出國報告（出國類別：研究）

赴澳洲參加 2018 年 CIFI 及 BSides Perth 研討會

服務機關： 內政部警政署刑事警察局
姓名職稱： 陳富添 股長
李立翔 警務正
黃翔偉 警務正
邱俊霖 警務正
許鈺晟 偵查員

派赴國家： 澳洲
出國期間： **2018** 年 **9** 月 **8** 日至 **2018** 年 **9** 月 **18** 日
報告日期： **2018** 年 **12** 月 **18** 日

摘要

網路安全涉及的領域及廣，包含網路智慧、網路安全、網路防禦及網路偵查等議題，解決方案有人工智慧(AI)、機器學習、密碼學、區塊鏈等方式，目前皆實作於國際資安廠商的商業軟硬體中，瞭解或引進國內增加國內的資安防禦能力或偵察能力便是重要的課題，另虛擬貨幣、硬體設備晶片拆解、滲透測試及惡意程式等相關議題，目前是我們數位實驗室及資安實驗室努力目標，唯有多接觸國外的實際做法及參予國際的研討會，才能促進我們研究方向與國際接軌，並與其並駕齊驅。

故此，世界各國均積極蒐集相關技術資訊、培育相關技術人才，尋求最佳解決方案或因應策略。本次參加的 CIFI 及 BSides Perth 高科技犯罪調查研討會即是國際間有關高科技犯罪及駭客技術探討與交流之重要年會，循例開設許多數位鑑識、資訊安全及網路犯罪偵查技術相關課程。

目次

壹、目的

2018 年 CIFI 安全研討會在雪梨舉辦，為全球知名的網路安全研討會，討論網路智慧、網路安全、網路防禦及網路偵查等議題，而 BSides Perth 研討會則是澳洲最富盛名的駭客年會，有各國專業人員參加，並有人工智慧、虛擬貨幣、硬體設備晶片拆解、滲透測試及惡意程式等相關議題展示，採密集與多項研習主題同時進行方式辦理，為持續提升本局科技犯罪偵查能力，指派本局股長陳富添率警務正李立翔、警務正黃翔偉、警務正邱俊霖及偵查員許鈺晟等 5 人參與會議，於同時間不同演講中學習國際最新科技知識，應用於科技偵查與數位鑑識中，期間訪視澳洲新南威爾斯州警局及澳洲聯邦警察局(AFP)數位鑑識單位等執法機關，相互研討問題、建立跨境打擊犯罪、資訊交換等國際合作管道。

此行藉由參加研討會及參訪等機會，瞭解新型態犯罪手法之最新數位鑑識與科技犯罪偵查方法，以作為國內科技偵查、數位鑑識技術發展與制度機制規劃之參考。

貳、過程

本次派員參加 CIFI 安全峰會及 BSides Perth 研討會參訪行程，規劃自 2018 年 9 月 8 日起至 2018 年 9 月 18 日止，共計 11 日。於臺灣時間 2018 年 9 月 8 日於桃園國際機場出發，搭乘中華航空前往澳洲雪梨，參訪執法機關及參加 CIFI 安全峰會；另於澳洲時間 2018 年 9 月 14 日自澳洲雪梨搭乘澳洲航空飛往伯斯，參加 BSides Perth 會議，於澳洲時間 2018 年 9 月 17 日至 9 月 18 日由澳洲伯斯搭機至雪梨轉機，由雪梨搭機返回臺灣桃園國際機場。

日期	預訂行程	內容	日數
2018 年 9 月 8 日	啟程	啟程赴澳洲雪梨（飛航時間計 9 小時 15 分）	1

日期	預訂行程	內容	日數
2018 年 9 月 9 日	整備會議資料	抵達雪梨 整備 CIFI 及 BSides Perth 會議資料	1
2018 年 9 月 10 日	參訪	參訪澳洲警察機關-新南威爾斯警察局(NSW)	1
2018 年 9 月 11 日	參訪	參訪澳洲警察機關-澳洲聯邦警察局(AFP)	1
2018 年 9 月 12 日	參訪	參訪數位鑑識設備廠商-UFED Cellebrite 公司	1
2018 年 9 月 13 日	研習	參加 CIFI 會議	1
2018 年 9 月 14 日	前往伯斯	搭機往伯斯 （飛航時間計 5 小時 5 分）	1
2018 年 9 月 15 日	研習	參加 BSides Perth 會議	1
2018 年 9 月 16 日	研習	參加 BSides Perth 會議	1
2018 年 9 月 17 日 至	返程	澳洲伯斯搭機至雪梨轉機，由雪梨搭機返回臺灣	2

