內政部國土測繪中心廉政專欄（110.05）

本期目錄：

壹、廉政檢舉多元管道：

一、內政服務熱線：1996

二、國土測繪中心 e-mail 檢舉信箱：k0@mail.nlsc.gov.tw

三、國土測繪中心廉政檢舉信箱：臺中黎明郵局第 99 號信箱

四、國土測繪中心廉政服務傳真：「 04-22592557」

五、法務部廉政檢舉專線：「0800-286-586」(0800-你爆料-我爆料)。

六、調查局反貪腐專線：舉報商品屯積免付費專線電話「0800-007-007」

「廉能是政府的核心價值，貪腐足以摧毀政府的形象，公務員應持廉潔，拒絕貪腐，廉政檢舉專線 0800-286-586 」

貳、法令園地：

避免重大公眾運輸及公安事故情重法輕，行政院會通過「中華民國刑法」第 183 條、第 276 條修正草案

避免重大公眾運輸及公安事故有情重法輕情形，行政院會今（22）日通過法務部擬具的「中華民國刑法」第 183 條、第 276 條修正草案，將由行政院函請司法院會銜送請立法院審議。

行政院長蘇貞昌指出，法律為人類智慧結晶，是社會規範準繩，也是公平正義防線。世界各國法律對各種犯罪型態有其規範，但必須與時俱進。院長以刑法中的過失致死罪為例表示，當時立法的交通工具不如現在龐大、快速，犯罪態樣也因人們生活型態不同，社會互動狀況不一，以致各種犯罪態樣也會有所差異，因此對於罪及責之間的規範，其相當性極為必要。

蘇院長進一步指出，此次修法，將區分犯罪情節輕重及侵害法益結果程度，加重過失致死罪的處罰刑度，最高可處 10 年以下有期徒刑，以與殺人罪的最低 10 年以上有期徒刑，彌合銜接。

此外，針對傾覆或破壞現有人所在之交通工具的犯罪行為，因而致生死亡或重傷結果者，也有增訂加重結果犯處罰規定的必要，以符合罪刑相當原則。

蘇院長表示，本案會銜司法院送請立法院審議後，請法務部積極與司法院及立法院朝野各黨團溝通協調，早日完成修法程序。

法務部指出，鑑於近年來發生多起重大公眾運輸及公共安全事故，對於一個行為卻造成多人傷亡，適用現行刑法第 276 條過失致死罪的結果，法院最重也僅能處有期徒刑 5 年，未能符合罪刑相當原則，且與社會觀感不符，為避免此類重大公安事故有情重法輕情形，因此擬具「中華民國刑法」第 183 條、第 276 條修正草案。

該草案修正要點如下：

一、就傾覆或破壞現有人所在之交通工具罪，增訂加重結果犯。（修正條文第 183 條）

二、就過失致死罪，區分其情節及侵害法益結果之程度，另訂加重處罰規定。（修正條文第 276 條）

（摘自行政院新聞稿）

參、廉政宣導小站

「政府與企業雙贏的有感施政」－破除圖利與便民迷思

為了破除圖利與便民迷思，進而讓公務人員勇於任事，守法守紀安心便民；同時回應總統府秦國策顧問嘉鴻(中華民國工業區廠商聯合總會前理事長)於 108 年間多次對於政府應引導公務員勇於任事、提升行政效能，以及促進產業發展等面向提出之國是建言，法務部及法務部廉政署自 108 年 6 月至 110 年 1 月間協同經濟部、科技部、臺北市、新北市、桃園市、臺南市及高雄市政府等中央及地方主管機關，於全台辦理 9 大場次「促進產業發展 提升行政效能—破除圖利與便民迷思」廠商交流座談系列活動。

此次的系列活動參與人數，包含公部門代表計 1,142 人、廠商代表計 1,331 人，合計 2,473 人。透過跨部會、跨縣市的合作及全國專案性宣導，不僅讓產業界體會政府為建構完善投資環境所作的努力外，獲各地方政府首長支持，更獲得公私部門代表熱烈響應，不僅讓產業與政府的連結更加緊密，也傳達政府行政透明與簡政便民的理念及企業誠信經營的重要性。

為擴大上述系列活動效益，並感謝秦國策顧問親自出席各場次之交流活動，法務部特別於今(21)日司法記者茶敘中，以「政府與企業雙贏的有感施政~破除圖利與便民迷思」為主題，播放此次的系列活動成果專輯影片；並特別邀請秦國策顧問親臨現場分享心得，讓現場出席的記者們充分感受到公部門積極展現提升效能及便民化措施，以及政風人員擔任溝通橋樑，促成公私協力建構政府廉能透明環境所做的努力。

蔡清祥部長特別在活動中，致贈這次廠商交流系列活動紀錄影片予秦國策顧問，除了再次表達感謝之意，更向國人展現持續致力公私部門交流，推廣企業誠信之決心。未來，也將持續與中央機關與地方政府合作，持續倡導簡政便民措施，讓公務員勇於做事，提升行政效能，達成全民有感、接地氣的施政目標，促進產業發展及政府與企業合作協力的雙贏。

（摘自法務部廉政署新聞稿）

肆、反詐騙宣導小站

＊凡遇不明可疑電話，不論手機或市話，只要撥打「165」即可由專人為您說明並研判是否為詐騙事件。

教你識破網友的甜言蜜語

2021/03/31

曾以為在網路上遇見真命天子

沒想到他只是愛情騙子

曾以為他真的想見妳

沒想到他只是真的想騙妳

曾以為愛情有了寄託

沒想到只是步入詐騙的漩渦

（內政部警政署）

伍、資通安全視窗：

智慧城市中的 5G 運用

◎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。

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。

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 Denialof 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。

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。

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。

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。

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。

（摘自法務部調查局清流月刊）

陸、機關安全維護宣導

自衛消防編組應變能力驗證步驟

（摘自內政部消防署）

柒、消費者服務專欄：

慎防個資外洩，保障消費安全

（摘自行政院消費者保護處）

捌、內政服務熱線：1996

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※

內政部國土測繪中心政風室