5G 網路 引爆萬物互聯

生物學家威爾森（E. O. Wilson）提出三合一矛盾：認為人類仍處於舊石器時代的情緒、中世紀時期的制度、但卻擁有神般的技術。

5G 網路帶來「心之所向即身歷其境」之神般體驗，然在人性掣肘、政治角力的暗潮洶湧下，民主社會該如何接招？


5G

5G 的風險與國安

◆ 成大電機系教授暨資通安全研究與教學中心主任 — 李忠憲

5G 世代來臨，人類所有行為幾乎全在其覆蓋服務下，若系統建置、零件供應和服務營運所託非人，輕則 24 小時受到嚴密監視，重則隨時被敵人癱瘓。

美國封殺華為主因

5G 通訊設備是現代化國家必備的關鍵基礎設施，5G 建置或營運商是誰，便攸關國安問題，若系統建置、零件供應和服務營運所託非人，輕則 24 小時受到嚴密監視，重則隨時被敵人癱瘓，整個國家將陷入嚴重危機。

美「中」這場貿易戰，表面上是為平衡貿易逆差，實質上是美國希望中共能有結構性轉變。在中共進入世貿組織（WTO）後，利用自由世界得到很多好處，但其持續對出口補貼、嚴格管制市場不准外資自由進出、利用國企壟斷市場，加上「不求所有、但求所在」的政策，強迫外企轉讓

美國封殺中共的華為、中興等公司，不只是爭奪 5G 主導權，也不單純是資安問題，而是國安考量。

技術等措施，讓美國認為這些問題若未改善，貿易戰很難落幕。5G 世界，人類一舉一動難逃監視，美禁止華為與中興等公司，不止是爭奪 5G 主導權這麼簡單，更著眼於國安考量。

中共與俄羅斯、朝鮮向來關係密切，在非洲大幅投資與同地盟友組成同一陣線，在南海問題以金錢拉攏菲律賓、巴基斯坦、柬埔寨等，最近更在美國後院的委內瑞拉背後支持反美勢力。種種跡象顯示，中共試圖在各種戰場上對抗美國，這也是美國朝野兩黨對中共政策有共識的主因。因此，美國對華為或中興的作法，不單純是資安問題，而是國安考量，關係國家生死的 5G 基礎建設，讓美國封殺華為成為必然結果。

「數位獨裁」VS.「社會維穩」

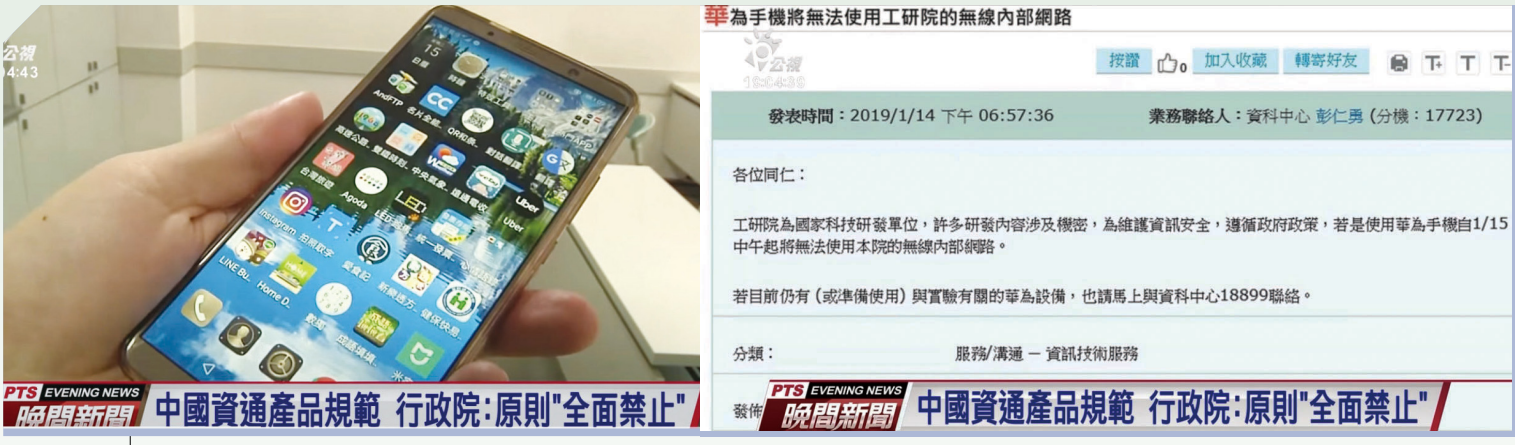
筆者在擔任國家高速網路與計算中心副主任兼資安長時，曾帶隊參加世界超級電腦年會，看到大陸展示多種電腦，每個攤位我都會去問一下，他們到底應用在那方面？據說很多都用在監控人民上面，例如影像辨識、人臉追蹤、人工智慧情緒判斷等等，真的令人感到害怕。

華為研發的高品質攝影機，能即時辨識臉孔，並根據表情推測使用者有無說謊，這將使極權政府可藉此「數位追蹤」，獲得「涉嫌人」的情緒狀態與心理意圖，認定其有影響國安之虞。（圖片來源：Kárlis Dambráns, https://www.flickr.com/photos/janitors/46931581075；路透社／達志影像）

民主臺灣不管任何人，聽到「數位獨裁」，全都感到非常害怕，其實「數位獨裁」在中共已經算是非常成熟的技術，也已經過時，最新版本就是在新疆施行的人工智慧恐怖統治，這是「數位獨裁」的進階版，又可稱為「數位恐怖」。

華為等高科技公司，在半導體製程進步後，所發展出來的超高畫質的攝影機，可在受控制的區域，進行即時的臉孔識別，不僅可以判斷這個人是誰，還能根據表情、眨眼頻率與瞳孔放大情形，來推測這個人的心理狀態，如果與之對談，甚至可以判斷其是否說謊。

利用這些高科技的設備與技術，可以鎮壓所有對政府不滿之運動，即使這些反抗運動都還只是存在於某些人心裡而已。因為在「數位恐怖」時代，極權政府可依「數位追蹤」獲得「涉嫌人」之情緒狀態與心理意圖，而認定其等有影響國安之虞；因此，當大規模抗議運動開始前，幾個抗議領袖可能就會被抓起來，這就是極權政府使用人工智慧來進行「社會維穩」時的可怕之處。



我國政府禁止機關同仁使用華為等陸製手機，惟恐這些手機於機關內部收集資料，再利用沒有管制的電信網路服務傳送予中共管理者。（圖片來源：截自公視新聞，https://youtu.be/Q8oUV6EObos）

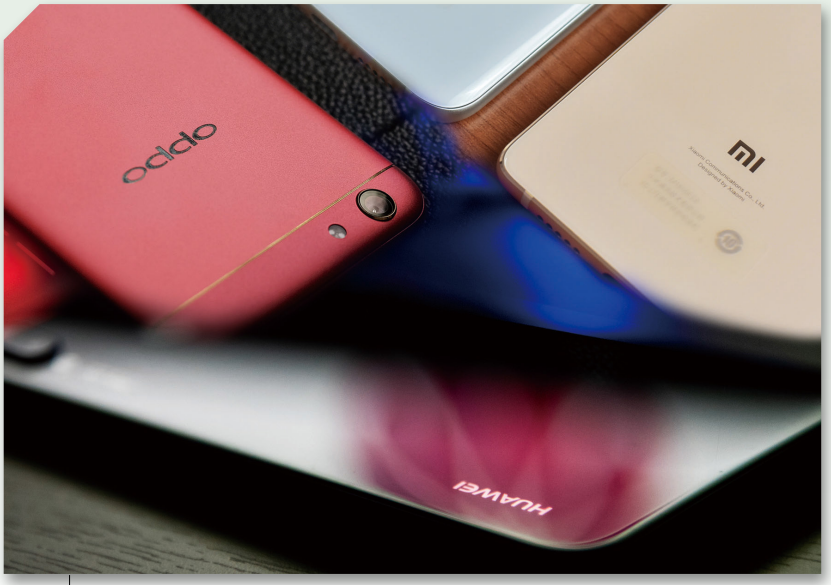
為何政府機關員工不能使用華為手機

很多資安研究者發現，華為手機裡有很多莫名其妙的東西，就是手機隱藏的後門程式，沒觸發時像大海撈針般難以發現。例如房子內如果發現一隻蟑螂，就能推測整棟房屋內應該也有很多蟑螂潛伏其中，但卻很難直接看到蟑螂們出現在屋內的各個角落，手機的後門程式也是如此。

華為手機暗藏後門，然後傳到中共管理者之終端設備。基本上政府不會自找麻煩，儘量不會去限制一般民眾使用華為手機。然為何要禁止我政府機關員工使用華為等陸製手機？因為依據過往之分析經驗，縱使對機關內部使用華為手機的員工進行嚴格的網路管控，這些手機一樣有可能在機關內部裡面收集資料，然後再利用沒有管制的電信網路服務傳送予中共管理者。這就是網路技術的基本特性，應用層可向下多工，利用不同網路層的連線傳送資料，因此，若只管理機關內部之資安設備，還是沒辦法完全防止洩密，所以機關必須嚴格管制員工使用華為手機。而且現在的手機功能非常強大，不管運算能力、儲存空間、網路傳輸速率與各種不同介面，完全可以成為一個分散式資料庫來源，所以要防止洩密，除管制外，很難有其他技術上的辦法更適用。

「陸牌」與「陸製」通訊設備之安全性比較

以國安而言，理論上應禁止使用敵製通訊設備，但因臺灣處境特殊，且資訊戰爭中，戰時和平之定義困難，所以政府處理此問題有相當難度。個人認為，以盤點「陸牌」和「陸製」通訊設備之安全性為優先考量。「陸牌」通訊設備在設計流程開始，能夠加入後門的機會較多，而「陸



