

行政院所屬機關出國報告

(出國類別：考察)

參加「英國 2023 安全及警務裝備展」

服務機關：內政部警政署

姓名職稱：副署長鄭明忠

專員陳承浩

出國地區：英國漢普郡拉什穆爾區法恩伯勒城

出國期間：2023 年 3 月 11 日至 3 月 18 日

報告日期：2023 年 5 月 1 日

摘要

本年度警用及安全裝備展（SECURITY & POLICING），於 2023 年 3 月 14 日至 16 日在英國漢普郡拉什穆爾區法恩伯勒城舉辦，該展覽係由英國內政部聯合安全與韌性中心（JSaRC）主辦，自 1983 年起每年舉辦，今年為第 41 屆，據大會人員表示本次計有超過 65 國與會，並有超過 30 個英國政府執法機關及 300 家設備廠商（包含警用裝備、警械、無人機反制、鑑識技術、應用程式開發商等）提供該國執法應用及相關技術展現，參與人數超過 6,000 人。本次展覽主要有三大主題，分別為「促進國家安全及復原力」、「警務創新」及「保護人民及領土」，並以各項裝備、應用技術、政府部門解決方案等圍繞該主題呈現。提供與會人員了解科技發展趨勢，並可依各國需求選購、採用。

本署由副署長鄭明忠率團赴英參展，其間與我國駐英代表處、英國內政部所屬警務學院、國家通訊局、警察犯罪預防學院、邊境部隊及國家警察反無人機部隊等重要領導幹部進行會談藉以建立高層互動、溝通管道，並於參展期間多方了解各項技術現況。

另近年來，自歐洲利用空運寄送來臺的毒品案件持續增加，據本署刑事警察局自 110 年 9 月迄今年 1 月止之統計，已接獲關務署通報此類案件 160 件，其中發貨地來自歐洲有 61 件（占 38%），為最大宗發貨地區。而本署目前派駐歐洲之警察聯絡官僅 1 名，該聯絡官負責之地區面積約 1000 萬平方公里，內含 50 餘國（含特殊地位領地及屬地等），地幅廣大，事務繁雜。為使本署派駐歐洲之警察聯絡官能在歐洲延伸相關合作及協調聯繫夥伴，應可酌增人數，俾利打擊犯罪相關事宜之推動。

目錄

壹、目的.....	3
貳、參展過程概要.....	4
一、展覽綜覽.....	4
二、開幕儀式.....	5
三、個別廠商及政府機關代表參訪(談話)紀要.....	6
四、參加展場重要活動.....	24
參、機關拜會.....	24
肆、與會心得.....	25
一、主題豐富、活動多元.....	25
二、目標明確、切合主題.....	25
三、受限政策等因素,較難觸及深層技術、應用原理的核心技術.....	26
伍、建議事項.....	26
一、機關整合的重要性.....	26
二、專注研發,並結合產、官、學努力創造經濟價值.....	27
陸、結語.....	27
一、我國警政科技建置並不落後英國.....	27
二、對於英國的保持訓練應看齊.....	27
三、持續派員參加,掌握產業脈動.....	28

壹、目的

警用及安全裝備展 (SECURITY & POLICING), 於 2023 年 3 月 14 日至 16 日在英國漢普郡拉什穆爾區法恩伯勒城舉辦, 該展覽係由英國內政部聯合安全與韌性中心 (JSaRC) 主辦, 國防和安全出口處商業貿易部門 (Defence and Security Exports, Department for Business and Trade) 協辦, 自 1983 年起每年舉辦, 今年為第 41 屆。

據大會人員表示本次計有超過 65 國與會, 並有超過 30 個英國政府執法機關 (包含內政部及所屬放射與核能部門、安全行業管理局、反制無人機部門、國家核實驗室、數據通信小組; 警政相關之警務學院、國家反恐安全辦公室、國家反恐警務總部、國家打擊犯罪局; 邊境安全相關之聯合海上安全中心、邊防部隊、國家警察反無人機部隊) 及 300 家設備廠商 (包含警用裝備、警械、無人機反制、鑑識技術、應用程式開發商等) 提供該國執法應用及相關技術展現, 參與人數超過 6,000 人。

本次展覽主要有三大主題, 分別為「促進國家安全及復原力」、「警務創新」及「保護人民及領土」: 「促進國家安全及復原力」部分主要以國家層級角度考量近期俄烏戰爭所帶來之影響, 提供相關安全防護主題; 「警務創新」部分匯集主要執法機構和官員, 展示最新科技, 包括關鍵主題的項目和計畫, 以未來警務、專業能力塑造未來的行動和國際視野; 「保護人民及領土」部分則是匯聚邊境安全之主要政府官員, 地幅自海外、邊境和國內, 包括貨物、人員, 使參展人員能更了解英國政府內目前正在進行最具創新性的項目和計畫, 並輔以各項裝備、應用技術、政府部門解決方案等圍繞該主題呈現, 提供與會人員了解科技發展趨勢並可依各國需求選購、採用。

本次參展前, 本署與英國國防和安全出口處商業貿易部門 (Defence and Security Exports, Department for Business and Trade) 先行聯繫, 並由副處長 Stuart Cole 先行自英國來臺灣拜會, 期間了解因展覽廠商眾多, 且參與人數也相當可觀, 為使參展期間, 廠商方能儘可能多推銷及參展方能真正理解廠商實際技術應用, 英國主辦單位決定參展方式以媒合雙方意向序位方式辦理, 亦即由本署先行挑選有意願參觀並深入了解技術之廠商, 同時提出參展意向書, 由廠商收齊各國意向書後, 再決定及安排相關參展時段之優先序位; 若未納入正式安排時段, 即須在他國結束展覽後之空閒時段方能再於現場安排參展。

因應我國近期社會發展及犯罪型態轉變, 最後擇定本次參展目標, 希望能獲取「用於調查犯罪之新興科技」、「AI 人工智慧」及「感應式裝備」等技術資訊, 並交由英國主辦單位做規劃。

本署由副署長鄭明忠率團赴英參展, 其間與我國駐英代表處、英國內政部所屬警務學院、國家通訊局、警察犯罪預防學院、邊境部隊及國家警察局委員會等重要領導幹部進行會談, 以建立高層互動、溝通管道, 並於參展期間多方蒐集整理各項技術現況。希望能帶回有助益之資訊, 並能幫助我國警政科技持續發展。



圖 1.1 英國國防和安全出口處副處長 Stuart Cole 與本署副署長等合影



圖 1.2 英國國防和安全出口處副處長 Stuart Cole 與本署副署長合影

貳、參展過程概要

一、展覽綜覽

本次英國主辦方，將展場規劃為 6 大區塊，分別為「政府專區」、「融合論壇」、「密室逃脫互動體驗區」、「國家反恐安全辦公室商務會議」、「反威脅展館及展示區」以及「創新區」。

「政府專區」邀請了超過 30 個英國政府執法機關（包含內政部及所屬放射與核能部門、安全行業管理局、反無人機單位、國家核能實驗室、數據通信小組；警政相關之警務學院、國家反恐安全辦公室、國家反恐警務總部、國家打擊犯罪局；邊境安全相關之聯合海上安全中心、邊防部隊、國家警察反無人機部隊）在場協助參與者了解英國政府機關解決治安及其他社會議題之方式、方案或技術，展區並提供一開放空間供各國代表相互交流。

