第二章　科技冷戰

曾怡碩*

壹、前言

美國在 2019 年對於華為的圍堵，以及華為的反圍堵，體現出科技冷戰的氛圍。只是，過去冷戰時期美蘇全面圍堵對峙局勢，這次是呈現在與高科技產業發展相關的各個面向。美國除對外勸說友盟共同構築陣線以圍堵中國大陸科技產業擴張，也鑒於在此圍堵藩籬初步成形階段，友盟因缺乏明確依循規範而遲疑不定，故加緊腳步從自身做出示範—美國接續對於科技進出口加強管制，除加強對於中國大陸投資高科技產業的審查限制，並強烈關切中共運用在美中國留學生與科技移民於科技實驗室竊取營業秘密，還限制國防產業及政府採購不能採用中國大陸製產品或關鍵零組件。美國甚至要求關鍵廠商將生產鏈移至美國境內設廠，藉由美國製造的鮮明旗幟，號召友盟加入美國陣營，從法律、規章、審查、監管各個層面，加速築造科技藩籬，以共同對抗中國大陸製造的科技產業。

貳、科技冷戰的本質

冷戰的傳統概念，是源自二次世界大戰結束後，以美國為首的民主自由陣營圍堵以蘇聯為首的共產主義擴張。這樣的兩極世界格局因各自擁有的核武與傳統軍力而達成均勢之對峙。壁壘分明的界線，從軍事聯盟、意識形態、國際組織與外交場域的鬥爭，一路延伸到先進高科技，尤其是軍民兩用科技的發展、移轉與進出口，一般都會對貨品、服務與人力資源施行出口管制措施，對於違規者，往往施加經濟制裁予以懲罰。若是單方或雙方應用議題連結，則甚至波及到安全合作的範疇。

美中貿易戰自2018年3月以來，美方即以中方侵犯智慧財產權以及中方補貼其科技業者造成不公平貿易為由，遂行關稅、出口管制及禁止輸入等貿易制裁。其後美國以國家安全威脅隱憂為由，於全球大肆圍堵華為第5代行動通訊網路（5G）系統。由於傳統盟友仍未能全面禁用華為系統，美國甚至威脅將切斷情報交換機制。在2019年5月，美國川普政府以國家安全為由，祭出出口管制「實體清單」（entity list）；華為在全球分支企業均列入制裁清單。緊接著的是一連串美國科技軟硬體系統及服務大廠陸續宣布終止支援華為產品與服務。

中共商務部隨後在2019年5月31日公布出口管制「不可靠實體清單」機制，以反制美國商務部之「實體清單」，美中科技戰於此正式展開。由於科技戰開打時機，正值中方宣布在6月1日起對600億美元商品加徵關稅，而美國揚言將對約

* 曾怡碩，網路作戰與資訊安全研究所助理研究員，負責本章。

3,000億美元的中國大陸商品開徵25%的關稅，也拉開後續美中兩國斷斷續續的貿易談判的序曲。這不免讓人聯想，各自除反擊對方貿易關稅報復，也是在增加自身之貿易談判籌碼。

然而，美中科技戰本身並非兩國貿易戰籌碼或由貿易戰衍生。科技業者咸認，無論美中貿易戰是否平息，美國與中共之間高科技產業已然由美國提供技術、中國大陸提供代工組裝與廣大市場的互利模式，逐漸進入衝突零和競爭態勢的科技戰模式。因此，美國基於國家安全與科技競爭力之國家利益，美國對於中國大陸科技產業的圍堵，不會因為貿易戰歇息而就此罷手，反而加緊腳步構築科技藩籬，形成科技冷戰態勢。[1]科技冷戰所呈現的圍堵與反圍堵態勢，決不僅止於華為，而將體現在科技產業對於關鍵原物料與零組件、軟體應用程式、人力資源、銷售市場所劃出的分明界線與對於違規越線國家的懲罰。

回顧冷戰的歷史，美蘇陣營在冷戰階段，因惟恐爆發不可挽回的相互毀滅，開始建立熱線等信心建立措施。美中若未來形成分庭抗禮局面，全球各國也將紛紛選邊站，無國界網路安全成為相互攻防無煙硝戰爭的戰場。未來發展壁壘分明的趨勢，也提供了未來建立網路安全區域信心建立措施的基礎。