「陸牌」通訊設備在設計流程開始，就有很高的機會加入後門，因此「陸牌」的資安威脅遠大於「陸製」。

製」通訊設備則是在製造過程後才有加入後門機會，因此，「陸牌」的資安威脅遠大於「陸製」。

資安防護並不在能杜絕所有安全威脅，亦即世界上沒有絕對安全，也沒有絕對資安，政府應做風險高低的優先順序表，再依可執行的資源配置由上往下嚴格管理。理論上臺灣是面對中共威脅的第一線國家，資安考量應最嚴格，然實際上因臺灣現階段政治局勢，施行較為困難，但至少應該比國際作法更嚴格一點。

人工智慧時代，「資料比錢更有用」

一般民眾在乎的是個人隱私，包括個人行蹤、拍攝的影片及照片，各種應用服務的帳號密碼，尤其銀行的資金往來，甚至自己感興趣的東西，或在網路及社群媒體瀏覽及發言的內容，都不願意讓別人知道；這些連對親屬都要保密的隱私資料，若外洩到國外的資料庫，變成別人茶餘飯後的八卦話題，您不會感到毛骨悚然嗎？

駭客攻擊中有一種稱為「進階持續性威脅」（Advanced Persistent Threat，下稱 APT 攻擊）的手法，就是針對個人或組織所做的複雜且多方位的網路攻擊，潛伏攻擊時間可能長達數週、數月甚至數年，不過，內藏後門的手機比 APT 攻擊更簡單方便，手機上任何資料，都可備份經由後門傳送到遠端，甚至直達敵方的國安單位。

之後，敵方的國安單位不僅知道您是誰、電話號碼、住哪裡、通訊錄內有誰，還可知道您跟他們的關係、長相、和誰吃飯、在手機上聊天內容、傳什麼新聞故事病毒給你最有用等等。人工智慧時代，「資料比錢更有用」，因此，呼籲大家不要貪小便宜，一定要慎選手機品牌。

「乾淨網路計畫」

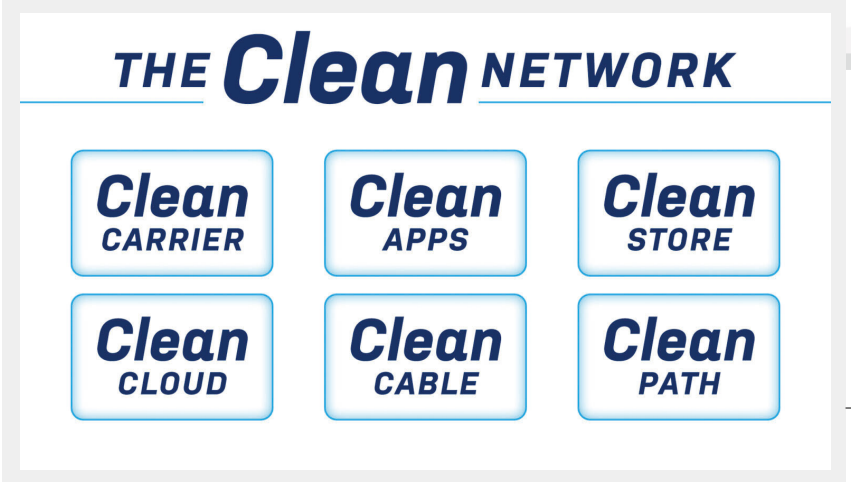
德國是世界上與中共最友好的西方國家之一，然在西藏抗暴 60 週年之際，原先非常支持西藏的德國，也因受中共經濟誘

惑而有相當大的退讓。惟德國第一電視臺最近在討論華為 5G 問題時，也開始提到其可能讓國家機密被監聽，甚至政府運作遭癱瘓等問題。

坦言之，華為技術還算不錯、也很認真經營，但華為是中共企業，得聽從國家政策指示；而中共又不是民主政體，且其法律早規定企業要配合國家蒐集情報，這就是華為安全性的關鍵所在。

中共 5G 建置帶來的風險，已經引起全球警覺，因此，2020 年 8 月間，美國發起「乾淨網路計畫」（The Clean Network），之後英國、波蘭、澳洲與瑞典等國家也陸續跟進。

面對始終不放棄以武力併吞臺灣的對岸，我們真的不能不小心因應 5G，或使用「陸牌」及「陸製」通訊設備所可能帶來之風險。



2020 年 8 月美國發起「乾淨網路計畫」，英國、波蘭、澳洲與瑞典等國家也陸續跟進，與美國簽署備忘錄，共同抵禦中共 5G 建置帶來的風險。（Source: U.S. Department of State, https://2017-2021.state.gov/the-clean-network/index.html; https://2017-2021.state.gov/the-transatlantic-alliance-goes-clean//index.html）

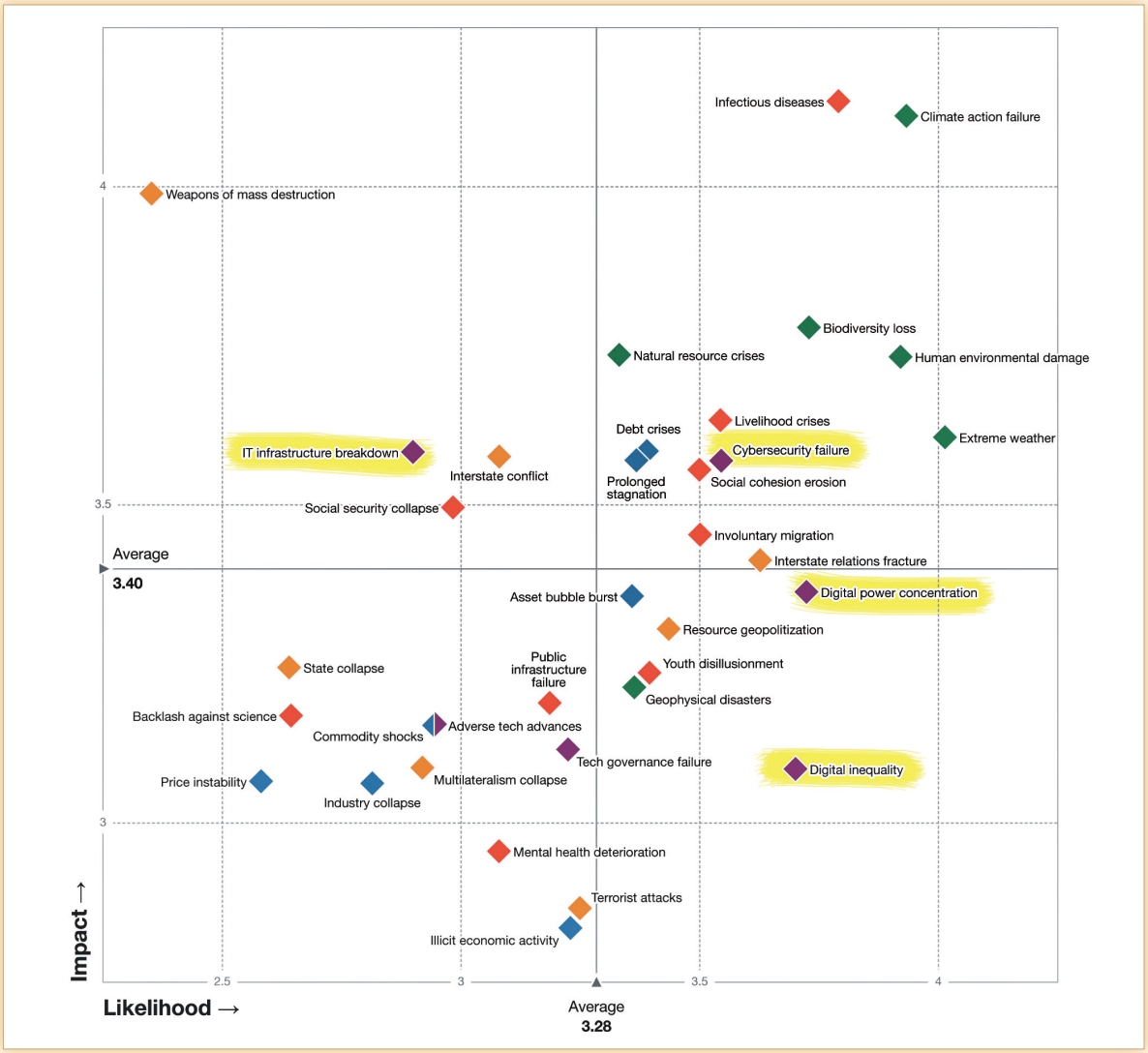
臺灣資安布局——由「布拉格提案」談起

◆ 淡江大學國際事務與戰略研究所博士候選人 — 陳永全

2019 年 5 月，全球 32 個國家齊聚捷克布拉格並公布「布拉格提案（The Prague Proposals）」，這是因應 5G 時代網路安全威脅的首次國際會議。

網路攻擊，已躍升為全球前十大風險

世界經濟論壇（World Economic Forum，下稱 WEF）每年都會發表「全球風險報告」（The Global Risks Report）。過去 15 年來的風險前 5 名都與環境有關。惟根據 WEF 2021 年「全球風險報告」（16 th Edition）顯示（如下圖），「資訊科技基礎設施故障」（IT infrastructure breakdown）已躍升為 2021 年全球風險具影響力的第 10 名；「數位權力集中」（Digital power concentration）、「數位不平等」（Digital inequality）及「網路安全失效」（Cybersecurity failure）則晉升為 2020 年風險加劇的第 6、7 及第 9 名。