一、 CIFI Security 研討會

CIFI Security Summit 每年都於亞洲、歐洲、澳洲及北美洲等世界各地分別舉辦，其包含研討會及商業展示，聚集各處資安專家共同討論「網路智慧」、「網路安全」、「網路防禦」及「網路偵查」等議題，

此活動亦是目前唯一由專業資安公司在議程內同時進行趨勢分析、案例研析及實作展示等大型研討會，本次參訪人員參加 2018 年 09 月 13 日於澳洲雪梨舉辦的場次，其上午為大會演講及座談會，下午則依上述主題分於 3 處會議室舉行專題演講，參加者可自由選擇相關議題聆聽及交流：

（一） 大會演講

會議首先由新南斯威爾州網路安全組織主任 Todd Williams 進行開場歡迎演說，該機構資金來源主要由該州政府資助，以大學內資安研究計畫為主軸，並從中介接產學合作，機器學習、雲端安全、資料分析、安全保證、加密學、應用程式安全等項目均為該機構之主要研究範圍。

接續由風險評估 SAI Global 公司 Andrew Bissett、James Whetherly 介紹如何建構主動式網路服務復原能力，其藉由風險評估與分析公司優先業務項目，找出關鍵網路復原能力元素，建構威脅預測之整合儀表介面，從而制定防災策略。

第三議程則以座談會形式舉行，會中邀請新南斯威爾州消防隊資訊安全長 Asaf Ahmad、Data61-CSIRO 資訊安全及隱私研究主持人 Dali Kaafar 博士以及 Newcastle 大學 Vijay Varadharajan 教授談論對付網路犯罪的政策及合作機制，例如機關組織間如何排解衝突，有效合作對抗網路犯罪、網路犯罪及科技治理在充滿網路風險時代的重要性以及藉由威脅情報共享建立互利關係。

資安公司 Darktrace 之網路安全部門經理 Tina Maugeri 於第四議程中展示以機器學習之網路防禦新方法，其以圖像化界面顯示攻擊來源及受害地點，讓人一目了然，該公司除說明如何用機器學習方法進行網路防禦以及視覺化效果之益處外，更以實際案例說明該系統如何

檢測到未知之威脅。

上午場次最後議程再度回歸座談會方式，以不斷更新的網路威脅環境中如何解決各處安全技術鴻溝為主題，席間邀請 Expeditors International 公司北、南亞區網路安全部門主席 Eddie Ng、Primary Healthcare Limited 公司資訊安全長 Wouter Veugelen 以及新南斯威爾州大學資訊安全及隱私研究實驗室主任 Sanjay Jha 教授，與會者分享主要著重於如何獲取專業人才以控制網路風險、如何帶領所屬團隊以確保其技術實用價值以及各種技術人員，如人工智慧 AI/機器學習 ML 或區塊鍊專業人才之未來。

（二） 專題演講

此研討會下午場次則分三主要科目「網路智慧」、「網路安全」、「網路防禦」及「網路偵查」在不同會議室同步進行專題演講，以下簡要說明各項目講者分享內容：

1. 網路智慧

(01) **建構網路風險雷達**：SAI Global 公司提出藉由解析內外部影響及威脅，剖繪關鍵商業活動之連結，評估驗證後，持續監控後續效果以達成主動式防禦功效。

(02) **如何偵測資料外洩管道及降低發生可能性**：Varonis 公司說明現今偵測資料外洩管道之時程冗長原因，以及其解決方法，並包含查得資料外洩管道後之應變措施，如何降低發生的風險。

(03) **了解顧客驅動的雲端應用程式安全性**：Netskope 公司發表現今雲端時代工作方式

的改變，例如 SaaS 及 IaaS 的應用及其帶來的開放和協同合作，在此應用情況下應如何採取對策以實現網路安全，該公司以資訊流為中心出發，說明如何一步步選擇採取正確方法，確保與公司之安全政策無違。

(04) **物聯網、雲端及大數據時代的網路安全**：Newcastle 大學教授於此議題中闡述來自物聯網隱私議題的主要挑戰及其研究和創新機會，辨識資料外洩或服務停擺之弱點以及物聯網的未來。