參、華為模式：圍堵與反圍堵

過去冷戰為美蘇兩核武強國帶領各自陣營對峙，美國圍堵共黨赤化，而共黨陣營防制西方和平演變。如今所謂「美中科技冷戰」雖為各自媒體與網路渲染，但是截至目前為止，主要體現的還是美國與中國大陸華為在技術與服務市場的雙重圍堵與反圍堵。此外，美國防制措施還包括針對中共藉「千人計畫」等措施，鎖定美國高科技產業營業秘密與高等教育機構科研實驗室，以人員情報及網路攻擊遂行滲透竊密，而中方對這些措施也有反彈。華為的圍堵與反圍堵模式，已開始複製擴散，美國對於「抖音」的疑慮即為一鮮明例證。

華為即使面對美國圍堵衝擊—依影響程度排列依序為「安謀（ARM） 停止交易」、「Google 限制 Android 服務」、「射頻晶片（RF）零件」和「英特爾（Intel）製伺服器用晶片」，其他還包括社群媒體與App停止提供服務，仍在營運獲利上有所成長。然而，由於軟體相容性受限，華為後續推出的手機新機型，包括率先全球推出的5G手機，在中國大陸以外的市場銷售受挫，只能仰賴中國大陸國內市場以民族主義情緒支撐其營收。華為的反制措施，除大肆宣傳營收不受美國封鎖的影響，也在美國興訟，控訴美國政府的不當干預。

[1] Michael Schuman, “China’s Likely to Lose a Tech Cold War,” *Bloomberg*, June 11, 2019, https://www.bloomberg.com/opinion/articles/2019-06-11/why-china-is-likely-to-lose-technology-cold-war-with-u-s.

一、美國對華為的圍堵

首先，在技術層面，科技冷戰迄今最具體的呈現，是在於美國切斷中國大陸資通訊產業技術與服務系統之供應鏈，迫使中國大陸必須尋求自力發展之軟體作業系統暨相容之App、硬體之記憶體晶片以及資料傳輸之5G通訊天線、基地台、資料節點、處理器，甚至包括光纖海纜與接收站。

中國大陸在技術方面，迄今仍欠缺形成足以與美冷戰對峙的「核武級」技術。中國大陸不僅在硬體的半導體晶片與快閃記憶體方面，宣稱2019年年底即將量產的「長鑫」動態隨機存取記憶體（DRAM），據信與美國仍有5至6年的差距，[2]而快閃記憶體則因良率趨近於零而陷入停滯困境。在軟體作業系統方面，華為即將推出的「鴻蒙」作業系統未能持續與美國微軟、蘋果之作業系統或臉書等社群媒體服務相容，不僅市場預期不樂觀，中國大陸也承認該系統未臻成熟。因此，中國大陸一方面釋放「長鑫」與「鴻蒙」等軟硬體自主的訊號，並以民族主義驅動消費者購買華為新推出之5G手機，衝高市場銷售量，以彰顯華為雖受困仍大有可為之氣勢；另一方面則謹慎營造其科技自主論述，不諱言其硬體技術差距與作業系統使用友善性，均仍有相當大的精進空間。

其次，在市場層面，美國則積極遊說並施壓各國排除華為5G，但力有未逮，連「五眼聯盟」（Five Eyes）的組成國都未必買單。前英國首相梅伊（Theresa May）允許華為向英國5G工程提供通訊天線等非敏感核心設備。英國聲稱將限於非敏感核心網路，例如天線與基地台，才能採用華為5G系統。此外，身為北約盟國的德國，其首相梅克爾（Angela Dorothea Merkel）也不主張排除華為5G系統，因此德國也可能比照英國區隔核心網路與非核心網路的作法。

敏感核心網路包括設備認證、語音和數據傳輸、計費等運算功能，而非核心網路則為天線與基地台等傳輸電波以接取（access）核心網路的設施。若依照華為的5G部署規劃，其提供的完整解決方案（total solution）包含基地台、核心網、承載網與終端等產品和技術服務。換言之，英國與德國可能允許採用華為5G的範疇，其實包括：基地台、承載網與終端等產品和技術服務。另一方面，美國的國安官員則強烈質疑，隨著5G時代帶來的寬頻與快速運算，核心網路與非核心網路在4G時代存在的界線將逐漸消失。因此，想要降低風險，就得要全面禁止採用華為5G網路。

