經不是單純的竊取資料，很有可能從看不見的戰爭演變成為大規模的破壞，造成人員的傷亡。特別是在關鍵基礎設施防護（Critical Infrastructure Protection, CIP）上，超過90%的美國基礎建設如：電力、自來水、交通等都由電腦系統來作控制，透過網路連結進行通信。[12]在有心人士的利用之下，很可能會造成大規模停電，或是大眾交通系統、股市交易系統的癱瘓，會造成民心恐慌以及意外事故的發生。[13]讓網路戰從虛擬走向現實生活，從數位空間走向現實環境。

參、近年大陸網軍的特色與實際作為

大陸很早便提出網電一體戰概念。早在2002年，當時身為共軍總參四部（電子對抗雷達部）部長戴清民在一份內部報告中透露，共軍總結「信息戰」的10大樣式聚焦於「網電一體戰」。[14]美國國防部於「2008年中共軍力報告書」中便宣稱：「針對中共民用和軍用網路的攻擊能力，正是共軍發展不對稱戰法的非接觸作戰中的重要組成」。[15]共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

11 Otto Kreisger 著，宋家駒譯，「資安漏洞危及全軍」，**國防譯粹**（桃園），第35卷第5期（2008年5月），頁7。

12 Benijamn S.Lambeth 著，李永悌譯，「空權、太空權與網路權」，**國防譯粹**（桃園），第38卷第4期（2011年4月），頁23。

13 「近8成關鍵基礎設施在2010年遭駭客入侵」（2011年4月7日），2012年4月6日下載，《**網路資訊**》，http://news.networkmagazine.com.tw/classification/security/2011/04/07/23452/>。

14 林勤經著，「中共網軍建設與未來發展」，林中斌主編，**廟算台海**（臺北：學生書局，2002年12月），頁439。

15 劉宜友，「淺析中共網電一體戰」，**國防雜誌**（臺北），第26卷第3期（2011年3月），頁121。

將「網電一體戰」視為「一體化聯合作戰」的基本形式之一。[16]

普遍認為正式大規模的網路戰首次出現於1999年的科索沃戰爭，駭客利用入侵北約網路系統，以及透過電子郵件夾帶電腦病毒、甚至利用更換官方網站首頁的方式來對北約轟炸表達抗議。[17]隨後在美國誤炸中國大陸駐南斯拉夫大使館後，自稱為「中國紅客聯盟」的駭客團體也開始在網路上對美國展開攻擊。前總統李登輝在1999年提出兩岸「特殊國與國關係」後，也引發大陸駭客攻擊中華民國政府、大學、商業網站，將網站首頁更換為大陸五星旗以及播放義勇兵進行曲，此舉也讓臺灣駭客發動反攻，引發兩岸駭客大戰。[18]2002年5月1日，美國白宮、國務院、五角大廈3單位的官方網站同時遭到大陸駭客蓋臺（更換首頁），雖然攻擊方自稱為「中國紅客聯盟」的民間駭客團體，但一般認為，這些都與傳聞中的大陸網軍脫離不了關係。[19]這些在21世紀初期的網路駭客大多都以騷擾為主，但隨著科技化以及人類對於資訊系統的依賴加深，也讓網路攻擊的影響產生更大的效果。

一、大陸網軍與電子商務

電子商務的興起也加深了人類對科技的依賴：電子商務是全球化無國界，偏重在無形的事物、想法、資訊，和這3者的關係相連產生一種根植於電子網路上的新興市集與社會。[20]在電子商務中：銀行電匯、ATM轉帳報稅、網路信用卡的使用都讓資訊技術走進人類生活，也因為電子商務創造了龐大的商機，更加吸引駭客的覬覦，2010年便有駭客透過網路銀行網站的安全漏洞，取得大量顧客個人與信用卡資料。[21]而「資料挖礦」（Data-mining）研究的興起，更加深駭客對公司資料的覬覦。資料挖礦是一種統計學的應用，記錄顧客的購買行為，並加以量化，期望從中發現顧客購買的習性以及商品可能的關連。由於在進行資料挖礦時，需要大量的消費者個人資料、過去的購買明細、可能做過的問卷調查，這些數據都透過電腦來進行統計分析。若有心人士透過資安的

16 Military Power of the People's Republic of China 2009，黃引珊譯，「中共軍事戰略與準則」，**國防譯粹**（桃園），第36卷第7期（2009年7月），頁7。
17 東鳥，**中國輸不起的網路戰爭**（長沙：湖南人民出版社，2010年11月），頁45。
18 辜樹仁，「大陸駭客 臺灣練兵」，**天下雜誌**（臺北），454期（2010年8月），頁127。
19 劉台平，**島計畫**（臺北：時英出版社，2004年5月），頁45。
20 Jeffrey F. Rayport &Bernard J Jaworski ，黃士銘、洪育忠譯，**電子商務**（臺北：麥格羅希爾出版社，2003年7月），頁2。
21 中央社，「客資外洩玉山銀遭罰400萬」（2010年12月9日），2012年4月1日下載，《**中央通訊社**》，http://tw.news.yahoo.com/%E5%AE%A2%E8%B3%87%E5%A4%96%E6%B4%A9-%E7%8E%89%E5%B1%B1%E9%8A%80%E9%81%AD%E7%BD%B0400%E8%90%AC.html。

