2017 TWIGF工作坊提案書

Submission Date	2017-04-06 22:45:47
提案名稱	人工智慧時代的資安挑戰與展望
預計主持人	

姓名	組織/單位	職稱
林宗男	國立臺灣大學/電機工程學系	教授

聯絡人	林 宗男
組織/單位	國立臺灣大學/電機工程學系
E-mail	tsungnan@ntu.edu.tw
所屬利益關係者類別	學術機構
提案所屬子議題	網路安全

請描述擬討論之議題

緣起說明：

隨著人工智慧(Artificial Intelligence, AI)技術的快速發展，歐美各國無不紛紛發表白皮書，爲即將到來的「人工智慧第一的年代」(AI-First Era)進行國家政策與安全議題等討論。2016年10月，美英兩國政府就分別發表了兩份有關AI的國家報告，討論面對即將來臨的AI時代，國家的整備度以及對挑戰的因應。隨即在11月，英國政府科學辦公室（Government Office for Science）發表政策研究報告，將AI視爲推動第四次工業革命的未來技術，指出該技術將對勞工需要的技能產生衝擊，許多傳統工作將隨之改變。吳軍博士在《超級智能時代》一書指出：第四次工業革命來臨，2020年前有500萬個工作機會消失，.....智慧革命中，前2%的人掌握世界，其餘98%將被淘汰。

對於資通訊與網路安全專業人士來說，不斷演變的環境代表新威脅挑戰與發展機會。目前網路駭客已能綁架電腦去攻擊其他系統，若再加上AI，網路攻擊將可能更爲凶猛難測。以網路常見的釣魚和贖金勒索攻擊爲例，攻擊者一旦駭入裝置和電腦監控使用者的通訊後，只需基本的機器學習演算法，經過一段時間的觀察，就能模仿使用者的寫作風格與他人聯繫，並說服受害者點擊惡意鏈接或附件，達到惡意攻擊的目地。相同的機器學習演算法，同樣可用於綁架社交媒體帳户或竊取網路購物資料。當然，從防駭的工作者與資安產業而言，AI也代表著成長的機會，可透過AI研究分析攻擊者過去的行爲，發展自動化的調查演算法來追踪駭客，反而可預測並防止未來類似資安事件的發生。

有鑒於此，特於「臺灣網路治理論壇」(TWIGF)年度活動中，以「人工智慧時代的資安挑戰與展望」爲主題，探討AI對資安帶來的挑戰，以及展望如何運用AI來提升資通訊安全。

議程規劃：

●人工智慧、社會網路及網路安全

今日IT與AI的快速發展，個人隱私與資通訊安全益形重要。透過Facebook等社會網路的研究，人與人在網路有密切的連結關係，如何進一步透過人工智慧掌握情資及網路上各種大數據，以追蹤掌握駭客、詐騙集團動向，用來防範犯罪成爲一個重要的努力方向。

●人工智慧應用領域的法制規範

人工智慧的關鍵在於大數據的採擷，蒐集、處理，運用大數據將是機器學習是否成功及有效率的重要因素。如何讓人工智慧在運用大數據時能夠發揮其應有的功能，而不會遭到誤用、惡用，對人類造成危害與侵權，這方面的道德倫理、法律及隱私等相關議題，有待進一步的研究規劃與討論。

●「智慧服務」發展的資安議題

簡總經理曾經說過：短期內的人工智慧只有兩個字來代表，一個叫做大數據、一個叫做機器學習，而「智慧服務」將是這些「技術」的最終目的，會有拿些資安議題？「智慧服務」加上「資安防護」是否有可能創造出另一個新的產業?

●人工智慧之資安衝擊與因應

隨著智慧聯網與人工智慧蓬勃發展，駭客攻擊行動也朝向自動化與智能化，彈性的躲避與隱匿技術、仿正常的行爲造成資安的威脅，有如矛與盾的競賽，藉由資安技術與AI的結合，追蹤與防止駭客威脅，將成爲資安防護發展之趨勢。

預期時間

90分鐘 （建議）

預計與談人（建議 3~5人）

姓名	組織/單位	職稱	確認參加
洪偉淦	趨勢科技	台灣暨香港區總經理	已確認
顧振豪	資策會科技法律研究所	主任	已確認
毛敬豪	資策會資安科技研究所	組長	已確認