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 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」

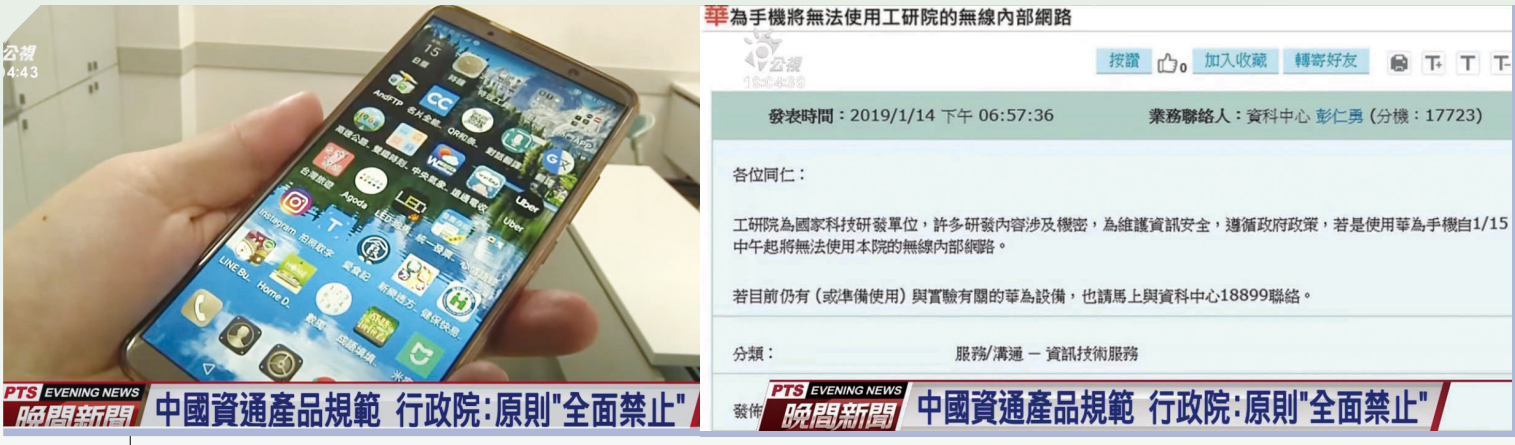
筆者在擔任國家高速網路與計算中心副主任兼資安長時，曾帶隊參加世界超級電腦年會，看到大陸展示多種電腦，每個攤位我都會去問一下，他們到底應用在那方面？據說很多都用在監控人民上面，例如影像辨識、人臉追蹤、人工智慧情緒判斷等等，真的令人感到害怕。