「融合論壇」則是規劃一個寬敞的場地空間，其間並由主持人(主講人)提供相關主題供參與者共同提問、討論及集思廣益，並由英國產業部門推廣該政府聯合跨部會(含政府機關、產業界及學術界)所提供的安全解決方案。本次所提供之討論議題有「應對恐怖事件－從安全控制室視角出發」、「馬丁定律」……等。

「密室逃脫互動體驗區」為主辦方提供一個定時逃生室之模擬空間，並以恐怖事件(今年為「乾草堆行動-搜索開始」)為主題，參與者可在其中體驗「數據分析」、「識別偽造文件」、「物證調查」及「地圖追蹤分析」等科技應用。

「國家反恐安全辦公室商務會議」是由英國國家反恐安全辦公室所舉辦，今年主題為提供與會者了解現階段英國政府如何應對不斷演進的公共場域威脅事件，並提供相關核心訊息、建議指南及指導方針，幫助企業或政府保護資產及抵禦恐怖主義的威脅。

「反威脅展館及展示區」是由英國航天、國防及安全工業貿易組織舉辦，今年展覽主題為「如何應對簡易爆炸裝置中爆炸性彈藥的威脅」、「化學、生物、放射和核防禦特別小組展示」、「無人機防禦系統展示」及「反制無人機部門聯合運作機制」……等。

「創新區」則集結了目前英國有關產業或供應商最新的科技、技術或跨領域解決方案，可由參展者個別實際接觸廠商提供之高科技產品，並以近距離互動、使用來決定是否再進一步採購至各該國家。今年的展覽項目類別區分為「反恐與情報」、「監獄監護相關」、「人身安全、人員防護和貼身保護」、「監視系統和影片分析」、「運輸安全」、「專業的訂製及規劃服務」、「化學、生物、輻射、核和爆炸材料」、「無人系統、機器人與對策」、「保護和運輸包裝」、「事件與應急反應」、「網絡安全」、「光學技術」、「數據蒐集與分析」、「個人防護裝備、服裝和配飾」、「法醫鑑證服務」、「信息技術」、「通訊、指揮與控制」、「秘密行動和能力」、「訓練」、「反爆炸彈藥、爆炸物和爆炸防護」、「生物識別、面部識別和圖像處理」、「系統訪問控制和進入系統」、「通信數據和數位採證」、「國家邊境和海事安全」、「車輛相關」等主題。

二、開幕儀式

首先由主持人邀請來賓依序發表短評，簡要摘整相關談話重點如下：

- (一) 感謝所有參與本次展覽的警務人員，不管是英方的工作人員或是來自各國的警察朋友，並說明了目前大環境不斷複雜化及持續變動對政府帶來的巨

大挑戰，因此亟需工業界、學術界、貿易機構與政府部門共同合作，共同創新並保持彈性反應能力，以確保人民及關鍵基礎設施之安全。

- (二) 鑑於烏克蘭與俄羅斯最近的事態發展，英方對於本國有關行業所應對的局勢感到有信心，因為在面臨此種危機時，政府各機關部門能毫不猶豫地提供快速的、有效的創新和解決方案，也感謝該國國防和安全出口處商業貿易部門的努力，讓這些產業以及技術能有效的推廣出口至全世界各地。
- (三) 在今年的展覽會場，除了以往的展覽項目，如警務及消防服務以及改善公共安全這些原有的主題外，因應俄羅斯入侵烏克蘭後，國際情勢緊張加劇，主辦方更加入一項針對性的計畫，即向「正在加強邊境安全的國家」提供「該國中小企業（商業與貿易部的出口學院及特定行業的英國國防與安全出口學院）更廣泛的支持和培訓」，有興趣者可以至相關展區獲取進一步資訊。
- (四) 根據官方內部最新一項統計數據，2021 年本次展出相關行業之產值已達到 82 億英鎊，在在證明英國向國際客戶提供的產品及服務非常受歡迎，政府將持續與業界合作，每年展示英國針對現有和新興威脅的領先技術和解決方案供各國使用，歡迎各位與英國成為夥伴，保持合作關係。
- (五) 本次展覽最大目的在於提供「參展者」與「參展商」一個極好的互動平臺，由英國廠商為全世界提出一流的實用解決方案及相關科技技術，並解決參展者國內之治安、安全等問題，以協助該國「創新」及「恢復」、並促進「增長」及邁向「繁榮」。

三、個別廠商及政府機關代表參訪（談話）紀要

（一）個別廠商

1、Garrison：

該公司指派政府銷售主管 David Cole 為訪團進行介紹，他主要負責之地區為歐洲、中東國家及亞太地區，他們公司是軟體設計公司，並非硬體公司。

該公司所展示之技術 Garrison SAVI 為提供政府組織或商業團體在調查網路內容時，以類似內置視訊鏡頭監視方式，錄製原本欲調查之網路內容，進而相關調查人員可以用瀏覽產出圖片的方式讀取相關資料，取代傳統電腦直接以網路存取相關調查內容可能帶來之安全風險。

該技術簡單來說，即以往調查人員調查網路的內容時，因需使用機關內的設備來上網，在上網期間因需點對點存取相關內容，此時容易讓有心人士藉機入侵機關內設備或是以其他非法方式來進行反偵察、滲透或是破壞；該

技術的設計原理為，在調查人員使用該技術時，會利用該公司所提供之設備連接電腦與對外連線之網路，但該公司設備裡設置了對外聯網及對內單線存取之 2 個晶片，該 2 個晶片在設計之初即以物理方式阻絕相關網路存取，僅能單向傳遞圖片、聲音等資料；調查人員下指令後，對外聯網之晶片會連線至欲調查之網路內容，並取得相關之資訊，同時對內之晶片則以類似視訊鏡頭監控對外聯網晶片之一舉一動，並將欲調查之網路內容同時轉換為圖片、聲音等資料，因為是以視訊方式單向讀取對外聯網之晶片所產生之圖片及聲音，均不會使對內之晶片被外部有心人士反偵察、滲透或是破壞，該公司聲稱此技術完全阻隔機關內的電腦設備與外部網路。用這種方式進行網路調查，最糟糕之情形即為對外聯網之晶片被病毒威脅或被駭客入侵，但內部之晶片則完全不會被影響，而且一但使用者完成調查後，將對外聯網之晶片完全重置，即可完全清除相關威脅。

該技術基本上可以連結現行市面上所有設備，舉凡電腦、平板及伺服器，該公司均能依客戶所提出之預算配合設計出可以負擔之有效解決方案，亦或是客戶可評估自身預算及機關內設備安全等級，自行選擇搭配該公司設備之特色功能來設計相關安全架構。

總結該公司介紹本項服務（Garrison SAVI）之特色為「安全的遠端訪問欲調查之網站」、「防止任何惡意軟體藉由調查過程開啟之網路通道攻擊機關內之設備」、「減少數據丟失風險，因為對內之晶片是以監視方式讀取對外晶片所得資料，理論上除非攻擊者使用光學字元辨識以上之設備及技術行反向調查，否則相關數據並不會有丟失風險」及「因為使用監視方式讀取，可以完全保留相關發送按鍵及滑鼠游標移動之完整日誌，這樣的採證行為，也可以當作監控分析下之基礎資料」。

最後展示人員更提及，該公司目前在英國已和政府部門（安全或詐欺網站調查部門）合作，而在臺灣也有 2 個政府客戶及一個代理商，若參展後有興趣，可以相當快速及方便的取得相關合作及資料。



