出國報告（出國類別：進修）

研習 AI 技術及資料分析用於犯罪偵查及預防之運用

服務機關：內政部警政署
姓名職稱：警務正王人幼
派赴國家：英國
出國期間：112.06.09~06.22
報告日期：112.09.06

摘要

鑒於資訊科技與新興科技日新月異、優越的處理效率，犯罪者常利用網路跨越時空、隱密性及匿名性等特性，以資訊科技、電腦網路作為犯罪聯繫、處理管道，造成執法機關的偵查斷點，面對毒品犯罪組織扁平化、詐欺犯罪專業分工、跨國犯罪證據移轉、黑道組織利益合流等新型態治安挑戰，執法機關日益重視運用資料分析技術分析整合犯罪海量資料，以強化辦案資訊即時化，有效壓制犯罪發生。英國政府現致力於提升執法效率及情資整合，有效提升執法人員各項勤務作為的精準度，準確預測並遏阻犯罪，減少偵查能量無謂的耗損。本計畫前往英國倫敦警察廳，進行犯罪情資分析及數位科技預警機制之交流，並參加倫敦警察廳舉辦的「Demystifying Cybercrime Course」課程，透過學習先進國家執法機關之犯罪情資分析模式，期能突破陳舊偵防策略思維模式，善用精進科技以提升既有偵查技能。

目錄

壹、目的

一、計畫目標

近年由於跨國與集團組織所涉犯之毒品及詐欺犯罪層出不窮，新興網路跨境犯罪日益嚴重、手法亦日益精進，執法機關越來越重視善用資料分析技術整理分析所得零碎資料，增進案件偵辦效率，儘速將嫌犯繩之以法。本計畫前往英國倫敦參加 Demystifying Cybercrime Course 課程，該課程訓練針對不同目標，使用資料進行網路犯罪分析，學習如何有效率地蒐集、分析資料，並透過與全球專業資料分析人士分享交流，以提升資料分析專業技術，充實資料分析人員專業能量。

倫敦警察廳是英國首都大倫敦地區的警察機關，肩負著重大的國家任務，包括配合指揮反恐、保衛英國皇室及政府高層官員和倫敦居民及遊客等。為達成各項任務，倫敦警察廳建立了新型態犯罪偵查與預警模式，並持續發展情資整合及對於 AI 影像辨識技術，本計畫前往英國倫敦警察廳及相關執法單位，進行犯罪資料分析與預警之交流，透過學習先進國家之犯罪情資分析、預警模式及影像辨識運用，對我國警察實務推動科技偵查犯罪及 AI 警政有所助益。

二、計畫預期效益:

透過派員參與英國專業情報分析培訓課程，加強培訓本署警政資料分析團隊分析人員之資料分析專業能力及資料分析工具運用，以及作為後續規劃及建立我國犯罪情資分析課程之參考，並透過與英國執法機關進行犯罪資料分析與預警之交流，學習先進國家情資分析模式，以推動警察 AI 資訊科技犯罪偵防及人才培養，協助員警更有效率的進行犯罪偵防，提升警政治安防護能量。

貳、參訪過程

本次參訪由中華民國駐英國代表處洪秘書世明協助安排及協調參訪行程，並全程陪同參訪事宜。

一、聯合國際犯罪中心(Joint International Crime Centre，簡稱 JICC)

(一) 背景介紹

全球正面臨利用跨國活動日益複雜的組織犯罪集團所造成的犯罪威脅，英國結合國家犯罪局 (National Crime Agency, 以下簡稱 NCA) 國際犯罪局 (UKICB) 和警務部門國際犯罪協調中心 (ICCC) ，於 2023 年 4 月成立聯合國際犯罪中心(Joint International Crime Centre，以下簡稱 JICC)，目的是推動、協調和支持英國警務和執法部門對國際犯罪的處理與反應。英國是重視安全生活與創造繁榮工作的國家，執法單位及聯合國際刑事法院將致力於識別來自國外的犯罪威脅，並建立應對和預防這些犯罪威脅的能力，英國安全部長 Tom Tugendhat 表示組織化的犯罪集團並不侷限於國界的限制，如果想打擊最危險的犯罪組織與犯罪者，就必須從上游和源頭查緝，新創立的 JICC 將達成這個目標，採取聯合多單位來識別來自國外的犯罪威脅並削弱其對英國的影響。