敏感核心網路設施不僅是關鍵資訊基礎設施的要素，其運算能量也是未來5G鏈結物聯網的「工業4.0」關鍵核心。因此，敏感核心網路的資訊安全將對供應鏈安全影響甚鉅。在供應鏈與關鍵資訊基礎設施中，隨著資訊科技（information technology, IT）與作業科技（operation technology, OT）界線漸趨模糊，不僅氣密隔離內網的工控系統資訊安全防護屢遭攻破，也等於讓敏感核心網路與非敏感核

[2] Diego Oré, "Huawei says it is readying possible Hongmeng software roll-out," *Reuters*, June 14, 2019, https://www.reuters.com/article/us-huawei-tech-hongmeng-launch/huawei-says-in-process-of-preparing-hongmeng-software-roll-out-idUSKCN1TE3E0.

心網路之間的安全隔離逐漸失效，這將增加關鍵資訊基礎設施保障與供應鏈的資安風險。

「五眼聯盟」及北約盟國若依循英國與德國可能的作法，在非敏感核心網路採用華為設施，即使成功隔離敏感核心網路與非敏感核心網路，若在非核心的使用端與通訊傳輸網路間，有別於過去運用wifi或藍芽，而全面改採用5G，進行邊緣運算（edge computing），並設置後門回傳運算結果，一樣可獲取大量情資，遂行即時大規模的網路竊密與監控。據此，當外界仍質疑華為會否成為中共政府遂行網路竊取機密及大規模監控的幫兇，英國與德國一旦在非敏感核心網路採用華為5G，將因核心與非核心之間，在安全風險管控與技術層次上都愈來愈難以區隔，讓「五眼聯盟」與北約盟國在國家間的情報交換，增添洩密風險，並使反制網路竊密與監控的反情報作業更形複雜。

二、中共與華為的反圍堵

前述的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。

(一)華為的「無間諜協議」提議

對於許多國家而言，華為 5G 不僅物美價廉，其售後服務具有更大的吸引力。由於 5G 技術尚未成熟，在數據傳輸品質與穩定性上，必須由 5G 設備供應廠商持續測試與改進。然而，這也意謂設備供應商提供服務與設定參數後，可能就掌握使用客戶的數據。若是對供應廠商不是完全信任，自然有安全疑慮。美國對華為就以華為總裁任正非具解放軍背景、華為資通訊產品暗設後門裝置，以及中共之《國家情報法》要求中國大陸公民與業者配合中共政府蒐集情報之三大安全憂慮為由，以「五眼聯盟」為起點，發動全球抵制華為 5G。中共反制之道，即由華為聲稱願意與德國、英國以及其他國家政府，簽訂「無間諜協議」（No Spy Agreement）。考量網路安全技術層面，若要有效防禦網路攻擊，「無間諜協議」其實技術層面意義不大，主要是在國安層面的宣示安撫意味濃厚。

美國為圍堵華為5G設備所提出的主要安全疑慮，就是華為會在軟硬體裝置上裝置後門，將資料非法傳輸回中國大陸。華為過去採用的反制論調，是以技術安全驗證為主，論證自身的軟硬體設備經得起使用國公私部門的驗證。雖然華為軟硬體如同其他廠商產品一樣存在資安漏洞，但以其在英國、德國設置實驗室之測試結果為例，強調並未發現華為有裝置後門之行徑。美國為了反制華為技術無安全疑慮之論述，特別強調5G技術尚未成熟，必須由5G設備供應廠商持續測試與改進，故設備供應商除可藉此掌握使用客戶的資料，並能於必要時，藉更新軟體或維修硬體以裝置後門。

華為借鑒德國於2013年對美國提議簽署網路「無間諜協議」（美國後來予以婉拒）、俄羅斯與中共於2015年5月簽署的《網路互不侵犯條款》（*Cyber Non-aggression Pact*），以及2015年9月美國與中共簽署的《美中網路協議》（*U.S.-China Cyber Agreement*），積極對德、英兩國倡議簽署「無間諜協議」，強調華為除了不會裝置後門，也將不接受中共政府提供用戶資料之要求。現在華為將目標轉向亞洲，開始對印度提議簽署類似性質的「無後門協議」，但由於過去華為在印度的資安紀錄欠佳，而且印度對中共的安全威脅有所忌憚，故印度各界迄今對此提議興趣不高。[3]

