熱點聚焦

從威脅演進看數位國土安全

Digital Homeland Security in the Era of Evolving Threats

林穎佑

中正大學戰略暨國際事務研究所

壹、前言

隨著資訊科技的應用逐漸深入人類生活，在享受科技所帶來的便利之時，資訊安全的議題也逐漸受到重視。雖然一開始所重視的議題大多只集中在密碼學與技術攻防的科技層面，但隨著行政作業電子化與資訊系統的運用，有心人士也開始利用這些資訊漏洞來達成其目的。雖說如此，但早期來自網路的資安威脅，大多都是駭客的個人行為，駭客只是單純地想炫耀技術或是藉由系統漏洞來獲得自身的利益，其危害有限。但隨著電子商務的興起，個人資料開始成為黑市的搶手貨；文書處理電子化，讓許多資料都可以輕易以數據資料的方式存取，自然也增加竊取的便利。而隨著系統控制的資訊化，國家關鍵基礎設施（Critical Infrastructure Protection,. CIP）也成為有心份子或國家網軍覬覦的目標。這也代表資安威脅開始從軟體走向硬體，從竊取虛擬空間資料走向實體破壞的直接損傷，直接對人類安全造成影響。而隨著網路社交平台與通訊軟體的普及，資訊快速傳播的背後所帶來的是不實訊息（disinformation）所帶來的騷動。雖說不實訊息的宣傳戰在歷史上層出不窮，早在二戰與冷戰

時就有透過廣播與各項媒體來進行宣傳輿論作戰的案例，但上述的模式經常流於大眾傳播，無法在受眾上進行「精確打擊」。

隨著資訊科技的進步，數位時代的輿論戰又讓訊息傳播的速度與影響性更為擴大，也讓資安威脅又進化到新的階段，不只從虛擬走向實體，更開始影響群眾的認知，甚至會開始結合實際的軍事行動來做到「奇正相間、虛實結合」的威懾行動。如：2014 年俄羅斯在烏克蘭所發動的混合戰就是最好的案例。

從上述資訊威脅的演進發展中可以發現，資安威脅除了隨著科技進步變化之外，也與社會對於資訊產品的高依賴度有關。這些都讓過去強調的國家安全產生了新的威脅來源，雖然在非傳統安全的研究領域中，已有開始強調網路威脅，但科技日新月異的變化，讓來自數位的威脅更為多元，甚至在形式上也難以使用單一的概念與定義來規範，這也與網路生態固有的特性有關，資安威脅存在於虛擬的網路空間中，同時具有超地緣、快速傳播的特性，且再配合技術與新科技的應用（如 VPN、遭到控制的殭屍電腦），都讓追蹤攻擊與防禦網攻存在一定的難度。

貳、資安威脅的演進與分類

過去的資訊安全議題，大多僅單純的討論資料遭竊取外洩的問題，而在大多國家中，這原本就是情報單位的任務，只是從過去的敵後特務行動、電子訊號收集監聽、公開資料收集加入網路入侵此一途徑。此種轉變也導致各國最初的網軍單位大多都與情報單位有互動。但隨著科技的進步，各國發現可以利用網路造成系統的崩壞或是癱瘓社會的運作，如伊朗核電廠遭到美國與以色列開發的震網

病毒（Stuxnet）攻擊、[1]烏克蘭大停電都是典型的例子。[2]而之後也發現透過網路宣傳的影響，比過往的文宣與傳統媒體，更能深入群眾與目標市場，雖說謠言止於智者，但在網路水軍的推波助瀾以及有心人士「帶風向」的影響之下，依然能達成激化矛盾、強化對立甚至造成人民對政府的不信任。這些網路科技的新應用都讓國家安全威脅更為多元也更難因應。

有鑒於網路空間的特殊性，因此在分析資安與國家安全的關係時，並不完全適用過往的模式，而是需要配合資訊科技的特色來進行分析。因此一般會考慮從手法與可能的來源來進行比對分析，如先從入侵的紀錄檔與技術手法來分析其目的，再從可能竊取的內容或所造成的影響來對資安攻擊加以分析。

從攻擊的方式來看，可以簡單從網路攻擊的發展來作討論：[3]最早只是單純的置換官方網頁或是藉由電腦病毒癱瘓系統的運作，其騷擾與宣示國家網路能力的意義大於實際效益。而在資訊科技的普及應用下，有心人士開始注意到可以透過網路途徑來入侵系統取得情資，因此開始網路情報戰的年代。但在入侵時，如何取得對手信任的關鍵經常不是惡意程式撰寫的優劣，而是在信件的內容是否合乎邏輯以及內文用語是否會露出馬腳，這也導致網路攻擊開始更為精緻，針對特別選定目標進行「魚叉式攻擊」（Spear Phishing）。在策畫攻擊前，會針對目標的個人喜好、交友關係、最近研究甚至是

