中共科技治理下的脅迫型態

曾怡碩

網路安全與決策推演所

壹、前言

本文按照本期特刊對於脅迫的認定，根據韋氏字典所述，脅迫（coercion）是使用明示或暗示的暴力威脅、報復或其他恫嚇行為，使對手對可能後果感到恐懼，進而採取違背其意志的行動。受到 2020 年下半年中國藉由貿易制裁脅迫澳洲的影響，以美國為首的印太友盟 2021 年以來，開始關注中國的脅迫行徑。2021 年 3 月 3 日由白宮發布的《國家安全戰略暫行指南》（*Interim National Security Strategic Guidance*）指出，「將支持中國的鄰居和貿易夥伴保護自身權利，做出免於受脅迫的自主性政治決定」。[1]在 2021 年美日領袖峰會共同聲明中，針對中國採取經濟與其他形式脅迫行為這類不符國際秩序的活動，拜登與菅義偉表達共同關切。[2]

在外界目光聚焦在中國運用武力、外交、經貿以及輿論等脅迫手段之際，近年來備受關注的中國科技產業生態系發展，出現一些新的變化，中共運用各式科技治理手法威脅逼迫國內外科技業者、研發人員、中國公民，除藉此達到其限制／鼓勵科技產業發展效果，並可讓國內外科技業者不得不配合北京管治維穩目標。

鑒於中共藉由科技治理之脅迫型態迄今尚屬發展階段，隨之而來的問題就是：中共現今如何假科技治理之名而行脅迫之實?為回答該問題，本文將首先嘗試臚列將科技治理主張轉具脅迫性的手法樣態；其

[1] 原文為「We will support China's neighbors and commercial partners in defending their rights to make independent political choices free of coercion or undue foreign influence.」，見 *Interim Natioanl Security Strategic Guidance*, White House, March 2021, pp.20-21, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf。

[2] 江今葉，〈美日聯合聲明 52 年來首提台灣 強調台海穩定重要性、關切中國脅迫行為〉，《中央社》，2021 年 4 月 17 日，https://www.cna.com.tw/news/firstnews/202104170028.aspx。

次分別針對技術移轉與滲透洩密、資料主權與長臂管轄兩項實務領域中的脅迫樣態進行探討；最後則將針對中共反制外國制裁以及標準制定兩項議題對於科技業可能之影響，提出未來研究建議。

貳、中共科技治理主張之脅迫性質

中共所有科技治理主張，亦即各項科技發展戰略以及其相關管制措施，均需服膺四個堅持中的一黨專政（堅持共產黨領導），必須有利於共黨持續執政與擁護領導核心，並預先消弭可能分裂黨國社會的任何禍端。一旦執政團隊或領導核心認定為禍端，即可運用科技政策主張予以徹底制壓，迫使國內外之個人、企業或他國政府改絃易張，以符合共黨持續執政利益。

與科技相關的治理主張中，最受西方先進國家忌憚的，首推中共高舉的科技民族主義。其強調要追趕先進國科技並形成自主創新，不斷體現在「科技強國」、「中國製造 2025」與「中國標準 2035」。基於主權不容受損且必須伸張的特性，科技主權的主張體現在對於外來投資技術審查、外商技術移轉等產業政策。此外，中共科技產業戰略主張可以憑藉中國廣大市場自主制定標準，但要成為國際主流標準，甚至具備主宰性質，就必須進一步主導國際標準組織。[3]

科技主權延伸擴張到數位時代的網路主權概念，除了必須能自主控管實體設施，還要將境內外公民所生成的資料予以納管運用，因此衍生資料主權與資料安全相關主張。不論是基於資料驅動的經濟誘因使然，還是一黨專政下言論控管與國家安全的考量，中共科技治理循此加強網路安全監管規定，並對各類外商科技廠加強黨組設置俾利進行人為監控。

[3] 黃健群，〈「中國標準 2035」戰略解析〉，中華民國全國工業總會《產業雜誌》，110 年 6 月，http://www.cnfi.org.tw/front/bin/ptdetail.phtml?Part=magazine11006-615-7。

網路安全標準的制定，將是中共瞄準的新戰場。華府智庫新美國安全中心（Center for a New American Security）學者 Elsa Kania 即指出，制定標準對塑造技術未來的競爭和格局有重要影響，不僅會決定商業後果，也會塑造出對企業有利或不利的架構。[4]此外，據業界人士指出，中共有意透過標準制定獲取關鍵資料，中共定義的技術和技術標準越多，相關資料就越會受到中共各種資料在地化的制約。[5]

