出國報告（出國類別：開會）

出席 2018 年物聯網安全會議(IOTSF)與歐洲黑帽會議(Black Hat Europe)報告

服務機關	姓名/職稱
國家通訊傳播委員會	劉邦灶 技士
財團法人電信技術中心	陳振銘 工程師

派赴國家： 英國倫敦

出國期間： 107 年 12 月 3 日至 12 月 8 日

報告日期： 108 年 2 月 23 日

摘要

物聯網安全防護是近幾年國際間熱門話題，我國政府也正積極累積物聯網安全防護能量，研訂相關重點設備資安檢測技術指引，期望為我國塑造一個安全可信賴的物聯網應用環境。為完備政策研訂並與國際接軌，安排參加本次會議，以掌握相關議題的國際發展趨勢。

本次行程第一站是物聯網安全會議，該會議是由物聯網安全基金會(IOTSF)每年在英國舉辦的年度會議。本次會議討論主題從往年會議的「建立可信任和安全網路」，延伸到全面性安全，討論議題環繞著企業如何讓自家產品安全功能符合國際要求，並且發揮最大效益，讓物聯網確實能夠提升人類生活品質。而值得注意的是，IOTSF 在會議上發布最新版本的物聯網安全合規性框架，為企業和使用者在產品設計、製造和使用上提供了一系列的安全建議。

本次行程另一場參加的會議是同樣在英國倫敦舉行的 2018 歐洲黑帽會議。黑帽會議為全球性的知名資安會議，在黑帽為期 2 天的議程中，舉辦了許多不同類型的研討會，最多有 4 場不同主題會議同時進行。考量物聯網安全和人工智慧是未來資安發展著墨的重點項目，所以本次選擇參加以物聯網相關和人工智慧在資安的應用為主題的研討會。

藉由參與本次兩場會議，可了解國際資安領域發展趨勢和相關的國際規範和標準最新動向，作為我國政策研析之參據，技術人員亦可與國際專業資安人員進行技術交流和收集可利用的資安開源工具，提升資安技術開發能量。

目錄

圖目錄

表目錄

壹、 目的

新一波網路安全挑戰將聚焦於物聯網安全，典型物聯網系統運用著巨量數據和交錯複雜的網路，而低耗能的設計讓物聯網設備佈點上更為彈性便利，也造就設備軟韌體在修補漏洞時困難性，隨著越來越多的設備連上網路，也不斷擴增駭客可以攻擊的面，讓他們的攻擊手法可以變得更多樣性。然而，安全防護產品從來無法宣稱百分之百，即便是經過安全檢測為防護能力完善的設備系統，也不代表日後不會被攻破。此外，雖然資安人員可以由電腦和行動手機汲取以往的資安教訓，類比應用於物聯網安全上，但物聯網的應用仍持續蓬勃發展，其安全挑戰也是不斷進化中。因此，持續關注物聯網和網路安全技術發展與國際趨勢有其必要性，基於撙節政府預算原則和會議的時間地點相容下，本次安排參加了 2018 年物聯網安全會議和歐洲黑帽會議。

貳、 過程

一、 會議介紹

(一) 物聯網安全會議

物聯網安全會議是由物聯網安全基金會(IoT Security Foundation，IOTSF)每年在倫敦舉辦的年會。IOTSF 創建宗旨在於確保物聯網安全，促進設備安全使用，並發揮其最大效益。因此，IOTSF 為製造和使用物聯網產品和系統的人員，提供適當安全知識和最佳實踐建議。

本次物聯網安全會議是 IOTSF 第四屆年會，於 2018 年 12 月 4 日在英國倫敦 The IET Savoy Place 舉辦。往年會議主題設定為「建立可信任的網際網路」、「了解安全連線」，而今年則延伸到「全面性安全」，討論企業如何提供安全功能和用戶如何實施這些功能，讓物聯網塑造人類智慧生活的宏大發展願景能夠順利實現。

(二) 歐洲黑帽會議(Black Hat Europe)

黑帽是全球上最具技術性和最具相關度的資訊安全系列活動。自 1997 年成立以來，黑帽從最早拉斯維加斯的單一年會發展成為國際上最受推崇的資訊安全活動，現今黑帽的培訓課程及研討會每年都會在美國、歐洲和亞洲舉行，為資安專家學者、從事人員和關注資安領域發展者，提供了一個專業技術交流平臺，討

論了最新的資訊安全研究、開發和趨勢，鼓勵學術界、研究人員以及公私部門之間的成長和合作。

這次 2018 年歐洲黑帽於 12 月 5、6 日在英國倫敦 Excel London 舉辦，研討會共有為應用安全、密碼學、漏洞利用開發、硬體/嵌入式元件、物聯網、惡意軟體、平臺安全、逆向工程和人工智慧等 17 類型主題，本次參加則著重於物聯網和人工智慧相關主題。

