全球政治評論　*Review of Global Politics*

第七十七期（2022）No.77 頁 19-24

焦點評析

數位時代的新國家安全觀

Approach To New National Security in Digital Generation

林穎佑 *Ying Yu Lin*
國立中山大學亞太事務英語碩士學位學程兼任助理教授
Adjunct Assistant Professor of International Master Program in Asia-Pacific Affairs
National Sun Yat-sen University

一、前言

過去在管理領域中曾有提及 1970 年代企業追求的是成本、1980 年代是品質、1990 年代是速度、2000 年後則是創新、2010 年追求的是數位、2020 年則是 AI。這也說明了自 1990 年網際網路出現之後，對於商業模式的改變，數位科技的應用會是一大革命性的改變。除了因電子商務的蓬勃發展而出現的不法交易之外，當數位科技的應用已成為生活一部分，萬物皆可聯網是否也意涵萬物皆可駭？2017 年國蔡英文總統上台後，不但將資安列為三大國防產業，更多次提到「資安即國安」的戰略概念，[1] 國家安全會議更在 2018 年 9 月正式頒布我國第一份資通安全戰略報告。報告中指出在便利的通訊環境之下，我國成為是許多資安威脅和惡意程式的練兵場。[2]

---

[1] 李德財，〈「資安即國安」政策推動進度報告〉，發表於「2018 台灣資訊安全大會」研討會（台北：IThome，2018 年 3 月 14 日）。

[2] 國家安全會議、國家資通安全辦公室，〈國家資通安全戰略報告：資安即國安〉，2018 年 9 月 14 日，
https://www.president.gov.tw/Page/317/969/%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E6%88%B0%E7%95%A5%E5%A0%B1%E5%91%8A-

固然資訊安全的議題並不是首次出現在國家安全的討論範疇中，過去在討論非傳統安全時，已有不少學者提到網路犯罪、駭客攻擊所造成的威脅，甚至在中國大陸所出版的《超限戰》中也有提及網路在作戰上的運用，[3] 都能證明其並非近期才出現的論點。雖說如此，但數位科技的應用無論是在傳輸數據的流量、穿戴裝置的便利、關鍵基礎設施（Critical Infrastructure, CI）在操控上的應用都讓民眾對數位科技更加依賴，也因電子商務龐大商機而衍生出有心人士的覬覦。除了黑帽駭客入侵系統竊取資訊之外，各國情報機關也開始利用網際網路做為情報蒐集的管道，甚至開始將網路作為攻擊的媒介，藉由癱瘓、破壞目標的關鍵基礎設施，達到攻擊對手的目的。此外，網路攻擊超越了地緣戰略的限制，且能透過科技的手法達到匿蹤的效果。這都讓資安戰略與過去傳統戰略有相當大的差異。而隨著數位金融的興起，個人資料的保護問題與數位貨幣的出現，都讓數位經濟走向另一個新里程碑。但也因數位科技的進步速度過快，相關的管理法規不一定能配合，也產生了不少灰色地帶問題，甚至出現新的犯罪手法。

二、新時代的網路攻擊

有別於過去單純透過網路進行的騷擾（如置換首頁網站癱瘓的手法）與竊取資訊，隨著物聯網科技的應用，只要能上網的設備都有可能成為攻擊的目標。特別是在關鍵基礎設施與重要的金融體系系統中，若造到網軍或是有心人士的攻擊，其對國家社會所造成的影響，不亞於傳統的軍事攻擊。特別在當前國際局勢之下，全球化供應鏈所形成的國際貿易體系，讓各國都不會輕啟戰端。特別是傳統的軍事攻擊都會限縮在有節制的威懾行動，以灰色戰略的形式運用於當前國際環境，對於國家的威脅主要來自於作戰空間與時間的壓縮，以及對民眾心理的衝擊，並無實質上的威脅。

