智慧城市中的5G運用

調查局資通安全處／雷喻翔

◆ 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。

本文摘自清流雙月刊中華民國110年5月 號P17-P20

又是洩密！英國、奧地利閣員相繼下臺

展望與探索雜誌社研究員／楊宗新

／展望與探索雜誌社研究員　楊宗新

今（2019）年5月的歐洲政壇並不平靜。5月1日，英國前首相梅伊（Theresa May）才開除涉嫌將國家安全會議決議洩漏的國防大臣威廉姆森（Gavin Williamson）。5月18日，奧地利副總理斯特拉赫（Heinz-Christian Strache）也因疑似意圖將工程標案資訊洩漏給俄羅斯人士而主動請辭，該宗導致奧地利總理庫爾茨（Sebastian Kurz，即擁有「全球最年輕政府領導人」稱號者）於5月27日被罷免，成為奧國二戰後任期最短的總理。

No.23 SEP. 2019. MJIB

英國：從「華為制裁案」演變為國家利益詮釋之爭

如果說美「中」貿易戰是近期國際上頭等大事，那麼「華為制裁案」便是貿易戰的主戰場。它不僅衝擊美「中」關係，世界各主要國家，尤其是「五眼聯盟」（Five Eyes，由美、加、英、紐、澳組成的情報聯盟）也在美國要求下，加入制裁華為的行列。

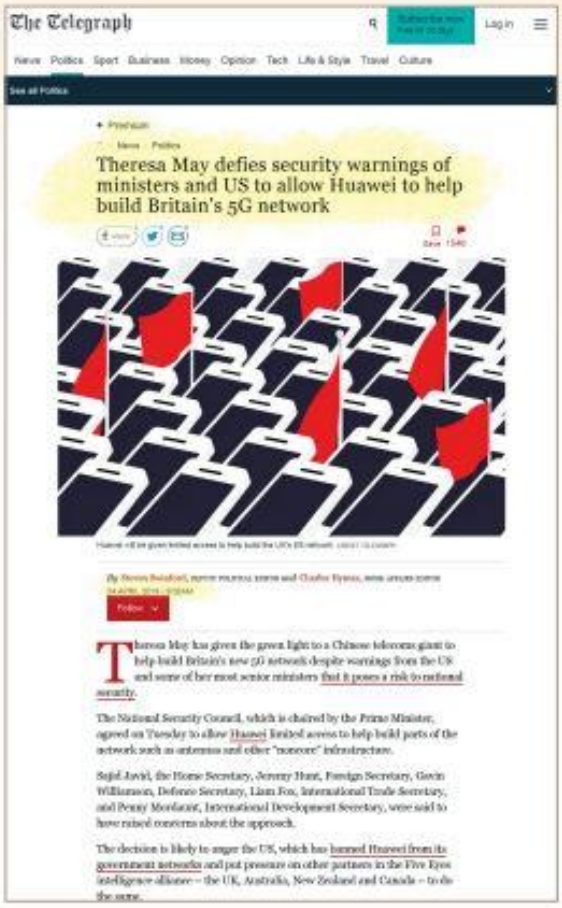
對於是否抵制華為，英國內部一直存在爭論，從而造成內閣成員之間的對立。4 月 23 日，梅伊召集財政、內政、外交、國貿、國際發展及國防 6 位大臣召開國家安全會議，討論是否有條件開放華為投資英國第 5 代行動通訊技術（簡稱 5G）。席間除了梅伊本人及財政大臣外，其餘均反對放寬限制，理由是應顧及美國的態度與政策反應。

在會議未取得共識下，梅伊獨排眾議，拍板定案「容許華為投資英國 5G 的非核心部分」。豈料在該會議結束後沒多久、政策尚未對外公布前，英國《每日電訊報》（The Daily Telegraph）隨即報導該會議內容，眾人乃將矛頭指向反對最甚的國防大臣威廉姆森，他被查獲在會後與報導此事的記者通了長達 11 分鐘的電話。儘管威廉姆森出面澄清絕無洩密，但梅伊仍於 5 月 1 日宣布免除其國防大臣職務。

「五眼聯盟」在美國要求下，加入制裁華為的行列。

英國前首相梅伊力排眾議，堅持容許華為投資英國的 5G 技術。（Photo Credit: UK Government, https://www.gov.uk/government/speeches/prime-ministers-statement-in-downing-street-24-may-2019）

英國前國防大臣威廉姆森被指控洩露國家安全會議上有關華為的決策內容，並於事件後的 5 月 1 日被免除職務。（Photo Credit: Kuhlmann/MSC, https://commons.wikimedia.org/wiki/File:Gavin_Williamson_MSC_2019.jpg）


The Telegraph

Log in

News Politics Sport Business Money Opinion Tech Life & Style Travel Culture

See all Politics

Theresa May defies security warnings of ministers and US to allow Huawei to help build Britain's 5G network

Theresa May has given the green light to a Chinese telecoms giant to help build Britain's new 5G network despite warnings from the US and some of her most senior ministers that it poses a risk to national security.

The National Security Council, which is chaired by the Prime Minister, agreed on Tuesday to allow Huawei limited access to help build parts of the network such as antennas and other "non-core" infrastructure.

Sajid Javid, the Home Secretary, Jeremy Hunt, Foreign Secretary, Gavin Williamson, Defence Secretary, Liam Fox, International Trade Secretary, and Penny Mordaunt, International Development Secretary, were said to have raised concerns about the approach.