二、 會議摘要

(一) 物聯網安全討論熱度升溫

隨著雲端運算、大數據分析和通訊技術發展成熟，物聯網在環境和技術條件俱全，也跟隨著水漲船高，物聯網結合不同領域激發了新興型態應用模式，如智慧工業、智慧城市、智慧醫療、智慧交通、智慧家庭及線上支付等，而且在設備將會朝向多功能與複合式應用。舉例來說，智慧型手錶原本只是消費者所使用連網穿戴裝置，也可具備測量使用者的心律，而測量人體心律則屬於醫療行為。此作法彰顯出物聯網裝置已邁向跨領域應用。然而，除非能夠確保物聯網是安全可信賴的，否則將無法順利發展下去，因此，物聯網如何做到安全防護與保護個人隱私變成為現今兩項重要課題。

IOTSF 主席 Paul Dorey 在物聯網安全會議開幕致詞表示，不安全的物聯網設備可能造成車輛失控、醫療資料外洩，駭客可透過無人機入侵無法到達的設備進行內部滲透，或重大基礎設施回報錯誤訊息。因此，必須讓每個人都能夠認識資安在物聯網中的重要性，了解如何對於物聯網攻擊進行防衛，並且鼓勵相關廠商及開發人員能很積極地提升本身的資安能量並將其物聯網產品具備資安防衛能力。

圖 1、IOTSF 主席 Paul Dorey 在物聯網安全會議開幕致詞

(資料來源：IOTSF)

考量物聯網跨領域且設備常分布廣泛的特性，以物聯網設備為標的網路攻擊預防及應變處理將變得相當複雜，各國政府逐漸認識到物聯網設備安全的重要性，嘗試著制定相關資安要求與法規。美國加州在 2018 年通過了一個與物聯網裝置相關法案，對於物聯網設備的密碼設定有了基本要求；而歐盟 2018 年底通過網路安全法(EU Cybersecurity Act)，設定了歐盟產品安全驗證架構，為產品安全驗證體制建置統整一致性架構，促進歐盟安全性產品發展。

(二) IOTSF 物聯網安全合規性框架

IOTSF 發表了一份最新的物聯網安全合規性框架(IOT Security Compliance Framework)文件，該文件參考了 3GPP、ETSI、NIST、FIPS、IETF、ENISA、GSMA、ISO 等指標機構的相關標準，為物聯網設備製造商和使用者提供了在設計、生產和使用階段，物聯網產品應具備安全功能要求的建議，以結構化程序引導文件使用者完成所設計的問卷和證據收集，確保安全程序和功能夠適當的被採用。

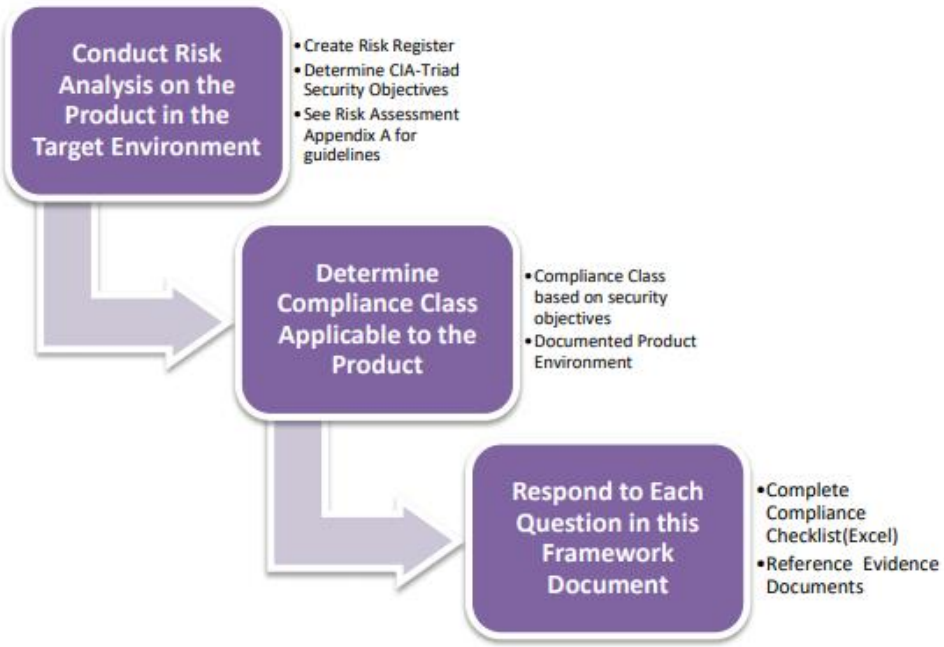

圖 2、物聯網安全合規性框架之評估步驟

(資料來源：IOTSF)