2021 年全球風險報告，橫座標由左至右代表風險發生的可能性，愈右側，加劇的可能性愈高；縱座標代表風險發生的影響力大小，愈上方，影響力愈大。紫色菱形為科技類型的風險。（Source: World Economic Forum, The Global Risks Report 2021, 16th dition, http://reports.weforum.org/global-risks-report-2021）

「布拉格提案」超過 30 個國家參與，強調各國於發展 5G 時，應考慮國家安全、經濟、法治與設備商不法行為等因素以及後續的管理問題。（Photo Credit: NUKIB, Czech Republic, https://nukib.cz/en/infoser-vis-en/conferences/prague-5g-security-conference-2019）

我國與美國於 2020 年 8 月共同發表「臺美 5G 共同宣言」，深化臺灣與美國在 5G 資安上的合作關係。（圖片來源：外交部，https://www.mofa.gov.tw/News_Content.aspx?n=8742dce7a2a28761&s=1baaa18886648d2f）

「布拉格提案」

歐盟、北大西洋公約組織、美、德、日、韓、澳等代表，於 2019 年 5 月齊聚於捷克布拉格，為 5G 安全召開國際會議。會議中強調各國於發展 5G 時，應考慮國家安全、經濟、法治與設備商不法行為等因素，以及後續的管理問題。會議成果經主辦國捷克彙整，成為「布拉格提案」。

「布拉格提案」為首次探討 5G 議題之國際會議，其強調 5G 網路的開發、部署與商業化，必須建立在自由與公平競爭、透明以及法治基礎上，並提出 5G 安全及關鍵基礎設施防護等面向需進行國際交流與合作。參與國期望此提案內容能成為世界各國之資安防護共識。

「臺美 5G 共同宣言」延續「布拉格提案」精神

基於「布拉格提案」精神，我國與美國於 2020 年 8 月共同發表「臺美 5G 共同宣言」（Joint Declaration on 5G Security），臺美雙方宣示承諾在自由、公平競爭、透明及法治的基礎上，對 5G 通訊安全重要性的認知，通過加強對 5G 供應鏈的把關，確保 5G 通訊網路的安全，同時深化臺灣與美國在 5G 資安上的合作關係。

此項臺美 5G 安全共同宣言，代表美國與我國政府均認同 5G 通訊服務安全的重要性，為確保 5G 軟硬體供應商與供應鏈安全，應評估供應商是否可信賴，具體做法包括評估 5G 供應商是否在沒有獨立

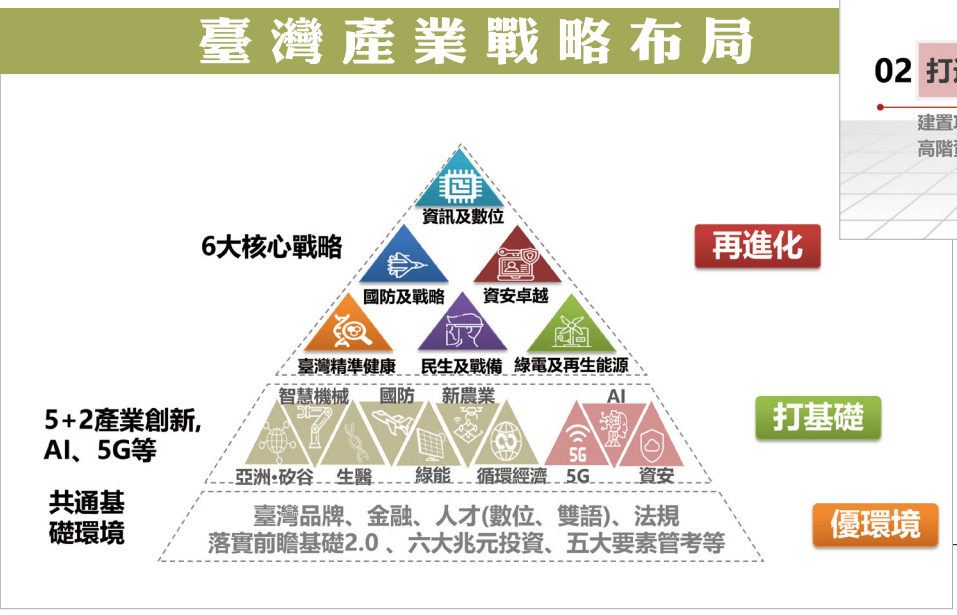
司法審查下，受外國政府控制；資金來源是否公開；還有供應商的所有權、管理結構、採購、投資等資訊是否透明；是否尊重智慧財產權等。共同宣言中也倡議透過定期的更新與評鑑，將現有不受信任的軟硬體供應商，移轉為可信賴的供應商，提升雙方的資訊安全，善用 5G 通信網路提供的各項服務，同時確保提供一個更安全、具韌性與可信賴的 5G 行動通訊網路生態系統，並為民間提供創新的機會，在自由公平的環境中，促進數位經濟發展。

他山之石，可以攻錯

蔡總統在 2020 年就職演說中提出 6 大核心戰略產業，其中一項就是「發展結合 5G 時代、數位轉型及國家安全的資安產業」。在「資安即國安」的戰略指導前提下，保持高度的資訊安全意識。在 5G 布設建置過程中，臺灣應竭盡所能，想方設法，完全排除具有資訊安全疑慮的軟硬體設備及相關供應服務。

基此，我國可參考以下先進國家之資安戰略：

一、英國 2016 年 11 月「國家網路安全戰略」（National Cyber Security Strategy 2016 to 2021），內容聚焦網路資安防禦、嚇阻、發展，並期望達成：1. 政府網路及關鍵基礎設施防護、2. 遏制網路犯罪、3. 發展網路安全相關科學研究等目標。



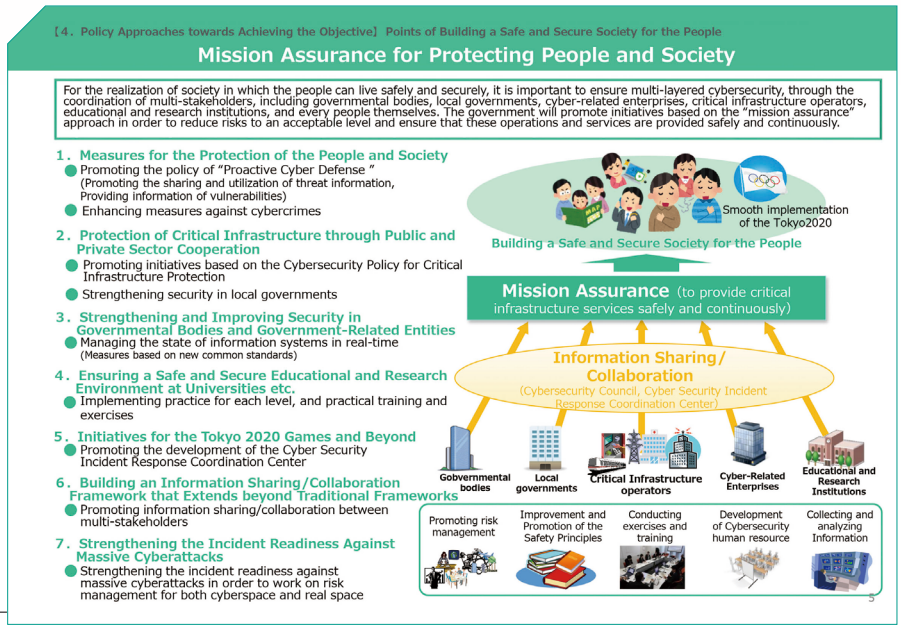
蔡總統在 2020 年就職演說中提出 6 大核心戰略產業，其中一項為「發展結合 5G 時代、數位轉型及國家安全的資安產業」。（圖片來源：國家發展委員會，https://www.ndc.gov.tw/Content_List.aspx?n=9614A7C859796FFA）

二、新加坡 2018 年 3 月「網路安全法」（Cybersecurity ACT 2018 (No.9 of 2018)），置重點於網路空間安全防護，包含關鍵基礎設施安全防護、網路攻擊反制與偵蒐、資訊、網路安全情資共享及建制資安服務供應商之管理機制。

三、日本 2018 年 7 月「網路安全戰略」（Japan's Cybersecurity Strategy），包含以下策略：1. 實現網路安全供應鏈及架構安全物聯網系統。2. 建構大學院校之資訊與網路安全教學研究環境。3. 制定網路犯罪之因應對策。4. 強化政府網路防禦應變、反制網路攻擊與應變大規模網路破壞之能力。

四、美國 2018 年 9 月「國家網路戰略」（National Cyber Strategy），置重點於採取主動防禦作為，保護國家資產

英國 2016 年 11 月「國家網路安全戰略」內容聚焦網路資安防禦、嚇阻及發展。（Source: Ministry of Housing, Communities & Local Government, UK, https://www.local.gov.uk/sites/default/files/documents/Building%20resilience%20together%20-%20William%20Barker,%20MHCLG.pdf）



日本 2018 年 7 月提出「網路安全戰略」，包含架構安全物聯網、制定因應網路犯罪有效策略、強化政府網路防禦應變，並建構大學院校資訊與網路安全教學研究環境。（Source: National center of Incident readiness and Strategy for Cybersecurity, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-shousaigaiyou-en.pdf）

