探討TikTok的資安威脅

●葉俊雄／前國家高速網路與計算中心主任

美國總統川普祭出兩道行政命令掐住中共的咽喉，震撼全球。第一道行政命令於8月6日簽署，美國政府將在四十五天後的9月20日，禁止美國企業和個人與中國「騰訊」及「字節跳動」兩家公司進行交易，以捍衛美國國家安全。8月14日發布的第二道行政命令要求「字節跳動」在九十天內拆售其下屬的抖音（TikTok）美國業務，且必須銷毀所有美國用戶的備份資料，並書面知會「美國外來投資審查委員會」（Committee on Foreign Investment in the United States，簡稱CFIUS）。

川普援引《國際緊急經濟權力法》（International Emergency Economic Powers Act，簡稱IEEPA）、《國家緊急法》和1974年《貿易法》第301條（Section 301 of the Trade Act of 1974）而頒布第一道行政命令，他指出「中國開發及擁有的行動應用程式，持續威脅美國國安、外交政策和經濟，包括自動蒐集用戶資訊，令中共政府有機會接觸美國公民個資，並進行要脅和滲透，以及審查中共認定的政治敏感內容，並持續監控赴美享受自由權利的中國民眾。」

第二道行政命令追溯至2017年11月，當字節跳動收購美國影音平台《Musical.ly》時，未申請CFIUS的批准。因而，CFIUS立即成立一個跨部會的審查委員會，對此交易案展開調查。此委員會已握有TikTok將使用者資料傳送至中國的證據，所以，全體委員一致建議川普引用《國防生產法》簽署此行政命令。

同時，美國國會也制定「政府設備禁用TikTok法案」，禁止政府機構、政府企業及國會的職員將字節跳動開發的軟體下載至公務設備上，但公務需要經核准後不受此限。

字節跳動為張一鳴於2012年在北京創立的。其開發的社群應用程式抖音讓使用者可以錄製15秒到1分鐘的短影片，也可透過對嘴、內建特效等功能編輯影片，並可針對影片留言。2016年推出後，甚受中國年輕族群歡迎。2017年8月推出中國之外的國際版TikTok，同年11月，收購「北美音樂短影音社群平台」《Musical.ly》，成功打入北美市場。此後，TikTok的使用者數量急劇增長，到2020年5月，全球下載數超過二十億次。目前，它有六萬多名員工，全球約有八億人使用抖音或TikTok，美國使用者約有一億人。它的營收大部分來自廣告、販售虛擬禮物和向直播主抽成。

字節跳動針對此兩道行政命令，一方面尋找買家，已有「微軟＋沃爾瑪」組合、甲

骨文等公司與其洽談。另一方面向法院提起訴訟，然而，第二道行政命令旨在要求出售TikTok在美業務，無需承受司法審查。此外，任職TikTok不到三個月的執行長於8月27日宣布辭職。

對於美國政府的指控，字節跳動極力否認，宣稱從未與中共政府共享使用者個資，也未應中共政府要求讓其審查內容。不過，中國的《反間諜法》及《國家情報法》明確要求中企必須配合中共政府的調查，且不得拒絕。也許有膽大的企業家會抗拒，但專制體制的中共政府就會慣常地祭出「莫須有」的低級伎倆刁難公司和下罪當事人，在此高壓力下，當事人可能會改變初衷。

字節跳動也宣稱其儲存美國用戶資料的主要數據中心位於美國弗吉尼亞州（Virginia），而備份數據中心在新加坡。這未能完全釋疑，例如，字節跳動也可在中國建置另一個「秘密」的數據中心，並將全球各地收集的資料「秘密」地送到此中心儲存。在資訊科技領域裡，有些分散式系統就採用三份相同資料並存的架構。

中共政府可能為了維護利益或顏面，立即更新「中國禁止出口限制出口技術目錄」，擴大技術出口限制，此包含TikTok使用到的人工智慧（AI）和電腦演算法等技術。這意味著字節跳動若出售TikTok的業務給「他國公司」，需要中共政府的批准。並且，在9月8日提出「全球數據安全倡議」，意圖以此反擊美國，保護TikTok。中共政府此時的介入有可能大幅增加TikTok出售案的複雜度，也加深惡化已經激烈對撞的美中關係。