物聯網安全合規性框架先以資安領域的 CIA 為評估基準(即機密性 Confidentiality、完整性 Integrity 和可用性 Availability)，依照產品運用情境(Context is Everything !)，經過風險評估判斷該物聯網設備適用的等級，而該框架設定的合規等級共分為五個等級，相同的產品在不同的使用情境，也會有不同的評估結果。例如，同樣是連網溫度計，商用溫室和高科技半導體實驗室的使用環境，依據 CIA 基準就會評估出不同的合規等級。

表格 1、物聯網安全合規性框架級別與 CIA 關係對照

Compliance Class	Security Objective		
	Confidentiality	**Integrity**	**Availability**
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

(資料來源：IOTSF)

然後，依據所評估的不同合規等級，該框架提供了相應不同程度應具備的安全功能和佐證資料的建議，而這些建議以類型區分，就可分為企業安全程序與政策責任、設備的硬體及實體安全、軟體、作業系統、有線無線介面、驗證及授權、加密與金鑰管理、使用者介面、行動應用、隱私保護、雲端與網路元件、供應鏈及生產安全、組態設定以及設備擁有權轉移等 14 個面向，可理解物聯網設備很難有一體性通用安全功能要求。

(三)　安全設計及情資共享

物聯網上所使用的設備具有多樣性和複雜性，而常見物聯網運作架構可分為感測層、網路層及應用層。開發商根據其產品標的和技術環境，選擇所採用的技術標準或通訊協定，開發出各式各樣不同的物聯網產品。選用不同的通訊協定或技術標準，同時也產生不同的資安風險，防護複雜度相應提升，再加上物聯網設備通常存在先天硬體資源有限的條件下，將使得事後補救難度大幅提高。每個物聯網設備都應需要具備基本防護能力，而最有效率提升防護能力的方式就是安全設計（Secure by Design），廠商在開發產品階段，應考慮國際間已經存在的解決方案，並尋求在物聯網資安研究的專家協助，透過安全設計的觀念，讓產品在開發初期就已經具備資安防護的功能。

而情資共享則是確保物聯網安全的另一個重點，透過即時情資分享和應變處理機制，可大幅降低惡意攻擊所造成的衝擊及損害。因此，情資共享平臺和通報機制是至關重要的，製造商需要及時通報產品弱點，而使用者在收到通知後，也需要進行適當應變處理。透過設備安全設計及情資共享機制，方能讓物聯網設備在不同領域上的應用更加安全。

(四)　建置資料庫及自動化

為確保物聯網安全，國際間相應陸續推出相關規範和標準，物聯網設備製造商將需要確定自家產品符合相關安全標準規定，而產品進入市場時效(Time to Market)又是產品能否獲利的關鍵因素，產品檢測文件準備繁複及送檢時間冗長會使得廠商望之卻步，如何節省時效和化簡流程是推動產品檢測的重要課題，專家建議可進行國際相關規定盤點，轉化為技術共通語言的文件(如共同準則的保護剖繪 PP 及安全標的 ST 文件)，再建置資料庫及發展自動化工具，以減輕廠商送檢負擔。

面臨物聯網高複雜及涵蓋廣特性，如何防禦大量及多元化的網路攻擊，成為企業和使用者的一大難題。專家指出，透過自動化的幫助可以快速協助防禦物聯網之相關攻擊。而且自動化也可以讓使用者快速布置其系統以防禦層出不窮的網路或針對設備的攻擊。開發自動化系統過程中，資料庫的建置為最重要的一環，

資料庫可提供相關研究資料、產業標準及已公開資安情資，並且可以讓自動化系統過濾不同攻擊方式，進而確保其準確性。

(五)　未來科技與物聯網安全

量子技術是目前加拿大、英國、美國、中國、俄羅斯及歐盟等所要發展的目標。而透過量子技術而製造的量子電腦則能提供更快速的資料處理能力。雖然量子運算可以帶來大幅升級電腦處理資料的速度，同時也將造成目前所制定的公鑰加密標準可以更快速的被破解，進而可能觸及國家層級的資安威脅。

目前很多資安專家與學者著手研究新的加密技術－敏捷性加密(Crypto Agility)，期望未來物聯網設備可藉由敏捷性加密的方式來保護資訊傳送與儲存。所有物聯網設備可以透過不同網路通訊協定存取合適的加密演算法。當敏捷性加密系統中的一個演算法被量子電腦所破解時，只需要對其加密系統做更新動作，並可以達成所有設備的加密更新。

表格 2、量子運算對加密技術的衝擊

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

(資料來源：Report on Post-Quantum Cryptography)

(六)　物聯網通訊協定漏洞

物聯網可被應用在工業、醫療、金融、零售、交通及農業領域上，而這些不同領域上的物聯網設備，常藉由清量共同通訊協議彼此傳送資料。其中，MQTT 及 CoAP 為兩個被廣用的通訊協定。在物聯網架構下，感知層設備多半使用微控制元件(MCU)，並且以電池供給電源，所以這些設備設計之初，必須考量在硬體能力有限及功率損耗等條件下，以較低的延遲及電力耗損傳送資料。