參、中共科技治理議題之脅迫籌碼與手段

一、技術移轉與滲透洩密過程對國家、業者與洩密者的脅迫

(一) 以市場進入作為脅迫技術移轉籌碼

科技發展除自主研發，中共還意圖以其國內廣大市場為誘因，要求外商進行技術移轉。對於嚴守智慧產權或營業秘密而不肯就範的業者，則施以非關稅障礙，輒以國家安全或產品安全檢查為由，要求釋出原始碼及程式設計演算法，俾利多層次檢視審核。尤其是 2016 年《網路安全法》實施要求開放程式原始碼供官方檢核，更引發數十家科技業者聯合反彈，經歷多年抗爭與往返交涉，跨國科技業者訴諸國際貿易法制與美歐多國政府出面談判，才在堅持非歧視性等原則之下，換取中共在技術安全產品檢測標準逐步與國際標準趨同，保障科技廠赴中國大陸營運或銷售之權益。[6]

(二) 以人身安全脅迫專業人員竊密

面對美中科技可能脫鉤的衝擊，科技供應鏈安全議題日益受到歐美

---

[4] Arjun Kharpal, "Power is 'up for grabs': Behind China's plan to shape the future of next-generation tech," *CNBC,* April 26, 2020, https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html.

[5] 林楓，〈《中國製造 2025》走後，又來了《中國標準 2035》〉，《美國之音》，2021 年 4 月 28 日，https://www.voachinese.com/a/china-standards-2035-20200428/5395187.html。

[6] 楊緣，〈中國《網路安全法》衝擊跨國公司〉，《金融時報》，2017 年 5 月 31 日，https://big5.ftchinese.com/story/001072794?archive。最近以市場進入要脅的顯著例子，就是蘋果公司對北京的妥協，但讓步的不是技術移轉，而是將資料留在中國境內，請見 Jack Nicas, Raymond Zhong, Daisuke Wakabayashi，〈審查、監控與利潤：為做生意，蘋果向中國政府妥協〉，《紐約時報中文網》，2021 年 5 月 18 日，https://cn.nytimes.com/technology/20210518/apple-china-censorship-data/zh-hant/。

日各國政府嚴格檢視，技術出口到中國的管制更趨嚴格，也讓科技廠商與中共交涉之際有所依恃。另一方面，這也意謂技術移轉與授權可能愈趨緊縮，恐讓中共加強訴諸其他管道獲取技術。這其中一個重要的管道，便是經由提供研發資金或高素質研究人力，或明或暗地資助國外學研人才、單位與實驗室，從中擷取累積技術經驗。過去幾年美國聯邦調查局全面清查千人計畫人員清單，就是反情報單位在為科技洩露進行止血。[7]

中共同時也汲取傳統諜報手法，吸收當地國人擔任經濟間諜，或藉當地人設立科技公司、以該公司資助學研實驗室、甚而贊助實驗室人員創立科技公司，種種行徑儼然已成為進行滲透收購或盜取科技營業秘密的模式。[8]前述不論是千人計畫還是經濟間諜，不論當事人是否為中國海外公民，一旦成為中共從犯成為叛國罪嫌，即為中共國安相關單位要脅而難以脫身。如從犯為中國海外移民，除留在國內家人可能淪為人質，自身若成為汙點證人控訴中共間諜行徑，中共國安部恐複製類似中共公安部的海外「獵狐行動」，透過監視、恐嚇等秘密行動，迫使這些汙點證人海外噤聲、甚至返國受刑。[9]

除傳統人員情報手法，中共或受美中科技脫鉤壓力使然，其行之多年的網路竊密手法，在近年規模大幅提升。美國司法部在 2021 年起訴中共駭客名單，已不同於過去為解放軍網路部隊或國安部特工，而是中共國安部委外資助的民間駭客團體。[10]鑒於2020年新冠肺炎疫情爆發後，全球多處遭受網路勒索駭侵頻率與規模都增加，然而網路駭侵難以明確究責，且民間駭侵團體或有其自主鑽營空間，通常難以連結

[7] Ellen Barry, Gina Kolata，〈美國執法部門緊盯中國「千人計劃」〉，《紐約時報》中文網，2020年2月7日，https://reurl.cc/rgzj0y。

