中國網路安全發展現狀與未來趨勢

曾敏禎

網路安全與決策推演研究所

壹、前言

中國自 2015 年通過《國家安全戰略綱要》與同年施行之《國家安全法》後，宣稱考量其整體國家安全，將加速推出諸多保障網路安全、有序發展的法律法規，冀從四面八方全面封堵網路領域存在的「漏洞和問題」。觀諸中國 2017 年公布的《網絡安全法》及 2021 年的《數據安全法》與《個人信息保護法》等法規，已構建出攸關數據和網路安全的三部基礎法律，然目前中國仍在網路上面臨網路輿論引發的政治威脅、各國駭客攻擊其各行業網路系統、龐大核心數據流出洩露風險。本文認為，上述問題反映出中國亟須解決包括加強網路秩序維穩、確保關鍵基礎設施和網路系統安全、保護網路資訊和數據安全等三方面，故中國持續在網路空間構建縝密合規的治理規範與機制，強化鞏固其網路安全利益對於國家安全至關重要。

貳、面臨問題

一、網路散布煽動言論威脅社會政治穩定

習近平自 2014 年出席「中央網絡安全和信息化領導小組第一次會議」首次提出「沒有網絡安全就沒有國家安全」，[1]此後便不斷在公開場合重覆強調此觀點，凸顯網路空間核心戰略利益是服從於中國總體安全與政權穩定，因此對中國而言，網路某種程度上沒有限制的表達及利用，造成大量資訊網路出現損害中國政權鞏固、政治

[1] 〈習近平的網絡觀：沒有網絡安全就沒有國家安全〉，《中國共產黨新聞網》，2014 年 10 月 20 日，http://cpc.people.com.cn/xuexi/BIG5/n/2014/1120/c385475-26061137.html。

制度穩定及各族人民群眾團結和諧輿論攻擊等，如自 2020 年 COVID-19 爆發蔓延以來，追蹤疫情的記者、具有專業知識的醫生與法律學者，加上網路評論者與網民們在網上發表有關散布新冠病毒的言論或分享，中國認為該類部分不實訊息破壞社會穩定的言行。另外利用網路策劃、組織與實施在香港各地動員，遊說民眾反對港版《國安法》，亦係針對中國領土完整和政權鞏固顛覆、分裂破壞和暴力恐怖襲擊。回顧 2022 年在中國各地掀起的白紙革命示威浪潮的參加人士，通過網路進行反政府、反社會活動，以及支持新疆地區穆斯林人權利，則係涉及煽動民族仇恨和恐怖主義網路活動，上述透由社群媒體傳播的網路言論已影響中國日常社會和政治穩定運行，進而屬於威脅其國家安全首要範疇。

二、境外勢力針對各行業網路系統發起網攻

中國國家安全機關指出自 2020 年以來，電信運營商、航空公司等單位內網和訊息系統先後多次出現無權限登錄、數據外傳等異常網路行為，而後發現部分骨幹網路節點設備、核心業務系統服務器等被植入特種木馬程式，已有部分數據被發送至境外。[2]據統計，2022 年中國重大網路攻擊事件涉及到各行各業，其中最主要攻擊針對三個行業，包括教育科研（西北工業大學指控美國國家安全局使用逾 40 種不同的網路武器對西北工業大學竊密）、[3]工業製造（中國電動汽車大廠蔚來遭駭客入侵竊取近 40 萬車主與 2.28 萬員工個資，被勒索 225 萬美元等值比特幣）、[4]醫療健康（北京「健康寶」APP 遭受境外網路攻擊，另澳門健康碼曾遭來自歐美地區網路攻擊達 300 多萬次）。[5]而 2022 年 6 月駭客以 10 枚比特幣（約新台幣 600 萬

[2] 〈國家安全機關公佈多起典型案例〉，《中國政府網》，2022 年 4 月 16 日，http://big5.www.gov.cn/gate/big5/www.gov.cn/xinwen/2022-04/16/content_5685561.htm。

[3] 〈西北工業大學遭網絡攻擊活動源自美國國家安全局〉，《央視網》，2022 年 9 月 5 日，https://news.cctv.com/2022/09/05/ARTIRpv9fAsIyfM6WrWukdzU220905.shtml。

