全球政治評論　*Review of Global Politics*

第六十期（2017）No.60 頁 127-132

書評

網路的安全與戰爭，每個人必須瞭解的真相

Cybersecurity and cyberwar: what everyone needs to know

黃 鈴 *Ling Huang*
中興大學國際政治研究所博士生
Doctoral Student of Graduate Institute of International Politics
National Chung Hsing University

身處在一個所有事物均與網路相關的世界裡(all this cyber stuff)，每個人須瞭解的真相究竟為何？

本書作者 P.W.辛格(P.W. Singer)及艾倫、弗里德曼(Allan Friedman) (以下本文簡稱作者)[1]，兩位來自美國布魯金斯學會(Brooking Institution)的資深研究員，秉持在網路世界裡，「每個人都需要知道」的這一核心理念，採用 FAQ(Frequently asked questions)常見問答的格式，透由大量軼事對網路安全的各種要素進行比對與解釋，呼籲所有人，不僅限於科研人員，舉凡從商業界、政治人事、軍人到媒體工作者等等，應對當前日漸依賴愈深的網路世界及有關網路安全問題，須更深入瞭解，以及注入更多的思考。

當作者決定採取此種(FAQ)的為本書撰寫的方法論時，首要工作為進行對問題的精準設定。作者試圖收集涵蓋網路領域的所有關鍵問題，經由

[1] P.W.辛格(P.W. Singer)，美國布魯金斯學會(Brooking Institution)資深研究員、二十一世紀防御計畫負責人；艾倫、弗里德曼(Allan Friedman)，美國布魯金斯學會治理研究部研究員、科技和創新研究中心主任。

赴圖書館「文獻綜述」到「線上期刊」及「微博」，以及布魯金斯基金會一系列講習、研討會，並與美國重要官員和專家進行會談，包括上至參謀長聯席會議主席等最高級別的美國軍官和國家安全局的局長等，下至低級別的系統管理員，從民選州長、內閣部長和首席執行官，到小企業主和年僅十幾歲的骸客，訪查對象範疇是全球性的，還包括來自中國的官員和專家（外交部長和解放軍將軍）等等，最後參觀現實世界中的網路關鍵設施和各種網路安全中心做為總結。從這一趟漫長的尋找與確定問題的旅程中，作者將有關網路問題歸納為三大類，亦即本書撰寫的脈絡。第一類問題為「網路是如何運行的?」，關於網路的基本輪廓和網路安全動態，描繪出網路世界的基本架構。第二類問題為「為什麼很重要？」，論述網路安全廣泛的影響。第三類為「我們能做什麼？」，歸納出前揭諸類問題的可能答案，作者依此基本結構，一一說明與解答。

一、網路是如何運行的?

當人人均已接受「網路即生活」此一模式時，作者試著以淺顯易懂的方式告知，有關網路發展歷程、網路威脅、網路安全定義、最脆弱環節為何等知識，以確認人們從瞭解經過整理後的網路背景知識，從而擴大對網路世界的關注程度。細數網路從 1969 年由美國加州大學洛杉磯分校研究人員試圖登錄史丹佛大學的一台電腦時，在輸入「log」前面兩個字母時，造成網路崩潰且登錄失敗，此為人類史上電腦對數據共享的開端，雖未成功，惟仍被視為開啟現代網路鼻祖(ARPANET)[2]先趨。從 1969 年迄今歷時 48 年，網路世界經過各個網路之間的串連、電子郵件開啟網路通信、網路商業化，以及域名系統(DNS)[3]權利爭奪戰，網路世界在私人企業及政府權

[2] ARPA(現在名為 DARPA，前面新增字母 D,意思為 defense), 此系統由美國國防部研發，開發目的係為使不同機構的人員能夠共享用電腦，其願景在建立共享的通信網路，共享電腦資源，每個機器可通過網絡資料處理器與實際網路連接，這種網路即為 ARPANET。

[3] DNS 為電腦連接的域名(便於人們記憶的名字)到其對應的 IP 位置(機器數據)所使用的協議為基礎設施，其特性為全球性及分散的。

力擺盪不斷加大，亦塑造出網路運行的獨特模式。

書中回顧 1997 年時任谷歌(Google)執行長 Eric Schmidt 於美國舊金山某記者會上表示:「網路是第一個這樣的東西:人類已經建立，卻完全不理解，是我們有過最大的『無政府』狀態的實驗」。所謂「無政府」狀態一詞，最為人們悉知係由國際關係現實主義學者主張，國際體系處於無政府狀態，意即沒有一個處於國家之上足以約束國家間互動的威權，即法律上國家平等，國家之間亦無權利號令另一國家之權力；而人們普遍對「無政府」狀態的認知則為，一種混亂(chaos)和無序(disorder)的狀態。因此，Eric Schmidt 點出網路世界運作發展的幾個重要因素，包括秩序、主權、安全、威嚇及信任等等。

