供應鏈網路安全的地緣政治因素

曾怡碩

網路安全與決策推演研究所

壹、前言

網路空間即使根路由與域名有地域區別，在過去基本運用上並無地域與國界考量。多年來網路攻擊事件頻傳、加上國家行為者紛紛將網路空間視為另一戰場之後，地緣政治逐漸成為網路安全防禦的重要考量。與此同時，過去依據地緣關係以及比較利益優勢形成的全球供應鏈，隨著資訊化運籌管理的普及，被迫必須面對逐步升高的網路攻擊威脅—特別是網路竊取營業秘密與勒索軟體。此外，美國自川普政府開始，對中國大陸發動貿易戰之餘，更加緊對中國大陸施行高科技管制出口以及乾淨網路的科技脫鉤（decoupling）或去風險（derisking），這除了讓供應鏈安全成為國家安全關鍵要素、並全面拉高網路安全防護在供應鏈安全中的優先次序，地緣政治儼然躍升成為供應鏈網路安全的核心考量之一。

然而，對於供應鏈網路安全如何考量地緣政治因素，猶待進一步研析。有鑒於此，本研究運用文獻分析法，首先探討 2018 年迄今，在美中科技脫鉤潮流下，美國如何驅動供應鏈安全加入網路安全認證；其次則是探究該樣態供應鏈網路安全認證如何結合地緣政治考量。

貳、地緣拒止戰略下的科技脫鉤

從地緣政治觀點來看，在自由開放的印太戰略之下的美中戰略競爭不再一昧依循圍堵，美國對中共除戰略嚇阻外，在高科技領域已逐步形成 2021 年美國國防次助卿 Elbridge Colby 在軍事上所論述之「拒止戰略」（Strategy of Denial），[1]依循地緣考量，設立各式資

[1] Elbridge A. Colby, The Strategy of Denial: American Defense in an Age of Great Power Conflict

訊流通關卡，拒絕、防止中共竊取或取得高科技關鍵技術，避免讓中共在高科技領域突破、甚至稱雄，在現下與未來都將極端困難。主要的操作策略呈現為科技脫鉤，鞏固此一拒止戰略的背後理念則為民主對抗威權的陣線串聯。

一、美中科技脫鉤

「美中科技脫鉤」的成型並非一蹴可及，中方考量到中國大陸、俄羅斯及「一帶一路」沿線國家的市場接受度，不太可能一開始就完全切斷與歐美國家之作業系統、通訊協定及社群媒體軟體規格之相容性。歐美科技大廠考慮到前述陣營之龐大市場與訂單，也會在利益驅動下遊說，緩步進行全面禁止支援中方技術規格與系統服務。如此將讓中國大陸自主開發的軟硬體一開始將強調相容性，以換取市場空間與研發時間。但隨著「美中科技脫鉤」的成形，國安因素將不斷介入，強化雙邊陣營間技術與服務的區隔，這將讓技術規格與市場也漸趨涇渭分明，進一步明確劃出技術限制移轉界線，導致市場區隔藩籬與技術限制鐵幕將趨向一致。

如同過去美蘇冷戰一般，科技脫鉤藩籬界線的劃訂，主要還是以民主與專制為區隔基準。中共代表的專制威權，隨著網路與人工智慧科技成熟而更加無所遮掩。在意識形態影響與思想控制上，中國大陸網路各式媒體興起，自媒體與簡訊、短影片尤其蓬勃發展。中國大陸字節跳動推出的「抖音」應用程式，不僅在中國大陸境內廣受歡迎，更是風靡全球。

然而在境內，北京除嚴加監控網路新媒體上的言論與行徑以進行輿情監測，更對於中共官方認定的有害資訊內容，予以嚴密審查管制。網路媒體內容審查的監管，落在「中央網路安全和資訊化委員會辦公室/國家互聯網資訊辦公室」，即「網信辦」身上， 每年「網路清朗活動」以網路生態治理為名，要求網路資訊內容服務平

(New Haven: Yale University Press, 2021).

