網路沒有距離，也沒有秘密

■ 陳鈺津

科技發展日新月異，短短幾年內大幅改變你我的日常生活，以前如同科幻電影中天馬行空的想像—智慧化的手機及家電，已逐漸成為我們生活中不可或缺的元素。

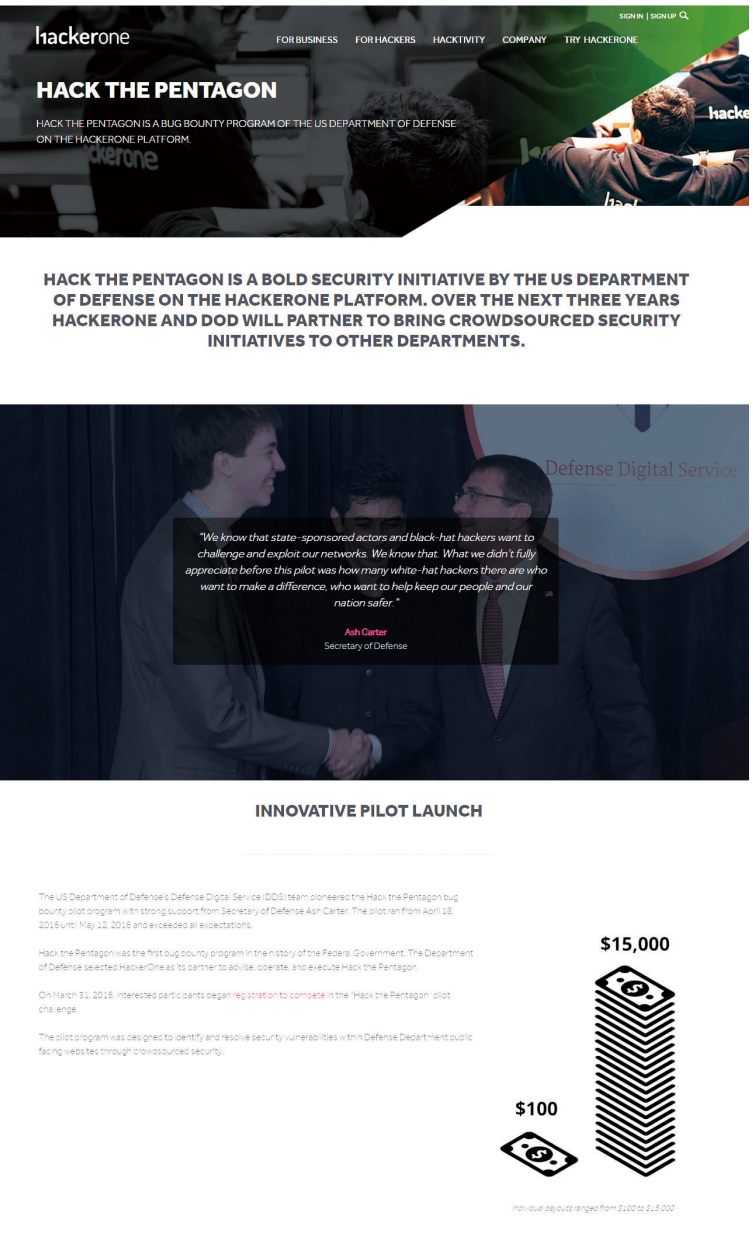
依據研究資料預測，到 2020 年全球將會有五百億筆資料在網際網路中流通，並透過網路空間交換、取得及蒐集等。也就是說，眾多機敏資訊在轉瞬間，便流傳於網路空間，無形中增大被滲透破壞與情蒐空間，不但極易肇生資訊安全危機，更將損及國家安全與利益。科技帶來生活上的便利，也同時伴隨潛在的問題，這些設備功能越是強大，我們對科技的依賴性越重，一旦遭到有心人士惡意破壞，所造成的傷害也越大。

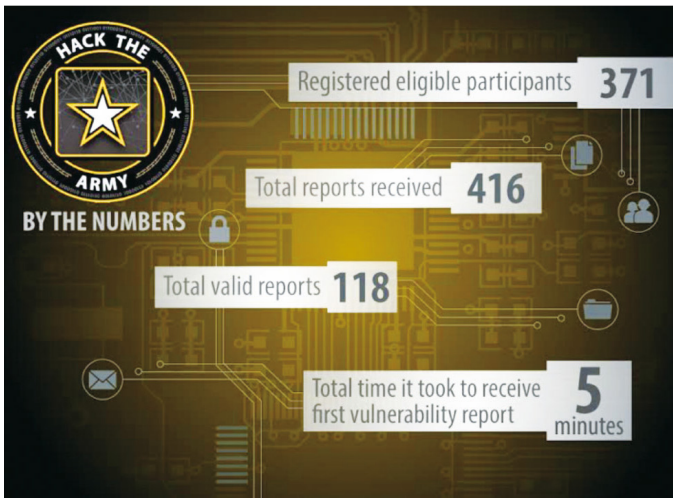
美國 2013 年《華盛頓郵報》曾報導，大批駭客企圖入侵美國國防部、國務院、能源部、國土安全部，甚至武器承造商的網路，並成功入侵眾多民間公司企業的網路；當時駭客隨意進出電腦系統，既沒有犯下鍵盤輸入上的錯誤，也沒有留下入侵途徑，過程僅僅不到 30 分鐘。美國國防部事後即意識到問題的嚴重性，並於 2016 年實施「駭入五角大廈」（Hack the Pentagon）計畫（之後陸續舉辦「駭入軍