有些國家響應美國封鎖TikTok的行動。印度早在6月就已禁用五十九款中國開發的應用軟體（含TikTok），並持續擴大審核範圍。日本多個地方政府宣布關閉TikTok官方帳號，有國會議員建議，為強化日本的經濟安全保障，政府要限制使用中國的應用軟體（含TikTok）。法國、荷蘭和歐盟也對TikTok的資安問題展開調查。

美國與印度之所以封鎖TikTok，最主要的原因就是個資保護，他們似乎已握有相關資訊，TikTok會把收集的資料傳到擺在中國境內的儲存設備。早在2015年9月，一家德國的資安公司就揭露，「中國製造的手機都被預裝間諜程式，竊聽通話、拍照、錄音、發送和閱讀簡訊等，用戶的一舉一動隨時都被監控。」2017年3月，印度政府也有類似的調查結果。

個人資料保護牽涉廣泛，是總體資訊安全與網界戰（cyber warfare）的一環，備受多數國家關注，並訂定相關法規，以保護個人、組織和國家的安全。歐盟（European Union）於2018年5月實施General Data Protection Regulation就是為了保護人民的個資。

TikTok的資安威脅大致可涵蓋下列數項。

一、收集個資：收集個資與探測設備及漏洞是資安攻擊的第一步。有資安公司指出，「TikTok曾繞過Google的隱私保護系統，蒐集數百萬用戶的裝置資訊。」當使用者

向某應用系統申請帳號時，通常會被要求提供一些個資（如姓名、手機號碼、電子郵箱），有些應用系統還會進一步要求更多個資（如住址、性別、照片）。這些個資若未嚴謹妥善地保護，而被黑帽駭客取得或洩露給某些特殊組織，就可針對某人做出「魚叉式網路釣魚」[1]攻擊，以騙取更重要的資料（如網路銀行、武器設計系統的帳號密碼）。

二、收集個人行為：有資安專家指出，「當TikTok應用程式初次安裝後，TikTok會以用戶無法拒絕的途徑，將裝置的MAC[2]位址與其他裝置數據綑綁，傳回字節跳動。」有了MAC位址，就有可能進而收集消費者行為（如地理位置、上何網站、與何人交往、搜尋什麼文件、政治和宗教觀點、健康狀態）。所以，行政命令提及，TikTok有可能讓中共政府追蹤美國聯邦政府的員工與包商，建立個人行為資料檔案，以便執行勒索和商業間諜的行動。

三、言論審查：美國參議院民主黨的調查報告《新的老大哥：中國和數位威權主義》指出，中共政府使用先進科技（如人工智慧、人臉識別）「監控網路和審查信息，不僅在中國境內靈活運用，更同時積極向海外輸出。」澳洲戰略政策研究所（ASPI）也發表類似的調查報告。也有媒體報導，TikTok配合中共政府，審查過濾有關香港反送中抗爭的影片，審查天安門、西藏獨立及法輪功等關鍵字，刪除批評中共政府的文章。TikTok掌握提供給用戶什麼內容的決定權，可以秘密地控制議題，使其居於影響全球政治行為的有力位置。

四、親中宣傳：TikTok掌握一億多美國人的注意力。字節跳動有可能居於愛國心或來自中共高官的強大壓力，透過TikTok協助中共從事大外宣、對年輕群體進行親中宣傳、散布不實訊息、塑造議題、帶領輿論風向、影響民主國家的選舉，進而控制媒體。

五、資安攻擊：有資安公司發現，TikTok存在嚴重的安全漏洞，駭客可以透過漏洞控制使用者的帳戶。當中國擁有大量美國民眾的資料時，就可以做大數據分析。從中，有可能得知某人的行事風格、生活習慣、嗜好、優缺點等，也可能知道某重要單位的規律、組織文化、安全破口等。依此，就可以進行細緻周詳的資安偵測和攻擊。如果在使用者的手機偷偷下載後門軟體或間諜程式，就可竊取更具敏感性的隱私（如信用卡資料、通訊錄、朋友圈、通話、簡訊、錄音、圖片）。這些都可用來竊取軍事機密、商業機密、先進科技、國際談判策略等極機密的資料，或者入侵總統候選人競選團隊和政治顧問的電腦，竊取競選策略的機密文件，以翻轉選情。