%E8%B3%87%E5%AE%89%E5%8D%B3%E5%9C%8B%E5%AE%89-。

[3] 喬良、王湘穗，《超限戰》（北京：解放軍文藝出版社，1999 年），頁 37-39。

但自 2010 年美國與以色列合作的震網病毒癱瘓毀損伊朗核子設備開始之後，[4] 2013 年北韓對南韓發動的黑色首爾網路攻擊行動（北朝鮮網軍癱瘓了南韓部分金融系統），[5] 俄羅斯網軍對烏克蘭發電廠的癱瘓攻擊，這些針對各國關鍵基礎設施的攻擊，雖然沒有對軍事設施造成直接的破壞，但是對人民生活與配合謠言所造成的恐慌程度卻對人民產生直接的影響。這也代表在數位時代，此類看不見的網路戰爭所造成的影響可能高於傳統軍事，也是當前各國都會設立網路作戰單位，以及積極發展資安的主要原因。

隨著資訊科技的進步與新媒體的應用，當前的數位科技對於傳播媒介的刺激是有革命性的改變。社群媒體與通訊軟體的出現改變了受眾對於資訊取得的方式，而也因為這些改變，讓傳統媒體做出了極大的改變。自然也成為有心人士利用並成為攻擊與干涉他國的工具。如近期對我國產生相當影響的「認知戰」都是類似的概念。固然認知戰的概念早在第二次世界大戰時就有出現，無論是電台的廣播或是傳統的傳單海報都可算是認知戰的先驅；而在兩次波灣戰爭時，美軍也利用宣傳戰來達到弱化伊拉克部隊的目的，除傳單之外，更是結合電戰技術對伊拉克電台實施「蓋台」，其後中共解放軍總政治部也在 2003 年提出三戰（輿論戰、心理戰、法律戰）的概念，在原先統戰的基礎上再做出延伸，並加以理論化。近期在數位科技的加持之下，透過演算法與大數據分析更能對鎖定「受眾」目標，如同行銷學中所談到的目標市場（Target market），針對不同族群設計適合的觀點與其最能接受的言論，來進行認知作戰。這也與黑帽駭客與網軍在進行網路攻擊時經常運用的 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）[6] 類似。

---

[4] 秦安，〈震網升級版襲擊伊朗，網路毀癱離我們有多遠〉，《網絡空間安全》，第 9 卷第 11 期，2018 年 11 月，頁 41-43。

[5] 趨勢科技全球技術支援與研發中心，〈APT 攻擊南韓 DarkSeoul 大規模 APT 攻擊事件事件 FAQ〉，《趨勢科技》，2013 年 3 月 29 日，*http://tech.huanqiu.com/it/2015-01/5452665.html*。

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

有別於過去只出現在虛擬空間的資安問題，當前的網路威脅已經從看不見的虛擬空間延伸到實體環境，近期更是開始從軟體發展到心理認知的層面。認知戰是結合宣傳與科技的新作戰，其非無目標的宣傳更非單純的文宣，而是利用民眾對於科技的依賴，將訊息結合科技進行傳播。其目的自然是希望破壞目標國內民眾的團結，製造對當前政府的不信任感甚至期望藉此影響民主機制（如選舉）。面對此種威脅，更因議題管轄的部會不同以及在應對上有可能會侵犯到民主國家的言論自由與隱私問題，甚至在應對不實訊息時，因危機管理的應對失敗，反而陷入更複雜的公關危機。這都是在數位時代所遭遇的新威脅。

三、數位貨幣的新金融時代

除了前述來自網路的各種新領域攻擊之外，數位貨幣的興起也對傳統經濟造成了新的影響。無論是單純的第三方支付、行動載具的支付或是網路銀行的興起，都讓電子商務又出現新的刺激與變化，但伴隨而來的也是新的威脅並挑戰過去的國家安全觀。

加密貨幣與過去各國發行貨幣有極大的差別，其無具體的型態外也無編號，特別是其交易的過程相當特殊難以追蹤，自然成為犯罪集團洗錢或從事金融犯罪的絕佳媒介。如近期相當猖獗的網路勒索軟體，期將組織部門中的重要檔案加密後，要求受害者支付贖金才能給予解密的金鑰。有別於過去支付贖款的方式，透過加密貨幣可以讓這些網路犯罪集團輕易且安全的收到款項。勒索軟體雖然破壞有限，但若是運用得當亦能在重要時間癱瘓系統運作。而在龐大的地下經濟中又有高額的黑市暗網交易，自然會影響政府稅收與財政運作。固然加密貨幣可能會出現監管的問題，但當前不少國家開始承認加密貨幣並要求課稅，這雖然會讓不少持有者與交易者開始擔心，但也代表政府開始承認其地位。