台業者，擔負起內容審查的責任。對於推薦演算法與生成式大型語言模型，中共也加以管制，實現從資料到演算法到生成語言的一條龍管控。

循此發展可能導致中共借助俄羅斯獨立自主根伺服器之網路系統 Runet，並在中國大陸的國內市場與「一帶一路」沿線國家之外，把反圍堵陣線擴大到俄羅斯廣大市場，以形成中俄陣營與美歐陣營之間壁壘分明的對峙。華為已針對俄羅斯提出以 Aurora 為架構的作業系統，而希望順利進入俄羅斯市場。此外，在二分的格局下，不排除華為可能買回已售出之華為海纜，為將來中俄陣營進行海纜布局，形成從資料傳輸到消費者使用端設施均為完整自主系統局面。

二、價值取向的友盟鏈結

隨著「一帶一路」倡議推展到東南亞、南亞、南太平洋，以及歐亞大陸、巴爾幹等中東歐國家，北京藉由「一帶一路」倡議中的基礎建設，佈建海外航港營運與 5G 通訊系統。這些舉措的戰略性質引起美國嚴密警覺與注目，川普政府開始以「印太戰略」作為因應對策。在美中兩強之外，歐盟是唯一具有空間與實力提出「印太戰略」與「一帶一路」以外的戰略途徑，但受英國脫歐、歐盟決策模式的影響，歐盟在經過數年謹慎觀察與評估之後，在 2018 年先提出「歐洲與亞洲連結戰略」（Connecting Europe and Asia – Building Blocks for an EU Strategy），時隔近 3 年，才在美國拜登政府多邊合作戰略架構下，於 2021 年 4 月提出《歐盟印太合作戰略》（EU Strategy for Cooperation in the Indo-Pacific）。針對其中鏈結的部分，尤其是基礎建設發展議題，緊接著 G7 在 2021 年 6 月提出的《Build Back Better World（B3W）夥伴倡議》，歐盟於 2021 年 7 月 12 日發布「全球連結的歐洲」（A Globally Connected Europe），有意在「印太戰略」與「一帶一路」之外，提供另一個戰略路徑選項。

面對美國「印太戰略」與中共「一帶一路」在基礎建設全球布局的開展，「全球連結的歐洲」意味著歐盟在對自身境內基礎建設布局之外，也將觸角延伸面向全球，對於歐洲以外地區展開以歐盟價值為依歸的連結戰略。

參、供應鏈網路安全的地緣政治因素

各式鏈結倡議所構建的產品或服務之供應鏈的輸送通道，在現今數位年代，互通有無過程生成資料通訊網路即面臨網路安全的議題。民主陣營主要依循美國「乾淨網路」倡議，原則上硬體、韌體與軟體均須注意網路安全管理，具體而言，硬體方面還包括資料傳輸所經地、資料傳輸管線通路、資料儲存中心所在地，以及天線、路由器、伺服器、晶片，與硬體維運及軟韌體開發維運人員等人事物地之安全認證，均須列入分級管理。

一、資料傳輸安全

近年引人矚目的光纖纜線，由於佔全球資料傳輸量的九成以上，在資料已然成為生產要素大宗物資之際，隨著數位化的普及，資料產出與流通的需求與日俱增，大型網路營運平台業者近年自建海纜，已然為時勢所趨。海纜經過國家所設之海纜登陸站及資料中心，尤其在美國更動海纜規劃以避開中國大陸後，海纜路線儼然成為地緣政治熱門議題。美國提出「乾淨網路」倡議，此關鍵資訊基礎設施的硬體便是海纜，受海流、海底地形變化、漁撈拖網及海底生物啃咬，均可能造成「斷線」，必須依賴國際專業維修船業者。此外，陸上海纜接收站軟體也必須定時更新，這二項維運極易成為情蒐目標，因而必須納入國安考量。