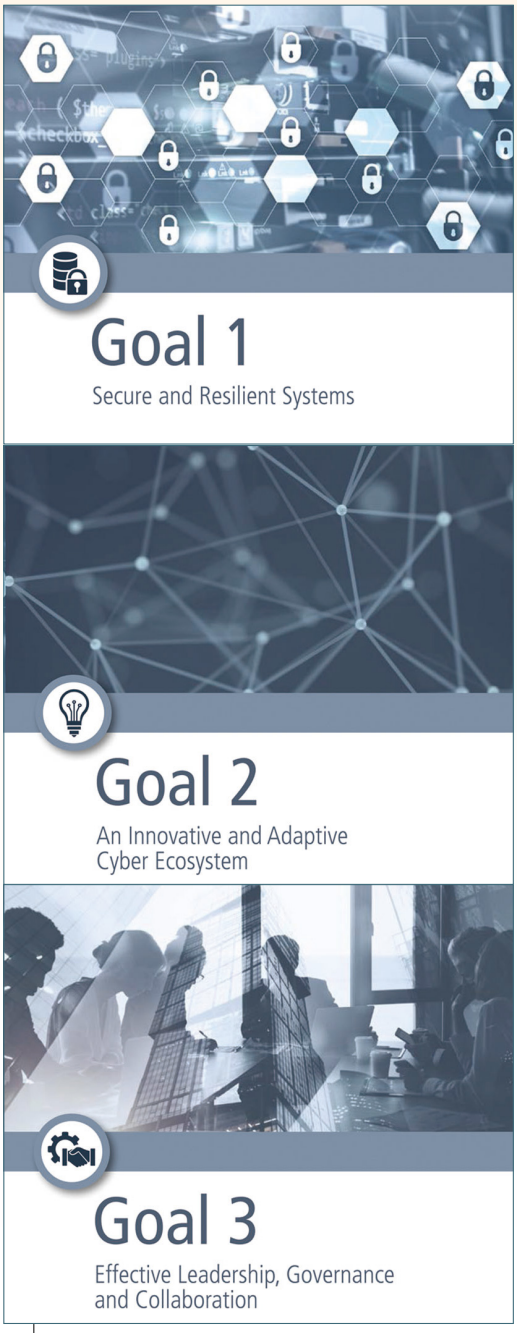
及民眾隱私安全，並提高惡意攻擊破壞者代價。

五、韓國 2019 年 4 月「國家網路安全戰略」（National Cyber Security Strategy），內容重點包括：1. 加強國家關鍵基礎設施安全、2. 提高網路攻擊應變與復原能力、3. 建立具信任的網路治理能力、4. 奠定網路安全環境、5. 培養網路安全文化、6. 領導國際網路安全合作。

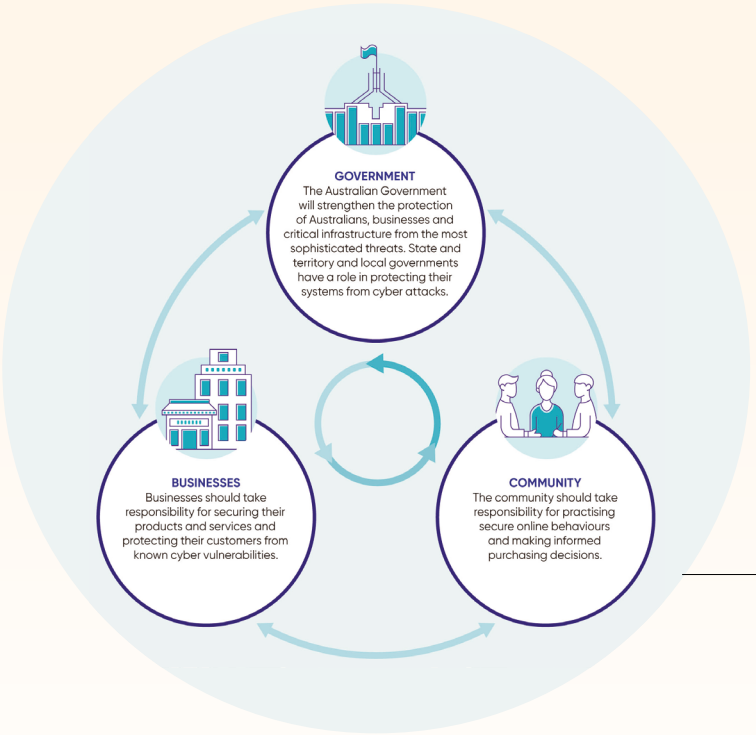
六、加拿大 2019 年 5 月「國家網路安全行動計畫」（National Cyber Security Action Plan 2019-2024），內容有 3 大目標：1. 強化關鍵基礎設施防護並增強網路犯罪偵查能力、2. 支持前瞻研究並協助創新企業發展、3. 國內、地方與民間具體合作，結合國外盟友共同塑造網路防護環境。

七、歐盟 2019 年 6 月「網路安全法」（The European Cybersecurity Act），重點為：1. 強化網路環境治理權限，2. 挹注更多人力與財務資源，3. 建立「歐盟網路安全驗證框架」驗證計畫，4. 評估網路資通訊產品、供應商服務及製程是否符合國際安全規範。

八、澳洲 2020 年 8 月「網路安全戰略」（Australia's Cyber Security Strategy 2020），重點為澳洲政府預計將於 10 年內投資 16.7 億澳幣，投資要項：1. 強化對人民、企業及關鍵基礎設施的具體防護能力，2. 保護企業產品和相關資通訊服務免受威脅或防護弱點的侵害，3. 透過公、私部門通力合作，促進網路安全。



加拿大 2019 年 5 月「國家網路安全行動計畫」包含 3 大目標。（Source: Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf）



澳洲 2020 年 8 月「網路安全戰略」指出，期望透過公、私部門通力合作，促進網路安全。（Source: Department of Home Affairs, Australia, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf）

綜合上述各國資安戰略，歸納重點：國家應於初始規劃階段，即建置安全的網路環境、建構國家網路資安聯防體系、培養大量優質的資安人才及尋求跨國合作之可信賴供應商等作為，方能超前部署，防範未然。

共同構建綿密的國家資安防護網

我國於 2019 年 1 月正式施行《資通安全管理法》，成為我國首部「資安專法」；調查局旋即於 2020 年 4 月成立「資安工作站」，具體落實了我國資通安全戰略的重要關鍵作為，持續強化網路安全的具體防衛機制，構建綿密的國家資安防護網。

未來更應**在戰略層級規劃**：賡續推動政府網路資安集中共享，擴大國際參與及深化跨國情資分享，制敵機先阻絕境外攻擊，提升科技偵查能量，防制新型網路犯罪。**在政策面向考量**：輔導企業強化數位轉型之資安防護能量提升，強化供應鏈安全管理具體作為，建構智慧國家網路資訊安全環境。**在教育面向推動**：擴增高等教育網路資安師資員額與教學資源，挹注資源投入高等網路資安科研，培育頂尖網路資安實戰及跨域人才。**在執行面向具體**：建立各領域公、私部門協同治理運作機制，增強人員網路資安意識與安全防護能力建構，公、私部門合作深化平、變時情資交流與相關預防、應變、復原演習演練等；建立各層級持續營運能力，及強韌、相依、可靠的網路資通訊安全環境。

備註：本文中 Cyber Security 均翻譯為網路安全，涵括資訊、通訊與網路部分。

智慧城市中的5G運用

◆ 調查局資通安全處 ── 雷喻翔

4G 與 5G 之間的差距，比起前幾代之間的應用鴻溝更為巨大，它幾乎實現了早年人們對於未來世界擘劃的景象。物聯網（Internet of Things, IoT）便是在 5G 技術下所達成的萬物皆可連網的境界，裝置連上網路進行通訊已不再侷限於桌上型電腦、筆記型電腦或是智慧型手機，家庭中的空調、掃地機器人，或是日常馬路上所見的路燈、紅綠燈等都將是物聯網世界參與者。智慧城市（Smart City）是物聯網最重要的應用之一，藉由物聯網的架構，智慧城市將可大幅改善公眾設施的運用、提升公眾設施所帶來的服務品質，而且還得以同時降低日常維運的成本，營造出有效率的政府並提升民眾的生活品質。

以下可由下列 4 個面向討論智慧城市：

智慧個人及家庭空間

雖然蘋果公司及安卓陣營已推出許多的智慧型穿戴式裝置，例如 Apple Watch 或健康手環等，但是其普及率相較於智慧型手機仍有一段距離。隨著 5G 的發展，穿戴式裝置將可預期地逐漸流行，而且不像目前的穿戴式裝置通常是以藍芽與手機搭配使用，在 5G 的環境，它將是獨立的上網個體，裝置可以依據它所感測的身體資訊做出對應的活動建議，並且可以即時地將資料傳送到雲端，讓醫療專家作為保健評估之用，不再需要透過手機當作中轉。

在 5G 的環境中，穿戴式裝置無需透過手機中轉，可直接轉送資料至雲端，讓醫療專家據此為保健評估；而智慧家庭更可讓使用者藉由快捷、安全的遠端監控，對家中家電發出開關、調節等指令。

智慧家庭則將提供一個更為舒適、安全的居住環境，藉由遠端的安全監控，可對家中的任一家電發出開關或調節指令。

智慧公共設施

智慧公共設施可藉由廣布感測器監測城市中公共設施的使用情形，像是路燈、交通號誌、路口監視器等，讓政府有效率地蒐集相關資料，進而做出對應的決策。除了經濟效益之外，智慧公共設施的另一個目的則是在急難發生的當下，讓政府可以在第一時間作為，避免民眾遭遇急難所帶來的損傷及災害。

智慧產業

近年來幾近爆炸式成長的資訊技術（包含大數據、雲端計算、人工智慧及 5G 等），吸引了許多公司極欲在其工廠或辦公環境中導入相關應用，用以提升產能、降低成本、建構友善且具吸引力的工作環境。資訊業或半導體產業無須贅言，傳統產業反倒是最有潛力的受益者。舉例而言，農業便是一個相當適合導入資訊技術的產業之一。原本廣大的農地僅靠人力及機械工具不懈地運作，所能發揮的效益有限，若能布下大量的智慧感測裝置藉以輔助農業開發，在農作物種植採收的過程中，對於農藥、肥料或水資源使用進行監測，不僅事半功倍，且能有效地節省開發成本。