漏洞，取得個人資料用來犯罪。除了冒名使用之外，許多的電話詐騙犯罪，更是讓民眾不勝其擾，這都是個資外洩所帶來的問題。因此對駭客而言，資料庫就是利潤的來源，透過販賣個資給偽卡集團利用，更讓恐怖組織的活動以及地下經濟更加猖獗。這也代表未來銀行、社群網站，以及存有大量客戶資料的單位，或是目前各資訊科技公司所主打的雲端資料庫，都可能成為未來駭客的攻擊目標。雲端運算（cloud services）是以使用者為核心，透過本地端之網路連線，在任何時間、地點運用終端設備取得遠端主機提供的網路服務；它是由分散式運算及網格運算（grid computing）的概念演進而來。[22]雲端技術所強調的是：多用戶、大規模、高彈性以及透過自助式資源將資料檔案都設置在於網路空間中，[23]消費者透過智慧手機、筆記型電腦、平板電腦、甚至桌上型電腦任何一個「端點」都可以同時接收分享同一塊「雲」。雲端技術雖然提供高度的便利性，但也帶來高度的風險，等於通知駭客，直接攻擊雲端資料庫，因為這邊擁有最完整的檔案。由於資料過於集中，一旦雲端失守，帶來的損失更是難以估計。[24]

而大陸除了網軍駭客部隊之外，也利用商業的機會將網路戰發揮淋漓盡致。由於大陸為目前世界主要電子零件生產地之一，許多電子廠以及資訊公司的亞洲主機皆設置在大陸，這也造成其利用商業作為掩護的機會。美國眾議院情報委員會曾對大陸電信設備龍頭華為技術有限公司和中興通訊有限公司進行調查，懷疑這兩者與大陸軍方有相當關連，並提醒美國企業不要與上述公司合作。華為公司內部與大陸政府組織一樣設有黨委，也向共軍網路戰部隊提供服務。[25]雖然在日後的調查中，並未發現華為公司進行間諜活動，但一致認為華為的科技產品中，容易被駭客入侵的資安漏洞較多，特別提醒消費者注意。[26]

---

22 王平、林文暉、郭浦村、王子夏、盧永翔，「雲端運算服務之資安風險與挑戰」，**資訊安全通訊雜誌**（臺北），第16卷第4期（2010年10月），頁45-49。

23 Tim Mather,Subra Kumaraswamy,Shahed Latif，胡為君譯，**雲端資安與隱私企業風險應對之道**（臺北：碁峰資訊，2012年5月），頁8。

24 中廣新聞，「繼SONY全球付款公司也傳駭客入侵」（2012年4月2日），2012年4月5日下載，《**中時電子報**》，http://news.chinatimes.com/tech/12050903/132012040200457.html。

25 何怡蓓，「美國指華為中興疑涉間諜活動 美大選貿易保護主義是始作俑者」，**亞洲週刊**（香港），第26卷第42期（2012年10月21日），頁8。

26 康彰榮，「未發現華為從事間諜活動」（2012年10月19日），2012年11月3日下載，《**中時電子報**》，http://tw.news.yahoo.com/%E7%99%BD%E5%AE%AE-%E6%9C%AA%E7%99%BC%E7%8F%BE%E8%8F%AF%E7%82%BA%E5%BE%9E%E4%BA%8B%E9%96%93%E8%AB%9C%E6%B4%BB%E5%8B%95-213000475.html。

二、大陸網軍與個資外洩

隨著社交網站、網路通訊軟體的普及，資安問題也進入一個新的層次。Facebook以及大量的社交平臺出現，讓人類對於網路世界又多一層認識。透過Facebook的連結以及分享資訊，都讓人在無意之間透露許多的訊息。在一些行銷手法的推廣之下，Facebook的「打卡」已經成為系統中十分受歡迎的功能，但打卡的同時也等於向外界宣告自己的動向。更不用說智慧型手機的普及，讓行動上網功能更加的便利。這些高科技用品雖然代表消費者可以隨時隨地上網，但從另一角度而言，也代表其他人可以透過你的上網紀錄來追蹤你的動態。而在Facebook的確認好友名單中，也經常洩漏許多的資料以及朋友間的人脈網絡，甚至有可能會出現藉由冒用身分來獲得其他好友動態與生活習性。這些資料都可能會在日後變成日後駭客攻擊的參考依據。