MQTT 是一個非常輕量級的發布/訂閱消息傳輸協定，因而被大量運用在物聯網的環境中。由於當初在 MQTT 的設計中，並無任何資訊安全的考量，造成許多隱私資料可以藉由明文傳送。並且並無任何安全控管，造成任何人皆可訂閱 MQTT 所發布的資訊，尤其在工業控制的環境中，採用大量的物聯網裝置傳送資料進行分析，所以相關設備商應留心自家設備是否已針對此漏洞已進行修補，以避免惡意者有機可圖。

(七)　資安不再只是技術性議題

黑帽會議創辦人 Jeff Moss 於本次歐洲黑帽開幕致詞指出，理解與溝通將是資安人員的一大新挑戰，因網路安全議題已經從專門技術領域延伸到其他領域，不再僅是傳統的網路犯罪，也出現了選舉干預、假新聞流竄、負面宣傳等應用模式，大大觸及國家安全和社會動盪，各國政府也紛紛重視相關議題。因此，技術人員不僅是需要具備專精技術，更需要理解與其他領域與溝通詮釋能力，才能夠與其他利害關係者解釋和解決問題。

圖 3、黑帽會議創辦人 Jeff Moss 開幕致詞

(資料來源：歐洲黑帽)

而全球網路空間穩定委員會（Global Commission on the Stability of Cyberspace，GCSC）主席也是前愛沙尼亞前外交部長 Marina Kaljurand 在黑帽專題演講提到，愛沙尼亞是第一個國家遭受具政治動機的網路攻擊，這個事件發生在 2007 年，當時愛沙尼亞的國家關鍵基礎設施遭受散式阻斷服務攻擊(DDoS)

攻擊，公共和私人機構網站和服務因此而停擺，至此之後，資安成為愛沙尼亞國家重大政策。Marina Kaljurand 表示，網路攻擊日後將變成常態，且攻擊規模也將越來越大，而網路沒有邊界，多方利害關係人合作是在網路空間建立規範和防止資訊網路戰升級的唯一途徑。因此，Marina Kaljurand 呼籲各國和各界應盡早協力合作，方能抵禦未來的網路攻擊。

圖 4、全球網路空間穩定委員會主席 Marina Kaljurand 呼籲國際資安聯防
(資料來源：歐洲黑帽)

Marina Kaljurand 並提及，GCSC 在 2018 年 11 月宣布了發布 6 項規範，幫助促進全球和平使用網路空間。規範導入解決個別風險影響網路穩定的通用規範，這將有助於指導身為全球社會一分子的各國政府、企業及公民團體促成網路穩定。這些規範分別就防止資料竄改、ICT 設備入侵感染、公平程序、減輕損害、非國家攻擊者和網路衛生等面向提出建議。

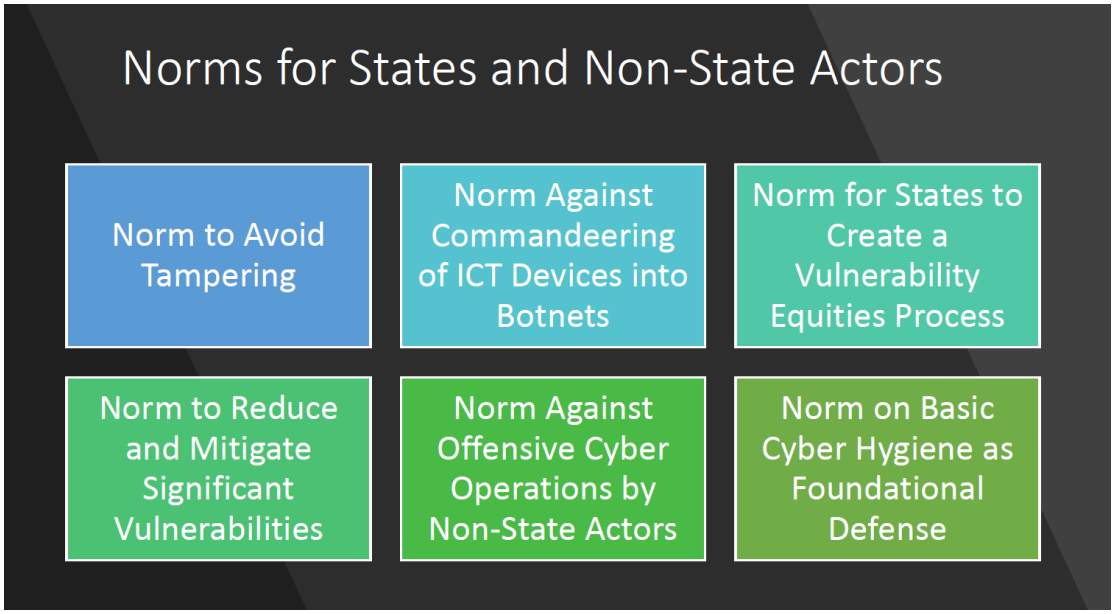

圖 5、全球網路空間穩定委員會發布六大規範

(資料來源：講者簡報)