二、資料儲存安全

資料中心的地點選擇，除避開地震帶、電力基礎設施與電價考量，例如中共「東數西算」工程，將東部資料輸往西部資料中心儲

存暨運算。其餘還有在資料落地趨勢下，各國基於司法互助而進行之資料存取，例如美國與他國簽署之《雲端法案》，可作為資料中心選擇之依據之一。抖音海外版 TikTok 備受美國官方與國會質疑美國用戶資料會遭中共官方以情報法要求存取，TikTok 提出解決方案之一，即為將資料存於與美國具司法互助關係之國家的雲端資料中心。

三、資料運算及晶片安全

至於資料中心所需算力，一來仰賴不斷修正精進之演算法更新，對此中共視為網路主權，除立法管制出口，還出言制止美國要求 TikTok 出讓股權成為美國控股公司。[2]另一方面，算力還仰賴高階晶片，而美國拜登政府為釜底抽薪，於 2022 年推出的《晶片與科學法案》，為美國半導體生產提供約 520 億美元的政府補貼，對晶片製造投資實施稅收抵免，並計畫在此後 5 年內授權超過 1,700 億美元的預算，以提升美國半導體產業的競爭力，並紓解晶片持續短缺的現象。[3]在此之前拜登在 2021 年還簽署行政命令點名台灣、日本、韓國與美國組成半導體 CHIP 4 聯盟，後續搭配 2022-23 年諸多出口管制新措施，[4]以遏制中國大陸半導體產業的增長，並嚴密管控中共借殼規避晶片出口管制。[5]

由於台積電已成為高階晶片最大宗來源，鑒於資安考量與台海衝突之地緣政治風險，要求台積電前往亞歷桑納州設廠。美國官員並不諱言台積電晶片攸關美國國防產業之供應鏈安全，美國在台協會日前針對台積電的決定，即直指台積電晶片為 F-35 關鍵零組件。

---

[2] 〈中國批美禁 TikTok 是「沒自信」 中網友反酸：那你禁推特臉書是?〉，《自由時報》，2023 年 3 月 1 日，https://news.ltn.com.tw/news/world/breakingnews/4225095。

[3] 黃松勳，〈拜登簽署《晶片與科學法案》以鞏固美國在未來科技的領導地位〉，《科技產業資訊室》，2022 年 8 月 11 日，https://iknow.stpi.narl.org.tw/post/Read.aspx?PostID=19456。

[4] 蕭逸夫，〈晶片四聯盟 (Chip-4) 和美國新晶片出口管制對台灣與中國晶片產業的影響〉，《Newtalk 新聞》，2022 年 10 月 13 日，https://newtalk.tw/citizen/view/58922。

[5] 陳昭宏，〈晶片大戰！華為正在中國建秘密晶片網絡 規避美國制裁〉，《Newtalk 新聞》，2023 年 8 月 23 日，https://newtalk.tw/news/view/2023-08-23/885350。

其餘多國也提出比照設廠需求，而台積電則選擇性進行海外布局，除在美國亞利桑那州廠投資金額擴增至 400 億美元，將投入 4 奈米及 3 奈米製程生產，並在日本熊本投資建廠，預計 2024 年底前以 28 奈米、22 奈米、16 奈米及 12 奈米製程生產。[6]

肆、轉向資料流安全管控

美國國防部鑑於國防供應鏈核心廠商與協力廠商遭受來自惡意網路攻擊以及竊取營業秘密，讓美國先進科技優勢不斷流失，尤其眼睜睜看著中共毫不遮掩地仿造美式武器，面對中共點點滴滴的全面情蒐模式，聯邦機構及國防廠商所產生、經手、儲存與處理的諸多類似「受控非分類保密等級資訊」（Controlled Unclassified Information，CUI），自然而然成為中共之情蒐高價值目標，也讓美國國防部採購部門與反情報部門對於國防工業基礎網路安全防護繃緊神經，積極制定足以拒止中共竊密的機制。[7]