2. 網路安全

(01) **網路 AI 企業防禦免疫系統**：Darktrace 公司運用演算法及機器學習加強網路安全防禦，實作該免疫系統，其運用優先權概念及以視覺化分析威脅，讓使用者能更有效率的分配資源並同時降低風險。

(02) **新雲端時代的密碼金鑰解決方案**：SSH.COM 公司以亞太地區憑證管理狀態為始，帶入雲端存取控制之概念，以及該公司研發之系統架構如何以不使用密碼即 zero passwords 方式達成安全控制。

(03) **網路安全整體解析**：Horangi 公司第一步說明如何整合技術及人力資源，續將網路安全提升至企業範圍之風險評估，針對評估結果進行全面性的戰略考量追求最佳化的方

法。

(04) **網路安全及詐欺之風險管控**：Downer 集團藉由調整安全及詐欺的管理策略以及人工智慧來解決不斷變化的威脅，建構出資料來源及潛在威脅的全面性觀點。

3. 網路防禦及網路偵查

(01) **雲端空間偵查**：Magnet Forensics 公司探討雲端空間偵查，認為其重要性在於了解如何回復與取得雲端資訊，現今此類偵查日趨重要，尤以企業偵查為甚，另該公司亦指出電腦及智慧型手機資料相乎連結運用之重要性以求釐清事件全貌。

(02) **利用深度學習技術革新網路安全**：Deep Instinct 公司表示，機器學習技術可強化終端偵測效能，該公司運用 AI 人工智慧預測達成預防、偵測及回應如 APT 進階持續性滲透攻擊、zero day 零時差攻擊及 Ransomware 勒索軟體等惡意攻擊。

(03) **運用航空業案例增強網路安全**：(ISC)2 公司首先說明航空業如此安全之關鍵因素，再將相同的因素應用於網路安全，針對人、過程及科技進行研究，進而找出成功與失敗之方法。

(04) **網路安全、加密學及機器學習之未來**：Wollongong 大學教授分享其預先處理未經

分析之原始資料如何使用於機器學習，如何建構、應用並評估其演算法以偵測潛在威脅，過程中藉由自動化調整，最佳化其學習模型。

二、 Bside Perth 研討會

Bside 研討會所展示的議題主要與資訊安全有關，分別從系統漏洞、安全開發、滲透測試、數位鑑識等多種主題進行探討，並邀請不同領域的專家學者進行介紹，同時現場亦舉辦 CTF（Capture The Flag）搶旗賽，供與會人員進行駭客攻防演練競賽。整場研討會較無商業資安產品展示或介紹，純就技術層面進行研討，以下將針對本次研討會中，就較為重要之主題進行介紹及說明。

（一） 人工智慧如何應用於未來的資訊安全

講者目前擔任 Cylance 公司的副總裁，主要負責建立安全和信任機制以及公司營運，目前正與美國聯邦調查局 FBI 合作解決安全問題。

（二） 虛擬貨幣自動化交易

講者目前於 Hivint 服務，講者自行撰寫程式，運用自動交易技術，完成自動化虛擬貨幣交易，藉由本次講習，分享程式於開發過程中，所面臨到的障礙。

（三） 硬體設備晶片拆解及利用 root 權限存取

講者長期於資訊安全及滲透測試領域進行研究，同時也是多個企業及政府機關的資訊安全顧問。在本次演講中，介紹了從嵌入式設備讀取內部資料的破壞性方法。 特別是針對從電路板上卸除嵌入式多媒體媒體控制器（eMMC）晶片，以及存取內部資料的過程。同時也介紹如何將拆解後的設備恢復到原始正常狀態。讓我們得以理解整個運作過程及方法。

（四） 無線訊號無形中洩漏的訊息

講者是一名網路安全專家，在本次演講中，提到日常生活所使用的數位設備，其實不斷的透過無線訊號發送各種可能的

訊息，而講者便針對這個部分，展示如何擷取這些無線訊號，以及擷取後，資料呈現的效果。並且說明如何調整這些設備，以確保防護使用者的隱私。

（五） SecDevSecOpsSec

講者是一位雲端安全專家，講者提到在業界中，大家都喜歡將「DevSecOps」這類的流行用語掛在嘴邊，但並非所有人都清楚這些名詞真正的定義是什麼，所以講者在本次演講中，嘗試每個常見的資訊安全專有名詞進行定義，並使用她自己創立的自動安全流程的經驗為例，來解釋如何有效地使用每個流程。