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）

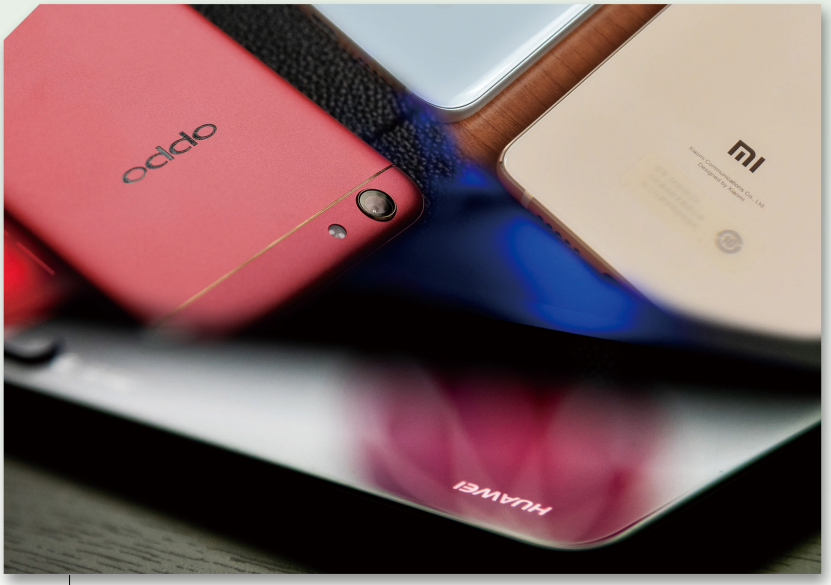
為何政府機關員工不能使用華為手機

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」

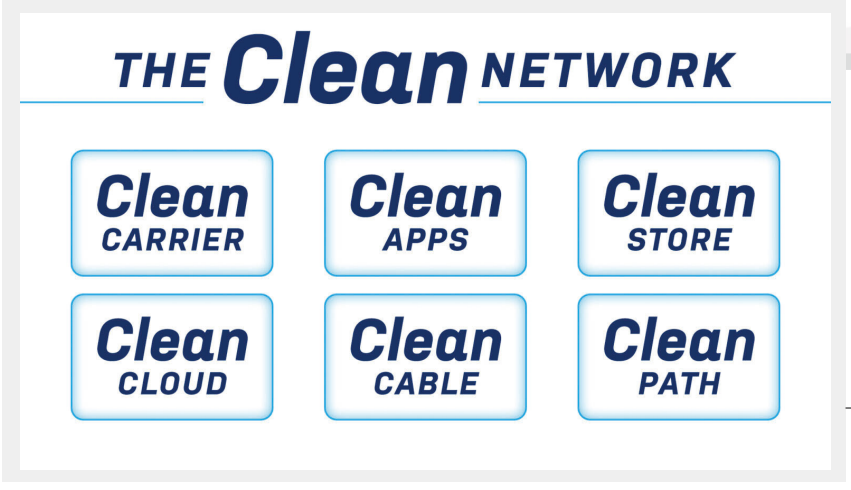
德國是世界上與中共最友好的西方國家之一，然在西藏抗暴 60 週年之際，原先非常支持西藏的德國，也因受中共經濟誘

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）

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

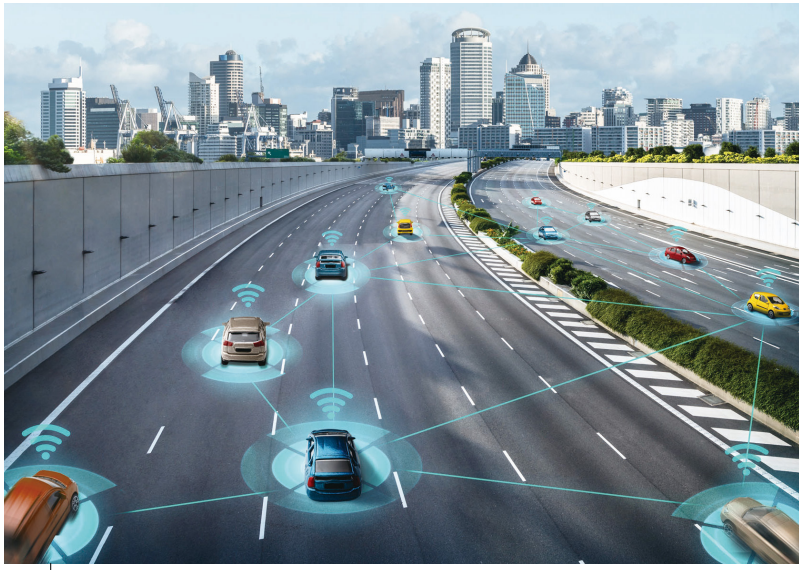
5G 固然便利，但也如雙面刃般面臨更多的資安挑戰。尤其隨著上網的裝置大量地增加，如何在便利的使用 5G 技術之餘仍能保持資安的要求，將是智慧城市的最大挑戰之一。以下簡介兩種 5G 應用於智慧城市可能發生的資安議題。