(二)中共官方配合華為反圍堵舉措

美國對華為的安全疑慮，還包括華為總裁任正非具解放軍背景，以及在中共的《國家情報法》下，華為必須配合中共政府要求，將資料提供情報部門。如此一來，華為從後門竊取的資料即可為中共「國家安全部」等情報部門所用，對使用華為5G的國家而言，形成重大的國家安全威脅。英國智庫「亨利·傑克遜學會」（The Henry Jackson Society）於2019年5月中旬發表的研究報告，即為最有力的例證。該學會研究人員在研究大量華為員工簡歷後，發現華為與中共情報部門和軍方的聯繫，以及許多華為員工與中共安全部門及軍隊曾經合作的經歷。[4]然而，科技產業員工與國安部門合作計畫，其實並不少見，故該智庫報告尚不足以坐實美國的指控。

前述所呈現最大的癥結，還是在於中共的《國家情報法》所造成的安全威脅。但僅有華為高層單方面承諾不接受中共官方要求提供資料，還不足讓其「無間諜協議」具有說服力。中共駐英大使利用回應「亨利·傑克遜學會」研究報告的機會，趁勢表態不會要求華為替中共情報部門提供用戶資料，並表示英國若採用華為設備，華為不會被當作蒐集英國情報的工具。中共官方此舉無異於替華為的「無間諜協議」背書，在美國對華為全力圍堵之際，中共官方除在「孟晚舟事件」後抵制加拿大，此刻在美國川普政府對華為箝制尚未實質鬆綁之前，更積極出擊，配合華為倡議，以突破美國的圍堵。

（三）中國大陸將更難以推動海外科研合作

伴隨中國大陸境內與世界多國的5G布局與智慧城市建設，中共勢必加強鼓吹與推銷中國大陸的華為5G布建及其他諸如「抖音」之短影片軟體。中共為消除各國安全疑慮，甚至可能由官方出面積極為「無後門協議」背書。但隨著「學習強國」App暗設後門以及「中譯語通」協助中共國安機構在新疆從事大規模監控等種種疑雲的擴散，預料將讓中國大陸5G「無後門協議」前景愈加不樂觀。此外，中共國企或者私營之科技營運商為確保創新技術可持續產出，過去積極投資或捐助海外科研高等教育或研究機構，隨著技術用戶個資經後門而外洩到中國的疑雲

[3] Rahul Satija, "India still wary of Huawei's 5G despite 'no back door' pledge," *Nikkei Asian Review*, July 8, 2019, https://asia.nikkei.com/Spotlight/Huawei-crackdown/India-still-wary-of-Huawei-s-5G-despite-no-back-door-pledge2.

[4] Bob Seely, Peter Varnish, and John Hemmings, *"Defending our Data: Huawei, 5G and the Five Eye," The Henry Jackson Society Report, May 2019,* https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf.

升起，加上先前即甚囂塵上的竊密風波衝擊，以及美國從2018年延續到2019年反制中共「千人計畫」風潮，未來中國大陸科技廠商之海外產學或產研合作將因諸多資安疑慮而愈發困難。

（四）華為與海纜業務布局

根據《法新社》2019 年 6 月 3 日報導，華為的合資企業、全球第四大海底電纜業者華為海洋（Huawei Marine Networks）將出脫他們的大部分股份。根據上海證券交易所的資料，江蘇光纖通訊網路商亨通光電股份有限公司，將買下華為海洋 51%的股份。華為海洋已成為海底電纜工程界第 4 大業者。除了參與約 90 項海底電纜鋪設或升級工程，更負責不少重大的海底電纜工程，包括 2018 年 9 月連接巴西與喀麥隆之間的 6035 公里海底電纜完工，橫跨墨西哥加州灣的海底電纜則即將完工，而連接歐亞非三大洲的 1.2 萬公里海底電纜也在 2019 年開工。2015 至 2020 年，華為海洋預計鋪設完成 28 條海底電纜，占這段期間全球完工數量近 1/4。華為可藉華為海洋在海底電纜的全球擴張，介接其全球擴張的 5G 建設，構成不受制於美歐國家的全球網路基礎設施。[5]