[4] 〈蔚來信息洩漏被勒索 225 萬美元，汽車網絡安全值得關注〉，《第一財經》，2022 年 12 月 21 日，https://m.yicai.com/news/101629961.html。

[5] 〈繼北京健康寶後，澳門健康碼又遭境外勢力攻擊〉，《騰訊》，2022 年 11 月 14 日，

元）兜售上海公安系統數據庫，包括 10 億中國公民的戶籍等個資及數十億筆向警方報案的詳細摘要紀錄、[6] 2023 年 7 月武漢市應急管理局地震監測中心遭網攻，[7]凸顯中國政務單位的資安防漏洞更新疏失與治理監管不力。2022 年中國國家工業互聯網安全態勢感知與監測預警平臺累計監測發現各類網路攻擊 7,975.4 萬次，同比增長逾 23.9%，遭受網路攻擊企業累計超 1.8 萬家，同比增長 50.9%。從網路攻擊類型分析，2022 年以僵屍網路感染（41.1%）、非法外聯通信（20.5%）、木馬後門感染（15%）等為主，合計占網路攻擊總數的 76.6%，是當前工業互聯網網路面臨主要安全威脅。[8]

三、海量網路資訊和數據缺乏監管審查

鑑於網路海量的資訊和數據蘊藏最新科技、社會動態、市場變化、國家安全威脅徵兆、戰場態勢和軍事行動等重要情報，資訊與數據已作為「網路時代的石油」，成為未來社會生活、產業競爭、大國博弈最重要的戰略資源，故中國自 2021 年逐漸加大對掌握大量數據的網路平台企業管控力度，包括點名阿里巴巴、騰訊等中國網路科技巨頭濫用個資、[9]整改螞蟻集團、[10]施壓叫車 App 滴滴出行（DiDi）從美股退市，致健身應用 KEEP 、醫療數據公司零氪科技（LinkDoc Technology）、有聲課程分享平台「喜馬拉雅」等紛紛擱置赴美上市計畫，[11]亦凸顯中國監管整頓的力度。對中國而言，由於這些涉及到國計民生數據的平台，如「滴滴出行」掌握大量包括面

---

https://cloud.tencent.com/developer/article/2161976。

[6] 〈中國恐遭史上最大網攻 駭客稱兜售 10 億人個資及警方紀錄〉，《中央社》，2022 年 7 月 5 日，https://www.cna.com.tw/news/acn/202207050167.aspx。

[7] 〈是誰網攻武漢地震監測中心 北京官媒栽給美國〉，《中央社》，2023 年 8 月 14 日，https://www.cna.com.tw/news/acn/202308140090.aspx。

[8] 〈2022 年中國工業互聯網安全態勢報告〉，《工業互聯網產業聯盟》，2023 年 7 月 3 日，https://www.aii-alliance.org/index/c319/n4017.html。

[9] 〈阿里、騰訊把持個資數據 中消協：消費者淪平台巨頭「玩物」〉，《自由時報》，2021 年 1 月 7 日，https://ec.ltn.com.tw/article/breakingnews/3404694。

[10] 〈螞蟻集團遵從政府要求，全面整改業務〉，《華爾街日報中文版》，2021 年 4 月 14 日，https://reurl.cc/Y0721o。

[11] 〈滴滴效應發酵？傳中國健身軟體 Keep、課程平台喜馬拉雅皆取消在美 IPO 計畫〉，《數位時代》，2021 年 7 月 9 日，https://www.bnext.com.tw/article/63832/keep-usa-app-china-july。

部識別數據之用戶訊息、高度精確的地圖位置、道路交通流量數據，存在被境外勢力利用不可控風險，為防止海量數據跨境安全隱患，強化掌控「數據主權」與「數據出境流通」已成為其首要目標。

參、解決方法

一、升級掌控帳號信息監管網路言論

中國為遏止欲破壞中國穩定的不實言論發表、有害資訊散布，自 2015 年發布《互聯網用戶帳號名稱管理規定》按「後台實名，前台自願」原則，僅規定「用戶帳號名稱」，至 2022 年的《互聯網用戶帳號信息管理規定》，則將約束範圍由「帳號名稱」進一步擴大至「帳號信息」，修訂為全面納入用於標識用戶帳號的訊息（名稱、頭像、封面、簡介、簽名、認證訊息等），並公開網路「IP 屬地」。[12]接續公布的《互聯網跟帖評論服務管理規定》亦將控管網路發文擴展至跟帖評論。基此，凸顯為貫徹網路言論管制，除強化核驗個人帳號實名制，到帳號相關訊息等多層審查，且網路企業背負「事前審查」、「事中控制」和「事後監督」等全週期義務責任，平台問責將治理的觸角從「網路訊息服務提供者」、「跟帖評論服務提供者」延伸至「公眾帳號生產運營者」。