（六） VoIP 駭客攻擊的目的主要是樂趣及利益

講者對於 VoIP 安全及駭客攻擊技術有濃厚的興趣及研究，VoIP 技術雖然發展很久，但仍少有相關研究團隊注意他的安全問題。在這次的演講中，講者介紹有關 VoIP 駭客的標準商業模式，而且所使用的方法通常都是跨境或跨司法管轄權，因此提高偵查的難度，同時利用一些範例，快速找出這些不安全的節點。

（七） 快速的運行 SDLC

講者提到在撰寫程式的過程中，會面臨許多挑戰，尤其是要在符合資訊安全的議題下，會有更多狀況，講者在本次演講過程中，完整的說明整個安全開發生命週期流程，並透過案例的介紹，說明如何找出這些漏洞，並且如何改進，讓整個程式可以更加安全。

（八） 關心滲透測試夥伴

講者是一位資訊安全專家，針對安全開發及滲透測試等領域頗有研究。目前程式開發相當注重團隊協作，尤其是安全測試人員與系統開發人員，通常是兩個不同的團隊，彼此間對於系統開發的認知也存有極大差異，所以講者認為應該要將這兩個團隊進行更多的溝通，加強彼此間的交流，以讓整個團隊合作更加順暢，並且讓程式開發更加安全。

（九） 開源軟體的漏洞狩獵

講者對於開源作業系統相當熟悉，長期從事尋找安全漏洞的工作，並在演講過程中，展示講者所發現有關 Linux、Linux、FreeBSD 及 NetBSD 等作業系統核心的漏洞。

（十） 利用微軟文件中的資訊隱藏圖片

講者是一位惡意程式及逆向工程的資訊安全專家，講者提到近年來越來越多駭客喜歡利用資訊隱藏技術將惡意程式寫入圖片，以規避相關安全防護措施。並在圖片裡面植入惡意程式或是中繼站資訊，然而目前已有許多軟體可以偵測這些惡意圖片，所以需要再載入其他文件檔案，已完美規避各種安全防護措施。講者並於現場展示如何完成一連串的攻擊行為。

（十一） 接管子網域名

講者是一位安全顧問，在本次演講中，講者說明駭客如何接管子網域，利用各種可能的方式進行攻擊，並且透過實際案例介紹方式進行說明。

（十二） 當惡意程式遇見工業控制系統及其結果

講者是一位工業控制系統研究人員，以最近中東地區工業安全系統遭受到惡意程式攻擊為例進行介紹，有一款名為

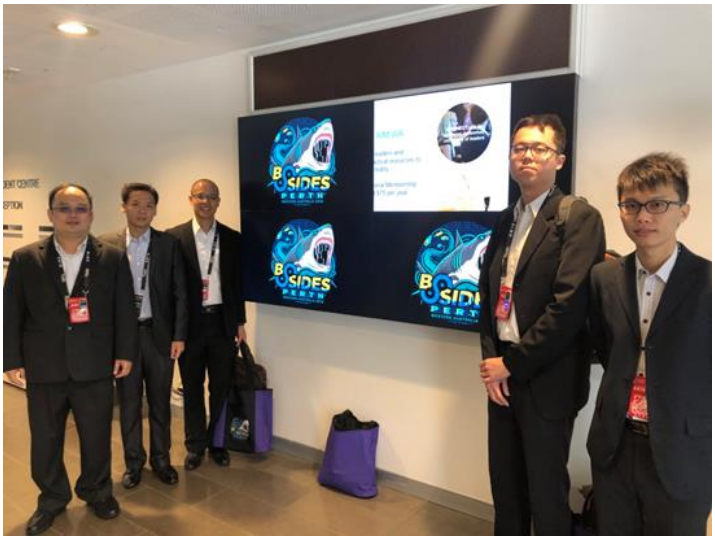
Triton 或 Trisis 的惡意程式會干擾或關閉這些系統，並且說明這款惡意程式如何影響相關設備，由於這些惡意程式專門設計用來破壞工業控制系統，而且這些攻擊可能都是來自有國家資助的組織所發動，整場演講便詳述這些攻擊時間及流程。