美國全力抵制華為 5G，強調 5G 安全風險不分核心與邊緣，而海纜傳輸一直是監控資料流的目標，尤其華為持股 51%的華為海洋已成為全球第 4 大海底電纜工程商，美國也絕對不會予以輕忽。由於華為海洋可以接觸海底電纜，可能暗中裝設監控設備或是引導資料傳輸轉向的裝置，一旦爆發衝突時，便能隨時切斷整個國家的網路連線。另一方面，美國電信業者與網路內容提供業者也不樂見華為在海底電纜的擴張，畢竟華為可能藉此確立其通訊傳輸標準的全球領導地位，進而威脅美國的國家競爭力與國家安全。美國的國安單位因此發動類似抵制華為 5G 的圍堵攻勢，先於 2017 年藉由「五眼聯盟」成員澳洲，試圖擋下華為海洋承建連接雪梨與索羅門群島的海底電纜合約，聲稱這將讓中國大陸有能力透過雪梨電纜登陸點連到澳洲網路系統，形成資安風險。澳洲隨後宣布出資鋪設這條電纜，並將工程轉包給一家澳洲廠商。類似抵制華為 5G 作為之成敗互見，在 2018 年 9 月，美國、澳洲與日本即未能成功擋下華為海洋與巴布亞紐幾內亞簽訂海底電纜工程合約。

華為在 2019 年 6 月初決定出售華為海洋股份給中國大陸本土企業，極可能是以限縮業務、累積財力，作為因應川普下重手之避險手法。未來若受歐美進一步圍堵抵制其 5G 系統，則將可能重新購回，讓自身可以由海纜到接收站、以及 5G 系統之資料傳輸，一直到 5G 手機、含晶片在內的手機元件與其作業系統，都一一發展出自主系統，以擺脫歐美箝制，並以中國大陸以及「一帶一路」國家為市場，期能在系統運作及資料應用上有所突破，形成足以與歐美分庭抗禮的局勢。

（五）中共營造科技自主論調

至目前為止，所謂「美中科技冷戰」所體現的，主要還是美國對中國大陸華為在技術與市場的雙重圍堵，包括社群媒體與App停止提供服務，造成2019年5至

[5] Adam Satariano, "How the Internet Travels Across Oceans," *New York Times*, March 10, 2019, https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html.

6月華為智慧型手機銷售下跌4成，華為因此暫緩推出新型筆電及折疊式手機。[6]為穩固市場，華為甚至開始在菲律賓推出新銷售方案，將來華為智慧手機若不適用Facebook、Instagram、WhatsApp、YouTube和Gmail，可享全額退費。[7]然而，中國大陸在技術方面，迄今仍欠缺形成足以與美歐匹敵的技術。因此，中國大陸一方面釋放軟硬體自主發展的訊號，並以國內市場支撐銷售量，另一方面，則謹慎地營造其科技自主論述，避免科技民族主義在網路上暴衝，造成國際負面觀感而導致進一步反彈與圍堵，如此反而不利於中共刻意營造之受害者與被迫害形象。

肆、民主科技聯盟 vs.中俄非民主陣營

「美中科技冷戰」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「美中科技冷戰」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，進一步將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，科技冷戰藩籬界線的劃訂，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。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。根據中共國務院工業和信息化部所轄「中國信息通信研究院」2018 年 9 月發布的《人工智能安全白皮書》指出，中共官方所認定的資訊安全，不單是資訊傳播安全，還涵蓋了資訊內容安全。[8]據此，網路媒體內容審查的監管，便落在「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，準備以「網路生態治理」為名，要求網路資訊內容服務平台業者，擔負起內容審查的責任。

---

[6] Dan Strumpf, "Huawei Postpones Launch of Mate X Foldable Phone," *Wall Street Journal*, June 14, 2019, https://www.wsj.com/articles/huawei-postpones-launch-of-mate-x-foldable-phone-11560502468.

[7] Zak Doffman, "Huawei Special Warranty Offers '100% Refund If Google And Facebook Stop Running'," *Forbes*, June 18, 2019, https://www.forbes.com/sites/zakdoffman/2019/06/18/first-huawei-offers-of-100-refunds-if-google-and-facebook-apps-stop-running-appear/#50a3e00160c6.

