5G 浪潮來襲！
應用領域潛藏資安危機，關鍵在「資安合規」

毛敬豪*

血拚購物，不再需要看店員臉色，因為只要臉部辨識就可以毫無負擔的結帳；蔡依林演唱會的票搶不到也沒關係，只需戴上虛擬實境（VR）裝置，家裡客廳就是你的搖滾區；智慧交通讓道路暢行無阻，哪怕是上下班尖峰，也不用再忍受塞車之苦，更不用花時間找停車位。這些生活場景，都將乘著 5G 浪潮一波接著一波來，成為你的日常。

臺灣即將釋出第一波 5G 執照，5G 應用無所不在，各行各業都想搶搭這班 5G 的金礦列車，5G「大頻寬、高速率、低延遲」的三大特性，帶動多元應用加速發展，無可避免地，都必須面對隨之而來，資安的嚴峻挑戰。

全面性導入資安防護、隱私與資安陸續法制化、產品安全、資料安全保護技術等，都將受到高度重視。預估 2020 年，光是全球企業在資安防護上的投資，將比 2017 年增長 28%，資安危機的背後是龐大的商機。本文就先帶您盤點 5G 在以下這些應用領域背後的資安危機。

*財團法人資訊工業策進會資安科技研究所所長。

壹、智慧交通

1982 年，美國影集《霹靂遊俠》中主角李麥克的黑色跑車「夥計」，搭載 AI 人工智慧，擁有連 Siri 也甘拜下風的語音溝通能力，同時還配備醫療掃描儀甚至是防衛性武器。2002 年史蒂芬史匹柏執導，湯姆克魯斯主演的科幻電影《關鍵報告》中，2054 年的未來世界裡，人類交通也已經智慧化。如今這些不思議的電影場景，都將跟著 5G 時代的來臨一一實現，人人都可以是李麥克，也都有機會擁有「夥計」般的智慧汽車，在城市的大街小巷暢行無阻。

除了交通工具本身 AI 化，數位道路的時代，所有道路也都會被編碼，透過 RFID（無線射頻辨識）發射訊號，在智慧交通控制中心的掌控下，所有智慧汽車透過訊號讀取精準定位，並沿著數位道路行駛，能有效降低車禍肇事率，縮短行車距離和時間，還能降低油耗，當然，哪裡有停車位也一目了然。而車聯網下的自動駕駛、編隊行駛、遙控行駛、車輛生命週期維護，一直到計程車、大客車等大眾運輸、交通資訊等，都在 5G 連結下，高效穩定的運行。

資安隱憂：軟體漏洞遭駭客攻擊，危害乘客安全

《霹靂遊俠》曾上演「夥計」被駭後成為反派的劇情，並非毫無科學根據和邏輯。事實上，軟體漏洞確實為智慧交通系統和工具的一大風險。2015 年就已有安全專家與 Wired 雜誌合作展示，透過遠端入侵並控制克萊斯

Uconnect 中控系統。若是智慧汽車本身具備 OTA 無線更新功能，可和交通號誌相互通訊，很可能因而連帶從遠端遭到漏洞攻擊，或者收到假冒的 OTA 更新，掌握車輛部分功能、發送錯誤的交通資訊給駕駛人，都將引發難以想像的後果。

交通運輸工具連結應用程式、智慧交通號誌等，高度便利的背後也必須承擔高度的風險，一旦駭客找到漏洞並發動攻擊，輕則免費使用交通工具或停車位、拖慢車流，重則遠端駭入系統，使油門失去作用或關閉安全氣囊等，癱瘓交通甚至危害乘客生命安全。別說是駭客，2013 年美國舊金山灣區捷運系統（BART）也曾因軟體升級不當導致捷運系統發生故障，導致早上 7 點尖峰時刻嚴重交通堵塞。

貳、 聯網無人機

過去十年，無人機廣泛運用在物流、救災、農業、建築、專業巡檢和安防等各領域，在 3G、4G 網絡中實現部分應用，未來，這些應用隨著 5G 時代的來臨，型態和品質上都將都大幅升級。

以電力或基站巡檢為例，電塔或基站設備位處高空，應用無人機巡查，可免除人力巡檢的高風險作業，還可 360°全視角查看設備細節，而過去 4G 網絡下只能達到 1K 的傳輸，影像解析度明顯不足，未來在 5G 的特性下，影

像流暢的同時，細節更加清晰，也大幅提高巡檢的效率和品質。救災應用上，除能傳回災難現場的清晰影像，還可結合邊緣運算能力和 AI 技術，快速進行人員辨識和周邊環境分析，提高救援效率。