中國以廉價勞工、提供土地和稅務等優惠方式吸引諸多企業到中國建廠製造，當其經濟力量壯大後，姿態也大幅更動。中共政府享受民主國家自由開放的國際貿易，但却奉行保護主義，對中企提供補貼，對他國企業施加很多障礙，如封鎖谷歌、臉書（Facebook）、推特（Twitter）、YouTube等網站，以及禁用WhatsApp、Telegram、LINE。美國國務院還推文指出「中國官員可以投書到美國媒體，但美國官員的演講在中

國五分鐘就消失了。」

此外，中共政府自2010年實施強制性外交，針對「不遵循指示辦事」的國家或企業從事貿易制裁、投資限制、法律處罰、旅遊禁令和煽動民眾抵制等舉動。如果民主國家的政府和企業對中國市場的依賴度增強，強制性外交的力道也會增強，這將增加商業和安全的風險，嚴重影響國際政局與貿易的穩定。

中國為遂其世界超級強權的野心，一再採用不公平和不合國際規範的霸道措施，粗暴地霸凌他國，以壯大其實力。因而導致美國和其他多國的警惕及反擊，以致於封鎖那些威脅國安的中國製應用軟體。然而，這只是美國總體大戰略的一環，美國於8月發表「淨網計畫」（Clean Network program），其目標之一就是要清除「不受信任」的應用軟體與通訊企業，這還包括「乾淨5G」、海底電纜的保護、終止中國電信廠商在美國提供服務。美國也對使用美國製半導體設備的公司，訂下產品不得售於中國的規範。也嚴格審查中國派至美國的學者、研究員及留學生，尤其是從事先進科技研究者，以防止他們充當中共政府的間諜，偷取重要的尖端科技。

美國總體戰略旨在防範中共政府及中國公司以不正當手段操控美國市場和消費者，偷取寶貴資料，由此製造武器來攻擊美國，或散播假訊息和輿論，煽動人民的紛爭及分歧，造成社會對立和混亂，破壞穩定。美國副國務卿畢根（Stephen Biegun）說，美國與印度、澳洲和日本成立「四方安全對話」（Quad），就是為了共同抵禦中國的挑戰，遏阻其侵略性和破壞力。

【註釋】

1. 魚叉式網絡釣魚（spear-phishing）是網絡釣魚的一種。就一般性網絡釣魚而言，駭客擬定一封利誘或威脅的電子信，寄給一群收信者，信內有一連結。若點此連結，顯示器上會出現駭客特意設計的網站，此網站極為逼真地仿製某網站（如銀行或政府機構）。收信者若輸入帳號密碼以登入駭客網站，駭客就取得資料，再以此帳號密碼登入真正的網站，偷取金錢或機密資料，或以此為跳板攻擊其他更重要的系統。魚叉式網絡釣魚攻擊是駭客依據某人的詳細個資，客製化一封給此人的精緻電子信，此信有很高的「說服力」，以致於就「自然地」點下連結，而洩露機密資料。有研究指出，91%成功的資安攻擊始於網路釣魚，而魚叉式網絡釣魚成功的機會又更高。
2. MAC的全名為medium access control。於1980年，國際標準組織International Organization for Standardization出版了Open Systems Interconnection (OSI)的網路模型，OSI模型將網路服務分成七層，MAC為第二層資料連結層的子階層，負責將上層的資料送到實體的媒體（如光纖或電纜），以及接受來自媒體的資料。在國際網路標準組織的管控下，MAC位址是網路卡公司賦予網路卡的「身分證」，通常不會改變。它是由一組十二個十六進位數字所組成，全球惟一，不可重複，否則網路組件無法正確交換信息。◆