二、CII 防護成為保障國安核心

中國 2017 年生效的《網絡安全法》首次提及「關鍵資訊基礎設施」（Critical Information Infrastructure, CII），僅針對運營商在 CII 運行安全中的法律責任作出原則性規範。鑑於 2020 年美國軟體供應商「SolarWinds Orion」遭駭，致使美國聯邦政府機構、私營企業、非營利組織在內約 1.8 萬名客戶皆受巨大影響、[13] 2021 年美國最大

[12] 〈《互聯網用戶帳號名稱信息管理規定（徵求意見稿）》公開徵意見〉，《新京報》，2021 年 10 月 26 日，https://m.bjnews.com.cn/detail/163523813814104.html。

[13] 陳曉莉，〈美國國土安全部發布緊急指令，要聯邦機構立即關閉被植入木馬的 SolarWinds 系

燃油管道運營商 Colonial Pipeline 遭網路攻擊，造成美國多州進入緊急狀態，致中國亦感受到威脅CII網路設施與訊息系統，等同破壞國家安全、國計民生、公共利益，故習近平亦多次在公開場合宣示加大力度防護 CII，至 2021 年審議通過《關鍵資訊基礎設施安全保護條例》，突出特點在於建立「網信公安—保護工作部門—運營者」三層架構的CII安全綜合保護體系，專章細化有關規定「誰主管，誰負責」。2023 年 5 月正式實施《信息安全技術關鍵資訊基礎設施安全保護要求》，確立CII安全防護包括分析識別、安全防護、檢測評估、監控預警、主動防禦與事件處置等 6 個關鍵環節，並以此為基礎建構CII安全防護技術體系，並明確提出每年至少組織開展一次應急演練，更重要的是使用自動化工具（而非人工）管理 CII 系統帳戶、配置、漏洞、修補、病毒庫等，[14]通過智慧化技術提供更高安全防護水準。

三、統一控管網路數據豎起壁壘

中國政府意識到資料數據已成為經濟增長和價值創造的重要資產，但凡數據的蒐集、存儲、管理、加工、應用、流通等任一環節出現破口，均造成難以估計的損失，致中國在 2021 年開始強調強化數據治理。主要圍繞一是數據安全維護、二是數據發展與利用，《數據安全法》建立數據分類分級保護制度，尤以「關係國家安全、國民經濟命脈、重要民生、重大公共利益等」屬於國家核心數據。[15] 2022 年通過的《數據出境安全評估辦法》要求多數企業遵守數據本土化要求，而如須將數據轉移至海外，則須進行安全評估合規性審查。另《個人信息保護法》並擴大至 2023 年通過的《個人信息出境標準合同辦法》，針對處理大量個資的企業單位，明確規範

統〉，《iThome》，2020 年 12 月 15 日，https://www.ithome.com.tw/news/141666。

[14]〈我國首部關鍵信息基礎設施安全保護國家標准在京發布〉，《中央網絡安全和信息化委員會辦公室》，2022 年 11 月 8 日，http://www.cac.gov.cn/2022-11/11/c_1669799139872481.htm。

[15]〈中華人民共和國數據安全法〉，《中國人大網》，2021 年 6 月 10 日，http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml。

「敏感個資」的處理使用規則、跨境傳輸、個人資訊處理活動權利，與個資處理者方義務、監管部門職責、罰則。而 2023 年中國「兩會」後組建「國家數據局」著重於數據的處理、分配、共享與運用，[16]有助集中統一管理並進行監控，凸顯數據庫建置在中國內部強化本土化策略，同時打造中國的數據出境流動框架，控制數據流出管道，旨在確保核心數據和個人資訊統一由中國當局掌控。