智慧交通

繁忙的都會交通一直都是許多國家頭痛的難解題目，如果車輛及交通號誌也開始變得有智慧了，那會是如何的場景呢？理想的情境將是讓所有的大小車輛規律地遵守交通號誌，減少了不必要的繞路、不必要的塞車，更重要的是自駕車也將帶來

更少的汙染及更舒適的乘車環境。當然智慧交通不可能毫釐無錯地運行，難免會有偶發狀況，但是在車禍發生的當下，智慧交通系統可以立即協調並規劃出救護的路線，即刻排除車禍現場。以上由成千上萬車輛交織而成的複雜場景，若非借助 5G 技術，將很難實現。舉凡像是自駕車煞車所需的緩衝時間或是車輛接收車流量交通訊息的網路覆蓋率等，都需要藉由 5G 的低延遲、高覆蓋率的特性才得以實現。

安全議題

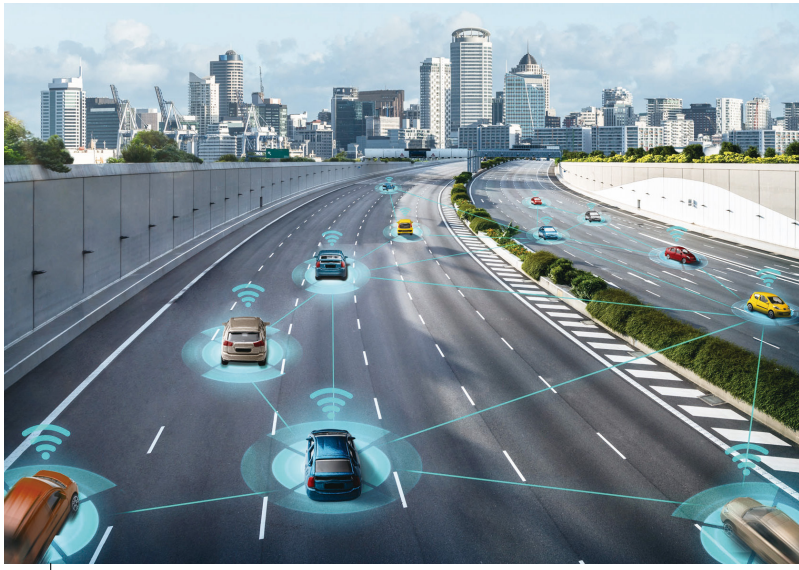
5G 固然便利，但也如雙面刃般面臨更多的資安挑戰。尤其隨著上網的裝置大量地增加，如何在便利的使用 5G 技術之餘仍能保持資安的要求，將是智慧城市的最大挑戰之一。以下簡介兩種 5G 應用於智慧城市可能發生的資安議題。

一、分散式阻斷服務（Distributed Denial of Service, DDoS）攻擊

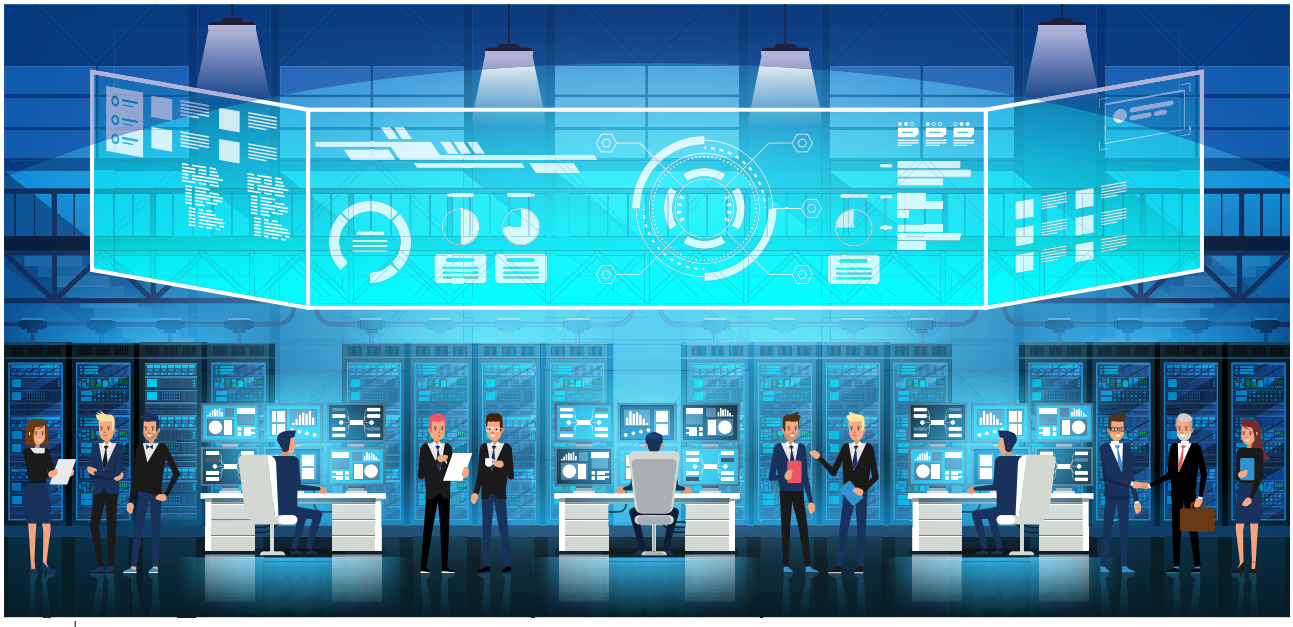
DDoS 並不是一種新興的網路攻擊模式，最早可回溯至 2000 年左右已有網路駭客使用此攻擊手法。由於此手法相對簡單、有效，且成本也不高，故攻擊案例層出不窮。DDoS 是利用大量受控制的電腦同時對目標伺服器發出連線請求，藉此癱瘓目標伺服器原本所能提供的正常服務。無論是網路層的 TCP 協定或是應用層的 HTTP 協定，在開始一個資料連線傳輸之前都需要先配置一部分的系統資源，然而伺服器的系統資源是有限的，一旦被無意義的連線消耗殆盡後，將無法正常使用。

5G 網路由於本身的特性，無線通訊資源也同樣會受到上述 DDoS 的攻擊，智慧城市的物聯網既然是萬物皆可連，可能連路邊馬路上不起眼的灑水器皆可連上網

透過 5G 網路，布下大量智慧感測裝置輔助農業開發，亦可對農藥、肥料或水資源使用進行監測，有效節省開發成本。



借助 5G 技術實現自駕，能讓所有車輛規律地遵守交通號誌，即便發生車禍，智慧交通系統也可立即協調並規劃出救護的路線，順利排除車禍現場。



由於 5G 網路的特性，無線通訊資源也同樣會受到 DDoS 的攻擊，若其中一個監控節點遭到惡意操控，整個網路將不再安全，因此異常行為的監測將是智慧城市極具挑戰的任務。

路，一旦大量的裝置被駭客惡意劫持後，即可透過同時發送網路連線要求進行DDoS攻擊。舉例來說，攻擊若是發生在智慧城市原本運作良好的車輛自駕網路中，若其中一個監控節點遭到惡意操控，整個網路將不再安全且有效率地引導車輛流向，交通安全岌岌可危。

異常行為的監測將是智慧城市正常運作下重要的一環，也是極具挑戰的任務。在某個設施的流量發生異常的當下，若能緊急切斷與該設施的資料傳遞，則能緩解系統遭受癱瘓的可能。

二、自攜電子設備（Bring Your Own Device, BYOD）的衝擊

所謂的自攜電子設備是指在工作的場域中攜帶自身的行動裝置（諸如智慧型手機、筆電或行動裝置等），在經過核准後透過自己的帳號連上工作網路。此種模式在現今新創產業蔚為流行，一方面公司可以降低硬體維運成本，另一方面員工可以更自由地連網工作。但與此同時，公司的敏感資料也將曝露在風險之中。智慧城市的物聯網設備過於多元，某個裝置上運行的作業系統、應用軟體等都不盡相同，且資料流也更為複雜，一旦資料流中的某一個裝置被有心人士遠端利用，機敏的企業資料將面臨洩漏的可能。因此，在 BYOD 盛行之下，安全性的多重認證將變得更加重要。機關必須嚴格落實資料安全性分級，並在對應的認證身分下允許對應的資料流在自攜電子設備中流動。

結論

智慧城市帶來了令人期待的生活遠景，但與此同時，它所帶來的衝擊若無法事前提出有效的因應，那麼事後的修補可能必須付出加倍的代價。

5G 時代的網路安全：以對華為施行禁令的妥適性為例

◆ 中興大學國際政治研究所副教授 — 譚偉恩

網路安全（cybersecurity）的維護工作在 5G 時代更加不易，因為需要更多的資源、更早的預防、更快的反應、更好的復原。

前言

全球現在除了臺灣與美國之外，很多民主國家都在思考與抉擇是否該禁止中國大陸的華為技術有限公司（下稱華為）參與自己國家關於 5G 的相關基礎建設，禁或不禁之間既有「網路安全」的考量，亦有「政治選邊」的壓力。5G 已被公認是許多國家未來 10 年內在社會與經濟發展上必須要走的方向，它是人類現有文明與通訊科技深度交織的成果。正因為事關重大，不少人認為應該禁止華為的產品，理由是這間公司與威權色彩濃厚的中國共產黨有關，基於合理的懷疑或推論，北京當局極可能利用華為及其研發的相關產品來從事諜報情蒐工作。因此，開放與華為貿易將無異於是自招風險，把網路安全置於中共的虎口之中。

上述對於中共政權的顧慮雖然是合理的，但對華為的禁令是否就是有效維護網路安全之方法？通訊科技在帶給人們更多便利性的同時，也必然增加更多的風險，[1] 從技術層次來說，5G 時代的網路安全需要的是分散與管理這些風險。

[1] Paul Mee and Rico Brandenburg, "Digital Convenience Threatens Cybersecurity," *MIT Solan Management Review* (April 14, 2020), via at: https://sloanreview.mit.edu/article/digital-convenience-threatens-cybersecurity/.