資料的外洩造成的問題除了詐騙之外，更大的問題是有可能會偽造身分來騙取他人的信任。2012年一位身兼NATO最高統帥的美國海軍上將，便懷疑遭到大陸網軍的利用，開設假的Facebook帳號，並利用好友功能，藉此探知其他資料。[27]而也有越來越多的駭客利用電子商務的漏洞來進行非法金融交易進而破壞世界的金融秩序，一般的網路犯罪形成可能危害國家安全的重大威脅。除了駭客入侵之外，有許多資料外洩皆源自於有關單位的忽視，在進行職務交接，或是單位合併辦公遷移時，由於時間以及成本的考量，並沒有對客戶相關資料進行銷毀，因此在有心人士的留意之下，很容易取得相關個資。[28]隨著資訊化的程度，過去龐大的紙本資料已不復見，取而代之的是硬碟以及電子資料庫。對駭客而言，資料的取得更加方便，只要單純的複製以及傳輸就可以在短時間內取得大量的資料。特別是民間企業並不會像政府或軍方單位有相對較嚴密的保防制度，如保險公司、航空公司、銀行、各種商店會員卡為了營業推銷上的需求，大量的收集個人資料，但只要一個硬碟的遺失以及一個小巧的USB隨身碟很有可能在短時間內就會帶走大量的資料。[29]這些都是目前個資外洩嚴重的原因之一。

雖然個資外洩問題嚴重，但在多數人的心中仍與國家安全有一段差距。個

27 「冒名北約統帥／中國網諜臉書竊密」（2012年3月12日），2012年4月6日下載，《**自由電子報**》，http://www.libertytimes.com.tw/ 2012/new/mar/12/today-int1.htm。

28 「千筆中信局客戶個資丟馬路」（2010年6月20日），2012年4月1日下載，《**蘋果日報**》，http://www.appledaily.com.tw/appledaily/article/headline/20100620/32600661。

29 中央社，「買二手硬碟赫見銀行往來資料」（2012年2月29日），2012年4月5日下載，《**聯合新聞網**》，http://udn.com/news/LIFE/LIF1/6930184.shtml。

資洩漏的嚴重性在於讓駭客瞭解你的職業、喜好、與友人的關係。擁有這些資料之後，可提供駭客做出針對目標進行網路攻擊，利用重要相關人士的信箱（帳戶）來轉發內藏惡意程式的郵件。[30]過去夾帶電腦病毒以及內藏木馬程式的攻擊手法，之所以能被防毒軟體發現，是因為其攻擊的樣本數多到讓防毒軟體公司重視其危害。但在有組織駭客集團甚至國家網軍的策劃下，針對目標量身打造的策略，讓被害人放鬆警戒直接將密碼或是相關資料交給對方，利用人性的弱點，讓被害人在開啟有興趣的檔案時，啟動了木馬程式或是開啟入侵系統的後門，藉此突破防火牆以及資安防護網，藉此取得內部機敏性資料。特別是由敵對國家所組織的網軍，竊取的資料有可能是作戰電子參數，重要軍火裝備的研發資料、情報人員的身家背景...這些都嚴重的危害國家安全。大陸網軍便利用網路多次入侵英國國防產業BAE system的電腦系統，嘗試竊取與美國合作研發的F-35匿蹤戰鬥機的相關數據，都會影響未來F-35在戰場上的存活性。[31]甚至利用其資料協助自身開發先進的戰鬥機。[32]因此透過電腦的入侵、利用竊取的個人資料來通過原有資安系統的認證，為公司與國家提供了一種新的間諜手段。[33]

但新型態的網路攻擊，與過去傳統植入電腦病毒、木馬程式截然不同，過去駭客著重的是入侵技術，透過網路的入侵來達到癱瘓對方資訊系統的目的，而現在關鍵則在於戰術，利用個資的取得，來突破人心的防線。也因此出現社交工程以及APT式攻擊等兩種新的攻擊手法。

肆、大陸網軍與新型態攻擊

一、中共網軍與APT攻擊

進階持續性滲透攻擊（Advanced Persistent Threat ,APT）[34]是2005年以來，駭客的新攻擊手法。其主要是利用人性以及社交工程（Social

30 Martin C Libicki, ***Cyberdeterrence and cyberwar*** (CA: Rand Company: 2009)，pp13-19 。

31 （2012年3月13日），2012年4月6日下載，《**自由電子報**》，http://www.libertytimes.com.tw/2012/new/mar/13/today-int5.htm。

32 「中國駭客入侵BAE竊取F35機密」（2012年11月5日），2012年11月8日下載，《**中時電子報**》，http://news.chinatimes.com/mainland/11050501/132012110500837.html。