圖 2.1 訪團聽取 David Cole 展示

2、Signum Intelligence

該公司指派首席技術官 Matt Milne 為訪團進行介紹，他是該公司技術面（軟、硬體開發）的最高負責人，他們公司業務包含了軟、硬體設計規劃、軟、硬體整合服務、也包含了為客戶規劃相關訓練計畫。

Matt Milne 首先說明了該公司業務領域有 3 大類別，分別為「智慧應用部門」、「程式應用設計部門」及「工程部門」；「智慧應用部門」負責訓練（員工或客戶）、提出安全解決方案、策略分析服務、戰術指導服務，並已經有和監獄及其他類似的基礎設施機關合作之經驗，「程式應用設計部門」負責整合電信、網路預防故障及安全系統、網路分析，並有與掌管數據的相關基礎設施及法律部門合作之經驗，「工程部門」則負責工程機原型製作、產品開發、材料科學及解決方案實際應用開發。

該公司是整合型服務公司，可以為客戶量身訂做打造符合需求之軟體解決方案，並搭配製作硬體協助實際解決相關問題，詳細詢問 Matt Milne 後表示，該公司目前主要業務主要還是著重在電信、電子訊息等領域，以下 Matt Milne 為訪團展示 2 項技術。

首先登場的是，有關於 2G 至 5G、FDD、TDD、LTE+ 等有關通訊頻譜「干擾」、「設置虛擬基地臺並獲取嫌疑人 SIM 卡之 IMSI 碼」及「訊號指向尋找詳細位置」等技術，該公司展示了為客戶所設計之機器，其中涵蓋了手持式、車用式（含隱密安裝服務）、背包式、定點式、搭載無人機式等，均依照客戶需求進行設計，產品功能如前述，端看客戶如何應用，舉例來說，曾有政府部門為了調查恐怖攻擊行動，利用干擾技術並以設置虛擬基地臺取得 SIM 卡之 IMSI 碼，確認要找的人後，再利用訊號指向尋找功能查找嫌疑

人位置，期間並展示了搭配監視系統及人臉辨識系統後，可以完全掌握及追蹤對象之一舉一動。

再來，Matt Milne 展示了該公司所設計之相關應用程式，如搭配前揭「干擾」、「虛擬基地臺並取得 SIM 卡之 IMSI 碼」及「訊號指向尋找」等技術設計客戶所需之人性化使用界面，可以從「現場執行人員」至「戰術指揮人員」均設計不同之軟體介面，讓使用者能在不同情境切換使用，提供最有助益的解決方案。

最後 Matt Milne 總結了該公司的服務，即「用於檢測手機 2G 至 5G、FDD、TDD、LTE+等有關通訊頻譜和管理的戰術解決方案(含括擷取、攔截、測向 IMSI、Wi-Fi 跟蹤、衛星攔截)」、「協助基礎設施設置控制、管理系統」及「戰術監視和反監視解決方案及服務」，並再次強調該公司的特性就是彈性極大，可以為客戶進行所有客製化的服務，也表達希望與臺灣合作之意願。

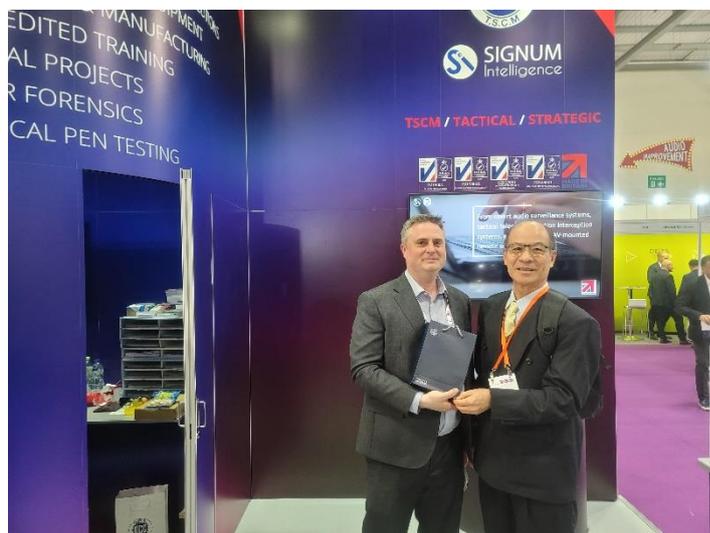


圖 2.2 Matt Milne 與本署副署長合影

3、BAE Systems (英國宇航公司系統)

該公司指派營業部主任 David Tan 為訪團進行介紹，該公司目前提供一些世界上最先進、技術領先的國防、航空、航天技術和相關安全解決方案。他們在大約 40 個國家及地區僱用了 93,100 名技術熟練的員工並與 16 個國家客戶或當地合作夥伴合作、開發、設計、製造和支持相關產品和系統，以提供合作國軍事能力、保護國家安全並確保關鍵信息和基礎設施的安全。

因為本次展覽主題係針對警務方面的技術，故有關國防、航空、航天等技術，就沒有在這次展覽中呈現。David Tan 為訪團準備了「BAE Systems IntelligenceReveal IP Analysis Solution」、「IntelligenceReveal Content Monitoring from BAE Systems」及「Search&Analysis Module」等簡介，並依序介紹。

「BAE Systems IntelligenceReveal IP Analysis Solution」部分：這是 BAE 公司針對原始數據轉換為有價值情報的解決方案，David Tan 首先指出現今加密技術對於產業帶來的優勢（例如維護個人權益免受侵擾），但如果這項技術被應用在恐怖攻擊活動或犯罪活動，那可不被樂見，該公司在與各個合作國合作的 30 年間，逐漸在網路及 IP 通信區塊有所斬獲，雖然各個網路領域的加密技術均逐步成長，但該公司的研發團隊與調查人員總是能同步找出提取情報的新方法。在這個不斷合作精進的過程中，他們也認知到 Sols（感興趣的對象；嫌疑人；下同）的通信內容越來越隱晦，加密技術也越來越高級越來越難以被破解，與其執著於越來越沒有情報價值的資料內容，或花太多的調查資源在解密，倒不如將調查關注在其他有用的資訊。該公司技術人員發現，因為現今網路交流的頻率越來越高，各項手持設備、移動裝置應用程序不斷普及，造成可以蒐集供調查人員使用的數據以及該數據呈現的報告的最佳模式也會不斷演進，該公司的經驗中，有時反而是這個訊息本身所帶來的附加訊息，更能提供有價值的情報，舉例來說，他們的調查人員慢慢的發現 Sols 間互傳訊息的文字內容現今已常常得不到有價值的資訊，反而是這封訊息怎麼傳的、在哪裡傳的，使用什麼社群軟體傳的等等資訊中有沒有其他相關的連結或突破點反而才是更有調查價值的資訊。

綜合以上條件，他們開發了這個 IP 分析的解決方案來監控 IP 數據及 Sols 間的通信，並提供視覺化界面供調查人員便利的調查 Sols 的活動（所使用的應用程式及社交媒體上的實際活動）。