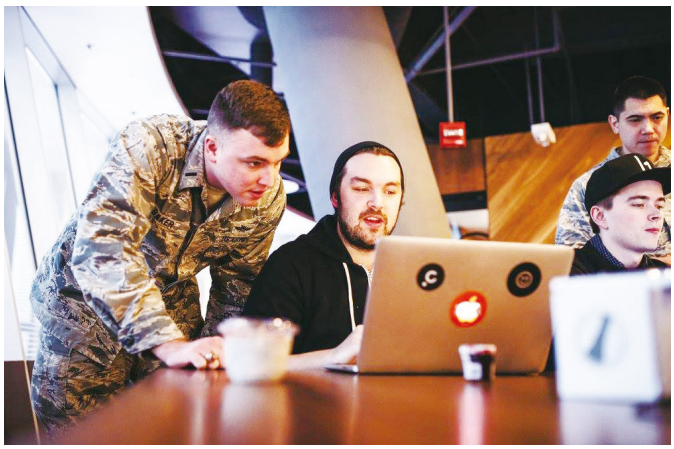
智慧化手機及家電為人們提供便捷的生活，但在日益依賴網路科技的同時，卻也可能衍生出不少潛藏的資安危機，造成國家安全與社會利益的損失。

隊 Hack the Army」及「駭入空軍 Hack the Air Force」等計畫），自實行迄今（2018）年，已藉由外部人員找出美國國防部等網站超過三千個以上的漏洞，美國因此頒發了逾廿七萬美元的漏洞獎金。此種僱用大批駭客，邀請他們測試及入侵官方電腦的方式，有助於美國國防部對症下藥，防患資安危機於未然。

市面上充斥著各式各樣的科技產品及五花八門的 APP，但其中隱藏許多資安漏洞與後門程式，往往在一時疏忽下，輕







美國國防部交由 HackerOne 承辦營運的 bug 賞金計畫「Hack the Pentagon」，此後更續推出「Hack the Army」、「Hack the Air Force」計畫，已為美國國防部等網站找出三千個以上的安全漏洞。（Photo Credit: HackerOne, https://www.hackerone.com; Official United States Air Force Website, https://www.af.mil/News/Photos/igphoto/2001855476/mediaid/2397030）

易將個人資料外流，因此，在使用產品或軟體時，應更加謹慎小心。現今由中國大陸設計、研製的部分行動裝置，因價格低廉、功能完善，吸引不少民眾青睞。但早在 2012 年美國眾議院提出的調查報告中，即指出部分中共廠商背後所隱藏的軍方背景，並已引起國安及商業機密遭竊疑慮。美國國防部更於今年 5 月初下令禁止全球的美軍軍事基地內零售商店銷售由華為和中興通訊製造的智慧型手機。

美國前資安長達布斯基（Lance Dubsky）於 2016 臺灣資訊安全大會上公開表示「臺灣是全球被網路攻擊最多的地區」；另依據微軟 2018 年亞太資安研究報告指出「臺灣 2017 年總計因資安威脅造成 270 億美金的經濟損失，將近臺灣 GDP 的 5%」。

面對資安威脅所造成之經濟巨大損失及國安風險，各機關除應持續落實「實體隔離」，建置嚴密的資安防護機制外，更應加強教育所屬建立正確保密觀念。使用各項科技產品時，應體認「網路上沒有距離，也沒有秘密」，公務機關更應避免透過社群媒體、通訊軟體談論機敏公務或傳輸資料，以免國家機密資料遭竊取。

全民若能有健全的保密認知，慎選資訊產品，便能在享受便利的同時，大幅降低資安威脅的風險。唯有每個人具備高度警覺的資安意識，個人隱私、企業利益及國家安全方能永保無虞。

美國前資安長 Lance Dubsky 來臺參加 2016 臺灣資訊安全大會時指出，臺灣是全球被網路攻擊最多的地區。（Photo Credit: Lance Dubsky's twitter, https://twitter.com/CyberCondor/status/706693272769576960）