[1] 關於震網病毒，可參閱：Kim Zetter 著，李雲凡譯，《震網病毒解密》（Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon）（北京：國防大學出版社，2016 年）。
[2] 劉作仁，〈網路入侵案例解析以烏克蘭大停電事件為例〉，《安華聯網科技》，2016 年 12 月 12 日；http://www.ipv6.org.tw/summit2016/presentation/20161212/4-2.pdf
[3] 關於網路攻擊的案例與發展歷史，可參考: Bruce Middleton, *A History of Cyber Security Attacks* (UK: Taylor& Francis Group, 2017).

使用的資訊系統，量身打造網攻策略，此種針對目標結合情報社交工程的網路攻擊，一般稱為 APT 攻擊(進階持續性滲透攻擊 Advanced Persistent Threat，主要透過社交工程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）。[4]

倘若從攻擊者的目的來看，大致可概括分為：[5]網路間諜（Cyber Espionage, CE）、網路戰（Cyber-Warfare, CW）、網路犯罪（Cyber Crime, CE）、網路激進主義（Hacktivism）。[6]普遍而言，所謂網路間諜是透過網路作為竊取情報的媒介，主要目標多為政府組織、國防工業、研究智庫，攻擊目的是為了取得情資，大多針對特定人士進行 APT 攻擊。網路戰定義較廣，除純粹透過技術攻擊關鍵基礎設施之外，透過 DDoS（分散式阻斷服務攻擊 Distributed Denial of Service Attack, DDoS）[7]來癱瘓網站運作，甚至近年利用大量不實訊息企圖影響目標國的選情或是製造內部矛盾都可列於網路戰的範疇。上述這些攻擊都與國家網軍有關，畢竟對於唯利是圖的網路犯罪者來說，癱瘓維持社會運作的關鍵基礎設施並無利益可言，而部份涉及國安的情報在黑市中除非有政府單位授意，不然經常呈現有「有行無市」的狀況。且此類情報的交易由於過於敏感，特別容易引起國安單位的追蹤，因此一般的黑帽駭客除非與其他政府的合作，不然不會輕易對政府機關下手。

---

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

[5] 請參考此網站〈http://hackmageddon.com/〉，其中收集當前世界重要的網路資安事件，並對其做出明確的定義與追蹤。

[6] 關於各攻擊的深入分析請參閱：林穎佑，〈必也正名乎：從國安角度論網軍〉，發表於「淡江戰略學派年會暨第十一屆紀念鈕先鍾老師戰略國際研討會」（台北：淡江大學戰略所，2015 年 5 月 30 日）。

[7] 關於 DDoS 又稱為分散式阻斷攻擊。請參考：洪海、曹志華、鮑旭華，《DDoS 分散式阻斷服務攻擊深度解析》（台北：碁峰出版社，2014 年）。

而對網路犯罪者而言，其憑藉的是利用其卓越的技術從事不法勾當來換取利益，故其目標多為擁有個人資料的商家、銀行。但隨著資訊科技的進步，勒索軟體與透過殭屍網路控制肉雞的數位貨幣挖礦，也逐漸成為網路犯罪的新主流。電子商務所衍生出來的龐大利益，成為黑帽駭客進行網路攻擊的最佳動機，龐大的跨國「黑色產業鏈」，除造成經濟的損失之外，也嚴重破壞社會秩序。[8]

網路激進主義的成員較為複雜，與和國家有關連的網軍以及利益導向的黑帽駭客不同，其會為了「自認為的真理」而針對特定目標（有可能是政府、財團、犯罪團體、恐怖組織）進行網路攻擊、癱瘓系統或是分享其所竊取的機密。[9]理論上，這些團體都以身為團體的一分子為榮，自認為網路世界中的俠客，也多次號召全球網民參與其行動。雖說其曾經主動打擊恐怖份子，但不受控制的行為也成為各方擔心的不定時炸彈。

從上述的模式中可以發現到網路攻擊開始從虛擬的網路空間演進到現實社會的實體攻擊。一旦有心人士從網路癱瘓關鍵基礎設施，便會對社會運作產生立即的影響。但隨著通訊軟體的廣泛應用與社會對於網路新媒體的依賴，透過網路發布的不實訊息，又是國家安全的新挑戰。

參、網路威脅的新發展：數位輿論戰

雖然早在二戰時期就有不實訊息的應用，但受限於當時的媒體技術，受眾有限且無法針對特定的「目標市場」進行宣傳，同時宣

[8] 騰訊安全聯合實驗室，〈2018 上半年互聯網黑產研究報告〉，《騰訊電腦管家》，2018 年 7 月 27 日；https://guanjia.qq.com/news/n1/2382.html

[9] 最具代表的類似團體為匿名者（Anonymous）。關於該組織，可參閱：Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York: Back Bay Books, 2013).