據訪團詢問，該解決方案首先仍應取得當地政府機關如法院之許可後，在電信公司端設置攔阻器並開始監錄 IP 位置相關活動，監錄後的資訊再進行後續資料分析與運用；該公司開發了一套 AI 系統，可以自動從所攔截之數據分類、分析、存檔、視覺化呈現並儲存於其大量儲存設備（容量可達 PB 級的存取量），該 AI 目前已學習並可識別 4,000 多種協議及所使用之應用程式（目前該公司致力於每日更新至最新狀態），調查人員可以利用該分析軟體針對已儲存之數據進行搜索及分析，當找到調查人員指定的參數及關鍵字後，該系統會將 Sols 所使用之應用程式、所造訪網站，甚至在某種特殊條件下，其語音通訊內容（取得軟體的原始代碼），這個軟體甚至能夠針對廣告訊息加以識別並過濾，減輕調查過程的負擔，展示過程中 David Tan 指出，該系統可以快速回答「Sols 是否近期會去旅行？」、「Sols 有哪些家庭設備？」之類的問題供調查人員參考。有了前揭的分析數據，該系統也可以幫助建構

情報網路圖，方便調查人員利用其他所取得資料執行聯合搜尋，並可再強化此一情報網路圖的豐富性。

針對「BAE Systems IntelligenceReveal IP Analysis Solution」部分，David Tan 做了以下總結：該系統係專為情報機構、執法機關所設計，係為使調查人員更容易調查嫌疑人的網路足跡，以便更快速及有效地達成任務。該系統的特點有「分析嫌疑人網路活動趨勢（含偏好網站及應用程式）」、「可進行地理位置分析」、「可進行人口統計分析」、「可了解加密協定及相關趨勢為何」、「可判斷嫌疑人所使用系統及瀏覽器」、「可追蹤異常網路活動，如 Tor（暗網）及 VPN（使用跳板）」、「地理位置分析」、「家用網路設備分析」、「生活模式（作息）分析」、「聯繫對象分析」及「識別設備上所使用之 ID」等。

「IntelligenceReveal Content Monitoring from BAE Systems」部分：這項內容監控技術，可以使調查人員利用網路監控 Sols 的 5G 網路電話電信流量，蒐集通話對象、IP、位置等數據並可對通信對象進行分類及分級，建構情報網路圖，方便調查人員分析與利用，該項技術甚至可搭配語音辨識系統，對於語音訊息自動轉換成文字，並可以翻譯為 40 幾種語言，並自動轉化為調查人員熟悉之母語系統，所有的流程都是自動化的。

另外 David Tan 有特別提到，所有的界面都可以為客戶客製化，功能特點總結「可安裝數據緩衝裝置，緩解數據流暴增可能帶來的數據漏失風險」、「因為監控系統必須安裝於執法監控機關，可確保只有被授權者才有權閱覽相關資料」、「音頻解碼並可以通用格式來儲存並可同時將原始數據保留方便調查人員調閱原始資料」、「安全的儲存，避免被無權者濫用或外流」、「設定優先條件，便利調查人員每次重新開啟系統能立即審閱重要事件，排除冗長的過濾時間，甚至能預先設定緊急通知警報，若系統自動檢測到預設條件，可以第一時間優先通知調查人員」等。

「Search&Analysis Module」部分：最後 David Tan 為訪團展示了搜尋以及分析模組的功能，首先展示了現代社會中，數據是無所不在的，每個用戶、每個設備、每個系統每天都會產出大量的數據，這些數據大部分都散在各個數據庫中，沒有任何交集及連結，且最困難的是，這些數據可能格式、種類、儲存方式、加密方式都不同，加深了調查的困難，但其實個別看待各個數據可能是沒有意義或是沒有價值，但如果整合在一起，就可讓調查人員以高效率的方式來解析並建構情報數據圖，而這樣的技術的優勢在於「不須移動相

關數據，原始數據得以保留」、「現有設備的數據及安全並未改變」及「透過腳本編寫，可快速輕鬆完成數據集成」。

該模組可以自由搭配該公司的個別解決方案中，這個模組簡單來說就是提供調查人員以單個查詢系統同時搜尋多個獨立數據資料庫，並可將所蒐集的結果放入通用格式並暫時儲存於臨時存取裝置中，所顯示之查詢結果也可以在單一介面為之，調查人員無須重複開啟多個視窗或是軟體，便利調查人員，節約調查時間。利用最便捷、最直覺化的方式來輔助調查人員執行調查任務。

最後 David Tan 也提到，該公司所提供之服務定能解決我國面臨的各項挑戰，也歡迎後續與他們合作。



圖 2.3 David Tan 與訪團成員合影

4、Detego Global

該公司係軟體開發公司，主要業務為提供政府客戶及公司或商業團體針對設備、網路進行數據蒐集、採證、並加以識別及分析，該公司由全球銷售部協理 Alex Kirk 負責為訪團進行簡報。

首先，Alex Kirk 首先展示了該公司的統一調查平臺，該平臺整合了該公司的 7 大主要解決方案(功能)，可依客戶需求購買不同等級之軟體組合包。以下針對個別功能進行簡介。

「Bullistic Imager」：號稱世界上最快的電子設備採證工具，可以用於採證現場以及實驗室中，是針對電腦、筆記型電腦或伺服器，在不移除硬碟及相關設備的情況系，使用 Bullistic Imager，可以透過內建的多個收集器繞過硬體限制來提取數據，在不到 8 分鐘的時間內採證並保護高達 1Tb 的資料，而採證後所得之資料會轉換成圖像格式，方便後續的分析軟體進行下一

步分析。而且這個採證工具非常輕便，非常適合攜帶至各個現場使用，而且，Alex Kirk 特別強調，這套工具設計得非常直觀且易用，就算不是資訊專業人才，也能僅用 30 分鐘培訓，就能完全上手。(小結：Bullistic Imager 主要是用於電腦、筆記型電腦或伺服器的快速成像採證軟體)

「Field triage」：Alex Kirk 稱這個軟體也非常適合現場快速搜索敏感資源，他們公司的客戶（執法機關）會在出勤前，將這套軟體設定搜查例如詐欺、人口販運、恐怖攻擊、兒童不雅照片、金融犯罪等特定圖片，到了現場後，將裝有此軟體設備插入目標電腦、筆記型電腦或伺服器，即可在現場快速識別目標，這個軟體介面也非常直觀好用，帶有類似警報的系統，一旦發現目標電腦、筆記型電腦或伺服器有相關預搜查案類之圖片，即會提醒調查人員，Alex Kirk 稱客戶反饋這個軟體主要可用於現場快速取得突破犯嫌心防之關鍵圖片或立即而快速的決策某些調查策略，這也是這個軟體設計之初的目標，使調查人員無須在現場耗時的採證及分析。另外也提到，該軟體可以在 30 秒內獲取所有使用的用戶名稱及密碼。(小結：Field triage 主要是用於電腦、筆記型電腦或伺服器的分類採證軟體)

「Media Acquisition」：同樣是設計給現場採證之軟體，但其主要標的為數字證據，可以同時分析及保護多個移動儲存裝置，速度非常快速，更特別的特點在於，這個軟體不但可以從已經損毀（非物理性）的系統中移除的裝置提取資料，也可以從已經刪除資料的硬碟中還原相關數據，犯罪者欲隱藏的資料將無所遁形。(小結：Media Acquisition 主要是用於硬碟 HDD、SSD、SATA、USB 隨身碟、SD 卡等記憶卡及無人機上的存取設備提取數據採證軟體)

「Detego Md」：這個軟體是為了手機、平板、隨身穿戴裝置、物聯網設備、智能電視、衛星電視、導航設備及無人機等智能設備和應用程式所設計，它可以針對多達數千款型號之手機及 2 千多個應用程式蒐集可用數據，並具備解密、分析、自動化等特色。

