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/.

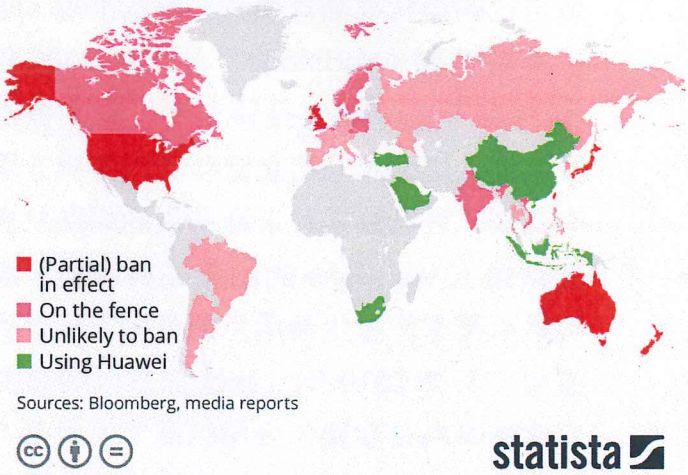
[4] Christopher Balding, "Huawei Technologies Links to Chinese State Security Services"；此外，Huawei's ownership structure is not transparent, raising suspicions of effective party-state control over the company.

[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。

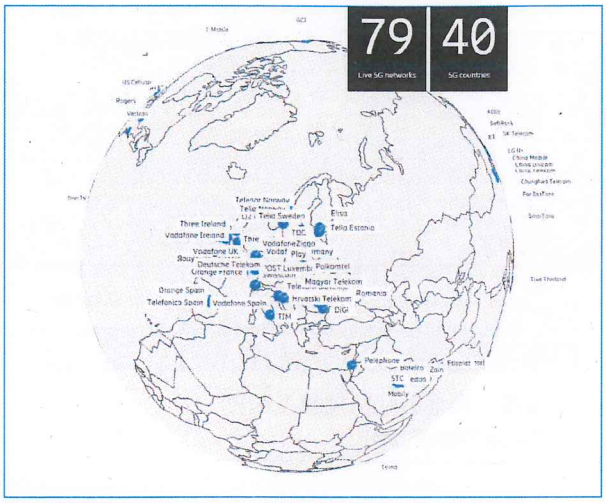
安全應優於價格

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。