5G 的使用意謂著國家更加依賴行動網路的相關功能，像自動駕駛、遠距教學、視訊醫療、健康即時監測及許多跨時空地理的業務活動，而一旦 5G 網路無法正常運作，損失與損害將難以想像。

5G 的特點及優勢

5G 的使用意謂著一個國家將更加依賴行動網路和它所帶來的相關功能，像是自動駕車、遠距教學、視訊醫療、健康狀況的即時監測，還有許多跨越時空與地理因素限制的業務活動。其結果是，經濟與日常生活的效率變高，但過程中也變得更加脆弱，因為一旦 5G 的網路無法正常運作，損失與損害將難以想像。

當大家都在網路中相互聯繫，也就自然在網路中相互影響。相較於過去的網路只是聚焦在人與人的即時聯繫，5G 進一步讓人可以與許多設備即時聯繫，甚至做到遠端操控。同時，人工智慧的應用讓設備與設備之間也可以相互自動化聯繫，因此是一個史無前例的網路環境。

5G 時代下華為引發的安全疑慮

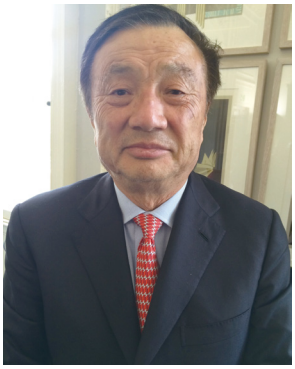
目前已在進行中的 5G 之爭並非只是幾間科技大廠於全球市場上較量市占率，[2] 而是同時涉及主權國家間（特別是美國與中共）下一個 10 年的權力消長。北京當局近幾年在科技研發這一塊越來越積極，而中國大陸的公司在 5G 相關設備生產上已

[2] 5G 通訊晶片的爭奪戰中，主要都來自國際的晶片大廠，如高通、英特爾、華為、三星等，皆為晶片專利的搶奪競爭者。在通訊網路規範與標準的爭奪戰中，主要則是以 Nokia、Ericsson 和華為 3 大通訊設備供應商（NEP、Network Equipment Provider）為主要競爭者。

是全球舉足輕重的行為者，其中最赫赫有名的供應商就是華為。[3] 文獻指出，高度的人事重疊存在於公部門的國安單位與華為公司。而華為創辦人任正非的背景也一直成為關注的議題，他曾在解放軍工程部門任職，然後以上校軍銜退役，於 43 歲創立華為。他的女兒曾任華為副董事長兼財務長，但在加拿大接受司法調查時被發現持有多年的中國大陸公務護照。[4]

華為引起的爭議不單只是與中共官方的關係，還包括其在共產黨的決策下輸出相關的電子監控設施給不少第三世界威權體制國家。有論者因此認為，中共是在全球推行數位威權主義（digital authoritarianism）。從許多消息來源觀之，華為不像是一般的民間企業，而是北京當局一項很重要的工具，[5] 而 2017 年中共施行《網路安全法》後，這樣的懷疑被更進一步確認，因為《網路安全法》明文要求中國大陸的企業應將資訊交給情資與安全部門進行管理，並遵守相關規定。[6]

至於在政府相關的補助方面，華為收到優惠待遇不單是一般貸款上的便利，還包括來自中共的中國發展銀行和中國進出口銀行給予總金額約 98 億美元的資助。除了上述與中共官方的聯繫外，用戶隱私權和軍民兩用科技的問題也是讓民主國家憂心華為的原因之一，畢竟這些資訊一旦淪為諜報工具，將對使用國造成嚴重的國安威脅。



華為公司的創辦人任正非（上圖）曾在解放軍工程部門任職，他的女兒（左圖）曾任華為副董事長兼財務長，在加拿大接受司法調查時被發現持有多年的中國大陸公務護照。（圖片來源：cellanr, https://www.flickr.com/photos/rorycellan/14101800091；路透社／達志影像）

[3] 中華人民共和國在全球資／通訊科技的價值鏈（the global value chains of information and communications technology, ICT）已是相當具有影響力的行為者，而華為又是之中 5G 設備與基礎建設的領先供應商。由於各國政府都很看重 5G 這一塊市場的前景，所以其實不少國家的相關產業都在一定程度上接受國家的資助，華為是特別受到北京當局支持的科技公司，與中共的國安部門聯繫甚深。參考：Mark Wu, "The "China, Inc." Challenge to Global Trade Governance," *Harvard International Law Journal*, Vol. 57, No. 2 (2016): 261-324; Douglas Black, "Huawei and China: Not Just Business as Usual," *Journal of Political Risk*, Vol. 8, No. 1 (2019), via at: https://www.jpolrisk.com/huawei-and-china-not-just-business-as-usual/; Scott Bicheno, "Huawei is Still the Leader on 5G Commercial Contracts," *Telecoms* (February 20, 2020), via at: https://telecoms.com/502562/huawei-is-still-the-leader-on-5g-commercial-contracts/.

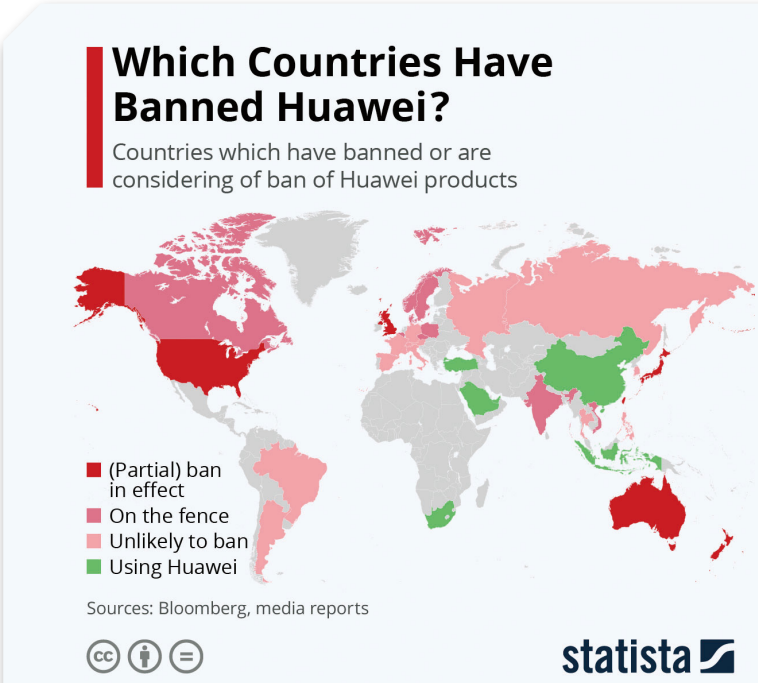
[4] Christopher Balding, "Huawei Technologies Links to Chinese State Security Services"；此外，Huawei's ownership structure is not transparent, raising suspicions of effective party-state control over the company.

[5] Rick Umback, "Huawei and Telefunken: Communications Enterprises and Rising Power Strategies," ASPI Strategic Insights 135. Barton: ASPI, 2019.

[6] 相關資訊可詳見：「《網絡安全法》施行前夕國家互聯網信息辦公室網絡安全協調局負責人答記者」，網址：http://www.cac.gov.cn/2017-05/31/c_1121062481.htm.

上述顧慮讓臺灣和美國成為全球最先對華為採行禁令的國家，避免華為參與自己的 5G 建設，後來有些國家（例如：澳洲和日本）也相繼跟進。由於中國大陸的許多企業很難區分是黨營還是民營，臺灣早在 5 年多前就全面禁止中國大陸製造的通訊零組件進入臺灣的 4G 系統。所以在臺灣的公家機構、關鍵基礎設施，以及任何可能危及國安的地方，都一律禁用中國大陸製造或生產的電信物件（devices）。[7] 相較之下，美國在川普任職總統期間，開始對華為施行禁令，而 2020 年 8 月更進一步限制華為取得美國的通訊設備和軟體，美國商務部同時將 38 家華為的子公司或關係企業列入禁止與美國公司合作的名單中。[8]

有別於臺灣和美國，歐洲國家在禁止華為的立場並不鮮明，甚至還帶著猶疑或不確定性。以英國為例，[9] 首相強生曾表示允許華為有限度地參與英國的 5G 建設，但這個決定引來美國的政治壓力，也同時讓首相面對自身政黨的質疑。隨著〈港版國安法〉生效，英國漸漸調整立場，強調

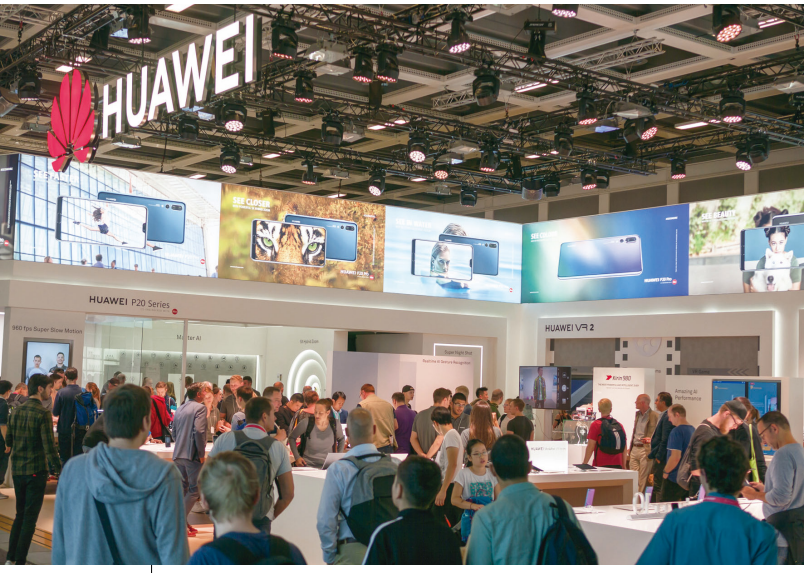


美國和臺灣為全球最先對華為採行禁令的國家，後來澳洲、日本等國也相繼跟進，圖為 2019 華為在全球的禁用情形。（Source: statista, https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products）

美國商務部在 2020 年 8 月將 38 家華為的子公司或關係企業列入禁止與美國公司合作的名單中。（Photo Credit: U.S. Department of Commerce, https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and）

[7] 我國行政院自 2019 年 1 月起即宣布，所屬之中央部會、國營企業、國家研究機構，還有具官股性質的中華電信、中華航空和兆豐金控等公司，全面禁止使用華為所生產的手機和電腦。此外，針對中國大陸籍公司所生產的硬體、軟體、網站，也皆加以禁用。不過，對於非公務以外的民間經濟活動或消費，則沒有禁止。

[8] USDOC, "Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List," via at: https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and.