對於 Android 的設備，這個軟體可以進行設備解鎖及訪問相關數據；對於 iOS 系統則支援備份文件解密，Alex Kirk 表示 iOS 系統目前業界應該不存在可以破解的技術。(小結：Detego Md 主要是用於無人機上的存取設備及手機及平板上的邏輯數據或進階的實體數據採證)

「Remote Acquisition」：這項技術並非應用於現場採證，而是透過網路遠端連線獲取相關數據。所採證資料會轉換為圖像，以便保護數據來源，並不

會改變原始數據，以利作為法庭證據使用，另能取得之資訊包含了系統訊息、RAM 數據、用戶名稱與密碼。(小結：Remote Acquisition 主要是用於網路遠端數據採證軟體)

「Analyse」：這項工具可以整合上述所有採證軟體所取得之數據(證據)，並利用其 AI 系統自動深入分析情報，並可產出相關報告，這個工具可以自動識別人物、武器、毒品、裸體、不雅圖片等影像紀錄，也可以利用光學辨識字符功能，從圖像及影像證據提取文字資料，並利用離線翻譯功能，將多達 230 種語言轉換為英語，針對照片，也可以利用 Photo DNA Matcher 快速辨識並比對帶有照片 DNA 相關的圖片及影像。據 Alex Kirk 向訪團表示，這個工具可以輕鬆解密 300 多種文件類型的密碼。(小結：Analyse 主要是用於分析上述 5 種採證軟體所取得之證據)

「Fusion」：這項工具則可以讓調查人員利用進階構建功能，來找出人員、地點、設備和案件關聯點，再加以突破。這個工具含有強大的 AI 系統，可以透過所採證資料中之關鍵字快速找出相關嫌疑人，並可以視覺化圖像呈現，方便查看及進一步分析。(小結：Fusion 主要是用於分析上述 5 種採證軟體所取得之證據並可產出報告)

Alex Kirk 最後提到，上述 7 大主要解決方案(功能)，他們基本上都是一起販售，但仍區分成 3 種版本(標準版、專業版跟終極版)，其中的區別在於可支援採證的設備項目多寡，但若客戶有需求，也可以單個模組單個模組來購買。



圖 2.4 Alex Kirk 與本署副署長合影

5、SESANTI

該公司係光學儀器相關之公司，主要販售之產品是攝影設備系統，以下由業務發展部主任 Mark Whitehouse 為訪團進行介紹。

該公司所研發之攝影機目前服役於英國軍事部隊、邊境警察等執法機構，會受這些執法機構的青睞，原因在於該公司所提供之設備可以在低光源或者無光源的環境下，辨識出目標面部特徵並可以持續追蹤，而且監視的最遠距離視設備型號，可以從 1 公里到 30 公里都能完成情報蒐集任務，且該攝影設備系統均搭載 AI 軟體，設備可自主監控，更能產出高清晰之影像，確保不會因距離而改變影像之品質。

該公司除了攝影設備外，更推出了無線傳輸設備，無論基地臺是否運作，都能利用 COFDM LOS 和 NLOS 無線電鏈結或其他基於乙太網路設施之設備將所取得之蒐證影像傳輸給調查人員。

現場更直接由 Mark Whitehouse 展示了攝影機捕捉嫌疑人之面容並加以追蹤之功能，期間也提到，該公司所推出之設備，目前多用於反恐怖攻擊及邊境部隊追蹤非法移民，因為近期俄烏戰爭，產生了多難民，常常有利用偷渡的方式進入英國，因此邊境部隊都有部署這類的設備。

接下來介紹的，是實際安裝的案例，因現場機器看起來雖然不會很笨重，但仍有一定的大小及體積，在實際應用中，有可能容易被發現，但是 Mark Whitehouse 強調，這些都可以拆解並客製化偽裝成客戶想要的樣子。例如裝於車上、牆邊、電話亭……等。

介紹完攝影設備後，再來登場的是熱像儀及多光譜儀，均可搭配攝影機共同給客戶使用，在低光源或者無光源的環境下，藉由 AI 互相搭配，尋找最有效的監控及追蹤機制，讓調查人員得以實時監控嫌疑人，甚至該公司還推出輕質材料（如塑鋼及碳纖維材質）所製作之攝影機設備，方便攜帶、快速部署。

最後，Mark Whitehouse 展示了該公司目前實售的幾項產品，如「CT-M（反恐多光譜儀監控系統）」、「ACP 4（超輕型監控系統）」、「ACP 5（隱密部署監控系統）」及「ULARI（超遠型監控系統）」，但特別聲明，並他也特別強調，並非每一個國家都能獲得授權出口，若有需要，仍需視英國政府的評估，獲得許可後才可以出口販售。



圖 2.5 Mark Whitehouse 與本署副署長合影

6、Cyacomb

該公司是軟體公司，主要業務對象為政府執法機關，技術特點在於採證，由銷售開發經理 Alina Kichigina 向訪說明及介紹。

首先，該公司軟體主要厲害的特點在於，它針對犯嫌的設備採證時，速度是傳統採證工具的 100 多倍！而且比傳統採證工具更優勢的是，它不但不會漏掉分割檔案及被刪除的檔案，它更可以避免傳統採證方法為了採證方便所用的便捷手段可能威脅到原始證據的安全。而且隨著科技的進步，每個人手邊有越來越多的設備，個人數據也成幾何式的爆炸成長，若調查人員還再使用傳統採證方式，不但曠日廢時，更可能錯失破案先機。

Alina Kichigina 特別強調該公司軟體 AI 在識別「兒童色情」以及「恐怖攻擊」等資訊時特別厲害，現場經訪團詢問後，實際應用場景應該是，調查人員緝獲犯嫌後，取得其使用之手機或其他存取設備及穿戴裝置，或在其住處取得電腦、筆電及平板等電子裝置，這時即可插入安裝有該公司軟體之 USB 隨身碟，這時隨身碟內建的軟體會開始快速掃描及過濾該裝置內的硬碟或其他儲存設備，並將過濾結果分類分級，便利調查人員現場檢視該分析結果後，再決定其他調查策略（例如加強某地某處的搜索或必須轉移陣地至其他地方搜索）。

最後訪團提出請求，希望現場使用訪團成員之 iPhone 手機進行實際測試並了解該軟體實際運行效果，Alina Kichigina 卻稱 iOS 的系統尚無法破解，所以無法展示，不過她強調另一個全球市佔也很高的品牌 SAMSUNG 手機。該公司的軟體可以直接且輕鬆的破解，她也說明目前應該沒有公司能聲稱具備破解 iOS 系統的能力。



圖 2.6 Alina Kichigina 與本署副署長合影

7、Trust Stamp

該公司致力於提供可信賴的身分系統，使機關和個人在網路世界及其他地方進行交易時能安全無虞。其技術專注於身分識別的三個關鍵領域：「建立身份」、「為所有交易（含交涉、交換）提供中間支持」及「降低身份數據外流的風險」，由技術開發人員 Noman Po 為訪團進行簡介。

首先，Noman Po 先介紹該公司成功合作的案例，例如與美國最大的信用卡發卡銀行合作遏止身分詐欺取款之問題、與新墨西哥州的總檢察長簽署合作備忘錄解決人口販運受害者安全數據共享問題、與萬事達卡公司（MasterCard）合作提供生物識別化技術及與美國國土安全部合作提供移動設備生物識別服務。