大多數犯罪威脅受到來自英國境外的犯罪勢力控制，隨著越來越多的非英國國民成為嫌疑人、證人或受害者，前線警力越來越需要在國際上進行合作。並為英國警務和更廣泛的國際犯罪執法以及刑事司法 (LECJ)培訓和技能提升的需求提供長久性的支持。另自英國退出歐盟後，執法與刑事司法上都需要加強協調，由於多邊渠道（國際刑警組織和歐洲刑警組織）和雙邊渠道（國際勞工組織網絡）沒有充分發揮作用等因素，加上英國執法部門和國際合作夥伴一直希望有個單位在國際警務事務上進行合作。最後在英國，擁有太多的資料儲存庫和程序來管理國際事務上的查詢，綜合上述因素與需求，JICC 便在多方期待下成立。

圖 1：Joint International Crime Centre，JICC 成立

JICC 匯集了來自警務部門和 NCA 的專家，共約 300 名警官，其中三分之一是從警察部隊借調，並由國家犯罪局(NCA) 和國家警察局長委員會(NPCC) 共同監督管理。除此之外，除了罪犯管理、引渡以及國際刑警組織和歐洲刑警組織相關事務外，JICC 還將涵蓋數據管理和分析、資訊提供和交換以及出入境情報開發和分析等服務。

(二) 警政合作部門(Policing and Partner Engagement Unit，PPEU)

1. 單位介紹

英國的警察體系主要由英國各地的警察機構負責執行法律、維持治安和保護公眾安全，總共有 48 個獨立的警察部門，分別為英格蘭警察部門和威爾士警察部門共 43 個、蘇格蘭警察部門 1 個、北愛爾蘭警察部門 1 個、3 個專業部門(英國交通警察、民用核能警察、國防部警察)，以及 9 個檢察機構。由於英國未採取中央集權的警察制度，且長期以來,英國一直抗拒成立一個全國性的警察部門，英國警方沒有設立一個專責主導犯罪偵查的主體，在偵辦跨警察部門或跨國案件過程中常發生案件隸屬及偵辦等分歧問題，而這時 JICC 就擔任協調跨部門協調與溝通的角色，整合各部門案件偵查的支援，加強偵辦力道，提升辦案效率。

圖 2：英國地理位置與相關執法單位

2. 參訪內容

JICC 副組長 David Saffery 以簡報方式介紹 JICC 的成立背景及主要業務，隨後帶領我們參觀 JICC 內部各個部門，第一個警政合作部門（PPEU）扮演跨機構協調與溝通角色的重要性，我國駐英國代表處洪世明秘書也談到近期接到由臺灣民眾向駐英代表處尋求協助有關家人至英國工作失蹤並與臺灣家人失聯的案件，也是藉由 PPEU 從中協助才掌握到失蹤臺灣公民的行蹤，進而破獲雇主非法囚禁臺籍員工的案件，PEEU 部門向我們介紹英國警察體制運作情形與文化上的差異，英國警察體制是相對分散的，由多個獨立的警察機構和組織所組成。以下是英國警察體制的介紹：

- 地方警察局：英國地方警察局負責在各地區執法、維護治安和保護民眾安全。每個地區都有設立各地的警察局，負責該地區的警政工作。每個地區警察局由警察局長（Chief Constable）領導，負責指揮和管理所屬警力。
- 倫敦警察廳（Metropolitan Police Service）：倫敦警察廳是英國最大的地方警察機構，負責倫敦市的警政工作。具有獨立運作的特性，與其他地方警察局略有不同，是英國首都大倫敦地區的警察機關，於 1829 年在內政大臣羅伯特·皮爾主導下成立，負責重大的國家任務，包括配合指揮反恐、保衛英國王室、政府高層官員、倫敦居民及遊客等。

- 國家警察機構：在某些特定領域，英國設有一些國家級的警察機構，負責特定的執法工作。例如，民用核能警察（Civil Nuclear Constabulary）負責保護民用核設施的安全，而英國交通警察（British Transport Police）負責鐵路和公眾交通運輸系統的安全。
- 警察監督機構：英國設有獨立的警察監督機構，負責監督警察的行為和處理投訴。其中最重要的是獨立警察投訴委員會（Independent Office for Police Conduct，IOPC），該機構負責調查涉及警察不當行為的投訴和重大事件。