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

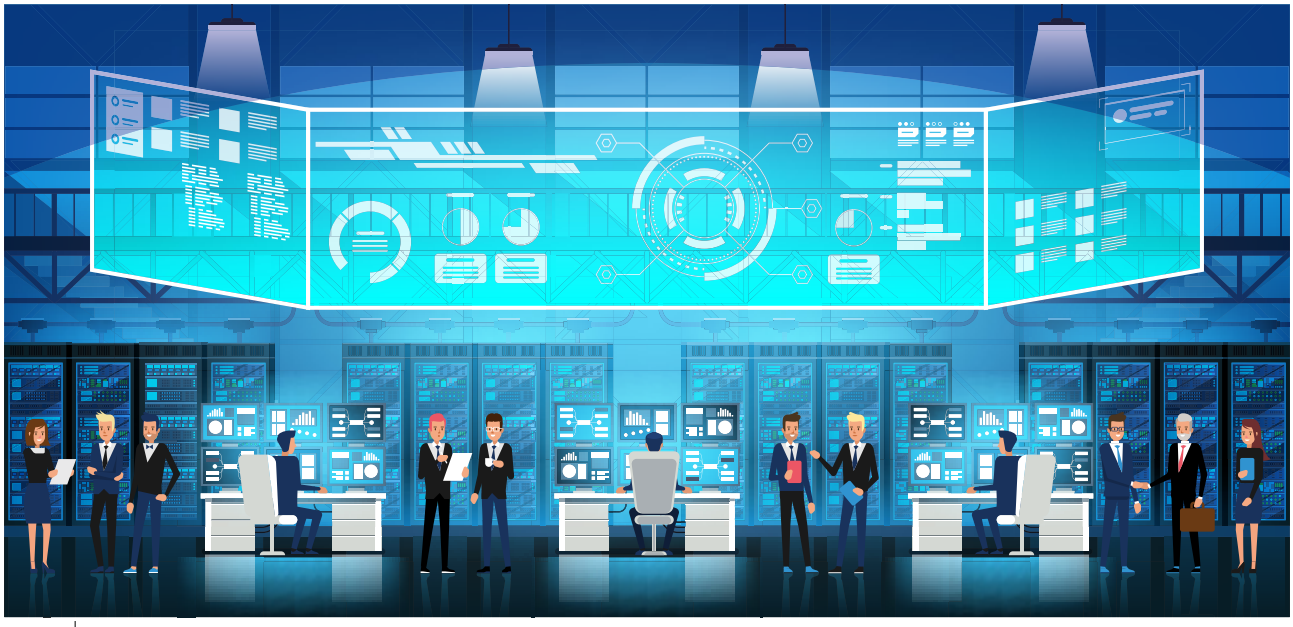
DDoS 並不是一種新興的網路攻擊模式，最早可回溯至 2000 年左右已有網路駭客使用此攻擊手法。由於此手法相對簡單、有效，且成本也不高，故攻擊案例層出不窮。DDoS 是利用大量受控制的電腦同時對目標伺服器發出連線請求，藉此癱瘓目標伺服器原本所能提供的正常服務。無論是網路層的 TCP 協定或是應用層的 HTTP 協定，在開始一個資料連線傳輸之前都需要先配置一部分的系統資源，然而伺服器的系統資源是有限的，一旦被無意義的連線消耗殆盡後，將無法正常使用。

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。

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

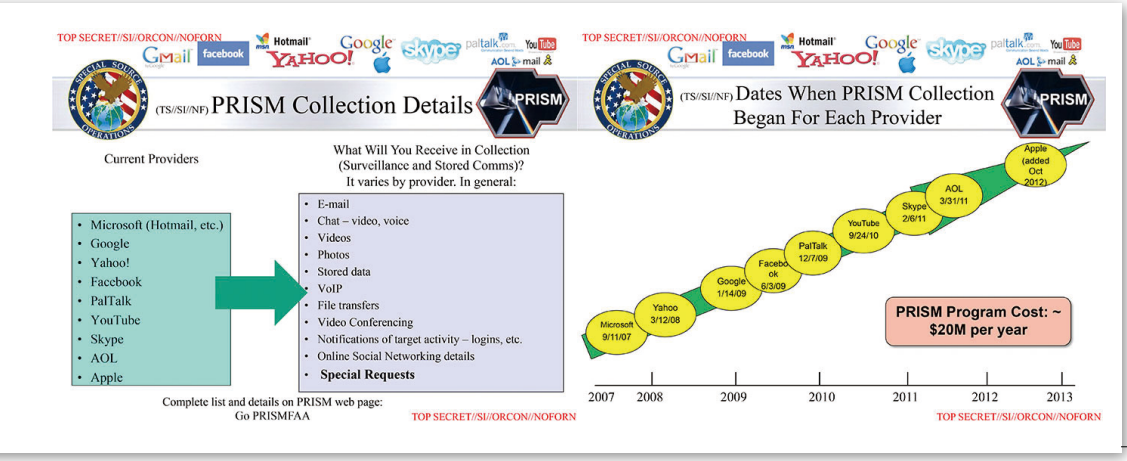
我們如今身處於第三波數位革命時代，正在全面推廣的 5G 網路傳輸技術具有「高速傳輸」、「信號低延遲回應」、「同時連結多樣裝置」等特性，配合更快速的「雲端計算」，遠端操控各項智能產品發揮更大效能，「生活與網路更加密不可分」，然而卻也因為「密不可分的智能產品」，留下更多的訊號傳輸紀錄—「數位足跡」。「數位足跡」具有危險性或機敏性？電影「美國隊長 2 —酷寒戰士」劇情，九頭蛇組織科學家索拉發明「索拉演算法」，將世界視為電子書，透過個人的

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。