[8] 中國信息通信研究院，《人工智能安全白皮書》，2018 年 9 月，頁 4，http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020180918473525332978.pdf。

對於內容審查標準，中共官方對於網路內容管制仍以負面表列居多。習近平於 2019 年 1 月 25 日在中共中央政治局第十二次集體學習時，強調官方傳媒及黨媒必須要加速融合各式網路新媒體，「探索將人工智慧運用在資訊蒐集、製作與傳播，以主流價值導向駕馭演算法」。這意味著官方傳媒需要轉型成為網路資訊內容服務平台業者的主體，方能承擔資訊內容安全審查之責任。依照《網路生態治理規定》所擬，網路資訊內容受鼓勵的有七項，遭禁止製作的違法資訊及不良資訊則各十項，顯見中共官方對於網路內容管制仍以負面表列居多。這樣的做法，除讓網路資訊內容服務平台業者在執行審查實務上有較為具體之標準可以依循，也有助於平台業者依照一定標準設計演算法以限縮內容審查範圍。

此外，北京在消極管制網路論言論行為內容與傳播手段之餘，轉為積極主導輿論走向。習近平所強調的官媒黨媒藉助人工智慧演算法，以強化官方價值輿論的主導性，各黨國喉舌紛紛呼應，除依指示積極結合諸如「抖音」、「快手」等工具，希望打入年輕族群，更強調在傳播手段上，藉助演算法之推薦技術，加速官方輿論之散播，並期能依照大數據分析後，針對個別特性之閱聽族群，以精準輿論導引與資訊傳播，形成網路聲浪，塑造官方輿論為主流輿論之聲勢。

人工智慧應用雖強調機器自主學習，但北京對於人為介入並未鬆手。在資訊內容方面，北京仍著重於資訊內容安全的管制面，對於前述負面表列之禁止與不良資訊，除列為有害資訊，並強調結合社會信用體系，對製作及散播有害資訊者施予聯合懲罰機制。習近平所謂的「以主流價值導向駕馭算法」，就是排除自主性人工智慧，並高度倚重人為監管的演算法，不斷調整負面表列清單，並視機器學習後的成果調節演算法。按照《網路生態治理規定》所擬，用來管制網路媒體內容與傳播手段的人工智慧科技本身，也必須要建立符合官方價值觀的推薦模式與人工干預機制，如此不僅為人為干預演算法奠定合法基礎，也毫不避諱只要依照官方價值，即為依循主流價值的演算法內建偏見。

中共運用官方強調管制與威權的價值偏見，將人工智慧應用於諸如網路內容審查、辨識虛假訊息與輿情監測之資訊內容安全，這方面舉措已展現相當成果。前述中共國務院工信部「中國信息通信研究院」的《人工智能數據安全白皮書》指出，百度所推出的「人工智慧+廣告打假」，僅2018年上半年，所處理的有害資訊就達145.4億條之多。2019年「阿里巴巴」推出「人工智慧謠言粉碎機」，對新聞內容的可信度識別，在特定場景中的準確率已達到81%。此外，「中國資訊通信研究院」基於所積累的標準樣本資料庫，開展對淫穢色情、涉恐涉暴等違法資訊識別的模式訓練，初步實現基於人工智慧技術的不良資訊檢測能力，識別準確率達到97%以上。[9]可以預見，北京勢將以網路生態治理之名義，運用網路內容審查所累積之機器學習與演算法，設計出足以製造虛假輿論訊息、具影響力的人工智慧演算法，以及足以迅速散播的網路媒體推薦模式，為境內維穩所施行之輿論戰、心理戰等資訊作戰預作演練。

[9] 中國信息通信研究院，《人工智能數據安全白皮書》，2019 年 8 月，頁 21-22，http://www.caict.ac.cn/kxyj/qwfb/bps/201908/P020190809481299621393.pdf。