二、重要性

作者以網路世界發生各式各樣的威脅與攻擊為例，提醒網路安全防護的重要性。而「所有與網絡相關的事物」的數據亦證明以下驚人事實，包括 97%的財富 500 強企業曾被骸客攻擊（餘 3%可能也已被攻擊，只是未發覺）；一百多個國家政府已進行網路戰爭備戰。網路從匿名攻擊至駭客入侵，對個人及國家間已能造成物理性的傷害與損失，網路攻擊從虛擬走向現實。美國前總統奧巴馬宣布：「網路安全風險造成了 21 世紀最嚴重的經濟和國家安全挑戰」，包括英國及中國等國亦不斷重申相同的觀點。

以著名的 2010 年「震網」病毒事件為例，從初期為視為是來路不明的網路蠕蟲病毒，經由一位默默無名的德國研究員奮力不懈的追查，始暴露驚人的真相。原來「震網」病毒係由美國及以色列情報機構合作的項目「奧林匹克運動會」，經由病毒滲透伊朗科學家的電腦，並巧妙地隱瞞攻擊的過程，使伊朗核科學家誤認為遭遇硬體故障的問題，進而破壞伊朗的核設施。「震網」病毒事件反映出，網路武器已開始使用於現實事件，而其運用的道德標準、與傳統武器差異等特性，促使政府與人們思考所謂「戰爭」

中，傳統的弱者與強者、進攻與攻擊等要素，已不具有絕對性的優勢，而網路所造成的威脅亦無所不在，事實證明，已有駭客攻擊具連網功能的智慧型馬桶。

三、我們能做什麼?

作者強調，「人」的因素是網路世界最脆弱的一環。2008 年，一名美軍士兵經過中東地區美軍基地外的停車場，發現一包未開封糖果，他決定帶回基地當午餐。這聽起來荒唐甚至有點噁心的行為，但是用 USB 隨身碟取代故事中的糖果，就是開啟洋基鹿彈(Buckshot Yankee)行動的故事。美軍士兵隨地拾回外國情報機關蓄意置放的隨身碟，並將其插入美軍中央司令部的電腦，內載名為「agent.btz」的蠕蟲病毒，事後造成五角大廈花費 14 個月去清理蠕蟲病毒，而起因來自一位士兵的網路安全常識的嚴重缺乏。

縱然網路世界中存在許多高深莫測的威嚇，惟許多攻擊仍是有效利用老派的人為錯誤，例如某 IT 公司的總經理在男子浴室裡發現存有惡意軟體的 CD，好奇的放入電腦，看看裡面有什麼?(想一想:你會拿起在小便池旁邊發現的梳子或是三明治嗎?)或是某網路防禦公司的員工以工作網路分享音樂，除在分享有版權的搖滾歌曲，也無意間與伊朗駭客共享關於美國總統直升機的電子零件設計。隨著與「網路事物」相關安全風險提高，影響層面包括個人隱私、網路的未來及潛在的區域威脅乃至引發全球大戰，作者建議讀者應培養看待及應對這些風險的能力，秉持正確的概念避免做出錯誤的決策，而非僅著重未來世界的變化。

「我們還能作些什麼?」通過本書作者告知的網路世界真相，其實身處的網路世界並非真的恐怖又糟糕，僅是被多數的網路事件報告描述得非常危險，然亦非一個絕對安全的領域。其中一個關鍵的因素是，人們並未對此類事件進行「風險評估」，多數網路犯罪受害者對網路中的風險一無所知。而對網路風險與威嚇的正確認識，可幫助人們理解學習網路安全知識

和保護自己的重要性。理解風險，並進行管理，加上調整對網路安全的態度，至少定期更新密碼，使用高強度複雜密碼，不輕易點開來路不明的電子郵件，以手機或電話再次確認與驗證，留意無線網路的加密方案是否仍安全，並隨時另備份重要的訊息，這些舉動雖不代表能全面阻止網路的威脅，惟突顯出我們致力於尋找更好方案的決心，從而保護自己與網路這個已不能分割的整體。最後，「對待電腦，別表現得太於愚蠢」！

責任編輯：郭佩儒