立法院第 9 屆第 1 會期第 12 次會議議案關係文書

專案質詢
9－1－12－0292

立法院議案關係文書

中華民國 105 年 5 月 4 日印發

案由：本院許委員淑華，鑒於電腦科技的快速發展，網際網路已經成為人們日常生活中，接收與傳遞信息時，最常利用的傳播媒介。要求行政院責成所屬於平時就必須建立起「資訊安全、人人有責」的務實態度與良好習慣，並藉由綿密的教育宣導及標準化作業程序，使用網際網路及資訊媒體設備，以確保資訊及相關系統之機敏性、完整性與可用性。爰此，特向行政院提出質詢。

說明：

一、近年來，由於電腦科技的快速發展，網際網路已經成為人們日常生活中，接收與傳遞信息時，最常利用的傳播媒介。如時下流行臉書（Facebook）、推特（Twitter）等社群網站及 Line、WhatsApp、WeChat、Juiker 等行動通訊軟體；這些平台都具傳播快速、成本低廉，且能迅速連結、整合、行銷等多元化運作特性。早已超越傳統郵件、報紙、廣播、電話或電視的功能，堪稱為可跨越時空、國界、深入家戶及人腦思維，影響力最無遠弗屆的另類神經體系。

二、在電腦、智慧手機與網際網路幾已與人類緊密相連下，應運而生的是全球物聯網（Internet of Things, IoT）裝置的大幅躍升。在物聯網上，每個人都可以應用電子標籤將真實的物體上網聯結，查出它們的具體位置。也能用中心電腦對機器、裝置、人員進行集中管理、控制，並對家庭裝置、汽車進行遙控，以及搜尋位置、防止物品被盜等，類似自動化操控系統；同時透過收集這些小事的資料，最後可以匯流整合成大數據，包含重新設計道路以減少車禍、都市更新、災害預測與犯罪防治、流行病控制等，讓人類生活行為巨變。

三、簡單來說，物聯網已將現實世界數位化。其應用前景，根據市場研究機構 Gartner 預測，2016 年全球將會有 64 億個物聯網裝置，比 2015 年成長 30%，屆時每天將有 550 萬個裝置連網。其產值在 2016 年，消費者物聯網硬體及應用相關的市場規模將可達到 5,460 億美元之譜，企業物聯網領域的支出亦高達 8,680 億美元。顯然地，未來我們在運輸和物流、健康

醫療、智慧環境（家庭、辦公、工廠）、個人和社會領域等，都已離不開此綿密網絡，它已主導、也改變了世界的潛能與風貌。

四、顯然，在人類對物聯網的依存度愈來愈高的同時，隨之而來的是駭客入侵、網路攻擊、病毒感染及惡意程式肆虐、重要資料被竊等事件層出不窮，甚至變本加厲。例如，去年發生在烏克蘭的網路攻擊導致停電事件，讓全球資安專家憂心，類態樣攻擊使大規模公共服務中斷的事實，已非紙上談兵；今年 2 月，孟加拉中央銀行在美國聯邦準備委員會下屬的聯邦儲備銀行紐約分行帳戶，傳出遭駭客取得，高達 1 億美元資金被成功轉走，造成史上最大宗銀行竊案之一；全球金融巨擘匯豐銀行（HSBC）傳出因遭到分散式阻斷服務攻擊，導致 HSBC 在英國的網路銀行服務無法正常運作將近整個營業日；中國大陸某駭客團體透過從他處取得的 9,900 萬筆帳密資料，對淘寶網進行比對測試，竟發現有多達 2,059 萬個帳戶真實存在，並成功取得部分帳號進行詐騙之用。

五、除了世界各國飽受駭客攻擊事例不斷外，我國因緊臨東北亞地緣政治情勢緊張的影響，加上高科技公司擁有進階攻擊者想要的重要資訊，不論企業體或政府機關比其他國家更容易受到網路攻擊。根據趨勢科技主動式雲端截毒服務（Smart Protection Network）資料，最新一波透過感染行動裝置，進一步取得家用路由器控制權的駭客攻擊事件中，受影響最大的國家與地區，分別是臺灣、日本、大陸、美國和法國；我國受影響使用者占全球 27.41%，被駭客竊取網路憑證位居第一。從上述的實例充分證明，資安威脅已嚴重導致個人、社會、企業與政府基礎設施系統的弱點進一步擴大，成為造成危害經濟與國家安全最危險的攻擊性武器之一。

六、鑑於頑強且複雜之網路攻擊行為日益增多，美國於 2012 年已將網路攻擊與生物武器、核彈、氣候變遷及跨國犯罪等，並列為未來 10 年對國家安全之前 5 大威脅。近年美、日和歐盟等國家，更針對網路與資訊安全，提出多項具體防護措施。美國的作法是，建立隱私權委員會、新設聯邦資安長職務，並在 2017 年預算案中，大舉提高年度政府資安預算 50 億美元至 190 億美元，期建立整體國家級資通安全防衛體系。本院在去年 12 月 14 日三讀通過「國家資通安全科技中心設置條例」，整合為「行政院國家資通安全會報」、「科技部」、「國家資通安全科技中心」資安三級制，使國家資安政策、管理和技術 3 個層次的能量大幅提升。另為讓民眾了解政府資安作為，政府刻正推動資安政策 2.0，與過去最大的轉變在資訊透明化、掌控全局及培育人才等 3 項措施，對增強我國資安防護的力道極具正面效益。