（十三） 如果執行安全的規則被破壞了，該如何修補

講者本身是一位律師，多年前進入資訊安全領域，本次演講主要是以不同面向看待資訊安全，分別由專業人士、職業、教育等觀點進行介紹及說明。

（十四） 診斷或爆炸

講者具有多年滲透測試經驗，是一名資訊安全專家，講者在演講過程中，提到許多有關過去執行滲透測試的案件，其中包含成功及失敗的案例，希望透過這樣的說明方式，將相關的經驗進行傳承及分享，避免未來其他資訊安全人員重蹈覆轍，浪費更多不必要的資源。



三、 參訪行程

（一） 參訪新南威爾斯州費明頓警區—澳本警察局

新南威爾斯州警政廳（NSW Police Force）目前計有 2 萬 725 名警力，轄區分「中央大都會區、西北大都會區、西南大都會區、北部地區、南部地區及西部地區」等 6 大區域，轄區面積約為 80 萬平方公里（約為臺灣的 22 倍大），並提供超過 790 萬人服務（約佔澳大利亞總人口數 32%），本次參訪費明頓警區(Flemington Local Area Command)總部位於澳本警察局中，地處雪梨中央商業區以西 15 公里的澳本市，該市在 20 世紀後半葉開始有一波波來自各國的移民群體，為澳大利亞最多元文化的社區之一，街頭隨處可見許多中東和亞洲的商店、餐館和超市。

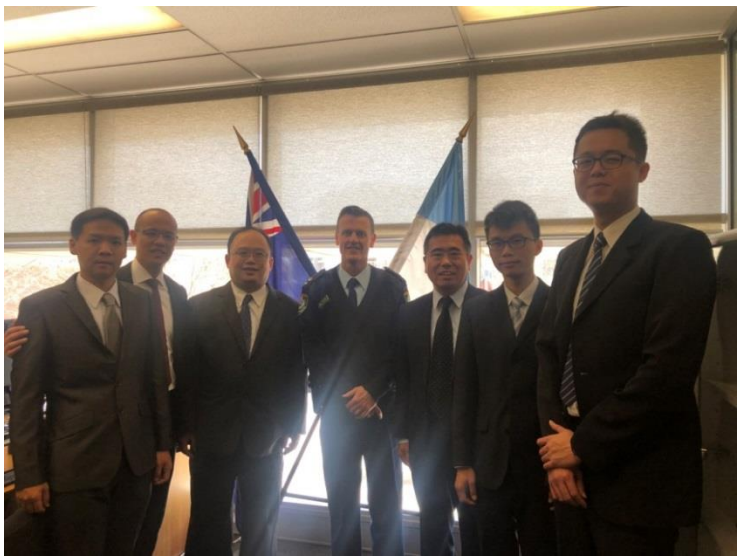
本次參訪由警區指揮官 Philip Rogerson 親自接見本局同仁，並由澳本警察局 2 名王姓及劉姓華人警察協助導引及翻譯(分別為 90 年代新加坡及中國上海移民)，另與該局刑事人員(Detective)及電子設備鑑識人員(Inspector)交流近期網路犯罪趨勢、執法技巧、偵辦方式及警察制度等，主題如下：

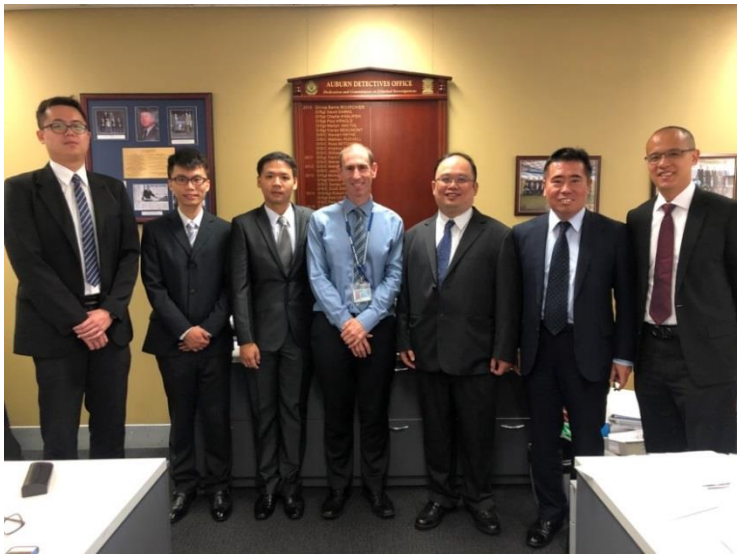
1. 澳大利亞是一個君主立憲的聯邦制國家，由6個州(新南威爾斯州、昆士蘭州、塔斯馬尼亞州、維多利亞州、南澳大利亞州及北澳大利亞州)和 2 個領地(首都領地及北方領地)組成，根據聯邦法律規定，州政府有自己的警察機構和統轄州內治安的獨立權力，故聯邦政府和州政府各自建立警察機構，分別執行和維護聯邦法律和州法律，行政上是平行、協助的關係，而不是上下級隸屬關係。