肆、發展趨勢

一、推促軟體全面國產化以維持自主可控

烏俄戰爭下，全球最大的獨立開源軟體公司 SUSE、美國開源軟體巨頭紅帽（RedHat）等紛紛於 2022 年 3 月宣布退出俄羅斯市場，隨後德國商業軟體巨擘思愛普（SAP）、資料庫巨頭甲骨文（Oracle）亦宣布停止在俄羅斯產品銷售和服務，[17]致中國意識須加快對其國產軟體研發與創新，防止在此領域被歐美國家制裁。根據 2023 年發布的《中國軟體根技術發展白皮書》，目前微軟 Windows 在桌面和伺服器領域占據統治地位，而谷歌 Android 和蘋果 iOS 在應用智慧移動設備形成雙寡頭壟斷。[18]揆諸近三年華為積極推出歐拉（openEuler）伺服器作業系統和鴻蒙（OpenHarmony） 移動終端／物聯網作業系統，主要應用在黨政、金融、電力、能源等領域，雖獲取中國國內部分市占率，但在傳統行業和中小型企業使用率仍較低，且大部分底層科研平台都使用國外軟體和開源資料庫。中國考量在中美科技摩擦加劇下，外國軟體隨時可能被禁用，甚至存在被境外勢力植入後門可能隱患，故當前除宣傳鼓勵單位與個人使用國產化軟體，更亟欲開展軟體國產化相關平台研究、開發與推廣應

[16] 曾怡碩，〈設立國家數據局是中共現階段拚經濟的藥引〉，《即時評析》，2023 年 3 月 23 日，https://indsr.org.tw/focus?typeid=0&uid=11&pid=1600。

[17] 〈紅帽、Docker、SUSE 在俄羅斯停服，開源軟體還安全嗎？〉，《騰訊雲》，2022 年 4 月 16 日，https://cloud.tencent.com/developer/article/1983179。

[18] 〈中國軟體根技術發展白皮書-基礎軟體冊〉，《中國軟體行業協會》，2023 年 2 月 23 日，https://www.csia.org.cn/content/5868.html。

用工作，其中朝建設自主、開源軟體生態將係其確保軟體供應鏈與實現科研安全關鍵。

二、雲端服務系統走向官方主導、民間協力

近年隨中國加強數據安全、隱私保障和加強反壟斷背景下，核心信號均圍繞在「黨管資料，資料安全」，其中國有企業的資料資源屬國有資產，保護資料資產國有化成為執政能力現代化基礎，故自 2021 年中國天津、浙江、重慶、深圳、北京、甘肅等各地方政府部門，下令國有企業將資料從「華為雲、阿里雲、騰訊雲」等第三方公用雲平台遷出，改存放到官方搭建的「國資雲」平台。[19] 2022 年 5 月國家級數據雲平臺——「人民雲」正式上線，定位為大數據「存、管、用」的安全雲，旨在為全中國各級各地黨政機關、央國企及各行各業的數位化轉型提供全程服務及解決方案。[20]當前中國阿里雲、華為雲、騰訊雲、百度智能雲等前四大雲端運算廠商雖仍占中國雲端服務市場 80%，[21]未來中國強化「人民雲」政務公有雲端市場逐步拓展應用，民營雲端廠商可能無法像以往直接作為雲端服務建設運營主體出現，而是逐漸走向產業鏈後端，為中國雲端建設和運營提供技術、產品和經驗支援。

三、制定管理規定打造「中國版」元宇宙

2022 年底美國企業 OpenAI 推出 ChatGPT（Chat Generative Pre-trained Transformer）的 AI 聊天機器人引爆全球後，中國視 ChatGPT 模型學習的資料庫來源帶有鮮明的西方意識形態，且在社會價值與熱點話題存在針對性、系統性滲透，故禁止中國用戶使用，隨之百度「文心一言」、阿里巴巴「通義千問」、華為「盤古」等諸多

[19]〈中國數據安全法 9/1 生效 天津要求國企數據改存官方雲端〉，《中央社》，2021 年 8 月 29 日，https://www.cna.com.tw/news/firstnews/202108290127.aspx。

[20]〈國家級數據雲平臺「人民雲」正式上線〉，《人民網》，2022 年 5 月 20 日，http://dangjian.people.com.cn/n1/2022/0520/c117092-32426198.html。

[21]〈2023 年中國雲計算市場規模預計突破 3,000 億元〉，《人民網》，2022 年 4 月 9 日，http://finance.people.com.cn/BIG5/n1/2022/0409/c1004-32395072.html。