(八) 人工智慧 + 資訊安全

這次歐洲黑帽研討會，有許多專家學者提出如何運用人工智慧與機器學習技術，輔助和提升資安防護能力。

機器學習中的監督式學習為最常被應用在資安的一項技術。監督式訓練透過大量的網路流量及惡意程式的行為，產生模型來判斷攻擊行為的能力，並進而判別攻擊類型與風險等級。而在人工智慧的應用上則被應用在偵測釣魚網站。近年由於網際網路普及和消費者習慣逐漸轉向線上購物，造成惡意攻擊者嘗試架設釣魚網站，以騙取受害者的金融資料。因此，許多資安專家致力於人工智慧技術，能更加快速辨別釣魚網站，更加迅速保護民眾免於受騙上當。

圖 6、釣魚網站氾濫趨勢

(圖片來源：APWG Phishing Activity Trends Report 1st Quarter 2018)

除了使用人工智慧或機器學習技術來研判可能的惡意攻擊行為或程式，部分資安專家也分享如何利用人工智慧的技術而產生的深度仿冒(Deep Fake)，而深度偽冒目前正最廣泛應用在生成虛構影片。

近年來，人工智慧技術成熟和公開免費資源大量釋出，Google 在 2015 年所推出的開源軟體「TensorFlow」以及 Facebook 在 2016 年所推出的開源軟體「PyTorch」，提供了大量人工智慧在圖片處理上的功能，如分析圖片中的物體、人臉辨識、物體偵測及人體圖像合成。深度仿冒則是架構在人體圖像合成的技術上。藉由已經存在的圖片或影片疊加在目標圖像或影片中，甚至是將知名人士的臉移植至虛構的影片中。

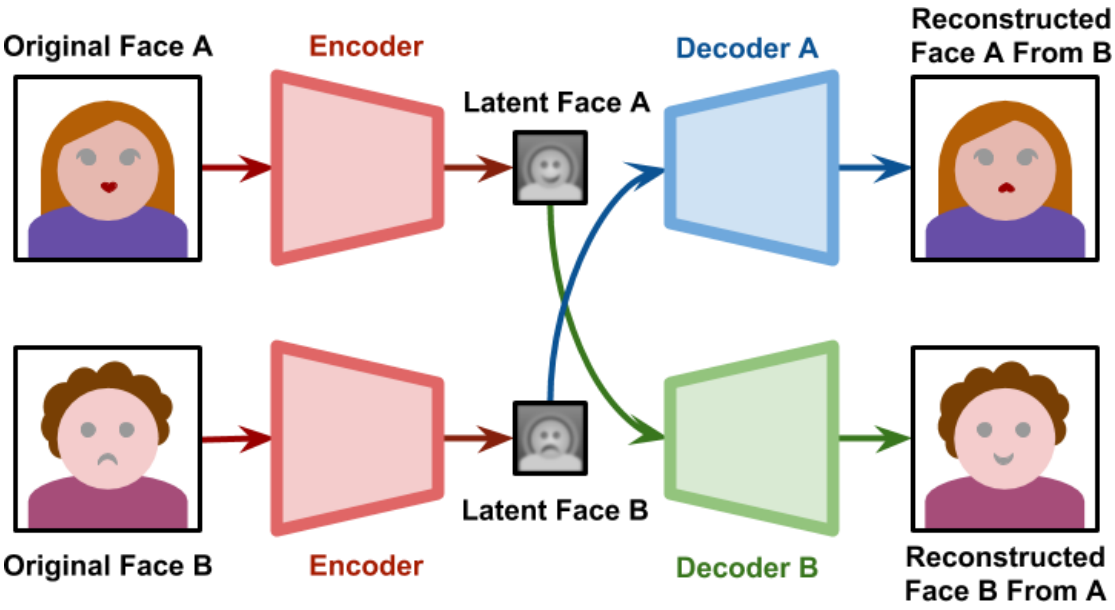

圖 7、深度仿冒技術基本原理

(資料來源：講者簡報)

仿冒影片可以不同方式形呈現以達不同目的，如名人假色情視頻，網路針對性政治宣傳等，而隨著經由神經網絡不斷嚴格訓練，識別虛假視頻將變得越來困難，進而造成災難性混亂。專家在會中說明，現今的仿冒影片仍可由一些生物特徵或習慣判斷真偽，如人類眨眼頻率，但隨著深度學習可能讓仿冒影片更為仿真。

圖 8、深度仿冒影片

(來源資料：講者簡報)

