中共網軍發展與攻擊

◎林穎佑

前言

從 2005 年開始，對於來自中國大陸的駭客攻擊相關訊息便一直未曾中斷過，從針對 Google 的極光行動、能源公司的夜龍行動、美國國防相關產業與智庫進行的驟雨行動，乃至於包含全部產業的暗鼠行動，駭客們利用各種管道與方式攻擊，對美國許多重要單位進行網路入侵，除了國防相關機構與產業之外，其他如煉油公司及國防科技有關的企業智庫等重要關鍵基礎設施，都遭到駭客的攻擊。更有消息指出，總部位於上海的 61398 部隊就是大陸網軍的大本營，隸屬於共軍總參謀部(四部－電子對抗雷達部)。這一系列的新聞說明了大陸對網路戰的重視，甚至與民間學校合作（如武漢大學、藍翔技校、交通大學、信息工程大學等)，藉此培育未來共軍的資訊人才。

網軍的價值

共軍對網路戰的認識始於 2000 年。網路戰原先是在波斯灣戰爭後所制訂的高技術條件下的局部戰爭，隨著資訊科技的進步，2002 年，當時共軍總參謀部部長戴清民少將在一份報告中透露，共軍總結「信息戰」的十大樣式聚焦於「網電一體戰」，並將「網電一體戰」視為「一體化聯合作戰」的基本形式之一。特別是一體化作戰是根據美軍網狀化作戰所發展出來的，除了單純地協同各軍種火力之外，指揮體系的同步才是美軍聯合作戰的最終精神。對共軍而言，資訊化是構成一體化的第一步，發展的過程中也了解若是能在重要節點（C4ISR）上打擊敵人，便能爭取戰場的主動權，破壞敵人的指揮。但隨著科技發展，透過網路也能竊取或蒐集相當的情資，特別是許多重要資料都已電子化，相關參數或資料的外洩都會造成國防科技或是實戰上的危機。例如根據 2013 年 5 月美國的華盛頓郵報報導，研發中的 F-35 閃電式戰機、F/A-18、V-22 魚鷹機、愛國者飛彈系統數據等，已被來自大陸的駭客所竊取。這些科技資訊的洩露可能加快解放軍的軍事發展，並減弱美國的防衛能力（例如獲得的電子參數對無人機系統的威脅甚鉅)。

商業為後盾

而大陸除了網軍部隊之外，也利用商業往來將網路戰發揮得淋漓盡致。由於大陸為目前世界主要電子零件生產地之一，許多電子廠及資訊公司在亞洲地區的主機、伺服器皆設置在大陸，讓大陸得以利用各種手段，伺機竊取其間的機敏資訊。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官方組織一樣設有黨務組織與相對應的官職，也向共軍網路戰部隊提供服務。故在大陸從電子零件逐漸走向品牌(如長江、小米)、軟體系統(如 wechat、

QQ)，並開始普及全球時，也是其網軍最大的助力，這是消費者在選用大陸品牌時，不能不思考的問題。

進階持續性滲透攻擊（APT）

APT 攻擊首見於美國空軍在 2006 年所提出的報告，從英文（Advanced Persistent Threat）字面上，我們可以注意到 APT 攻擊的三大特點：針對性、潛伏性、高威脅性。它是有組織、有計畫的間諜行為，是一個為目標物量身打造的攻擊策略。此外，APT 攻擊會根據目標者的習性與人際網絡，假冒被害人的朋友、師長、同僚而冒名發送被害人感興趣的電子郵件，將惡意程式夾藏在相關新聞、文章、表格中，以 Word、PDF、Excel 檔案的方式附加在電子郵件中，讓被害人誤以為是重要文件或是其感興趣的主題而下載，在檔案開啟的同時，被害人的電腦就被入侵了；接著駭客透過該電腦的電子郵件紀錄或主機裡的資料，繼續規劃下一步的攻擊。而在 APT 攻擊中，與社交工程的配合會是攻擊成功的關鍵。社交工程是一種不需要科技的入侵方法，係利用人性的弱點來突破綿密的資安防護網。

網路戰特色

目前有資料顯示，大陸網軍的主要位置是在南京軍區的信息戰情報研究中心，負責對臺通訊打擊辨識與選定，並從此過濾所竊取的情報；國防動員委員會的信息動員辦公室則負責吸收與培訓民間人才；外圍組織進行的是較為低階的資通攻擊，如紅客聯盟、網路水軍、五毛黨之類；共軍軍事院校則負責吸收較高階的資通訊人才，並與民間大學合作，達到真正的「全民皆兵」、「人民戰爭」。目前的攻擊行為除了竊取資料之外，更嘗試癱瘓對方的關鍵基礎設施運作，由虛擬影響到實體。需注意的是，網路戰不需考慮地緣戰略的因素（除了機房節點），因此是否設在南京軍區仍有相當疑問。

現今雲端科技及智慧型手機的越加普及，益使網路攻擊的價值大增。雲端技術正好將雞蛋全部放在同一個籃子之中，只要一點攻破，全部的數位裝置全部遭殃，連接「雲」的任何一端都會是攻擊的目標，特別是智慧型手機更常因下載 APP 軟體而將惡意程式同時載入；而利用智慧型手機以 USB 傳輸資料或是連結電腦充電時進行入侵竊取資料，則可突破實體隔離的障礙。這些都是近期大陸網軍的攻擊手法。

結論

曾有手機廣告以「科技始終來自於人性」作為推銷的手法，資訊安全也與此類似。唯有澈底執行資安規定，而非貪圖一時方便將隨身碟或 USB 器材插入電腦，同時避免公務家辦，才能落實實體防護，畢竟魔鬼就藏在細節中。（文摘自法務部調查局清流月刊 103 年 7 月號）

嘉義區監理所 關心您