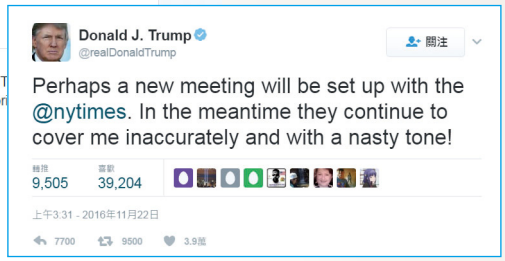
總統先生 別再 推特了！

■ 李書瑜

美國總統川普的推特首頁，目前已有 2,530 萬人進行關注。



川普總統於推特上直言媒體的不公報導。

最愛使用社群網站的總統

誰是世界上最愛使用社群網站的總統？美國總統川普肯定當之無愧。

川普對社群網站的成癮到什麼程度？根據紐約時報統計，川普自 2015 年 6 月準備參選總統到 2016 年 10 月間，共在推特（twitter）上發了約四千篇文，平均一天要發 7 ～ 8 篇，許多發文的時間甚至是在凌晨，其隨員更私下透露，川普連在如廁時都會把握時間發文。2017 年正式上任以後，依舊不改習性，每天持續在推特發文，且不忌諱的就重大政策表明心志，目前其推特帳號「@realDonaldTrump」追隨者已超過 2,500 萬人，讓白宮官方網站無用武之地，輿論更戲稱他為「推特總統」。

儘管多數政治人物也使用社群網站作為行銷工具，但一般普遍是將帳號委託競選團隊代為管理，如川普般親力親為者十分罕見。以本次美國總統大選兩陣營做分析，川普及希拉蕊在臉書（facebook）上的粉絲專業，分別有 1,300 萬及 900 萬名粉絲，在推特上的追隨者，川普仍以 1,400 萬名領先希拉蕊的 1,100 萬名。儘管就超前幅度而言，川普尚未到將希拉蕊拋諸腦後的地步，但若細看雙方在文章發出後的推文量，則可發現川普是希拉蕊的三倍之多。一般認為，川普的發文能夠引起共鳴，正是因為他直接跳入第一線與選民互動，而不像其他政治人物總是以冷冰冰的政治用語當作對推文的回應。

到選前的最後階段，有眼尖的網友發現，過去川普在發文時，底下顯示的都是「Twitter for Android」（川普使用的手機是安卓系統的三星「Galaxy」），但此時某些發文下頭顯示的卻變成「Twitter for iPhone」，當然這也許是川普交替使用兩支手機之故，但一位網路數據分析師大衛羅賓森（David Robinson）為了追根究柢，透過統計軟體分析川普的推特內容，結果發現標註「Twitter for iPhone」的發言，通常是在下午發的，內容較溫和，而標註「Twitter for Android」的發言，通常是在凌晨發的，內容常帶有情緒性字眼，且兩者的用字、標點、引用連結的習慣也不太一樣，顯然川普也開始將帳號交給其助理代管了。

什麼造成川普沉迷推特

川普幾近沉迷的愛用社群網站，可歸因於主流媒體對他的不友善。在本次選舉中，美國主流媒體普遍看好希拉蕊能夠當選，加上川普在選戰中經常有脫序演出，因此對於他的報導以負面新聞居多，甚至不斷對其私生活進行爆料，因此川普曾總結道：「不是我愛用推特，而是美國記者不誠實。」

無法透過主流媒體發聲，使得川普必須以不對稱的手法，為自己另闢發聲管道，而美國人普遍有在使用的社群網站，自然就成了川普的首選。川普在推特中，經常批評媒體的報導不準確，他尤其厭惡紐約時報及美國有線電視新聞網，還曾在推特上寫道：「它們一貫以不準確及讓人討厭的語氣報導我！」（In the meantime they continue to cover me inaccurately and with a nasty tone!）

在當選總統後，川普邀集了美國各大媒體的主管及當家主播到川普大廈閒聊，儘管對話內容並未對外公布，但據消息透露，川普在言談中，直接向在場人士表明，本次選舉中各家媒體的報導失衡，從此刻開始，希望各大媒體能夠克盡客觀公正報導的社會責任。