歐洲國家多半在華為問題上陷入兩難困境，很多電訊業者都和它有業務往來，且歐洲市場也是華為在中國大陸以外成長最快速之區域。（Photo Credit: Matti Blume, https://zh.wikipedia.org/wiki/File:Huawei,_IFA_2018,_Berlin_(P1070188).jpg）

妥善保護國家安全為首要，並在去（2020）年 7 月中旬，英國政府宣布自 2021 年起禁止採購華為的 5G 設備，且要求本土的電信業者在 2027 年以前移除所有的華為設備。（參考英國 2020 年 11 月公布之《電信安全法案》）

英國以外的其他歐洲國家也多半在華為問題上陷入一個兩難困境；一方面在安全事務上已和美國有很長時間的合作，是關係緊密的同盟，雖然川普執政期間，雙邊合作不甚愉快，但終究要比跟北京當局來得好。然而，在另一方面，華為已是 5G 科技的領導者，很多歐洲國家的電訊業者都和它有合作及業務往來；同時，歐洲市場也是華為在中國大陸以外成長最快速之區域。在上述進退維谷的兩難下，持續來自美方的政治壓力，還有歐洲國家本身對於威權共黨體制的憂心，讓它們開始認真思考是否應禁止華為。事實上，歐洲國家的問題也是國際社會很多其他民主國家的問題。

禁止華為或另尋它途？

當具體分析一國的通訊網路會不會因為禁用華為設備，或是斷絕和華為的貿易往來後，就得以避免破壞和癱瘓，便會發現其因果關聯並不若想像中的那般必然。直言之，由於中共的國際形象不佳，世人很容易會擔心華為會透過各種後門程式竊取自己的穩私或國家機密。舉例來說，電信商沃達豐（Vodafone）公司在 2009 年和 2011 年的網路安全報告中，兩次提到華為提供之通訊網路裝置在軟體系統方面有漏洞，可能會導致未經授權的網路惡意攻擊連上 Vodafone 的相關網路系統，導致數百萬家庭和企業用戶的資訊安全受到侵害。又如 2019 年，波蘭官方以間諜罪名逮捕華為在波蘭分公司的員工王偉晶，因為他進行的情蒐工作已危害波蘭的國家安全。[10] 這些事證似乎與許多民主國家對於華為的擔憂相呼應，因此強化了禁用華為的必要性與正當性。然而，美國的微軟

[9] 除了英國以外，不少歐洲國家也陷入抉擇的兩難，以目前市場上的使用情況和普及率來看，歐洲要在短期間內移除華為的通訊設備並不容易。以 2008 年至 2020 年的情況來看，歐洲國家的 4G 建設中有半數以上和華為或中國大陸籍的科技公司有關。因此，在商討是否要禁止中共的 5G 通訊設備進入歐盟國家的市場時，會員國的立場是分歧的。

[10] Bloomberg News, How Huawei Became a Target for Governments, Bloomberg, January 23, 2019.

2019 年，波蘭官方以間諜罪名逮捕華為在波蘭分公司的員工王偉晶，因他進行的情蒐工作已危害到波蘭的國家安全。（圖片來源：截自三立新聞，https://youtu.be/X4tswF_3j48）

（Microsoft）也同樣被發現在程式設計上有類似「後門」的瑕疵。[11] 同時，俄羅斯也曾發現美國政府長期安插於普丁總統身邊的間諜。[12] 顯然，民主國家和與官方無涉的私人性企業並非沒有危害網路安全的可能。

科技總是為人類帶來新的挑戰，5G 在帶來便利性的同時也因為它技術上的創新而讓人們對其依賴性增加，從而提高安全上的風險。首先，由於物聯與互聯而開放之多種網路連接方式，導致受攻擊面明顯增加，讓 5G 的脆弱性變高，資料的控制與取得變得相對容易，但這並非禁止華為及其產品後就不會發生之問題。其次，隨著物聯網的發展，彼此相連的設備數目增加，提升了分散式阻斷服務攻擊（Distributed Denial of Service）的機會。然而，此種攻擊形態的來源國並不只有中共，美國、德國、英國、荷蘭，甚至越南、印度在量上都不亞於中共。[13] 第三，5G 網路著重軟體的特性讓其必須與更多軟體開發和更新程式的業者合作，一旦其中一個環節設定不當或是成為安全防範上的破點時，風險都會升高。最後，在可預期的未來，因為 5G 建設持續發展，一定會有許多問題相繼出現但又缺乏 5G 專業人員來解決，此種科技升級與轉型的過程本來就是必經的脆弱期與調適期。

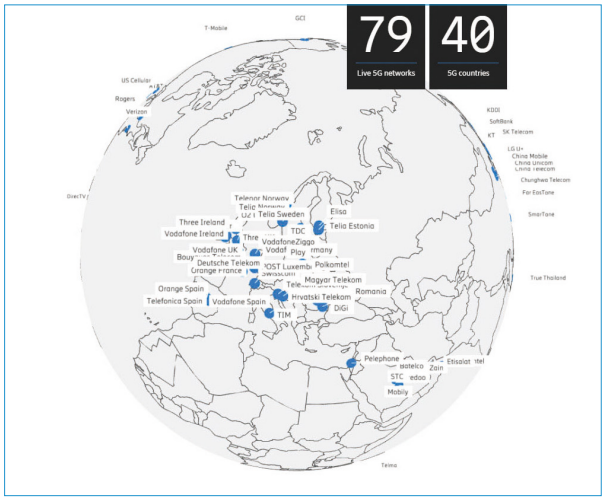
安全應優於價格

對華為及其產品施行禁令，排除這間中國大陸籍科技公司參與一國的 5G 基礎建設是有憑有據的做法，但並不是有效確保網路安全的策略。事實上，中共如果利用華為或其他法律註冊上並非中國大陸的科技公司來行使情報監控或網路攻擊，民主國家依然會面對網路不安全的風險。有鑑於此，讓本國 5G 市場多樣化，其實

[11] Ellen Nakashima, "NSA Found a Dangerous Microsoft Software Flaw and Alerted the Firm," *Washington Post* (January 15th, 2020), via at: https://www.washingtonpost.com/national-security/nsa-found-a-dangerous-microsoft-software-flaw-and-alerted-the-firm--rather-than-weaponize-it/2020/01/14/f024c926-3679-11ea-bb7b-265f4554af6d_story.html.

[12] "US Spy Worked in Russian President's Office," *France 24* (October 9th, 2019), via at: https://www.france24.com/en/20190910-usa-russia-spy-cia-asset-putin-office-intelligence-elections-extracted-clinton-trump.

[13] 詳見：Digital Attack Map, via at: https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16466.2&view=map.



Ericsson 已在十多國完成 5G 網路的鋪設，而在華為被美國施行禁令後，Qualcomm、Intel 亦成為市場上具有產品競爭力的新手。（Photo Credit: Ericsson, https://www.ericsson.com/en/5g; Linux Foundation, https://www.flickr.com/photos/linuxfoundation/albums/72157680650576335）

也是一種另類的民主化和開放市場的策略應用。**只是開放給業者的資格應以安全品質為最優先的考量，而非價格**。華為之所以有如今通訊科技霸主的地位，是因為從 2015 年開始在全球市占率一直穩居第一，2018 年的 3G 或 4G 設備市占率幾乎已占全球 30%。但當時多數國家並不重視華為與中共的聯繫，只在乎產品的價格，等到開始發現一些可能存在的安全疑慮，還有漸漸受到美國施加的政治壓力時，才考慮是否要對華為施加禁令。

5G 是未來 10 年攸關國家發展的重大項目，相關基礎建設的布局不能只從價格考量。事實上，愛立信（Ericsson）已在十多國完成 5G 網路的鋪設，而高通（Qualcomm）、英特爾（Intel）也都是華為在被美國施行禁令後，浮出市場的新手，但產品的競爭力未必較差，都是民主國家在營造自己 5G 相關環境時可以考慮的合作對象。

民主寶貴的價值之一就是多元，而開放市場讓 5G 服務業者多樣化，彼此維持良性競爭，才是管理 5G 時代網路安全的較佳方法。雖然這個方法不能全然避免網路攻擊或是相關的風險事件出現，但全面禁止華為也同樣無法避免。相較之下，多樣化的管理策略在網路危機發生時可以控制災損，並有替代方法可以即時提供救援。如果一國的經濟與科技水準不差，還可以再配合提升備用設備的儲量、端到端的加密（end-to-end encryption）、以及網路流量的監管等措施來優化自己的網路安全。