中國大陸的人工智慧應用於產製傳播內容，並將逐漸輸出境外，以竟「影響力作戰」之功。中國大陸各網路資訊內容服務平台業者運用主要來自境內之大數據資料，進行前述網路思想暨輿論維穩。在北京對於管制有害訊息嫻熟後，運用演算法實現推薦機制，以及運用機器學習推展官方論述成為主流輿論的作法，將逐漸成為輔助北京遂行「大外宣」以對外輸出中共價值觀的利器。在中共對外宣傳內容屢遭譏為刻板不入心的時候，以人工智慧輔助之宣傳內容輸出，一開始或許因資料不足，未能掌握國外各地民眾對中國的認知與心態，而導致內容不能達到足夠影響力，但隨著對境外資料積累，以及演算法能逐漸因地與因人制宜，長久下來將可望呈現機器學習的成效，讓「大外宣」的內容與管道，更加貼近境外閱聽眾，達到其「影響力作戰」之目的。

最後，中國大陸發展的App影響力開始受全球矚目，主要是因為「抖音」的興起。「抖音」已然成為全球最受歡迎的短影片App，但曾因其未善盡平台管理責任，未將不當內容移除，而遭印度政府暫時禁用。此外，美國對於「抖音」會否將用戶資料回傳中國，存有高度國安疑慮。儘管「抖音」雇用公關與法律顧問，宣稱在美先行加強內容管理之平台責任，且用戶資料會儲存在非中國大陸的第三地，但基於美國資訊平台服務廠商備受威脅，國會仍執意以國安考量，對「抖音」展開調查，美國國防部也開始關注美軍使用「抖音」會否造成國安機密外洩的風險。美國產官界對付「抖音」的方式與步驟，類似複製當初對付華為的招數與步驟，而「抖音」也積極消除疑慮，這除了體現華為圍堵與反圍堵模式的逐步擴散，也彰顯背後民主與專制價值的互斥，並將進一步鞏固科技冷戰兩極陣營的對峙態勢，雙方相互施展影響力的交手也將愈形激烈。

伍、小結

「美中科技冷戰」在資通訊設施軟硬體安全上的考量，驅動生產供應鏈的移轉，尤其是移出中國大陸，以及未來一旦中俄非民主陣營成型，生產供應鏈將進一步移出「一帶一路」沿線國家。台灣除藉此機會迎接台商回流，更藉此爭取高科技大廠來台加碼投資設廠，在台灣打造高科技生產供應鏈。

隨著台灣在高科技產業生產供應鏈重要性隨之提升，全球高科技產業也將因此更在意台灣的安全處境。這將促使美歐陣營對於中共的威脅更加積極注意並提出警告，以維持台灣這重要夥伴的安全穩定。因此，美方也將台灣納入反制陣線，對抗中方陣營藉科技輔助之影響力滲透。與此相關的美台之間互動交流，從軍事、經貿、文化、傳播、教育、科技轉移，均將隨之加強，為台灣之安全，帶來更大的保障。

「美中科技冷戰」讓台灣在高科技產業生產供應鏈重要性隨之提升，相關挑戰也伴隨而來。首先，中共官方與科技業者為尋求突破技術圍堵，極可能進一步加強滲透竊取我方高科技營業秘密。產官學研需加強與國安部門反情報單位之聯

繫合作，共同協防我科技產業。對於包括科技專案計畫之科研項目，均予以加強內控，並在通報可疑事件後，配合執法單位調查，以反制中方竊取營業秘密。

其次，「美中科技冷戰」本身的安全考量，也可能促使美歐科技大廠基於台海安全風險而將資金廠房轉移回美歐。美國對於科技冷戰有其務實的實踐途徑，尤其是在聯合友盟以限制華為5G部署力有未逮之後，開始從自身的生產鏈安全要求做起，而其對於台積電的做法，就是最佳例證。一方面，在台灣的台積電仍可維持對中國大陸的市場，並繼續控制美國製造之關鍵技術與零組件成份。另一方面，台積電被要求回美國設廠，讓美國得以落實技術管制，優先轉移最新技術下單給台積電美國廠，並遵循其國防產業與政府採購不使用中國大陸製關鍵零組件的規範。台灣對此必須予以正視，雖然科技廠基於風險分散原則，不將關鍵廠房全都集中在一地，實乃務實之舉。但是，對於「美中科技冷戰」衍生之台海安全風險，台灣本身可提出交易成本與風險投資組合的實證分析與安全論述，除藉此作為積極因應，並進一步鞏固台灣在民主科技陣營中的價值鏈區位。

（責任校對：洪瑞閔、林政良）