各界對川普使用推特的反應

對於川普使用推特的行為，美國社會普遍是持反對意見的。奎尼匹克大學（Quinnipiac University）對此曾做過民調，結果顯示，有 59% 的受訪者認為作為總統，應關閉個人的推特帳號，只有 33% 的受訪者支持繼續使用。前總統歐巴馬更曾直言：「如果有人連推特帳號都管不好了，我怎麼放心將核彈發射密碼交給他？」對於這些批評，川普僅回應，就任後將「克制」使用這些社群媒體。

多數人認為總統不應使用社群網站的原因，主要是基於資安考量。在本次選舉中，原本各方看好的是希拉蕊，但最後因媒體及 FBI 緊咬她在擔任國務卿期間以私人電子信箱收發公務電子郵件的「電郵門案」，使得希拉蕊終與總統大位失之交臂，由此亦可看出美國民眾對於領導人是否具有足夠的機密保護意識是相當重視的，如果因為此案否定了希拉蕊，自然也不樂見當選者再發生資安上的顧慮。美國總統的行程多屬機密，僅提前對白宮記者發放，如果日後川普隨時將當天活動公布於推特，容易遭恐怖分子鎖定，增加了維安特勤的困難度。

其實川普並非美國首次面對此問題的總統，歐巴馬在 2008 年當選總統時，也曾面臨類似的困擾。根據美國的規定，總統的所有通話都要列入紀錄，因此不能擁有私人手機，2008 年正值智慧型手機開始普及，歐巴馬是黑莓機（Blackberry）的愛用者，但國安單位擔心手機中內建的定位裝置將使總統行蹤曝光，堅決反對歐巴馬繼續使用，無奈這已是抵擋不住的時代潮流，最後歐巴馬與國安單位達成在白宮內有限使用的妥協，成為美國首位隨身攜帶私人手機的總統。

川普入住白宮後，對於國安單位的要求，勢必將採較前人更強硬的立場，美國總統如何使用手機、在社群網站上發文的範圍將擴大到什麼程度、是否可能造成機密保護問題及安全防護困擾等，值得後續關注。

（作者曾任職於警備總司令部）

網路攻擊的基本分類

■ 銘傳大學國際事務與外交學位學程系所兼任助理教授　林穎佑

追蹤網路攻擊一直是資安人員最大的難處，特別是在技術上仍難以突破，因此資安人員開始藉由受害者的類型來做出簡單的區分，期望藉此強化資訊安全。

Mobile devices

網路間諜（Cyber Espionage, CE）

當前資安界大多將涉及國家安全的網路竊盜事件，皆以網路間諜（CE）為分類的代號。

對國家級網軍而言，利益並不是其關注的目標，其可以不惜任何成本代價只為了得到具有戰略價值的情報。而其選取的目標也不會是具有商業價值的銀行或是一般公司企業，而是會以政府單位、關鍵基礎設施、軍火公司、重要智庫研究單位為攻擊目標。當然這些單位理論上都會有一定的資訊安全防護措施。因此對網軍而言，會為了竊取情報長期潛伏在上述單位之中，等待適當機會進行網路攻擊。甚至從組織外圍（外包商）進行滲透，只為了最終能夠得到情報。

如 2011 年，美國航太公司洛克希德馬丁（Lockheed Martin）所研製的 F-35 戰機數據資料遭網軍竊取。其攻擊的流程，便是先以洛馬所採用的動態密碼供應商 RSA 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。類似的攻擊手法也出現在許多國安相關產業中，如能源產業、航太公司、甚至國防安全的相關學術機構等也都是網路間諜覬覦的目標。

網路戰（Cyber-Warfare, CW）

有別於國家網軍所發動的間諜行為，國家級網軍從單純的竊取情資，升級成主動對政府或是媒體、企業進行大規模網路

攻擊，期望藉此干擾該單位的網路系統。類似的案例並不是首次出現，早從 2007 年俄羅斯對愛沙尼亞發動網路攻擊開始，類似的案例便層出不窮，早期可能只是單純置換官網首頁、更換領導人照片等騷擾行為，其宣示意義大於實際破壞。但隨著人類對於科技的依賴加深，網路攻擊開始透過所謂的分散式阻斷服務攻擊（Distributed Denial of Service attack，以下簡稱 DDoS）攻擊癱瘓目標的網路伺服器，使其失去作用。類似的攻擊手法經常出現於針對某國家政府單位的攻擊，以及一些立場相異的媒體。如 2014 年，對中國態度一向較不友善的蘋果日報，就遭到了國家級網軍有系統的攻擊，並且利用 DNS 反射與散布在各地的殭屍網路，同時發起大量的訊號，嘗試癱瘓該媒體的網路功能。