圖 3：參訪人員與 JICC David Saffery 副組長合影照片

(三) 國際司法互助部門(Judicial Cooperation Desk)

1. 單位介紹

國際司法互助部門主要工作為加強國際間的刑事司法合作，打擊跨國犯罪，確保公正和有效的刑事司法程序。在全球化的世界中，犯罪偵查協作比以往任何時候都更加重要。由於犯罪不止於國境內，國家間需要迅速有效地合作，保護公民並伸張正義。透過此部門在國際間建立起協作網絡，提供迅速、有效和合法的合作機制，以應對日益全球化的刑事活動和挑戰。該部門由一名警官監督，管理六名合約約聘人員。

2. 參訪內容

了解該部門如何協助第一線員警協助國際刑事案件的引渡程序，促進涉案人員的引渡和交付、處理國際法律援助請求，包括提供證據、文件和其他相關資訊、促進國際間的刑事司法資訊交換，協助調查和起訴跨國犯罪、協調和合作跨國刑事調查，與其他國家的司法機構分享情報和調查結果。

(四) 生物特徵與歐盟交換平臺部門(Prüm Biometrics Unit)

1. 單位介紹

Prüm 協定是一個跨國安全和執法合作框架，目的在促進成歐盟成員國之間的 DNA 和指紋資料交換。生物特徵與歐盟交換平臺部門主要負責協調和統籌 Prüm 協定的實施。該團隊主要的職責包括：

- 協調與 Prüm 協定相關的技術和操作事項，以確保英國與其他歐盟成員國之間的順暢資料交換。
- 處理和管理 Prüm 協定所涉及的 DNA 和指紋資料，包括搜集、分析、存儲和共享。
- 與其他國家的 Prüm 團隊進行合作和協調，促進資訊交流和協作。
- 確保 Prüm 協定的實施符合相關法律、政策和隱私保護標準。

2. 參訪內容

了解生物特徵與歐盟交換平臺如何協助英國執法單位，成功識別無法與已知犯罪嫌疑人或現有證據相匹配的犯罪案件。有別於我國只針對特定犯罪嫌疑人於拘捕後才能取得其 DNA 並加以建檔，當我們詢問有關英國取得犯罪嫌疑人 DNA 的相關規定，JICC 副組長 David Saffery 告訴我們在英國只要是犯罪嫌疑人，一經逮捕後便會直接取得犯罪嫌疑人 DNA 並建檔儲存。至今透過 Prüm 協定破獲犯罪類別與案件數如下：

- 謀殺案 54 件
- 強暴案 129 件
- 其它嚴重性侵案 37 件
- 嚴重攻擊案 39 件

■ 住宅竊盜案 1600+件

圖 4：參訪人員與 JICC 同仁、駐英代表處洪世明秘書(左一)合影

圖 5：參訪人員與 JICC David Saffery 副組長(左一)、Nick Tetstall 警官(右一)合影

二、倫敦警察學院(Metropolitan Police Training College- MPS Peel Centre)

(一) 背景介紹

MPS Peel Centre(皮爾中心，簡稱 Hendon)是倫敦警察學院的主要訓練機構之一，提供培訓和教育倫敦警察以及其他相關機構的執法人員，該中心以 19 世紀英國政治家羅伯特皮爾(Robert Peel)的名字命名，羅伯特皮爾被認為是奠定現代警察制度的先驅。

皮爾中心由培訓主任兼協調員管理，負責監督管理新進警察人員訓練。學員在該中心接受為期 13 週的課程。除此之外，所有特別警察（Special constables)都在 Hendon 接受培訓，並在 Hendon 或大都會警察局各地的「區域培訓中心」（Regional Training Centres）完成剩餘的 23 天課程（可於上班日加強訓練，或選擇連續 23 天假日受訓）。該中心開設許多有關警察實務工作方面的訓練課程，包含法醫和犯罪現場分析，到無線電操作及駕駛技能等。皮爾中心建立在現代、科學培訓方法之上，設有法醫科學實驗室、偵訊培訓設施和警察駕駛學校。現職警察也會在不同時期返回中心接受訓練以精進相關執法技能。

皮爾中心提供多種培訓課程和訓練活動，包括警察基礎培訓、專業技能培訓、駕駛技術訓練、戰術和應變培訓等。該中心配備了現代化的設施和訓練場地，包括模擬城市街區、駕駛訓練場、射擊場和體能訓練設施，以提供全面且實用的培訓體驗，在警察培訓和專業發展方面扮演著重要角色，確保執法人員具備必要的技能、知識和專業態度，以應對各種挑戰和情境，有助於提高倫敦警察的整體執法能力，保障民眾安全和社會秩序。