[8] 劉晙華，〈中國大陸招攬臺灣人才趨勢評析〉，《展望與探索》第 18 卷第 7 期，109 年 7 月，https://reurl.cc/mLWjzV。

[9] 劉孜芹編譯，〈涉嫌中共「獵狐行動」 美起訴 9 名特務〉，《青年日報》，2021 年 7 月 24 日，https://reurl.cc/6ap3KO。

[10] 徐薇婷，〈對 12 國進行網攻 4 名受雇中共國安部駭客遭美國起訴〉，《中央社》，2021 年 7 月 20 日，https://www.cna.com.tw/news/firstnews/202107200003.aspx。

政府牽涉唆使責任，[11]這樣的灰色模糊地帶，也創造出讓中共得以藉機要脅他國政府與企業的空間，形成一種新脅迫型態。

二、以資料落地與長臂管轄脅迫科技業者

鑒於歐盟推出數位主權戰略，加上美國推動乾淨網路倡議，讓中共刻意將其網路主權觀與歐美並列，並於 2021 年陸續推出《個人資訊保護法》和《數據安全法》中，強調中國境內蒐集之資料應在地存放，境外輸出資料須經中共網信辦審理核准。該法第 36 條規定非經主管機關批准，境內的組織、個人不得向外國司法或者執法機構提供存儲於境內的數據。另一方面，《數據安全法》的監管適用範圍包括在境外的資料處理活動，藉此確立長臂管轄原則。依據該法第 2 條第 2 款的規定，即使在大陸境外開展資料處理活動，舉凡任何以電子或者其他方式對資料的記錄，如損害中國之國家安全、公共利益或者個人、組織之權益，將依法追究法律責任，故具有域外管轄效力。[12]

北京高舉網路安全資料落地的大旗，刻意以資訊安全相關法規脅迫網路科技業者配合管制言論，進而達到其維穩目的。中共網信辦以網路安全法不當蒐集資料以及資料不當傳輸境外之國安疑慮，先對美國特斯拉電動車設限—2021 年 3 月中共人大通過「十四五規劃」並將電動車列入重點發展項目之後，就陸續傳出解放軍擔心特斯拉電動車的攝影鏡頭與偵測雷達蒐集軍事設施或政府機關大樓情資。中共即以造成國安疑慮為由，限制軍方、涉及敏感工業的國企，以及國家機關人員駕駛、或者在辦公處停車位停放特斯拉電動車。[13]中共藉此影響市

[11] 例如：中共外交部發言人趙立堅在 2021 年 7 月 20 日否認中國政府背後指使駭客行徑，強調「中方堅決反對並打擊任何形式的網路攻擊，更不會對駭客攻擊進行鼓勵、支持或縱容。」詳見：〈2021 年 7 月 20 日(中國)外交部發言人趙立堅主持例行記者會〉，中國外交部官網，2021 年 7 月 20 日，https://www.fmprc.gov.cn/web/fyrbt_673021/t1893709.shtml。

[12] 蔡步青，〈大陸《數據安全法》對台商的影響與因應策略〉，《工商時報》，2021 年 6 月 28 日，https://view.ctee.com.tw/legal/30277.html。

[13] 高鋒，〈輿論圍剿下被迫就範？ 特斯拉在中國設立資料中心〉，《自由亞洲電台》，2021 年 5 月 26 日，https://www.rfa.org/mandarin/yataibaodao/jingmao/gf0526a-05262021065527.html。

場消費意願後，進而收保護扶植國內電動車廠商之效；後又以類似理由對阿里集團之「滴滴出行」在美上市之舉下重手，以達到打壓異己、殺雞儆猴的維穩效果。[14]

港府也效法北京脅迫科技業者之行徑，意圖收管治維穩之效。在 2021 年對網路「起底」祭出《個資條例》修訂案，將「起底」行為之相關「法人」(person) 列為刑事究責對象。此舉無異於將相關網路科技服務業在香港從業人員予以匡列究責，圖藉此逼迫科技業者主動偵測審查並下架「起底」相關內容。科技業者為保香港員工免受刑罰，反成北京及港府打壓言論自由的幫兇。包括谷歌、臉書和推特在內的「亞洲互聯網聯盟」(Asia Internet Coalition, AIC)於 6 月 25 日致函香港個人資料私隱專員鐘麗玲(Ada Chung Lai-ling)，表示「……避免科技公司受到這些制裁的唯一辦法就是避免在香港投資和提供服務，從而使香港企業和消費者得不到服務，同時也創造了新的貿易壁壘」。[15]