該公司之技術，能將個人之生物識別化資訊（人聲辨識、臉部辨識、指紋辨識、掌紋辨識、虹膜辨識）轉換為「生物令牌」，這個令牌就是使用者在網路上可以用來識別身分的一個數據，但是沒有特定的讀取或交換協議時，這個數據本身並無任何意義，又該數據因為已經經過該公司的轉換算法，故要反向推算原始數據也近乎無解。

在展示及簡報期間，Noman Po 主動與訪團解釋，這項技術並非直接應用於警政相關業務，所以訪團成員可能會有疑惑，但它確實是可以成為警政機關與其他隱私需求極高的企業或團體的橋樑。

舉例來說，當美國政府執法機關希望向 Facebook 公司調閱相關可疑為犯罪的資料時，因為 Facebook 係用戶隱私至上的公司，它絕對不會願意提供任何有關客戶的直接隱私資訊，這時候 Trust Stamp 的技術就可以進行橋接，雙方各自提出之資訊經過 Trust Stamp 的技術，轉換成上述之「令牌」，在藉

由中間第三者的資料比對，來讓執法機關確定嫌疑人身分訊息。這樣的資料交換優點有很多，例如「個人識別化資料已轉換為令牌，就算令牌遺失，也不會有資料外洩的問題」、「Facebook 仍可以最大程度保護客戶隱私因為它所提供者，不過是一串無意義的數據」及「對於中間第三者而言，這兩個客戶（Facebook 及執法機關）所提出的資料，因為經過演算，都是一串無意義的數據，可以放心由中間第三者進行比對工作」

訪團經 Noman Po 說明後，理解了該公司本項技術的輪廓及警政應用的案例，最後 Noman Po 也表達希望與我國合作的意願。



圖 2.7 Noman Po 與訪團合影

8、METIS Aerospace

該公司致力於提供監控射頻（RF）信號的智能解決方案，主要客戶為軍隊、機場及監獄等機關，因訪團未事先預約，該公司由現場客戶帳號管理員 Dean Jones 為訪團做簡介。

該公司目前推出的 SKYPERION 系統，主要係為了持續檢測監控設置區域範圍內的無線電頻率，及有無未授權的無線電器械出現在監控設置區域，目前普遍做為監控無人機的運用，Dean Jones 指出，該公司這套設備的優勢在於「精確的於監控設置區域範圍內檢測訊號來源」、「可在所有嚴苛氣候下運作」及「搭載了最先進的 AI 系統，大幅降低誤報率」，目前這套設備服役於英國蓋特威克機場（Gatwick Airport）。

經訪團洽詢，該項設備目前僅能「檢測監控」，並無搭配反制之設備及技術，故若發現干擾源如無人機時，仍須搭配其他設備如干擾槍等迫其降落。

9、BLOCKCHAIN INTELLIGENCE GROU P：

該公司研發以區塊鏈為中心的技術，政府機關使用該公司提出的解決方案來處理加密貨幣或數字貨幣交易的犯罪活動進行複雜的調查。銀行和加密公司則依靠該公司的技術來監控加密交易。調查人員和執法機構則可以利用該公司的技術來快速識別並追蹤非法活動，因訪團未事先預約，該公司由在場的政府與戰略事務總監 William Callahan 為訪團做簡介。

William Callahan 首先自我介紹稱渠也是曾在政府機關任職，他是在美國緝毒局（DEA）任職，在職期間掌管之業務為洗錢調查。他在多次的行動與調查發現不法者利用基利用洗錢計畫、加密貨幣、暗網和市場操縱來混淆資金的真正來源。他在 DEA 期間，更建立了主動的洗錢審計團隊，並參與及製定相關打擊策略，並促進了緝毒局（DEA）針對加密貨幣的秘密行動。

接著，William Callahan 簡單介紹該公司對於政府機關執法機構所提供之追蹤加密貨幣的技術特色，「QLUE」是該公司為了執法機構所設計的一套軟體，因為區塊鏈技術加密的特性，加密貨幣都是一串一串的數字，這些數字中其實隱藏了非常多的交易資訊，例如以近年最火紅的 NFT（非同質化代幣）為例，該軟體能以視覺化、圖形化方式，將貨幣的轉進匯出做一關聯式分析，並產出相關報告，其中可以包含「名稱」、「描述」、「圖片」、「代幣 ID」、「代幣所有者」、「歷史交易資訊」、「交易詳細資訊」等，方便調查人員查找有可能的突破點，如果案件涉及多種加密貨幣，也可以利用該技術，跨區塊鏈追蹤加密貨幣或 NFT，形成視覺化分析，方便後續追蹤。

該公司目前在臺灣沒有服務站，最近的服務據點在香港，William Callahan 表示非常歡迎我國，如果有機會也可以後續聯絡進行相關合作商討事宜。

10、BlindSite

該公司於展場提供搭載採證成像軟體之產品，現場由首席技術官 Rob Thompson 為訪團進行簡介，該產品是一種手持、便攜、非接觸及非破壞性之採證工具，該工具無須事前使用化學或物理方式先行處理現場，也無特殊使用限制，他可以在非常明亮的大太陽底下使用，也可以在沒有光的情境下使用，使用時完全沒有噪音，且過程完全不會留下任何足跡，並且內建的儲存空間，可以保存所採集證據之數據。而它可以定位、識別及搜尋的證據類型包含了「潛在的指紋」、「爆炸後的炸藥殘留物及碎片」、「體液」、「血液」、「唾液」、「尿液」、「精液」及「違禁藥品」。它的技術特點為「可

以在儀器上使用不同波段光來尋找在金屬、塑膠、玻璃、牆壁、門、樹葉等表面含有多孔或無孔之材質上殘留的痕跡」。

Rob Thompson 指出，目前來自歐洲、美國、加拿大、澳洲及紐西蘭等國之指紋鑑定單位反饋，這項技術優於傳統的粉末法。而且該項技術對於爆炸後之指紋還原有較佳的成功率，可達 65%，優於傳統粉末法的 29%，且成功還原後，能有 44%的機率可以繼續鑑識。

另外針對血液的數據採集，這項技術未來還可以提供血液年齡的評估。且使用時，內建的現場攝影機會一直記錄每一個場景，爾後也可以據此來現場重建。

11、Thermoteknix

該公司主要銷售頭盔式/手持式熱成像儀、夜視鏡、融合成像及增強實境技術之設備，自 1982 年成立後，一直是英國業界頂尖之公司，相關熱成像技術榮獲英國女王企業獎（創新類），相關技術領先全球，由全球銷售經理 Andrew Morris 為訪團簡介。

首先介紹「頭盔式及手持式熱成像儀與夜視鏡」，這樣的配備可以使穿戴人員加強在低光源、無光源及城市中的複雜環境之操作能力，並可將所取得之成像連結相關設備回傳至指揮調度中心，或是回傳給同時攻堅，處在不同位置之其他友軍。「目標定位系統」則可以在各種光源各中環境中檢測及定位目標，並可明確方位、測距、並將目標標記，實時監控並可回傳資訊至指揮調度中心，或是回傳給其他友軍。「融合成像」及「增強實境技術」則是利用 AI 計算，增強監視感知能力，就算處在完全黑暗或很複雜的環境也無須擔憂。