此外，在科技農業的應用上，透過 5G 技術的大數據針對氣候、土壤、種子、肥料、用藥等系統化處理，可望更大幅度擺脫自然條件的限制，同時利用物聯網，把氣象站、盤商甚至農業機械製造商納入連結，實踐農業智慧化和精準化，解決糧食危機的問題。甚至在農業和其加工都精準監控的情況下，農產、加工和食品安全體系重新建構，食安問題也澈底解決。

不只是原有的應用，品質上大幅升級，應用領域上也將更加多元，像是今年五月，德國新創公司 Lilium 開發的無人駕駛噴射飛行器「空中計程車」，已成功完成處女航測試，目標 2025 年前提供「隨選空中計程車服務」。而物流業也將在 5G 普及化後，產生革命性改變，在傳統物流包裝、運輸、裝卸到倉儲等環節，注入物聯網、AI、無人機、遠端監控等技術，大幅提高產業的效率與品質。

駭客入侵強奪控制權，巡檢利器成犯罪工具

從應用領域角度來看無人機所衍伸的犯罪問題，輕則侵犯個人隱私，重則危及飛航安全，滅火的功能還恐將淪為恐怖分子的武器，或販毒走私的工具。從資安角度來談，以利用 5G-enabled 無人機進行鐵路巡航監控為例，影

像可能中途被駭客攔截後，再回傳像是「軌道狀況被實體偽裝之畫面」等假影像，也可能強奪控制權，任意操控飛行，甚至因為訊號被阻斷而墜毀，或是能挾持登入憑證，竊取無人機管理平台資料（Check Point）。

參、智慧醫療

5G 萬物聯網，人工智慧也將落實在醫療領域，逐步開展全面性的智慧健康管理，像是透過具備藍牙和 GPRS 的醫療儀器，全天候監測身體狀況，持續性處理分析收集到的資料數據再進行回傳，以提供最佳治療方案。以配戴 5G IoMT 感測器的心臟病患者為例，一旦有突發狀況，訊息隨即傳送到最近的醫院，進而提供最即時的治療，驗證 5G 在醫療領域的最佳體現—「醫療個性化」。

此外，AR／VR 也廣泛運用在像是遠端診斷，遠端遙控手術、醫療培訓（手術教學）、醫療監視器等，醫生只需戴上 VR 頭盔或眼鏡，就可進行遠端醫療，甚至在千里之外透過機器人進行手術。

醫療物聯網（IoMT）輕則病患隱私洩漏，重則駭命

智慧醫療系統與醫院內外大量設備連結，可隨時被讀取應用，也因此資料外洩的風險也跟著遽增，且系統架構複雜，病毒暗藏其中難以被察覺。2015 年美國與德國的醫療系統都曾被病毒攻擊，而根據後來調查，該病毒潛藏期

長達 1 年，因為醫療系統日趨龐大且複雜，病毒若是未啟動，系統偵測更是極其困難。

相較於企業單位面臨的風險為經濟損失，醫療組織所要承擔的，除了病患龐大的個資和病歷等隱私，更直接攸關生命安全。2015 年就曾發生美國安全研究人員 Billy Rios 發現藥物輸液泵系統中至少有 5 個模式存在漏洞，駭客可以利用遠端控制把藥物的劑量變到致命劑量。而遠距手術若遭攻擊網絡中斷，或生命監控系統遭駭，也將嚴重危及病患的生命安全。

肆、智慧居家

比爾蓋茲曾在 1995 年出版的《未來之路》一書中預言：「在不遠的未來，沒有智慧家居系統的住宅會像不能上網的住宅一樣不合潮流。」而就在這本書出版兩年後，他耗資 9,700 萬美元打造的智慧豪宅也正式完工，大從門窗小到燈具、電器都可透過中央電腦控制，而手機連接這台中央電腦，人還沒到家，就可遠端遙控開啟空調、調整浴缸水溫、預做簡單的料理等。當然，屋裡也配備了聲控和指紋技術，而未來，這些也不再只是富豪限定，因為他所預言未來世界已經近在你我眼前。

3G 和 4G 時代，透過手機遠端遙控智慧家居設備，如今 5G 時代來臨，進一步聚焦智慧設備的「自我感知」，智慧家居設備已能主動感應環境的變化

而做出相對應的處理，無須再仰賴人為控制，系統也能獨立運作。舉凡室內照明、窗簾、安全監控、家電、溫度和濕度及節能控制、影音播放、AI 機器人等，都能透過家庭智慧系統集中監控、自主管理，在 NB-IoT、eMTC 技術被廣泛採用後，我們所能享受的智慧居家甚至能超越比爾蓋茲。