此外，隨著關鍵基礎設施防護觀念的興起，人們對於許多重要設施的依賴程度日益上升，而這些系統也多半利用資訊化管理，因此若是有心人士透過資訊滲透的方式，進入關鍵基礎設施資訊系統中，適當的時機發出錯誤的訊息，或是藉機破壞資訊系統，使其失去效能，其所衍生出來的國安問題不亞於戰爭。如美國與以色列聯手開發的震網病毒（Stuxnet），便是針對伊朗核電廠的電腦系統所特別量身打造的惡意程式。先入侵工程師的家用電腦，再透過可攜帶式電腦裝置，進入機密的電腦系統，藉由干擾控制器的方式，讓核子離心機的轉速過快出現故障，成功地拖延伊朗在核子武器上的研發速度，日後的火焰病毒也有類似的模式。

從上述案例中，我們都可以發現國家級網軍的行為，已超脫過去單純的竊取資訊，其造成的影響已經從虛擬走向現實，透過網路攻擊是可以直接對國家安全造成直接的影響。這也是美國開始將網路攻擊視為戰爭行為的主要原因。

網路犯罪（Cyber Crime, CE）

相對於國家級網軍造成的損害，網路犯罪集團雖然不會將關鍵基礎設施列為攻擊目標，但其所衍生的國安問題以及造成的經濟損失，亦隨著資訊科技的進步而日益擴大。

對這些網路犯罪集團來說，如何獲取最大的利益會是關鍵，因此在目標選擇上，會以保存大量個資以及金融交易紀錄的組

織單位為主，如銀行、戶政事務單位、保險公司、或是經由第三方支付的線上交易平台，都是犯罪機團所覬覦的目標。如美國知名連鎖零售商 Target 便在 2013 年遭到黑帽駭客入侵其 POS 刷卡終端系統，竊取顧客資料、信用卡簽帳卡號碼、到期日與驗證碼，影響一億多名客戶權益，也導致其公司執行長引咎辭職，其公司的商譽也受到嚴重的影響。雖然在各國政府的強力要求之下，許多金融單位都開始使用雙認證或是其他保護措施來加強對消費者的資安保障，但道高一尺、魔高一丈，網路犯罪的技術仍然持續精進，並利用人性的弱點以社交工程做為掩護，令有關單位防不勝防。

而近年又出現勒索軟體（Ransomware）將資料加密要求使用者透過線上比特幣支付。近年受害者增加許多，讓勒索軟體都有中文版或是支付教學的說明，甚至出現所謂的早鳥票可以打折，這都代表其所帶來的暴利相當可觀。

網路激進主義（Hacktivism）

有別於網路犯罪以及國家組織的網軍，近年來在網路世界中也出現了一群特殊的駭客團體，其所做出的滲透和攻擊與利益並無關係，甚至會為了理念而去對特定政府組織網站進行攻擊，但他們並無受到任何政府的授意，完全是自發性的採取行動。

著名的網路駭客激進團體：匿名者（Anonymous）便擁有相當高知名度，其為網路上的一個虛擬組織，只要認同其理念歡迎任何人參與其行動。雖然其最終目的標榜是為了維護網際網路自由，但隨著其名氣與實力增長，其對抗的目標除了權威政府之外（北韓、中國），也在維護正義的名目之下對參與戀童與人口販運有關的網站展開攻擊，甚至直接對 ISIS 恐怖組織宣戰，這都是其近期知名活動。雖然上述行為可能都有違法的嫌疑，匿名者團體認為身為駭客，自然要為其所做的事負責，這些行為雖可能觸法，但絕對經得起道德的考驗。

經由以上的探討，可以瞭解雖然使用網路進行的惡意攻擊手法有相同之處，但是背後動機以及組織的型態有相當大的差異。經過追蹤以及攻擊特性的分析之後，經常可以發現，許多的網路攻擊與網軍的關係並不大，反而是企業自身的資安防護的疏失，而讓資訊犯罪者有機可乘。因此，對於名詞的使用與精確的定義是有其必要，且越瞭解自身的威脅才有助增進風險分析並擬定正確的資安策略。