33 Dorothy E Denning著，吳漢平譯，**信息與安全**（北京：電子工業出版社，2003年8月），頁326-336。

34 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（臺北：資安人，2011年12月6日）。

Engineering）的方式來達到騙取被害人信任，也是目前大陸網軍經常使用的方式。從英文字面上，我們可以注意到其3大要點:持續性、潛伏性、高攻擊性是其主要特點。APT攻擊是一個有組織有計畫的間諜行為，與以往資安事件不同的是，過去駭客強調的是表現自我的能力，主要目的是騷擾以及做出惡作劇型態的置換網頁或使用阻斷式服務攻擊（Denial of Service ,D.O.S）來嘗試癱瘓主機伺服器，[35]藉此表現出自己的高超技術。過去駭客尋找的是最脆弱的地方進行攻擊，但在APT攻擊中，由於事前需要專業團隊進行長時間的資料蒐集、發現漏洞、數據分析、環境測試與個資取得，並需要大量的資金投入，非一般普通駭客可以完成。因此在目標的選擇上強調是以目標的價值性作為攻擊的順序。[36]APT式攻擊是有計畫、有組織且有針對性的惡意網路活動，從政府到個人都是其攻擊目標，特別是針對公部門的滲透。APT其名詞首見於美國空軍在2006年所提出的網路安全報告。其主要是透過一群經過政府組織，施以專業訓練，並分工精密的數位化戰士。入侵之後再藉由重要目標的社交圈、供應商、往來客戶名單來擴大攻擊效果。APT所注重的不是攻擊的新技術，其特色在於長期潛伏，以及大量收集資料。雖然技術上仍然未突破傳統的Rootkit技術，[37]但防範APT攻擊不能單純的依賴防毒軟體或是防火牆，必須要做好長期對抗的心理準備，除了潛伏期長以及有所組織與計畫之外，APT攻擊更加的「智能化」，會不斷的嘗試新的攻擊方式來入侵電腦。[38]

APT攻擊與一般病毒郵件不一樣，不易被防毒軟體攔截。網路攻擊的特色在於被害人很難發覺資料外洩，數位化的資料可以輕易複製傳輸，造成資安部門知道的僅僅是冰山一角，在發現問題時，往往已經造成龐大的損失。APT攻擊，一般是利用惡意程式或是軟體公司的檔案漏洞來突破資安防線，常會偽裝成PDF檔或是WORD檔後，再附上該目標有興趣的標題，來吸引被害人開啟檔案並乘機將Rootkit殖入被害人電腦之中。如2006年大陸網軍便利用知名立法院國防委員會立委辦公室的名義發電子郵件給軍事媒體記者。許多記者誤以為是新聞稿或相關資料，一時不察，打開附加檔案後紛紛中毒。[39]雖然寄件人地址

35 黃祥哲、吳惠麟、盧長青、張峯誠、羅浩、潘正祥，**資訊安全原理與實驗**（臺北：碁峰出版社，2008年11月），頁10-25。

36 李青山，「APT發展趨勢研究漫談」，**信息安全與通信保密**（北京）， 2012年7 月，頁19-21。

37 Rootkit為一種隱藏程式行程的軟體。詳見：Greg Hoglund & James Butler , ***Rootkits: Subverting the Windows Kernel*** (MA: Pearson Education, 2006).

38 徐偉，「APT攻擊-狼來了及應對措施思考」，**信息安全與通信保密**（北京），2012年7月，頁17。

39 黃敬平，「記者收毒郵 疑中駭客搞鬼」（2006年4月14日），2012年10月12日下載，《**蘋果日報**》，http://www.appledaily.com.tw/appledaily/article/headline/20060410/2528327/。

與名稱可能有所細微出入，但一般人若未加細察，很難發現問題。除了立委之外，大陸網軍也有系統的收集，相關國防、外交、政治議題的學者相關人士，在適當時機利用其名義寄送相關文件，來達到突破資安防護的目的。2012年8月大陸網軍甚至直接在大學電子布告欄上，假造國防部公文，散布不實消息之外，也可能在附加檔案文件中夾帶木馬程式。這些手法都是利用人們的不察或是大意，直接下載有問題的檔案，讓木馬程式或是電腦病毒直接入侵成功。[40]美國白宮也有收到由大陸駭客所發出的「釣魚」信件，通過引誘電腦使用者打開隱藏有攻擊程序的電子郵件而達到入侵的目的。[41]

APT攻擊的流程可以與管理學的PDCA（Plan,Do,Check,Act）循環類比。[42]在計畫（PLAN）層面，駭客群要作的是鎖定目標以及收集資訊。而執行（DO）階段，對駭客來說就是入侵網路系統，並且建立資料基地與攻擊平臺。在第三步驟（Check）時，指揮駭客群的高層情資單位會分析解讀所得到的資訊，並評估戰果，最後階段（Act）會嘗試利用被害者的通訊錄與人際網絡或是提高攻擊權限，持續進行攻擊。[43]這便是典型的APT式攻擊循環。類似的案件層出不窮，每當軍方每年進行重要的演訓時，類似的攻擊郵件數量越來越多。這些攻擊許多專家皆認為是來自大陸網軍。由於兩岸關係錯綜複雜，臺灣更成為大陸網軍測試新戰法的實驗對象。[44]共軍網路部隊也利用許多臺灣主機當跳版，透過惡意程式入侵電腦之後，讓該電腦受駭客的控制，並作為攻擊或是發送垃圾資訊的主機。而這一些遭受到僵屍網路（Botnet）控制的僵屍電腦（zombies），更讓相關治安單位透過IP位置進行追蹤時，也只能查到被利用的受害人而已。[45]根據防毒軟體公司賽門鐵克的報告指出，臺灣僵屍電腦的數目是全球的7%，其中臺北市便占了其中5%，是全球最多僵屍電腦的城市。這些