傳的手法極易追蹤，這些都是過去應用不實訊息的限制。但隨資訊科技進步，網路的匿名性、複製性、快速分享都成為宣傳不實訊息的最佳助力。這些攻擊也會根據不同群眾的特性來進行規劃，因此再發動不實訊息攻勢前，需配合資訊科技進行全面的資料收集，並配合大數據分析來對目標進行細部的分析，針對不同的受眾（年齡、地區、政治偏好）設計不同的訊息內容。如 PTT（BBS 站）、Facebook、LINE、Instagram 各自有不同的使用年齡層，自然有不同的作為，如 PTT 需要文字配合看似親身體驗的感受文、Facebook 與 LINE 在考慮到使用者的習慣後，需要修改圖片配合簡單的文字來達到效果。

此種攻擊目標多為民主自由國家，其對言論自由的開放，竟成為有心人士利用的名義，藉由言論自由的保護與商業資本主義的方式，將主流媒體或是網路媒體都逐漸納入其控制，成為宣傳不實訊息的工具。如俄羅斯在 2016 年介入美國的選舉，便是經典案例。[10]雖說謠言不一定經得起時間的考驗，但若政府不能在短時間內作出反應，不實訊息已經在許多民眾心中留下深刻印象，或是已經對於選舉造成影響，便為時已晚，。這些都會造成民眾對政府的不信任，或是更為激化國內不同政治族群的對立，企圖達到破壞團結強化統戰的目的。

如同俄羅斯於 2014 年在克里米亞事件中所採用的混合戰，很有可能也會如法炮製出現在其他區域。[11]如在未來發生危機時，由內應出面組成親敵國的臨時政府，並宣佈接管軍隊與政府的指揮權，無論是否有效取得政治上的合法性，都能製造適當的混亂，甚至降低

[10] 楊中立，〈美國灰熊大草原事件之解析與啟示〉，《戰略安全研析》，第 146 期（2017 年），頁 55-65。

[11] 關於俄羅斯在克里米亞混合戰可參閱：倪一峯，〈俄國對克里米亞混合戰的運用：兼論對我國之啟示〉，《國防雜誌》，第 33 卷第 4 期（2018），頁 45-64。

該國的抗敵意志。另再配合特定媒體的配合，對內宣傳新政府已接管政權，瓦解抵抗意識，對外宣稱我國正當政府已經投降，降低他國介入的意願。在各種媒體的傳播方式可能都已經在網路攻擊下無法維持正常運作，只剩下部分具有特定立場的媒體持續播送下，極有可能利用傳媒贏得這場戰爭。中國在 2014 年提出的制腦權，便是針對數位時代的媒體宣傳戰，作出全新的詮釋。[12]

肆、代結語：數位國土安全

在國家安全的演進歷程中，最早是從單純的軍事安全著手，確保國家安全就是抵抗外來的軍事攻擊，之後隨著威脅的變化，政治、經濟、軍事、心理成為分析國家安全的基本架構。冷戰的結束，也出現非傳統安全的議題，2001 年的九一一恐怖攻擊更是帶出國土安全的概念。而在 2005 年的卡崔納風災後，證明天災的發生無可避免只能面對且做好危機管理，並透過強化關鍵基礎設施防護，讓其在面對災害時依然能維持運作，確保社會基本運行。

但隨著資訊科技應用，各關鍵基礎設施都會應用資訊系統，以及社會對資訊科技的依賴日益增加，來自網路空間的攻擊已經可以破壞社會安定，威脅國土安全，這也讓國土安全領域更為廣闊，數位國土安全此一名詞也正式出現。當然數位國土並無實際的疆域範圍，其包含硬體裝備與軟體系統，更包含所儲存的數位資料，甚至透過網路平台所散發的訊息都會是數位國土安全的一環。因此，未來在資安領域的研究，會更需要以多元的角度進行科際整合，除了純技術的研究之外，情報研析的觀點、傳播學的應用與行銷學中的

[12] 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）。

公關處理可能都會是建構數位國土安全研究中的重要環節。畢竟當前的網路攻擊已為跨越虛擬、實體、心理的綜合安全威脅，這也代表未來的資安管理不會只有資訊相關部門的責任，而是必須以更為全面的視野來思考資安戰略，才能制敵機先確保資訊安全，貫徹資安即國安的理念。