智慧進入家居，駭客也駭入你家，隱私外露、智慧家電遭非法入侵

科技串聯家庭內智慧裝置，增加生活便利性，提升居家安全，但水可載舟亦可覆舟，安全防護系統潛藏個人隱私洩漏的風險；智慧家電也有可能遭到非法入侵。2016 年 IEEE（電機電子工程師學會）研討會就曾公告三星 SmartHome 系統存在漏洞，駭客遠端攻擊用戶住家，打開與系統相連的門鎖。

美國亞馬遜日前也公開坦承，Alexa 設備記錄長期儲存使用者的互動紀錄，即使使用者刪除錄音檔，亞馬遜仍長時間保存，嚴重侵犯使用者個人隱私。此外，像是烤箱、電棒離子夾等，也曾被駭後遠端遙控開啟電源或調高溫度，演變成縱火案。

伍、智慧城市

傳統電網送電的模式為單向，從發電、輸電與配電再送往使用者家中，過程中常常有輸電效率不佳、再生能源難以整合等問題。但 5G、感測器和雲端技術崛起，發展出智慧電網，電力和數據從原本的單向轉為雙向交換互動，系統整合感測器和無線傳輸，透過數位技術進行電網監控及管理，電力公司更精準能掌握用電數據，調整尖峰時間內的發電量，進而預測能源需求，大幅提升安全性和穩定度。

不只如此，電力管理也開始設置饋線自動化系統。饋線自動化是智慧電網最重要的基礎工程之一，台電研究顯示，饋線自動化之後，事故發生時用於尋找故障與隔離處理的時間，可把原本 1 小時的人工處理時間，縮短到 30 秒到 1 分鐘。由於 5G 可提供 10 毫秒的超低延遲和千兆吞吐量，才能達成 5G 無線分布式饋線系統，達成更快更精準的電網控制。

除了水電、交通外，安防、水質監測、水位監控、地震偵測、颱風預測、污染監控等也都能透過 AI 影像監控提升城市的安全。以巴西為例，里約熱內盧透過 80 多台螢幕來顯示即時路況、天氣預報，以及來自 500 多台監視攝影機的影像，由 20 多位人員負責操作這些 360 度影像。此外，像是車站等特定場域，部署整合 5G、AI、影像監控的保全管理平台，也可即時性的把危險狀

況或可疑人物通報給警消單位。

市場研究機構 Marketsandmarkets 指出，影像監控的市場產值，正以每年 13.1%複合成長率的速度成長，與此同時，機器學習（ML）與深度學習（Deep Learning）等 AI 技術，也在提升監控系統效能和發展多元應用上成為重要關鍵，而 AI 前端（攝影機）與後端（雲平台）皆仰賴順暢、穩定的影像聯網，5G 扮演關鍵角色。

●智慧電網遭駭，市政服務全面癱瘓

以智慧電表為例，駭客可能竊取其中的資料，進而掌握特定家庭的用電狀況。HEMS（家庭能源管理系統）若無適當的防護，也可能遭歹徒暴力破解，連帶著駭入用戶家中其他連網裝置。此外，駭客也可干擾智慧電表的傳輸訊號，造成家用電表通訊延遲，或是透過掌握能源系統彼此之間的通訊方式，可對城市內大型系統發動分散式阻斷服務攻擊（DDoS），癱瘓重要的市政服務。

2015 年 12 月，俄羅斯駭客集團 Sandworm 成功攻擊烏克蘭電網，破壞供電，電廠操作員雖藉由手動重置斷路器在 6 小時內恢復供電，但若發生在美國大城市，可能需要更長時間才能恢復供電。

AI 影像監控遭殭屍惡意程式攻擊，成 DDos 幫兇

AI 影像監控也並非 100%安全，若是遭殭屍惡意程式攻擊，將導致大量網絡攝影機與數位影像錄影機變成 DDoS 的幫凶。

2016 年法國網站代管業者曾遭 14.5 萬台網絡攝影機組成殭屍網絡發動 DDoS 攻擊，其顛峰攻擊流量接近 1Tbps。2016 年 9 月殭屍網絡病毒 Mirai（殭屍網絡程式）在網絡發動多起攻擊。該殭屍網絡程式專門感染無線攝影機、路由器與監視器等 IoT 裝置，利用已知或未公開的安全漏洞入侵並控制這些裝置，在最高峰的時期操控數十萬台的 IoT 裝置，並用來執行分散式阻斷服務攻擊（DDoS），直到 2016 年秋天 Jha 把 Mirai 程式碼貼在網絡犯罪論壇，原始的 Mirai 殭屍網絡才終止。

陸、智慧製造

工控物聯網的目的，無非是能對工業製造實施精準控制，可應用於無線機器人雲端控制、物流和庫存監控、工業感測器等，同時透過感測器數據的採集、展示、建模、分析、應用等過程，在雲端形成決策，並轉換成工業設備可以理解的控制指令，進而操作設備。