40 吳明杰，「假公文臺軍漏餡 疑中共網軍散佈」（2012年8月20日），2012年11月2日下載，《**中時電子報**》，http://tw.news.yahoo.com/%E5%81%87%E5%85%AC%E6%96%87%E8%87%BA%E8%BB%8D%E9%9C%B2%E9%A4%A1-%E7%96%91%E4%B8%AD%E5%85%B1%E7%B6%B2%E8%BB%8D%E6%95%A3%E6%92%AD-213000848.html。

41 劉項，「中國駭客入侵美國網絡」，**亞洲週刊**（香港），第26卷第41期（2012年10月14日），頁9。

42 PDCA循環是由管理學界所提出的透過規劃、執行、查核與行動之循環來進行品質管理。褚，「PDCA循環(Plan-Do-Check-Act Cycle)」（2009年11月10日），2012年4 月6日下載，《**臺灣大百科全書**》，http://taiwanpedia.culture.tw/web/content?ID=19364 。

43 Roamer，「**APT教戰手冊**」，發表於「擋住資安骨牌效益」研討會（臺北：資安人，2011年8月11日）。

44 羅添斌，「中國網攻新戰法 拿臺灣試刀」（2011年8月4日），2012年4月6日下載，《**自由電子報**》，http://www.libertytimes.com.tw/2011/new/aug/4/today-p8.htm。

45 僵屍網路也稱機器人網路(Botnet)。江逸之，「你我都是受駭人」，**天下雜誌**（臺北），第454期（2010年8月），頁116。

電腦會自動跟控制中心連線，等待駭客的命令，隨時發起攻擊。[46]

近年大陸網軍發起的APT攻擊都造成各國相當大的威脅。如： 2010年攻擊Google的「極光行動」（Operation Aurora）[47]以及在2011年McAfee資安公司發表的一份報告中便指出由大陸網軍主導的「夜龍行動」(Night Dragon)，[48]其針對十多家能源企業進行APT攻擊，從外網主機web伺服器進攻使用SQL注入攻擊，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）。最後再利用社交工程將郵件破壞力發揮到最大。而2011年8月同公司又發布一項資安報告，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。整個行動歷時5年，目標遍布美國、臺灣、南韓、印度以及各大國際組織，聯合國、東南亞國協、各大新聞媒體與許多英美國防承包商以及許多關鍵基礎設施相關單位廠商。許多國家機密以及經濟優勢都隨著電腦駭客的入侵，逐漸流入敵意國家，這是知識產權史上最大的財富轉移。包括聯合國、中華民國等國家政府、國防承包商、多家國際企業等72個機構的網路都遭駭客攻擊。根據資安公司的分析這些駭客皆是來自大陸。除了嘗試入侵之外，駭客更直接針對Gmail用戶帳號，嘗試進行入侵，期藉此窺探重要相關人士的電子郵件。[49]

一、大陸網軍與社交工程學

社交工程（Social Engineering）是一種不需要高超技術的入侵方法。利用疏於防範的心態，來欺騙被害人，其技巧常透過交談、偽造文件、假冒身分利用一些專家術語，從合法用戶中套取用戶的秘密，如帳戶密碼、相關資料。一般資安人員都會強調軟體與硬體科技，但卻忽略人性是最後也是最容易疏忽

46 王平、林文暉、林孝忠、李奇軒、呂育華，「僵屍病毒解藥與監控系統之研發」，**昆山科技大學學報**（臺南），第9期（2012年6月），頁37-47。

47 Xecure-Lab研究團隊，「三起APT事件攻擊手法解析」，**2012資安趨勢專刊-換個腦袋作資安**（臺北：資安人，2011年12月6日），13頁。

48 Professional Services and McAfee Lab, “Global Energy Cyberattacks: Night Dragon.”（2011年2月10日），2012年4月6日 download，《***The Heartland Institute***》，http://heartland.org/policy-documents/global-energy-cyberattacks-%E2%80%9Cnight-dragon%E2%80%9D 。

49 陳成良、羅添斌，「最大規模駭客攻擊 指向中國」（2011年8月4日），2012年10月6日下載，《**自由電子報**》，http://www.libertytimes.com.tw/2011/new/aug/4/today-t1.htm。

的一環。[50]現在的社交工程大多應用在電子郵件詐欺上面，過去收到的垃圾信件，常利用成人網站或是一些購物網站的廣告作為掩護。但在與APT式攻擊結合之後，社交工程會分析目標的習性，以及對新聞的閱讀習慣，那類型的文章會特別感興趣都有特別的追蹤分析，最常收到的來信人是誰？以及兩人之間的關係，並在可能的時間點寄出含有惡意程式的信件欺騙被害人。[51]其中利用各種人類的基本情緒，以恐嚇、扮演、同情、諂媚、權威、壓力、虛榮等等方式來騙取目標的信任。「人」是資安防護網中最脆弱的一環，因為人性是無法修補以及進行軟體升級。[52]