透過人工智慧的深度學習，除了可以對網路攻擊進行分析並區分種類跟預防

外，還可以對在殭屍網路中，用來控制受感染電腦的 C2 servers 進行偵測，以及偵測新的漏洞工具。然而，要藉由深度學習去偵測 C2 servers 或新的漏洞工具，必須先透過已知 C2 servers 或是相似漏洞工具的資訊進行建立模型後，深度學習才會依照資訊建立模型去進行偵測。研討會中，資安專家提出如果缺乏建立模型中所需要的惡意程式樣本時，能成功建置深度學習中所需要的惡意程式樣本。資安專家認為日誌檔本身所包含資訊已足夠建立模型。將日誌檔所記錄的每一筆資料中與遠端連接次數，平均傳送資訊容量與平均接收資訊容量轉成每一張圖片。當每筆日誌檔轉為圖形後，便可藉由深度學習中的卷積神經網路進行分析與學習。

人工智慧技術也可以舒緩資安人員困境。根據 Frost & Sullivan 指出，2022 年全球資安人力將短缺 180 萬人，比 2015 年增加 20%。因應資安人員短缺，各國目前正積極在培育適格的資安人員。然而，資安人才培養需要大量人力及財力資源，並非每一個國家都能承擔得起龐大費用支出。在這次黑帽研討會中，有些資安專家與學者建議，透過人工智慧的協助進行資安防禦系統開發，可以彌補實際人員的短缺。藉由人工智慧的學習，資安防禦系統可更加快速回應已知網路攻擊，而資安人員僅需要做審核和確認工作，大幅精簡資安人員的需求。

(九)　資安攻防研析

由於雲端時代的來臨，開發人員可藉由容器 (Container)輔助，將複雜的網站架設環境透過雲端服務，快速將網站架構完成。因此，近年容器技術已經被企業廣為接受。而透過容器開發，也可以強化資安防護，在資安環境中通常採用沙箱測試方法對惡意程式進行分析，但在微服務環境中，無法以目前已知沙箱測試方法，對在微服務環境中的惡意程式進行相關分析，透過容器式環境則能夠分析在微服務中的惡意程式。

然而，公共容器映像卻是充滿了漏洞，在這次黑帽研討會中，專家分析了 DockerHub 上前 100 個官方 Docker 映像，發現了數以千計的漏洞和錯誤配置。容器本質上應該是有效地完成一項任務，意味著應該定制容器以僅運行一個應用程序；然而，使用者往往附加不必要的功能在容器上，這也提供漏洞存在機會。因此，容器精簡化是不可忽視的重要工作。

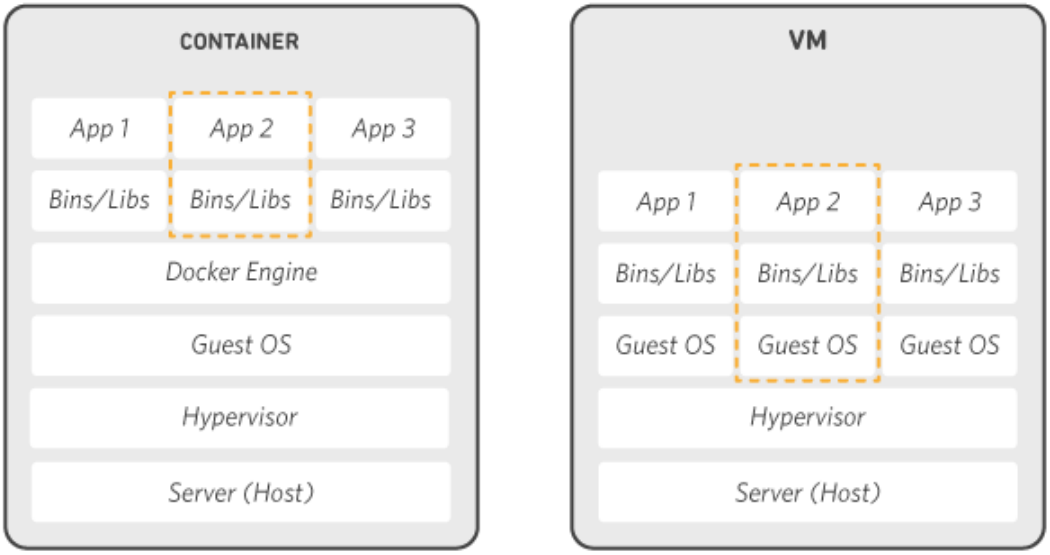

圖 9、容器 Container 和虛擬機器 VM 結構差異

(資料來源:亞馬遜雲端服務)

現今人們已經十分依賴智慧型手機,進行各種個人隱私和金融服務等相關操作,如訪問銀行帳戶、檢查電子郵件等。而隨著對智慧型手機依賴度越來越高,促使公共場所的免費充電站的拓展和攜帶式電池的推廣。儘管 Android 開發人員設計了預防措施來防止透過 USB 線傳輸數據,隱藏資料傳輸通道,讓裝置只進行充電功能(也就是所謂的「僅充電」模式)。但即便如此,這樣還是有機可乘的,黑帽研討會的專家演示,如何透過自己開發的一個 APP,藉由裝置硬體和電能特性如螢幕開關,將資訊轉成電訊號傳遞,並利用簡單電子元件模組接收訊號,進而成功竊取手機上的資料。