肆、結論—未來研究建議

總結前述分析，中共在科技領域的脅迫手法與樣態，多為效法美國制裁手段、俄羅斯滲透手法或冷戰時期美蘇制裁行徑。事實上，迄今中共對外脅迫行徑有很大一部分是針對外國議論其人權迫害所為，這相當程度呼應先前所提之維護共黨執政地位動機，也構成中共脅迫作為的特色。

就科技治理之下的脅迫行徑而論，目前雖尚未見到科技業者在中國域外管轄下被迫進行網路言論審查，但已逐漸看到科技業者借鑒中共對於澳洲、加拿大、台灣受到脅迫的前例，開始對於自身言行遂行自

[14]〈陸媒：滴滴赴美上市先斬後奏 令監管震怒〉，《中央社》，2021 年 7 月 5 日，https://www.cna.com.tw/news/acn/202107050052.aspx。

[15] Newley Purnell, “Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws,” Wall Street Journal, July 5, 2021, https://www.wsj.com/articles/facebook-twitter-google-warn-planned-hong-kong-tech-law-could-drive-them-out-11625483036. AIC 將信函全文公布於官網，請參閱：https://aicasia.org/wp-content/uploads/2021/07/Industry-Response-on-the-Proposed-Amendments-to-Hong-Kongs-Personal-Data-Privacy-Ordinance-and-Request-for-Virtual-Meeting.pdf。

我審查，不願因此得罪中共官方並引來粉紅或戰狼圍剿，進而導致在中國市場的挫敗。[16]在中共鑑於近年接連遭遇華為孟晚舟事件與後續個別企業及官員遭受美歐制裁，而於 2021 年頒布《反外國制裁法》後，外國科技業者是否會被迫進一步限縮自身以及網路言行，值得密切觀察研析。

中共多年經營科技標準制定，已經開始在主導國際相關標準制定組織，以及藉由帶路倡議進一步擴大標準適用市場規模這兩大領域受到矚目。美國積極圍堵華為 5G 系統布建，甚至不惜祭出脫鉤路線，就是明顯例證。然而，美歐等國也是從自身過去數十載掌控技術標準話語權，從而深切瞭解中共藉由標準制定而造成脅迫的潛在威脅。如今美國亟思重掌國際科技標準組織主導權，積極鑽研國際組織運作規則，[17]並同時從科研人員反情報下手，對於中共運用在歐美科研人員為其發聲效力，進行堅壁清野。美國能否藉此收釜底抽薪之效，中共能否／如何運用科技標準制定進行脅迫，勢將為未來研究的重要課題。

作者曾怡碩為美國喬治華盛頓大學政治學博士，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助理研究員兼所長。主要研究領域：軍隊與網路安全、中國資訊作戰、中國數位監控。

[16] 台灣科技廠的例子，請見：謝文哲，〈在中國官網嘲諷MIC 惹議　技嘉致歉產品遭多平台下架〉，《鏡週刊》，2021 年 5 月 11 日，https://www.mirrormedia.mg/story/20210511edi058/。

[17] Kristen Cordell, “How to Win at the International Telecommunication Union,” *CSIS Commentary*, May 20, 2021, https://www.csis.org/analysis/how-win-international-telecommunication-union.

China's Ways of Coercion in Technology Governance

Yisuo Tzeng

Assistant Research Fellow

Abstract

In recent years, the Chinese Communist Party has used various means to coerce technology operators, research and development personnel and Chinese citizens at home and abroad, demanding foreign companies carry out technology transfer with the lure of the huge domestic market. The flag of localization of Internet security information has also been waved, deliberately using information security related regulations to force Internet technology operators to cooperate by controlling speech. This is used to achieve the objective of restricting/ encouraging the development of the technology industry and it also leaves foreign and domestic technology operators with no choice but to cooperate with Beijing's objectives of governance and maintenance of stability.

There has yet been no case of a technology operator being forced to censor online speech outside China's area of jurisdiction, however, self-censorship by technology operators of their actions and behavior has gradually begun. Also, the Chinese Communist Party is attracting attention in two areas because, after engaging in technology standard formulation for many years, it has begun to lead international related standard formulation organizations and use the Belt and Road Initiative to expand the scope of the market to which standards apply. China's ability to use, and the ways it uses formulation of technology standards to carry out coercion is sure to become an important topic of study in future.

Key words: technology governance, coercion, cyber sovereignty, data localization