（二）政府機關代表

1、Police Crime Prevention Academy（犯罪預防警察學院）

犯罪預防警察學院是一個有熟練經驗的預防犯罪學習和發展的非營利組織，它為公部門或私部門提供經過認證的課程，並提供客製化的教學活動和網絡研討會。它是由英國警方所有，也是唯一一家獲得英國政府核准的機關。該學院與國家警察局長委員會（NPCC）和來自英國各地的高級警官以及專家、學者和政策制定者保持密切的聯繫，以確保課程內容都是最新的。

該院指派院長 Guy Collyer 接見訪團，他自我介紹曾於警界服務超過 40 年，雙方簡單就警察教育類型做簡單意見交流，期間 Guy Collyer 表達他們

學院可以為任何國家客製化相關線上課程或研討會（需收費），另外也可以親自前往該國提供相關課程及演說。



圖 2.8 Guy Collyer 與本署副署長合影

2、National Crime Agency（國家打擊犯罪局）

國家打擊犯罪局是領導英國執法機構打擊情節重大及有組織的犯罪活動，該局透過瓦解那些對英國產生嚴重風險的組織犯罪分子來保護該國公民。本次由技術合作夥伴經理 Simon Baker 與訪團進行談話。

Simon Baker 首先介紹 NCA，據稱該局官員來自各行各業，從犯罪調查、情報蒐集、犯罪分析到商業採購，而成員的多樣性是該局最大的優勢。他們調查工作的主要內容為「邊境管制」、「非法槍枝」、「網絡犯罪」、「詐欺」、「販毒」、「洗錢和金融犯罪」、「人口販運」、「有組織的移民犯罪」、「綁架勒索」、「兒童性虐待和性剝削」及「賄賂、腐敗和逃避制裁」等工作。

雙方簡單就各自國家目前常見之犯罪類型及應對策略做簡單意見交流。



圖 2.9 Simon Baker 與訪團合影

3、Home Office Counter-Drone Unit（英國內政部-反制無人機小組）

該反制無人機小組，由 Bethan Rowlands 小姐為訪團介紹，據她描述，這個反制無人機小組有點類似像整合理論與技術的一個單位，她們主要都在做整合資源的工作，例如說有那些技術可以應用，內部職員就會來研發，而實際應用的介紹，她則轉介紹 NPCC Counter Drones（國家警察反無人機部隊）的政策與立法的主管 Simon Bachelor 協助介紹。



圖 2.10 Bethan Rowlands 與訪團合影

Simon Bachelor 首先提到了近幾年英國也是飽受無人機氾濫應用之苦，他們目前將處理無人機的業務歸類為反恐怖行動部門，而對於無人機目前解決的方式也多是在事前呼籲注意使用安全或限制使用，如前一陣子該國女王國葬典禮期間禁用無人機，就是由政府機關事先預告。

而在該國也有在一些重要地點部署感應設備，但目前這套感應設備並無法達成感應到無人機後就直接干擾迫降或在一定區域設置干擾讓無人機直接無法飛入的技術，目前該國還是只能用傳統的「干擾無人機接收 GPS 信號」、「阻斷無人機與控制者間的通信網路」、「利用網路以後門駭入無人機系統植入程式並接管並控制無人機」、「使用高功率的微波直接破壞無人機的控制元件」或直接利用射擊設備將其打落等方式應對。

如何找出有效的反制及處置無人機的策略，也是他們一直在努力的目標；另外 Simon Bachelor 也提到，目前中華人民共和國為世界最大的無人機技術輸出國，該國的產品也以 DJI（大疆）的技術最為領先，目前該國應對 DJI（大疆）產品的最好模式就是直接拆解它的晶片進行破解，這是花最少資源的應對方式。

最後雙方簡單就各自國家目前應處無人機的策略做簡單交流。

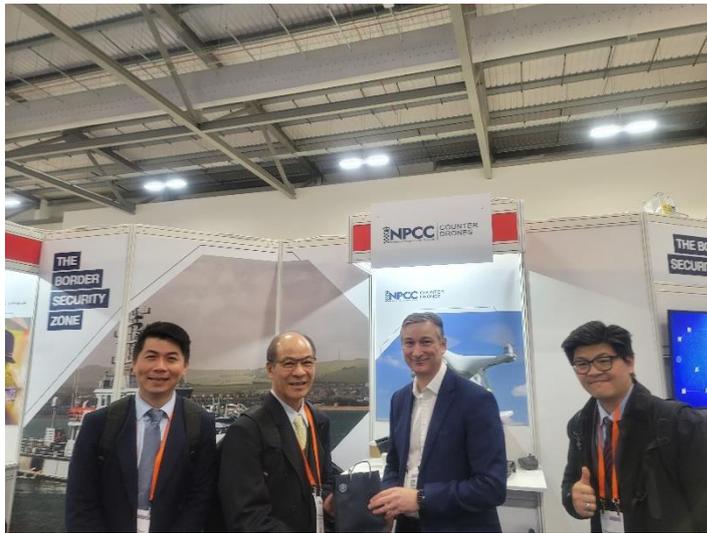


圖 2.11 Simon Bachelor 與訪團合影

4、College of Policing（警務學院）

警務學院是英國警察的專業機構，負責承擔國家警務改進的許多培訓和發展業務，該學院指派國際警察事務顧問 Julian Roadnight 與訪團交流。

Julian Roadnight 首先介紹警務學院的任務，包含了提供該國警察離開警察學校後的受訓工作，但這些課程都是選修，並非必修。不過在該國目前警務職涯的制度下，轉換跑道至更專業的警務部門工作或是升遷至某種職務都必須取得一定的進修時數，而該警務學院可以提供這樣的服務。

該學院也協助制訂一些標準作業程序供全國警察機關參考，因為英國並沒有一個類似警政署統管全國警察事務的機關，所以這樣的標準作業程序還是僅供各地參考，並無強迫遵循的強制性存在。

最後，雙方就各自國家制定標準作業程序是否強制適用做簡單交流。

5、Border Force（邊防部隊）

邊防部隊隸屬於內政部，該執法機關對進入英國的人員和貨物實施移民和海關管制來確保英國國境安全，由 Steven Osmond 為訪團進行介紹他們是如何將實際發生的偷渡案件轉換為實體課程，並教導新進人員如何拆解一輛車以搜索可能藏匿犯罪物品的位置，這個課程是目前該國警察機關指定教學的項目。

隨後，Steven Osmond 也展示了一些超出一般想像的車輛藏匿位置案例，而這樣的課程不但能增加搜索人員的經驗，也能提醒搜索人員在每一次的任務，都要具備想像力。



圖 2.12 Border Force 團隊與訪團合影

四、參加展場重要活動

在參訪的首日，主辦單位也特別舉辦了一個下午茶宴，提供酒水、場地供來自世界各國的訪團互相交流，在此期間，訪團與來自日本警視廳的代表 Shu Akiba 進行交流，同時交換名片、禮物。期間也互相討論各自國家目前的治安現狀及應對政策。



圖 2.13 Shu Akiba、英國國防和安全出口處副處長 Stuart Cole 與訪團合影

參、機關拜會

訪團原規劃前往倫敦大都會警察廳參觀，惟該國近半年以來適逢史上最大罷工，相關警力均投入因應，致取消原規劃。後透過外交部協調，前往拜會我國駐英國台北代表處代表謝武樵。

拜會行程，首先雙方就訪英行程規劃、我國警政運作現況以及如何推動促進臺英警政交流與合作打擊犯罪等交換意見。期間並就近期歐洲犯罪趨勢及近年毒

郵包案件大增，可能影響我國之犯罪型態深入交流，且就歐洲派駐警察聯絡官僅有 1 名部分提出雙方看法，以及提出員額是否可以突破及如何增加與相關合作協調聯繫等議題做討論。