「類 ChatGPT」相關產品如雨後春筍，中國 2023 年 8 月施行首份針對生成式 AI 監管文件《生成式人工智能服務管理暫行辦法》，鑒於該法從 4 月公開徵求意見稿，至 7 月正式發布，僅花費 3 個月，顯示中國最初從針對演算法（Algorithm）、深度偽造（Deepfake）、生成式 AI 等一系列改變生活的新型技術，急迫採取全面規範相關服務與應用，強化法律監管以防患未然。揆諸 2023 年 9 月中國工業和信息化部等五部門發布《元宇宙產業創新發展三年行動計畫（2023-2025 年）》，旨在加快重點行業工業元宇宙（Metaverse）佈局，[22] 而元宇宙融合 Web 3.0、區塊鏈、非同質化代幣（Non-Fungible Token, NFT）、5G、數位分身、AI 等多樣前端科技，可預見後續將加快制定中國版「元宇宙」法規標準，以未雨綢繆管控其貨幣交易系統、網路身分、社會規則等安全風險。

伍、結論

除上述所言，中國近年注重培訓網路空間治理相關的技術、法律、政策等人才，並將「網路安全」增加為一級學科，目前共 60 所大學新開網路安全學院和相關研究中心，[23]同時鼓勵網路企業、行業組織和學術機構積極參與「網際網路名稱與號碼指配機構」（Internet Corporation for Assigned Names and Numbers, ICANN）、「網際網路工程工作小組」（IETF）、「網際網路架構委員會」（Internet Architecture Board, IAB）等機構的人才培養和輸送。對中國而言，其網路安全兼顧技術性安全與秩序性安全，且必須置於總體「國家安全觀」和「網路強國」目標框架下，故對內重點是頒布法令實施控管審查資訊、嚴管科技業等網路治理方式，維持社會政治穩定性，對外亦藉由替「一帶一路」沿線國家打造「數字絲綢之路」（Digital Silk Road），持續輸出其網路空間國際規則制定，意

[22] 〈《元宇宙產業創新發展三年行動計劃(2023—2025 年)》解讀〉，《中國政府網》，2023 年 9 月 8 日，https://www.gov.cn/zhengce/202309/content_6903025.htm。

[23] 〈築牢全民網絡安全「防火牆」——我國網絡安全工作成就綜述〉，《人民網》，2022 年 9 月 5 日，http://cpc.people.com.cn/BIG5/n1/2022/0905/c64387-32519253.html。

圖在全球網路空間治理發揮核心主導作用，繼而提高中國對網路治理國際影響力。

本文作者曾敏禎為國立政治大學亞太研究英語碩士，現為財團法人國防安全研究院網路安全與決策推演研究所政策分析員。主要研究領域為：中國網路政策、網路威權。

China's Cybersecurity Development: Current Status and Future Trends

Min-Chen Tseng

Division of Cyber Security and Decision-Making Simulation

Abstract

China promulgated and implemented the Cybersecurity Law in 2017, which, with the Data Security Law (DSL) and Personal Information Protection Law (PIPL) implemented in 2021 are the country's three fundamental cybersecurity laws. Today, China is still facing political threats caused by online public opinion, hacker group attacks from different countries targeting China's infrastructure network and various industries, as well as failure to protect classified data, causing large scale data leakage. The aforementioned risks have all driven China's continuous efforts to strengthen cybersecurity in recent years, including ensuring the constant monitoring and maintenance of the Internet to keep public order, safeguarding the security of critical infrastructure and network systems, and prohibiting the information and data transfer of businesses operating inside and outside of China.

Under the impact of the war between Ukraine and Russia, and the Sino-US technology war, China will continue to promote software localization to increase resilience in face of the containment and sanctions of other countries in future. Domestically, China requires state firms to accelerate data migration to government-run cloud services, while private players such as Alibaba, Huawei and Tencent that used to dominate the market need to step behind the scenes. In order to support the development of a domestic Metaverse involving multiple parties, a centralized digital infrastructure and formulate data regulations will be operated to create a

Chinese version of the Metaverse. After all, the core purpose is to build norms and mechanisms which satisfy government regulatory requirements, with the intention of strengthening and consolidating China's cybersecurity and guaranteeing national security.

Keywords: Cybersecurity