從前述供應鏈網路安全的地緣政治因素考量，可以看出管控網安風險的層級考量，其實是伴隨著需受保護控管資料流之輸送、儲存或處理得實體或虛擬空間位置而定。美國國防部國防合約管理局（Defense Contract Management Agency，DCMA）因而自 2020 年 11 月底即已開始力推「網路安全成熟度模型認證」（Cybersecurity Maturity Model Certification，CMMC），要求國防廠商在競標國防契約時，必須證明自身於非聯邦機密網路中所儲存、傳輸或處理（含產出）之「聯邦合約資訊」（Federal Contract Information，FCI）及「受控非分類保密等級資訊」的保護，通過其網路安全成熟度層級的各項驗證，以符合美國國家標準與技術研究院（NIST）針對保護非聯邦系統和組織中 CUI 所出版之 *NIST Special Publication 800-171*

[6] 〈亞利桑那州廠明年量產 台積電：工作不以國籍區分〉，《中央社》，2023 年 3 月 2 日，https://www.cna.com.tw/news/afe/202303020200.aspx。

[7] "Controlled Unclassified Information," U.S. DoD CUI Program, https://www.dodcui.mil/. Also see: "Controlled Unclassified Information (CUI)," US Defense Counterintelligence and Security Agency Website, https://www.dcsa.mil/Industrial-Security/Controlled-Unclassified-Information-CUI/.

規定要求。[8]

伍、結語

俄烏戰爭讓世人感受食物與能源等大宗物資供應鏈因地緣政治衝突而中斷的全球衝擊，而數位時代資料儼然已為新興大宗物資，在美中科技脫鉤形勢下，供應鏈安全的考量還需涵蓋網路安全的地緣政治因素，以達到對中共戰略拒止目標，防止中共竊密轉為對美不利之軍事進展。CMMC 管制國防工業基礎的供應鏈網路安全，尤以資料流所經人地物均端視機敏等級與分類狀況，而可能列為不同等級下之控制項。若我國有意以 CMMC 對「受控非分類保密層級資訊」的管控為參考基準，須注意其最初積極推動應用在採購合約的三個美國政府機構，就是國防部、國家反情報安全中心以及網路安全暨基礎設施安全局。這也反映 CMMC 對供應鏈安全的著眼點，是把資安與反情報融入到從採購到製造、整合與應用端的整個過程。

本文作者曾怡碩為美國喬治·華盛頓大學政治學系博士，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副研究員。主要研究領域為：軍隊與網路安全、網電作戰、認知作戰、中國數位監控。

[8] 參閱 CMMC 認證機構（Accreditation Body）Cyber AB 官方網頁說明，https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles/DIB-Companies-OSCs。

Geopolitical Factors Affecting Supply Chain Security

Yisuo Tzeng

Division of Cyber Security and Decision-Making Simulation

Abstract

After the Trump Administration launched a trade war against China, decoupling and de-risking through export control over high technology and the Clean Network closely followed, making supply chain security a key national security concern. Cybersecurity therefore became the top priority in supply chain security, into which geopolitics jumped and became one of the core concerns. As far as supply chain security is concerned, data transmission, storage and computation must take account of related persons, hardware, software, and locations.

US defense industrial base core enterprises have encountered malicious cyberattacks and espionage aiming to steal commercial secrets, thereby compromising the US high-tech edge. With China making no disguise of its desire to copy US weapons through incremental piecemeal intelligence collection, controlled unclassified information (CUI) generated, transmitted, processed, and stored by federal agencies and defense industrial base (DIB) enterprises has naturally been given high priority in China's intelligence collection.

Layered cybersecurity risk control rests on physical and virtual locations of CUI generation, transmission, processing and storage. Following the direction of strategy of denial, US DoD DIBCAC has introduced Cybersecurity Maturity Model Certification, or CMMC, which will require DIB enterprises to satisfy requirements for managing CUI before bidding for and signing procurement contracts.

Keywords: Strategy of Denial, Supply Chain Security, Tech Decoupling, CMMC