The decision is likely to anger the US, which has banned Huawei from its government networks and put pressure on other partners in the Five Eyes intelligence alliance – the UK, Australia, New Zealand and Canada – to do the same.

英國《每日電訊報》在會議結束後隔天隨即報導會議內容，消息來源指向反對此案最甚的前國防大臣威廉姆森。（Source: The Daily Telegraph, https://www.telegraph.co.uk/politics/2019/04/23/theresa-may-defies-security-warnings-ministers-us-allow-huawei）

這項人事命令，在英國憲政史上是相當罕見的。當時梅伊擔任保守黨黨魁，其內閣大臣多為保守黨籍，在政黨紀律嚴明的英國，若非遭議會通過不信任案，原則上內閣應該是一個共進退的整體概念，此次特定閣員遭首相要求提前走人的先例並不多見。

威廉姆森反對的理由是，長期做為美國最堅實的盟邦，英國若不加入抵制行動，將嚴重影響雙邊關係；梅伊則顯然不願在美「中」之間選邊站。在雙方對於「國家利益」各有見解下，無論洩密案是否屬實，威廉姆森都必將成為政治犧牲品。

奧地利：「通俄門」延燒 導致執政聯盟遭倒閣

這邊所指的「通俄門」，與美國總統川普（Donald J. Trump）遭控訴在選舉

奧地利前副總理斯特拉赫（右下）於國會大選前夕和俄羅斯某財團老闆姪女會面，引發喧然大波。（Source: Guardian News, https://www.youtube.com/watch?v=Nz6BeEVVCjc）

前疑似與俄羅斯情報單位有所往來的案件無關[1]，而是一起上演於奧地利的獨立事件，因為剛好也與俄羅斯有關，所以被媒體冠以「通俄門」稱之。

2017 年 10 月奧地利國會選舉，並無單一政黨取得過半席次，獲得席位最多的人民黨與第 3 的自由黨組成聯合政府，兩黨黨魁分別擔任總理、副總理。今年 5 月 17 日，德國媒體《明鏡》（Der Spieger）、《南德日報》（Süddeutsche Zeitung）公布了一段密錄影片，內容是奧地利前副總理斯特拉赫在 2017 年選舉前，於西班牙維薩島會見了一名自稱是俄羅斯某財團老闆姪女的女子，斯特拉赫承諾，對方若願意捐款助其贏得選舉，上任後將以政府工程合約回報。

影片拍攝時間距今已逾一年半，卻在此時才公諸於世，動機令人質疑，德國媒體亦不透露畫面從何而得。儘管斯特拉赫在擔任副總理後，尚未被查獲洩漏工程標案資訊予該俄羅斯財團，但此事已對其政治威信造成極大影響，其乃於消息見報的隔日，火速宣布辭去副總理職務。然而事件卻並未因他的下臺而落幕。聯合內閣在失去自由黨的支持後，國會於 5 月 27 日通過不信任案，總理庫爾茨（Sebastian Kurz）及其內閣垮臺，成為二戰後第 1 位被倒閣的總理。

兩起事件的保防觀點

這兩起發生時間相近但互無關聯的事件，卻分別與保防工作的兩項重要概念「機密保護」、「防制滲透」相關。

[1] 該案業於今年 3 月 24 日經美國司法部宣布偵結，調查報告認定川普並未妨礙司法。

奧地利總理庫爾茨因聯合執政的副總理疑涉通俄醜聞，成為二戰後首位被倒閣的總理。（Photo Credit: European Parliament, https://www.flickr.com/photos/european_parliament/39788861053）

奧地利前副總理斯特拉赫因忽略了「機密保護」與「防制滲透」的保防工作，最終只能宣布辭職，為其行為付出代價。（圖片來源：美聯社／達志影像）

先說英國前國防大臣威廉姆森的洩密案。國家安全會議中，並未做成書面紀錄的研商對策，究竟是否屬於機密範疇，有待該國法律認定。然而就保防的角度看，此事涉及英國與美國、中國大陸之間的互動關係，影響國家安全甚鉅，實不可不慎，在政府正式公布結論前，試圖透過媒體力量干擾決議，並不可取，尤其當事人還是主管國防事務者。

至於奧地利前副總理斯特拉赫的事件，其實兼具「機密保護」與「防制滲透」雙重性質。渠以國家重大工程做為換取外國財團提供款項的條件，雖未明言許以標案的方式，但就法治國家的常理推斷，無非是藉由透露工程底價、評選人員等相關資訊助對方得標；而當時他身為國會大黨黨魁且被期望接任副總理的呼聲甚高，竟然在選舉前夕，與被歐盟國家視為主要假想敵的俄羅斯籍人士進行利益輸送，實難保在其任內不會遭俄羅斯以此挾持，進而做出有悖於國家利益的施政。

先不論該 2 位人士言論背後隱藏的政治意圖或可能只是酒酣耳熱下的狂言，其實像英國國防大臣、奧地利副總理等這些歷經各種考驗才能登上國家權力頂峰的人物，一定也都知道隔牆有耳，敵人可能隨伺在旁的風險，竟然還會犯下這種錯誤，做為一般人的我們，更應小心謹慎，「患生於所忽，禍起於細微」，國家安全存在於每個人的一念之間啊！

本文摘自清流雙月刊中華民國108年9月 號P25-P29