如今多數工業控制系統仍需設置在本地，受通信技術和處理能力的限制，工業雲平台涉及工業控制的深度仍不足，而 5G 可以滿足工業系統對通信

能力的要求，實現工業控制的目標。

- **工業物聯網智慧製造遭受攻擊，陷產線當機、機密外洩危機**

工業物聯網（IIoT）遭網絡攻擊的風險持續攀升，駭客藉由勒索病毒感染破壞設備、造成營運停擺，或竊取敏感的企業資料。2018 年下半年臺灣晶圓代工龍頭因為資安疏失造成產線大當機，營收損失高達新臺幣 52 億；2016 年德國鋼鐵工業巨頭遭網絡間諜攻擊，導致企業專業技術機密外泄（含工業解決方案、鋼鐵生產單元等）。

萬物聯網讓製造業不再受限人工勞力，轉而透過物聯網帶動智慧製造，但在發展智慧製造，自動化、數位化及網絡化的同時，伴隨而來的是極大的資安疑慮。電腦可安裝防毒軟體，但多數工業設備受限於軟硬體規格、網絡連線需求等無法比照辦理，一旦駭客把不安全的企業網絡設備當成跳板，再移轉到最容易攻擊的工業控制系統設備和資料庫，甚至可能只要簡單的病毒，就可造成運轉停擺、能源供應中斷等難以估計的損失。

柒、 消費娛樂

在 VR（虛擬實境）或 AR（擴增實境）需大量的數據傳輸、儲存和計算，對於頻寬有極大需求，高品質的 VR 和 AR 內容處理走向雲端，即能利用雲端的儲存和高速計算能力。同時預估在未來十年，因為 5G 強化了傳輸速度，

電視從 4K／UHD 邁向 8K，能顯示 VR 和 AR 的頭戴裝置也可望普及，應用領域從遊戲擴展到運動賽事、演唱會、影音串流等服務。未來辦公室或家裡的桌機和筆電的使用率將越來越低，轉而使用連接到雲端的各種人機介面，搭載語音和觸摸等多種模式。

● **個資安全如何防護？成為最大資安隱憂**

除此之外，5G 時代的來臨，感應技術日趨成熟，不只是影音多媒體娛樂的型態不斷升級，無論是世界盃足球賽，還是張學友的演唱會，只要戴上頭盔就能有如親臨現場，就連網絡購物的支付方式也都徹底顛覆傳統，像是科幻電影中透過虹膜辨識進入豪宅的情節，未來將應用在 5G 時代的支付技術，透過眼睛和虛擬的相連，只要眨眼就能完成支付，甚至可望發展出其他的人體部位辨識模式。只是，在沒有密碼的情況下，資安問題如何解套，仍是關鍵。

捌、 結語

一、資安即國安！安全合規是最重要的基本功

根據今年 4 月美國 IDC 公司發表《全球安全支出指南半年報》指出，2019 年到 2022 年，全球資訊安全解決方案支出將以每年 9.2%的速度穩定成長；2019 市場規模達 1,031 億美元，超過臺幣 3 兆元，2022 年的市場規模更將突

破 1,338 億美元，約新臺幣 4 兆元。根據行政院國家資通安全發展方案報告也顯示，臺灣資安產業產值，2020 年時，規模將上看臺幣 550 億元。

臺灣資安產業初步可歸納出 3 種商業模式：提供在地服務的資安維運管理服務、利用資安技術結合硬體銷往國際、提供資安軟體服務。5G 時代的未來世界已經近在咫尺，資安危機也為資安產業帶來新的市場機會，但在這之前，無論是哪一種商業模式，政策到位、資安達標，才能取得進入市場的入場券。而從軟、硬體，終端機到服務，所有的領域都需要建立相關資安機制。

二、應用領域不同，功能安全標準大不同

5G 時代資安挑戰的背後是商機，如何不讓「Internet of Things」成為「Internet of Threats」，無疑是政府和廠商共同的目標，而建立完善資安等級制度，不同領域產業，明定不同的資安檢測範圍，則是邁向目標的第一步，更是未來搶攻 5G 商機的關鍵。

我們常說：「資安即國安」，5G 時代來臨，這是個必須重視的議題，因為進入 5G 時代，所有能連結上網的基站、機台、設備都成為駭客的新入口，各式資料遭受盜竊、竄改與挾持的機會恐將直線上升。最後提供一個數據給大家參考，根據微軟亞太研究資安報告顯示，臺灣在 2017 年受到資安事件造成的經濟損失達 8,100 億元，等於是臺灣 GDP 總值的 5%，由此可見資安的重要性。在迎接享受 5G 所帶來生活上便利的同時，產學研以及消費者的資安意識也該同步提升。