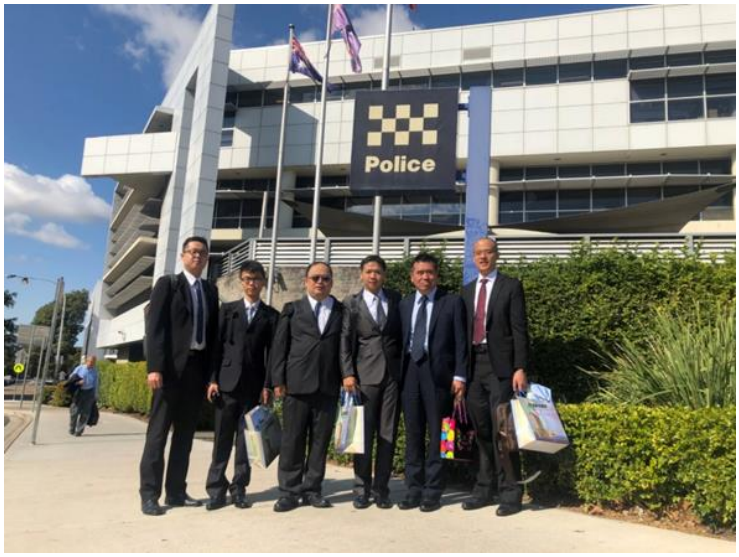
2. 警察每週勤務時數需服滿 38 小時，以澳本警察局為例，擔任綜合任務員警(General Duty)，負責處理各種突發的情況(如搶劫、謀殺、家暴、竊盜、鬥毆及交通意外等)，每天執勤時間為 12 小時，白天執勤時間從早上 6 點半到傍晚 6 點半，晚上執勤時間則從傍晚 6 點半到第二天凌晨 6 點半；另巡邏員警(Beat Police)開始值勤時間則視巡邏工作需要而定，每天執勤時間同樣為 12 小時。

3. 網路犯罪型態：該警局近年也遇到多件商務電子郵件詐騙(Business Email Compromise)，因絕大多數款項無法追回，如詐騙金額較高則向需往上報請總局調查，另亦有針對退休老年人以假投資詐騙手法發生。

4. 參觀人犯留置室、偵訊室、槍械室及偵防車等設施，會後該局致贈本次參訪同仁犯罪預防宣導紀念品及該局簡介。




AUBURN DETECTIVES OFFICE


Police

（二） 拜會駐雪梨台北經濟文化辦事處

目前本局在澳大利亞尚未設置駐外警察聯絡官，本次參訪警察局行程非常感謝駐雪梨辦事處秘書劉文章大力協助，不僅親自安排聯繫，更親自至下榻飯店接送參訪，大幅提升參訪效率，使得本次出國團員能在有限時程內完成任務，在此特向劉秘書表達感謝之意。另在劉秘書安排下，本次行程中亦抽空拜會我國駐雪梨辦事處，能在異國看到我國國旗，全體團員們有種莫名的感動！團員由我國駐雪梨辦事處處長王雪虹接見，過程中談到有關治安議題，部分國人從事非法打工行為，及針對華人社區的詐騙電話猖獗，常見詐騙手法為冒充領事館人員，聲稱受害者已經涉嫌犯罪或其身分已被盜用，進而被要求支付罰款或債款等，且受害者的澳洲居留簽證可能因此受到影響，也可能是接聽者本人或家人可能會受到傷害等威脅。據辦事處了解已有不少案例發生，並有多人受騙。團員們則提到，未來如有相關不法事件需我國警方協助，本局將全力協助查緝，共同打擊不法，會後並由王處長致贈全體團員紀念品及在辦事處門口合影留念。