事實上不應將加密貨幣視為洪水猛獸的威脅，相反在許多衍生性

金融商品上都開始有投資加密貨幣的相關產品或是相關的指數股票型基金（Exchange Traded Funds ,ETF），代表其成長的效益。而對許多無法立即兌換美元的國家而言，加密貨幣可讓其快速的在網際網路中進行全球交易，且在元宇宙、區塊鏈議題的延燒之下，數位資產與加密貨幣的討論勢必依然會持續。固然有不少觀察認為其泡沫化的可能性相當高，而加密貨幣的價格波動劇烈以及保存的資安問題，也是讓許多人裹足不前的原因。雖說如此，但加密貨幣的應用日益廣泛，當主權國家都開始討論時就代表其未來的機會。如美國聯準會在 2022 於一月所公布的報告《貨幣與支付：數位轉型時代的美元》(Money and Payments: The U.S. Dollar in the Age of Digital Transformation)，再次討論到了加密貨幣的優缺點與應用，此報告也代表加密貨幣融入美國的貨幣和支付領域。[7]

當前，美聯準會印發的紙鈔（即實體貨幣）是大眾唯一可獲得的中央銀行貨幣，未來若美國也開始發行央行數位貨幣（Central Bank Digital Currency, CBDC）憑藉美元的強勢，在過去可能其他國家可以利用開戶與匯兌的法規限制來保護國家法幣，讓許多想要大量持有美金的人只能實體保存而不能將其存入銀行。但若是隨著加密貨幣出現與區塊鏈技術的快速發展與普及化，央行數位貨幣不但和實體鈔票一樣可以跳過銀行，更因數位的特色讓民眾可以快速便利持有，當一國的強勢貨幣，能入侵弱勢政權的金融體系時，則代表其能搶佔目標國的「法幣市佔率」也等於入侵了該國的主權。[8] 而各國傳統的金融法

---

[7] The Federal Reserve, “Money and Payments: The U.S. Dollar in the Age of Digital Transformation,” January 20, 2022, *https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf?fbclid=IwAR2PTs3Xi7dAapMaKWIWPVURaHIbuboxRvXBrdsrLUGLQ3fGCqa-hQB6TNs* (2022/01/21).

[8] 何渝婷，〈XREX 創辦人黃耀文：CBDC 的關鍵意義，在於受歡迎的強勢法幣，會帶來國際政治間的新一輪競爭！〉，《奇摩新聞網》，2021 年 1 月 5 日，*https://tw.stock.yahoo.com/news/xrex%E5%89%B5%E8%BE%A6%E4%BA%BA%E9%BB%8*

規是否能跟上科技的步伐？ 都是未來在數位經濟時代中須注意的一環。

四、結語：科技始終來自於人性

國家安全的內涵相當多元，但在科技的進步之下，又經常會因為新科技應用產生新的刺激與威脅。這也代表當前的國安觀念須隨時代與時俱進，才能應變此動態的複雜環境。特別是在數位科技的進步下，許多新的領域的威脅都逐漸出現，但科技的背後還是由人來操作，這也代表組織部門、管理藝術、法規體制都依然會與科技應用產生新的互動。而在數位便利的背後是否也會出現新的威脅與危機？而國家是否亦能快速應變？都會是當前國家安全面對的新挑戰。

責任編輯：李欣樺

3%E8%80%80%E6%96%87-cbdc%E7%9A%84%E9%97%9C%E9%8D%B5%E6%84%8F%E7%BE%A9-%E5%9C%A8%E6%96%BC%E5%8F%97%E6%AD%A1%E8%BF%8E%E7%9A%84%E5%BC%B7%E5%8B%A2%E6%B3%95%E5%B9%A3-%E6%9C%83%E5%B8%B6%E4%BE%86%E5%9C%8B%E9%9A%9B%E6%94%BF%E6%B2%BB%E9%96%93%E7%9A%84%E6%96%B0-%E8%BC%AA%E7%AB%B6%E7%88%AD-025000512.html。