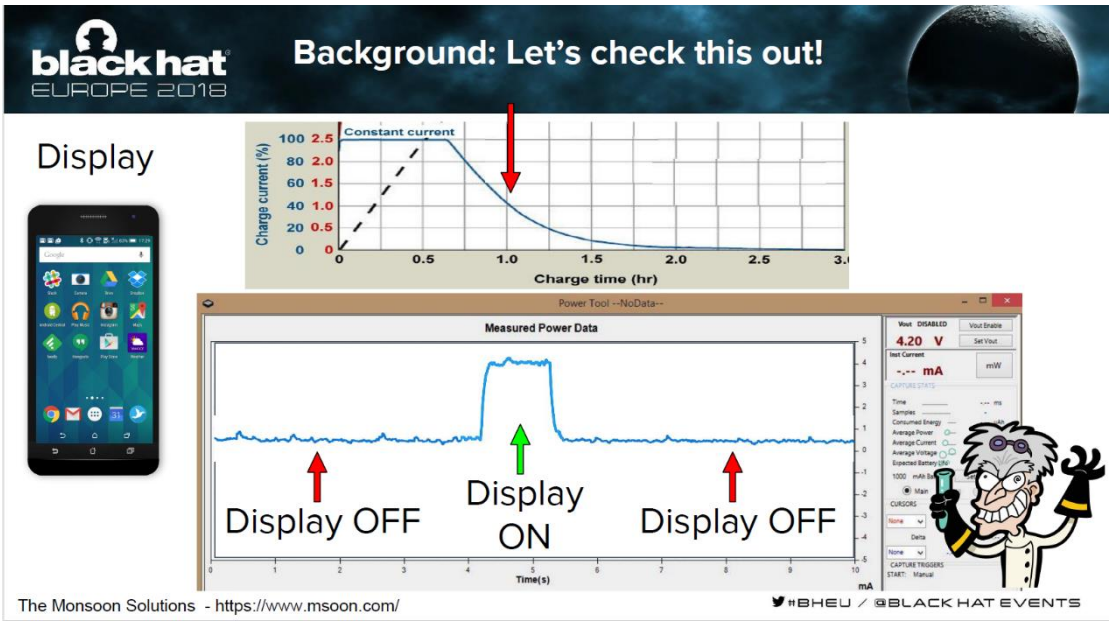

圖 10、手機螢幕開關與充電電流變化

(資料來源:講者簡報)

而如何密碼安全也是討論議題之一，在資訊安全領域中，密碼運用於使用者的身分鑑別，如何保護密碼而不讓其他人知道或以暴力破解的方式取得密碼，便顯得重要。駭客常會藉由社交工程、網站釣魚、或是透過字典檔猜測等手段取得使用者密碼。在今年的歐洲駭客大會中，一些資安專家分享了另一種竊取密碼的方式如溫度，由於人類是溫血動物，通常身體熱能會殘留在與所接觸的物體上。因此，當我們使用鍵盤輸入密碼時，所使用的鍵盤上就會留下熱能殘留。而駭客便可以透過熱顯像攝影機了解到我們在鍵盤上觸碰那些字元，進而加速他們猜測受害者密碼的機會。

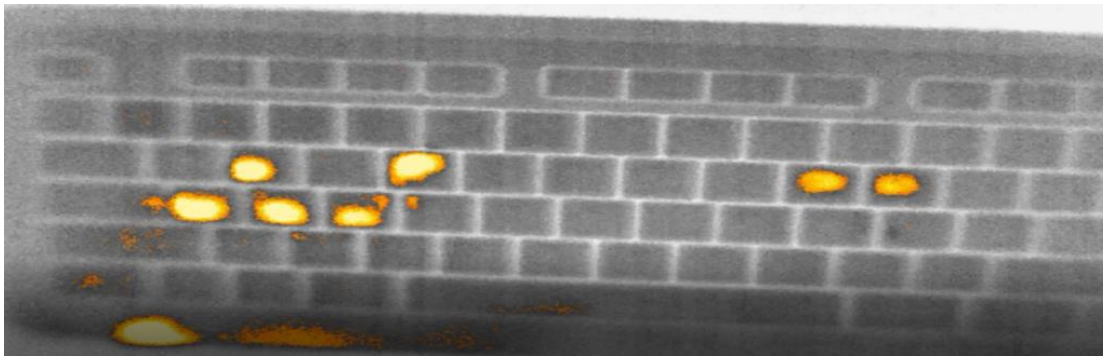

圖 11、鍵盤餘溫洩漏秘密

(資料來源:講者簡報)