（三） 參訪澳洲聯邦警察局(Australian Federal Police)數位鑑識實驗室

數位鑑識(Digital Forensics)主要係針對數位裝置中的內容進行調查與復原，常與網路犯罪案件相關，而澳洲聯邦警察局在布里斯本、雪梨、墨爾本、珀斯和首都坎培拉均設有數位鑑識實驗室，並為其他政府機關和執法機構提供服務，包括在搜查令執行期間，為識別檢查和保存電子數據提供現場協助、實驗室檢查電子設備和數據、恢復複雜的電子數據及法院出庭提供事實和專家證據等服務。本次參訪數位鑑識實驗室位於澳大利亞首都坎培拉近郊，由主管 Philip Goodwin 接待，會中並介紹該實驗室成員絕大多數為技術人員非警察人員，與我國迥然不同，另根據鑑識標的物不同而有其專用的鑑識實驗室(如手機、電腦、聲音及影像等專用鑑識實驗室)，並設有晶片解焊設備可將手機晶片解焊卸下進而讀取內容，因屬破壞性取證方式，一般而言非到沒有辦法時不會輕易使用。團員們則提到，目前有愈來愈多案件以數位證據作為犯罪事實證明，但數位鑑識實驗室能量終究有限，常需數週甚至數月處理待鑑識案件，無法即時滿足偵辦單位調查需求，此部分困境與澳大利亞警方相同。會後由本局股長陳富添代表致贈本局紀念品，並在實驗室大樓門口合影留念。

（四） 參訪 CBIT 數位鑑識服務中心(CBIT Digital Forensic Services)

該公司主要提供數位鑑識工具、各式資安訓練課程、電腦鑑識測驗及法院出庭提供專家證人證詞等服務，其數位鑑識軟體用戶遍及各州政府和聯邦政府執法部門，本局亦有採用，本次參訪該公司數位鑑識中心，由鑑識主任 George Athanasiou 接待，除參觀各項數位鑑識設備及軟體工具外，並了解到該公司各項採證及恢復數位證據作業流程，更進一步了解相關鑑識軟體訓練課程內容，以利本局評估參採。

參、心得及建議

CIFI 安全研討會常在亞洲、歐洲、澳大利亞和北美洲舉辦年度活動，匯集了來自全球的領先安全專家，討論領域極為廣泛，大都是資訊安全的廠商，針對廠商開發軟體提出專案說明，而今年的主軸在網路智慧、網路安全、網路防禦及網路偵查等議題，針對此議題有很多廠商提供結合 AI 或大數據的防禦機制，而 BSides 研討會則是澳洲最具指標性的研討會，現場亦舉辦 CTF（Capture The Flag）搶旗賽，供與會人員進行駭客攻防演練競賽，今年的議題提到了人工智慧、虛擬貨幣、硬體設備晶片拆解、滲透測試等新趨勢，會中主持人特別提到今年有台灣來參加本會議，因為澳洲是中國網路攻擊的

第三大國，他們也知道台灣往往是中國網路攻擊的第一現場，所以希望建立聯絡的管道，做情資的交流。

參訪新南威爾斯州費明頓警區，與該局刑事人員(Detective)及電子設備鑑識人員(Inspector)交流近期網路犯罪趨勢、執法技巧、偵辦方式及警察制度外，也交流偵辦詐欺案件的心得，另參訪澳洲聯邦警察局(Australian Federal Police)數位鑑識實驗室，除根據鑑識標的物不同而有其專用的鑑識實驗室(如手機、電腦、聲音及影像等專用鑑識實驗室)外，並設有晶片解焊設備可將手機晶片解焊卸下進而讀取內容，皆是本局數位鑑識實驗室明年努力的目標。

犯罪是全球性的問題，解決犯罪問題也是全世界警察共同努力的目標，藉由跨國性的打擊犯罪，縱使與台灣沒有邦交的國家亦有共同打擊犯罪的需求，惟有積極加入各項國際的研討會及警政交流，才能拓展台灣在治安努力的能見度。因此，建議持續編列相關出國預算，派員參與全球性組織所舉辦的各式研討會，即時掌握國際犯罪型態的發展及防制策略，更積極擴展、延續與國際司法機關的合作模式，才保障國民生命、財產的安全及對政府的信心。