潛藏的潘朵拉魔盒

◆ 政風室主任 — 馬維駿

5G 通訊速度將比現況快 10 倍以上，帶來便利也隱藏危機，若惡意運用數位足跡，將在不自覺下引發難以預估的危害，如同「潘朵拉之盒」。

九頭蛇組織已非虛構劇情

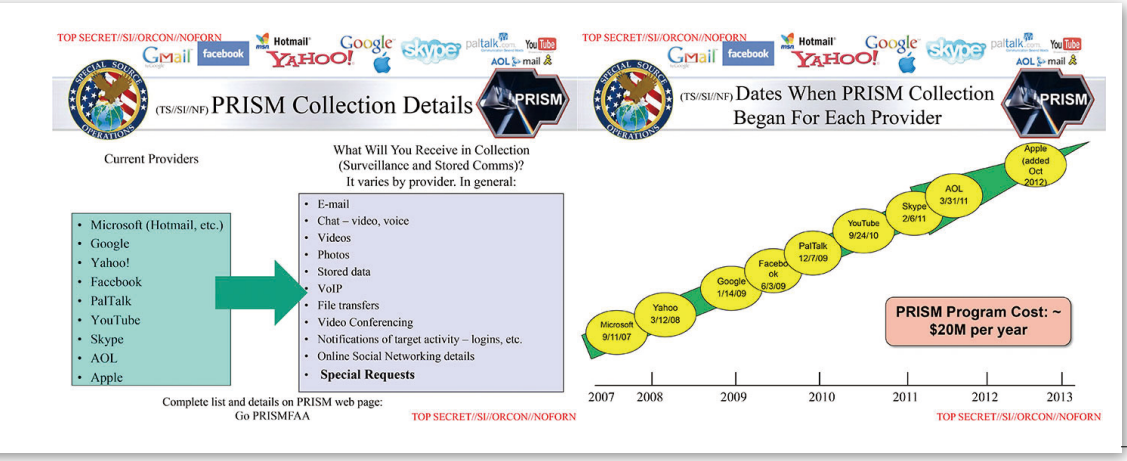
我們如今身處於第三波數位革命時代，正在全面推廣的 5G 網路傳輸技術具有「高速傳輸」、「信號低延遲回應」、「同時連結多樣裝置」等特性，配合更快速的「雲端計算」，遠端操控各項智能產品發揮更大效能，「生活與網路更加密不可分」，然而卻也因為「密不可分的智能產品」，留下更多的訊號傳輸紀錄—「數位足跡」。「數位足跡」具有危險性或機敏性？電影「美國隊長 2 —酷寒戰士」劇情，九頭蛇組織科學家索拉發明「索拉演算法」，將世界視為電子書，透過個人的

電影「美國隊長 2 ─酷寒戰士」中之九頭蛇組織科學家索拉發明「索拉演算法」，將世界視為電子書，透過個人的投票慣性、會考分數、銀行紀錄、病例、通聯紀錄、電子郵件等過去行為模式預測其未來行為。「索拉演算法」已非虛構劇情，而是現在進行式的真實！（Photo Credit: Marvel Studios, Walt Disney Studios Motion Pictures）

投票慣性、會考分數、銀行紀錄、病例、通聯紀錄、電子郵件等過去行為模式預測其未來行為，若該人隱含危害九頭蛇組織的風險，就發動航空母艦將其消滅。然而「索拉演算法」已非虛構劇情，而是現在進行式的真實情境！

著眼國家層次—網路監察蒐集數據作為戰略資源

現實中「索拉演算法」確有其事。閱覽維基百科，美國國家安全局（NSA）外包人員—愛德華·史諾登，在英國《衛報》和美國《華盛頓郵報》揭露 NSA 的「稜鏡計劃（PRISM）」。該計劃網羅眾多資訊公司參與，而參與公司包含「facebook、youtube、apple、skype 等知名企業」。該計畫自 2007 年發動網路監察，受監察之人員標的包括前揭公司的非美國客戶，或是任何與他國人士聯絡的美國公民；受監察之資訊標的包含電子郵件、視訊、語音、影片、相片、社群網路動態等「即時及既存訊息」，並透過操作智能產品攻擊特定目標。依據 2012 年統計，美國有 1,477 個情報工作計劃使用來自該計劃的資料。細思極恐！曾經網路是「保護面具」，如今我們每個人的「數位足跡」卻被未知眼睛窺探，並建構「真實的行為軌跡」及搜尋「可被攻擊的弱點」。



NSA 的「稜鏡計劃（PRISM）」網羅眾多資訊公司，監察電子郵件、視訊、語音、影片、相片、社群網路動態等「即時及既存訊息」，並透過操作智能產品攻擊特定目標。

廠商 Target 之所以比報導中的父親更早知悉女兒有孕，原因在於顧客刷卡消費後，電腦系統將自動記錄顧客的購買資訊，廠商以此建構「分析顧客喜好與需求的資料庫」，從中預測顧客需求，進而推薦商品。

無法察覺的侵略性銷售—運用數位足跡人格側寫，針對行為慣性誘導消費

如何運用「數位足跡資料庫」？不妨參閱 2012 年 2 月 16 日《紐約時報》這篇報導，題為《這些公司是如何知道您的秘密（How Companies Learn Your Secrets）》。某父親氣沖沖地向連鎖店—Target 投訴，質疑該廠商竟然郵寄嬰兒用品和孕婦服裝的優惠券給他尚為高中生的女兒！直到這位父親與女兒溝通後，始知女兒確有身孕。何以廠商比親生父親更早獲得相關訊息？在於每位顧客刷卡消費時都會自動予以識別編號，嗣後電腦系統將自動記錄顧客購買商品、時間等行為訊息，配合其他統計資料，建構一個「用於分析顧客喜好與需求的資料庫」。復以廠商分析人員開發數種預測模型分析前開資料庫，即可預測女孩可能懷孕，進而推薦相關需求商品，即為「關聯規則及預測推薦」技術。

相類技術不僅美國採用，各國企業同樣行之有年，對於企業來說，顧客偏好、生活習慣等相關資訊極具價值，而且這些

顧客偏好、生活習慣等相關資訊欠缺法令保護，經蒐集分析後可對顧客側寫，察覺顧客行為模式並誘導消費，使「數位足跡」成為可轉換成貨幣的資產。

資訊在通常認知非屬隱私，欠缺法令保護，經蒐集分析後，即可對顧客人格進行側寫，策劃相應銷售手段。企業如同獲得預知能力，機先察覺顧客行為模式，誘導消費，準確賺取營業額，「數位足跡」不再是某種指標或參數，而是一種可以轉換成「貨幣」的資產，隱私將因數據預測而被探知，不復存在。

新的壟斷者—掌控「數位足跡」的資本家

「數位足跡」能夠泛起波瀾？確實如此！關注兩岸新聞者，勢必知悉 2020 年的大事，11 月 2 日，中共金融權管機關約談「螞蟻金服集團」實際控制人馬雲等人，翌日由中共領導人直接下令阻止該集團公開募股，官方並於該年 12 月強力介入調整該集團金融商品，在這期間，各種官方媒體發聲，強調「制約壟斷者破壞國安」之正當性。姑且不論是否肇因馬雲言論引發政治打壓，平心而論，渠等創辦「阿里巴巴集團」，透過旗下「淘寶」、「天貓」等購物網累積豐富「顧客資訊」、又推動「支付寶」、「餘額寶」等數位金融商品，配合「花唄」、「借唄」等「借貸 APP」，建構引以為傲的「大數據（數位足跡資料庫）」。

該集團透過「關聯規則及預測推薦」技術誘導民眾過度消費、借貸，累積鉅額債權，再以鉅額債權做抵押向公營行庫取得資金，等同把撼動國家安全的「金融危機」「轉賣」給政府，再企圖以「轉賣金融危機」所得資金炒作股市，其影響不僅加劇貧富差距，更將兩個世代的民眾禁錮於低薪無尊嚴的勞動之下！

借鏡「保護規範原則」權衡資訊蒐集及運用

誠如前言，運用 5G 網路傳輸技術，遠端操作智能產品，有效「縮短時空侷限」，例如遠端醫療系統、遠端數位教學等，可

馬雲控制的阿里巴巴集團串流旗下「淘寶」、「天貓」、「支付寶」、「餘額寶」、「花唄」、「借唄」等金融商品及購物網，建構數位足跡資料庫。（圖片來源：Foundations World Economic Forum, https://www.flickr.com/photos/49344088@N04/39008130265；Leon Lee, https://www.flickr.com/photos/leondel/albums/72157594567186859；中新社／達志影像）

以拉近城鄉差距；全區域地理生態監控、全系統即時交通安全管制等，全面提高管理效能；然而，各機構從中獲得蒐集「數位足跡」作為背景資料使用，勢必無法阻擋。不論是國際戰略判斷或犯罪防治人格側寫，甚或民間企業的「關聯規則及預測推薦」銷售技術，對於「數位足跡」蒐集只會越加依賴、更為全面。

曾經「科技始終來自於人性」，現今「人性受科技刺激而改變」，吾輩究應如何看待這「潘朵拉魔盒」？管見以為：一、善用資安專才，研發核心技術以因應，誠屬必要。二、科技發展迅捷，則成文法恐有不及，或可運用司法判例及行政裁定之彈性，與時俱進，先行框列「資訊蒐集及運用範疇」。三、框列「資訊蒐集及運用範疇」，應受「保護規範原則」檢視、權衡，務求符合「立法意旨所保護價值」，更係維護「人性價值」的具體彰顯。