社交工程的破壞力會讓耗費高額成本打造的資安系統毀於一旦。國際知名的資安公司HB-Gary其主要客戶為美國政府單位與國防部，其提供的資訊服務內容涵蓋駭客身分識別、執行滲透測試，為美國資安防護中的重要一環。但該公司卻被駭客群入侵，大量資料遭駭客披露，連2011年2月舉辦的RSA-2011資安年會，[53]該公司也被迫退出。其最重要的關鍵在於駭客冒充該公司高階主管，寄出電子郵件給IT部門經理，聲稱其在國外開會，在情急之下需要更改密碼與設定。在IT部門經理修改之後，結果可想而知。[54]可見社交工程學可以繞過密碼保護、電腦安全防衛、網路安全防衛，所有技術上的安全措施，直接攻擊最脆弱的一環：人性。[55]再多的防火牆都抵不過一封信的威力。

另一案例則是美國著名公司EMC底下資安部門RSA所發生的入侵事件。目前坊間使用的動態密碼鎖(One time password)SecureID就是出自該公司。2011年3月RSA公開宣布該技術遭到駭客使用APT式攻擊，其產品認證資料已外洩。其受攻擊的過程與Google所遭遇到的極光行動同出一轍。Google公司在2010年1月公布的文件中便指出遭到大陸精心策劃且目標明確的攻擊。隨後亦有媒體根據電子數據的追蹤，認為大陸專門培訓駭客的學校位於上海交通大

50 Kevin D. Mitnick & William L. Simon，子玉譯，**駭客大騙局**（臺北：藍鯨出版社，2003年9月），頁14。
51 Johnny Long , ***No Tech Hacking :A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*** (MA: Syngress publishing, 2008),pp110-117.
52 Cyrus Peikari& Anton Cbuvakin，陳建勳譯，**防駭戰士**（臺北：美商歐萊禮股份有限公司，2007年5月），215頁。
53 RSA大會為1991年以來是資訊安全領域規模最大，最具影響力的國際盛會。胡曉荷、白浩、周雪，「RSA大會-信息安全界的不老傳說」，**信息安全與通信保密**（北京），2012年第4期（2012年4月），頁9-13。
54 Nate Anderson, “Anonymous vs. HBGary: the aftermath”（2011月2月25日）, 2012年4月5日 download，《***Ars technica***》，http://arstechnica.com/tech-policy/news/2011/02/anonymous-vs-hbgary-the-aftermath.ars.。
55 Bruce Schneier，吳蔓玲譯，**秘密與謊言**，頁341。

學與山東藍翔高校。[56]同時這也代表大陸對其網軍部隊的重視，利用國家資源透過嚴格的學術課程來培養網路戰士，[57]除了以「信息安全人才」為訓練的名目除了公安部門之外，也在軍事單位中設立相關系所藉此訓練培養網路人才。[58]也在網軍中挑選精英份子組成「藍軍」專門評估共軍的網路系統，發掘可能損害軍事戰備能力的弱點。運用官方資產來加以培訓之外，更招募大批「愛國駭客」，也就是具備某種程度的電腦知識，且願意對假想敵發動網路攻擊之非政府人員。雖然政府可以雇用此類專業人士來擔任政府專職人員。但對大陸而言，透過這些獨立作業的愛國駭客進行網路作戰，可辯稱為民間人士的個人行為，是屬於法律層面的犯罪行為，否認由政府負責。受到大陸所容許甚至鼓勵的類似獨立駭客團體約有二百五十個，[59]由於資訊化的普及，以及網路的便利，這類新時代的「民兵」對其他國家的威脅遠高於過去。「網路人民戰爭」，更是充分達到軍民合一的目的，大陸方面直接呼籲需要愛國的駭客一起加入網路作戰的行列。[60]若再加上刻意的培植與訓練，更能擴大網路戰的效益。如經過有系統的組織網路戰士，並透過刻意的收集個人資料與網路使用習慣，藉此選定目標，並分析其對網路系統的依賴程度與遭到破壞後對於軍事、經濟、政治、社會民心的影響，經過培訓後，再提供相對高品質的資訊設備，利用「飽和攻擊」的方式更能充分發揮網軍的作戰效用。[61]

著名資安企業RSA遭到入侵的起源，也是由兩封電子郵件揭開序幕。利用Excel檔案作為掩護，在開啟檔案時也被植入Adobe Flash零時差漏洞（CVE-2011-0609）並遭到遠端遙控工具的控制，在此時也開始入侵其他伺服器與相關人員的系統。[62]資料外洩之後由於許多重要企業與軍火商都採用該公司的系統，因此也間接導致日後重要國防產業公司洛克希德馬丁（Lockheed

56 管淑平，「Google駭客技術來自中國」，**自由時報**，2010年2月23日，第A8版。

57 John Bumgarner 著，周敦彥譯，「確保網路安全：重新思考新防禦時代之軍事準則」，**國防譯粹**（桃園），第38卷第4期（2012年4月），頁43。

58 趙俊閔、吳曉平、秦豔琳，「信息安全人才培養體系研究」，**北京電子科技學院學報**，第14卷第1期（2006年3月），頁27-31。

59 Richard Weitz著，高一中譯，「網路作戰威脅日增」，**國防譯粹**（桃園），第37卷第5期（2010年5 月），頁35。

60 張召忠，**網路戰爭**（北京：解放軍文藝出版社，2001年2月），頁62-65。

61 Rattray,Gregory J, ***Strategic warfare in cyberspaces*** (MA: Massachusetts Institute of Technology , 2001), pp188-199.