圖 3.1 我國駐英代表謝武樵與本署副署長合影

肆、與會心得

一、主題豐富、活動多元

這次展覽的主題集結了「反恐怖攻擊」、「情報蒐集與通信數據採證及分析」、「監視與控制」、「人身安全設備」、「影像、語音分析」、「應對輻射、核能及爆炸之處理技術」、「無人系統」、「AI 人工智慧」、「網絡安全防護及反制」、「光學辨識技術」、「數據蒐集、建置與分析」、「鑑識技術」、「通訊、指揮與控制」、「學術、實務訓練」、「生物識別、臉部辨識和影像處理」等各項與警政科技息息相關之議題，除適切的呼應展覽主軸，使參展者能在觀展期間，透過互動、交流甚至比較等方式來了解各該國家目前可能處於技術領先或是可能還需再進步的地方。

主辦方也很努力讓這個展覽多元豐富，所以除了廠商展示部分，更利用其他活動來讓參展者能更身歷其境，理解需求，所以就有了「融合論壇」、「密室逃脫互動體驗」、「反恐會議」、「反威脅展示」這些點綴的活動，其中最可惜的是，因為參與人數眾多，未能參加展區中最熱門的「密室逃脫互動體驗」，據主辦方表示，該體驗可以讓參與者完整體驗「利用先進的光學儀器辨識嫌疑人」、再利用「AI 人工智慧掌握及追蹤嫌疑人行蹤及相關數位證據」、「利用

先進儀器進行採證」、「再使用數據分析軟體研判嫌疑人目標」等英國科技產業在整個調查過程中所帶來的便利。

二、目標明確、切合主題

英國每年舉辦這個展覽，最主要的目的就在於推銷該國產業，因此本次展覽所呈現的技術均與警政息息相關，因此也能看見英國警政相關產業的發展趨勢。

今年英國策展方著重的主題在於「俄烏戰爭」後，所帶來的社會問題以及後續可能帶來的影響。所以很多的技術都圍繞此主題展開，例如戰爭中的防護設備、如何監視、監控恐怖主義、人臉辨識及搜尋、搜救電子犬、無人設備應用、國際難民的偷渡防制策略、甚至是加密技術、區塊鏈、虛擬貨幣追蹤等這些技術都能在這次展覽中呈現。這次的展覽無疑舉辦得非常成功，也難怪主辦方稱 2021 年時，本次參展的相關行業產值已達到 82 億英鎊（約折合新臺幣 3,100 億左右）。

三、受限政策等因素，較難觸及深層技術、應用原理的核心技術

本次參展，廠商所提出的都是解決某些特定問題的科技或技術的成果，但是這些成果的技術核心，廠商似乎僅能用某一類型的個案來介紹成效，或是單純介紹優點（例如呈現市售產品與該公司產品的比較，但未敘明為何比市售產品來的優良的主要核心技術），這可能與政策有關，也可能牽涉商業機密，這樣的結果會讓訪團比較無法辨明是真的技術層面或產品功能較優良，還是只是純粹的廣告效果。

伍、建議事項

一、機關整合的重要性

近數十年來，英國政府慢慢意識到，許多犯罪現象，並非單一原因所造成，所涉及與牽連者眾多，處理起來，已非單一機關能解決，於是他們就開始思考，如何應對這樣的狀況。整合各機關的資源，是一個好的選項。

而且另一個迫使英國政府開始重視整合的原因，那就是英國公務部門傳統的特色就是完全遵照規章，比較沒有彈性，好處是依法行政，比較負面的，會變成各部門各司其職，面對新興問題，很難能找到合適的機關來處理，而這樣一來一往又會耗費很多時間在處理機關與機關間的分工問題。

於是訪團這次在與英國內政部-反制無人機小組交流時，了解到它其實是一個整合單位，負責整合各領域的強項與優勢來處理無人機氾濫的問題。甚至是在與國家打擊犯罪局交流時，也發現英國竟然有很多類似的機關，例如

英國國家警察局長委員會，因為該國並沒有類似警政署的機關來統合全國的警察事務，所以他們為了整合政策的執行，就設了一個警察局長的委員會。無論在溝通、協調或聯繫上，均能幫助問題的解決。

也是因為這樣的經驗累積，該國目前的很多重要工作的推展或政策的訂定，都會利用這樣的模式去思考、應對，殊值我國在面對新型態犯罪或應處安全威脅之參考。

二、專注研發，並結合產、官、學努力創造經濟價值

隨著科技的進步、交通工具改變帶來的高速便利，也讓犯罪手法持續更新，且更難以追蹤及掌握，各國警察均面臨極大的挑戰，英國也體認到此現狀，持續研發反制措施等科技。但這些科技的持續成長需要資金的挹注，因此英國政府發現到單純以該國內部的需求，是無法支持這些產業的發展及進步，所以必須要有一個平臺，來將這些優勢產業及技術推往世界各國，以得到其他國家的資金挹注。

因此英國政府於 10 年前，以舉辦警用及安全裝備展之方式，建立互動平臺，由政府整合英國國內安全產業及學界一同參與該機制，並主動邀請外國政府參加，針對英國或其他國家執法機關面對之犯罪及或安全威脅，而提出之技術需求進行研發，並運用各界所提供之資金，挹注警用科技研發；藉以打造政府、產業及學術界於技術、服務及研發資金之交流平臺，進而以供需力量，強化安全產業之技術創新，共構打擊犯罪及降低治安威脅之安全環境。

陸、結語

一、我國警政科技建置並不落後英國

這次參展見識到了英國的相關警政科技，其中幾項科技的優勢與該國所面臨的問題，其實都與我國雷同，舉例來說，詳細定位手機位置（包含經、緯度及高度）的這個技術，其實我國也有類似的設備（M 化車）；再例如人臉辨識的技術，我國也早已有相關的應用經驗；另外例如無人機的反制，目前我國利用干擾槍迫降或物理式（攔截網、橡膠子彈）的處理方式也相差無幾；而手機破解採證的技術，各國也大概都對 iOS 系統無解。整體觀察本展覽所呈現出來的部分，我國的警政科技建置並未落後英國。

二、對於英國的保持訓練應看齊

本次參展所得之心得，有一部分在於參展廠商都會特別加註及附帶說明強調「會提供相關軟硬體的教育訓練」及犯罪預防警察學院及警務學院對於

在職警察的持續訓練，因為現今社會資訊成長的快速所導致的資訊爆炸，已經讓新、舊世代的警察對於資訊的掌握落差越來越大，若不時常提供保持訓練，很快就會被時代的洪流淹沒，也正因如此，他們政府主動提供了多元的教育訓練，讓他們的警務人員能掌握社會的趨勢及犯罪成因，並因應研擬有效的打擊策略。

三、持續派員參加，掌握產業脈動

參加是類展覽，除了可藉此進行警政交流、強化國際合作外，也可將外國的優良作法、先進技術與觀念引進國內，以拓展我國國際視野、提升打擊犯罪科技，並作為我國改善警政制度的參考依據，本次參展的相關資料也已奉署長指示，提供給刑事警察局參考評估於我國之應用。爾後仍建議持續編列相關預算指派或遴選優秀員警至類似之國際展覽、會議或訓練項目進行考察，讓我國警政能永續發展、掌握社會脈動及最新科技技術。