利用設備物理特性的另一個案例則是振盪原理，電子元件都存在著共振頻率，透過尋找特定電子感測器、可編輯元件或是電子元件的共振頻率，可以顛覆被那些元件保護的系統，如從支援語音的物聯網和行動設備中的麥克風進行高頻率音波攻擊，使得某些可編程邏輯內震盪，讓防護系統失能或是可被繞道。

(十)　物聯網檢測工具分析

每一次黑帽大會有許多資安專家學者發表最新的資安相關研究，而黑帽大會也提供一個場域讓資安人員展示他們所開發的工具。本次會議中也見識到不少與物聯網資安相關之開源工具。

1、 IoT-Home-Guard

這套工具協助資安人員偵測目前智慧家庭中的裝置是否存在惡意程式，工具是透過樹梅派硬體裝置與無線介面或是透過軟體安裝在筆電上進行偵測。

2、 CHIRON

這套工具主要是提供在家庭環境中物聯網入侵偵測系統，透過機器學習的方式去解析 POF、Nmap、與 BRO IDS 記錄檔，並將分析後資料透過網頁顯示。使用者可利用此工具得知所有連接上網的家用物聯網裝置。

3、 Universal Radio Hacker v2

由於物聯網的快速發展，無線相關通訊協定也變得更為複雜，如傳統的 IEEE 802.11 無線協定，演化成 ZigBee(802.15.4)、Z-WAVE、LoRA、Bluetooth(802.15.1)與 Bluetooth Low Energy。資安研究人員不一定對於這些新的無線相關技術非常了解。透過此工具收集無線訊號並產生模糊測試進行資安相關測試。

4、 IoXT Hunter

此工具針對物聯網相關設備進行遠端探索及滲透測試，透過遠端掃描整個網域後，將所有在此網域內的物聯網裝置列表後，再對應到 CVE 弱點資料庫。

參、 心得及建議

物聯網設備逐漸普及於周遭生活環境，像是智慧手錶、空氣盒子、智慧插座、掃地機器人、智慧音箱等，物聯網設備基本功能就是連網，以達到收集和傳輸資料至應用系統後端進行資料分析與運用之目的。而物聯網將是盤根錯節的，其每個端點都可能存在著大小不一的資安風險，任一端點如不具備一定程度防護機制和適當應變處理機制，就會危及整個網路系統，所以如何讓物聯網設備安全就顯得格外重要。經過觀察本次會議相關議題討論的密度，了解到物聯網安全在國際間和各個領域有越來越受重視的趨勢，國際間也陸續推出相關架構和標準。本次物聯網安全會議發布了物聯網安全合規性框架，針對物聯網相關產品開發和使用，在不同運用環境下所需安全功能不盡相同，該框架給予廠商和使用者自我評估和蒐證的建議，以確認其產品設計和運用符合現行普遍的資安防護要求。

目前國際間對於物聯網安全產品檢測普遍由產業推動，廠商藉由自主性安全檢測，確保所開發的產品之安全功能是符合目標市場的需求與期待。而為了確保物聯網安全，我國政府正積極完備國內產品安全相關檢測標準及制度，通傳會和經濟部合作推動「物聯網資安標章」，鼓勵產業將產品送檢取得安全標章，近期通傳會就物聯網重點設備如無線網路攝影機、無線路由器、無線接取器、MOD及有線電視機上盒等，推出一系列資安檢測指引，經濟部也在 2017 年制定了「行動應用 App 基本資安檢測基準」，而政府機構也將在相關資通設備採購的規格需求上，要求具有安全標章的產品，以提升廠商將產品送檢誘因，確保我國政府所用資通設備具備一定程度的安全防護能力。

隨著人工智慧的技術漸趨成熟，尤其在 Google 及 Facebook 釋放所開發的軟體工具後，許多企業紛紛採用該工具進行開發人工智慧相關應用。資安專家學者們也開始藉由所開放的工具，進行人工智慧與資安相關研究及開發。而安全防護系統藉由人工智慧輔助，可加快偵測異常網路行為及惡意程式的散佈，並利用深度學習去預測駭客可能的攻擊模式。因此，人工智慧運用在資安領域，可以提升防禦網路攻擊、系統建置及開發的效率，並且有助於舒緩資安人員短缺議題。

另外，黑帽會議是國際知名資安技術交流平臺，每年在美、歐、亞洲舉辦，每次會議除了舉辦眾多場研討會，也設有大型展覽攤位，供資安公司、專家學者或是學生展示開發工具成果，對於有志在資安領域耕耘的夥伴，黑帽會議是獲取新知和洽談合作的不二選擇。

鑒於未來網路攻擊趨勢將大幅結合物聯網和其他不同領域技術，產生複合式攻擊，所以掌握新興技術發展及國際趨勢是至關重要的，我國政府應持續關注相關議題發展，以協助相關政策制定和推動，並確保與國際接軌，故建議持續派員參與相關會議。