62 邱銘彰、吳明蔚，「網路有鬼APT陰魂不散」（2011年8月1日），2012年4月6日下載，《**資安人科技網**》，http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=6252。

Martin）[63]遭到駭客入侵，成功竊取大量資料。這些都是目前APT式攻擊與社交工程的結合。

伍、代結論：全民國防下的資訊安全

第一次世界大戰之後，德國魯登道夫（Erich Ludendorff）將軍曾指出：在現代戰爭中，很難區別前方與後方，因為人民與軍隊已合而為一，戰爭沒有軍民之分。[64]現今在綜合性安全觀的思維之下，非傳統安全的議題成為人類遭遇的最大問題。全民國防的理念，不僅表現在防衛動員準備體系的完整建立，更重要的，是全民透過一定程度的整合，建立政府、軍隊與民間互動與合作的機制，透過平民與軍隊的整合，共同維護國家安全。[65]網路戰是一場看不見的戰爭，更無分平時與戰時。在網路空間中，每一臺電腦都有可能會是網軍的戰場，特別是近年來智慧型手機的普及，上網不需要固定在某處操作電腦，駭客也隨著科技的進步，來增加其入侵的成功率，每一個網民都有可能成為新的網路戰士。如大陸透過網軍以及動員的網民，便可立刻在網路上發動攻勢。這些透過徵募以及專業培訓的網軍，在經過組織化的訓練後戰力非同小可。共軍更在廣州軍區成立聯通軍區、軍級單位、作戰師旅團和各訓練基地的「網路藍軍」來加強自身的網路戰實力，[66]也將大陸網軍提升自司令部層級的網路作戰單位。[67]同時也加強與民間合作，吸收具有資訊天分的人才進行培訓與收編，將網路戰發展成新型態的「人民戰爭」。[68]

只要資料存在電腦，同時該電腦擁有上網能力，就有遭到竊取的可能。雖然許多重要單位都採用實體隔離的方式來區分內網與外網，但由於工作的需要，若是將機密資料拷貝至私人電腦中，便有流出的可能。[69]或任何可以存取數位資料以及上網的工具，都有遭到植入木馬的可能。或利用社交工程學，掌握重要情資人士的關係網絡，從該要員的親人、師長、朋友下手，嘗試一層層的突破，取得關鍵資料或密碼。雖然人與人之間的關係隨著電子資訊的流傳逐

63 查淑妝，「美軍火商洛克希德馬丁遭駭客入侵網站 五角大廈影響輕微」（2011年5月30日），2012年4月6日下載，《**鉅亨網**》，http://tw.money.yahoo.com/news_article/adbf/d_a_110530_2_21ws9。
64 鈕先鍾，**西方戰略思想史**（臺北：麥田出版社，1999年12月），433頁。
65 羅慶生、李志誠，**國防安全**（臺北：華揚出版社，2005年3月），6頁。
66 羅印沖，「中共建網路藍軍 演練四面出擊」，**聯合報**，2011年5月27日，第A17版。
67 羅添斌，「中國網軍 升級司令部位階」，**自由時報**，2010年7月27日，第A2版。
68 楊念祖，**決戰時刻**（臺北：時英出版社，2007年2月），頁131。
69 李志德，「公務家辦 對岸網軍等者撈」，**聯合報**，2007年10月14日，第A1版。

日增加，也透過MSN、Facebook等社交網站的聯繫，讓人與人之間的距離越來越小，但這些認識都是透過網路線來傳遞的。網路上的交流都有機會成為社交工程的一環、在轉寄郵件以及下載網路資源的同時，可能也為駭客提供了一條捷徑。縱使擁有銅牆鐵壁的資安防護網，但若是忽略人員訓練可能釀成大錯威脅國家安全，如新武器的研發資料遭到網軍攻擊外洩，若是讓敵對國家取得F-35的相關數據，[70]便有可能危害日後其在戰場的存活性，而導致美國失去在空中的領先優勢。

過去不斷強調的「保密防諜」，在現今的網路世界中，更需要提倡，或是透過不斷的演練來達到效果。[71]來路不明的郵件最好不要開啟，或是透過電話與其他通信管道與發件者再次確定；在社群網站中切勿透露太多的個人資料以及最近動態（如Facebook中的打卡以及旅遊記錄），同時慎選網路朋友，避免有心人士的冒用，這些不只保護自己的隱私，更重要的是避免成為共軍網軍進行社交工程學的參考資料。特別是許多對軍事、國安議題有濃厚興趣的軍事迷，在網路熱烈發言的同時也被有心人士鎖定利用，利用「釣魚拉出」的手法吸收軍事迷。[72]對此，並不是說全面禁止相關人員使用社交網站，畢竟無線電廣播花了將近38年才累積5000萬名用戶；電視花了13年；網際網路4年；iPod3年，而Facebook不到1年便增加兩億個用戶。[73]因此，想要透過種種限制與罰則來避免人類接觸社群網站並不切實際，而應透過適當的宣導與規定來避免矯枉過正，美軍便在2011年公布社交網站的指導手冊，期望加強士官兵對資安的認知。[74]

也可以透過通信雙方都能瞭解的「暗語」，來建立屬於雙方的溝通密碼；或是注意電子郵件往來過程中的習慣來確定雙方身分。密碼仍必須避免單純的數字與字母組合，類似的傳統密碼在資訊科技的輔助之下，破解的機會日益增加。因此，透過文化傳統與當地特殊方言的協助，建立自己的密碼系統是可行的方式。如同在二次世界大戰中，美軍在太平洋地區便使用納瓦荷族語言來作

---

70 Richard A. Clarke& Robert K. Knake , ***Cyber War*** (NY: HarperCollins, 2010), pp233-235.

71 「李宗瑞影片千名公僕上鉤」（2012年9月15日），2012年10月13日下載，《**自由電子報**》， http://www.libertytimes.com.tw/2011/new/aug/4/today-p8.htm。

72 聞東平，**正在進行的諜戰**（香港：明鏡出版社，2009年4月），頁546-550。

73 James G.Stavrids and Elton C. Parker 著，高一中譯，「航向網路之海」，**國防譯粹**（桃園），第39卷第8期（2012年8月），頁6。

74 Office of the Chief of Public Affairs, ***US Army Social Media Hamdbook*** （WA：Department of Defense）, January 2011.

為溝通密碼，利用鳥類名字來代替各型戰鬥機型號，美軍在這方面獲得相當的收穫，戰後日本情報首腦有末精三也承認無法破譯美軍的納瓦哈密碼。[75]類似的情況也出現在2012年大陸對互聯網的封鎖，2012年2月王立軍事件後，大陸即刻在網路上封鎖該事件的討論，但大陸網民利用諧音（周永康用康師傅代替、王立軍用王捕頭）與流行次文化來避開網路管制。[76]

資訊安全是一個過程，不是一個產品。資安的防護必須從上到下每一單位的配合，才能避免威脅。密碼學的發展固然可以讓訊息加密，但科技始終來自於人性，最後導致防衛系統崩解的往往是人性的弱點。因此完整的員工教育以及資訊安全概論的提倡是必要的投資，資訊安全不是資安人員的專利，每一個可以上網的數位產品都有可能成為網軍利用的工具。同樣網路並無地理限制，國家領土的限制在網路空間中蕩然無存。因此需要國際合作以及情資的交換來確保網路資訊安全。[77]未來戰爭中的第一戰可能是發生在網路或是透過網域進行。除此之外，網路攻擊行動也可能結合實兵作戰，旨在切斷後勤支援乃至實體作戰系統等攸關戰力支援的各項服務。此外許多關鍵基礎設施雖然由民間持有與維持運作，但無論是民間社會本身或是政府軍方皆有賴類似設施維持日常重要能力運作，一旦遭到國家發起的一連串協同攻擊，勢將猝不及防，難以承受攻擊壓力。除了竊取重要資料之外，敵方亦有可能植入假資料來破壞資訊的完整性，來干擾或誤導我方判斷，甚至有可能造成民眾的恐慌與社會的混亂。[78]

法國戰略學者薄富爾曾指出：「當歷史的風吹起時，將壓垮人類意志，但預知風暴來臨，克服它們，並且就長期而言，使他們替人類服務，則又還是在人力範圍之內。這便要求擁有先見之明，以及一種精力作為後盾。要控制就要先知，最壞的就是觀望，那經常是無為的藉口。發現萌芽中的危險，並及時做成決定制止未來的危機。」[79]網路時代是無可避免的浪潮，隨著人類對科技的依賴，網路已無法從現代生活切割，因此資訊安全與國土安全的關係緊緊相連，在享受網路帶來的便捷同時，也需隨時注意資安問題，看不見不代表沒有發生，無知並不可怕，但將無知視為無所不知，只會帶來日後更大的損失。

---

75 Simon Singh，劉燕芬譯，**碼書**（臺北：商務出版社，2000年3月），頁231。

76 李永峰，「中國當局限制網民討論重慶事件，民間智慧催生各類暗語與代碼」，**亞洲週刊**（香港），第26卷第14期（2012年4月8日），頁8。

77 「美資安演習12國參與」（2010年9月29日），2012年4月7日下載，《**自由電子報**》，http://www.libertytimes.com.tw/2010/new/sep/29/today-int5.htm。

78 Robert A. Miller and Daniel T. Kuehl著，李育慈譯，「二一世紀之網域與第一戰」，**國防譯粹**（桃園），第37卷第5期（2010年5月），頁25。

79 薄富爾，鈕先鍾譯，**戰略緒論**（臺北：麥田出版社，1996年9月），頁192。