(二) 參訪內容

此次參訪倫敦警察學院由 JICC 警官 Nick Tetstall 安排，參訪各項不同訓練課程，一開始先體驗道路駕駛技術課程，再分別由負責不同課程人員介紹各項訓練項目，包含偵訊攻防訓練課程、資訊系統訓練課程及沉浸式危機模擬(九頭蛇系統，又稱 Hydra 系統)。

圖 6：皮爾中心正門外觀照片

1. 安全駕駛技術課程

該課程內容主要針對員警在開車追緝嫌犯時之安全駕駛訓練課程，整個課程為期 3 週，並在最後 3 天進行實地演練測試，測試通過才取得可以在道路上追緝嫌犯的資格，而這次難得可以一同參與全程測試過程，在課程前我們甚至還簽立了志願參與同意書，整體測試過程為由教官駕駛一般車輛扮演逃逸的亡命之徒，而接受測試的員警負責駕駛警車追緝歹徒所駕駛的車輛，而警車的副駕駛座則是另一名負責記錄並評分學員全程追緝駕駛是否遵照安全意識及相關作業程序，課程一開始先坐上扮演歹徒的教官 Neil Algate 所駕駛的車輛(英國為右駕)，Neil Algate 教官在測試開始前貼心地詢問我們是否會暈車及提醒我們如果過程中有需要急轉彎時會先告知我們預作準備，作為歹徒車輛，我們從皮爾中心旁的駕駛學校先行出發，再由受測試學員駕駛警車由後方進行追緝，追緝過程約 15 分鐘，由教官視需要調整時間，全程我們就在市區中心一般道路及高速公路高速行駛，教官試著前方車輛模擬嫌犯開車逃逸，後方警車追捕逃犯時之安全駕駛訓練，其訓練地點在一般的道路上行駛進行訓練，目的在提升員警在高速追捕和逮捕逃犯時的駕駛技巧和安全意識，此訓練課程在確保警察執行追捕任務時具備必要的技能和知識，同時保護公眾和警察自身的安全。

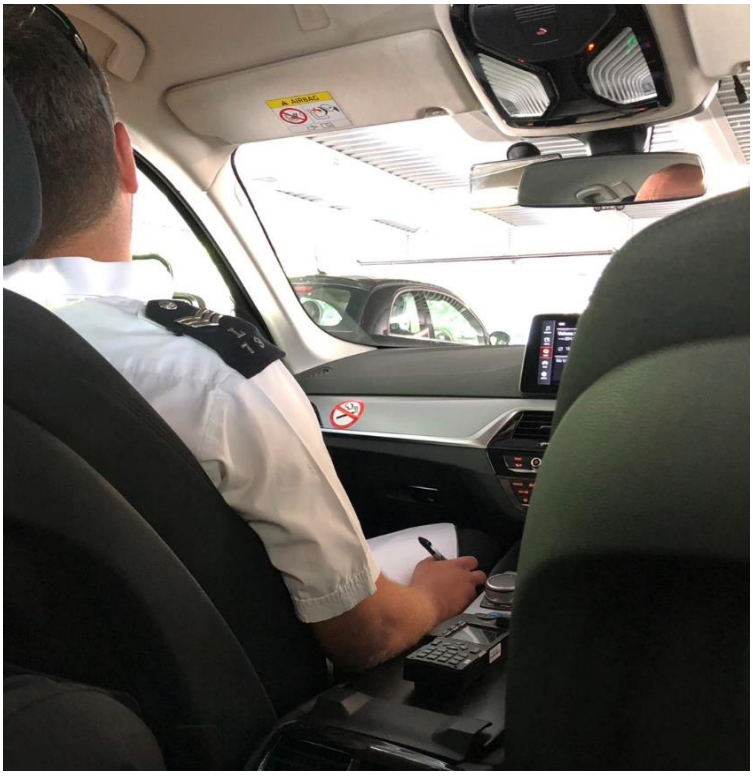

圖 7：安全駕駛技術課程教官記錄學員模擬測驗缺失

圖 8：安全駕駛技術課程教官討論參訓學員模擬測驗結果

圖 9：參訪人員與安全駕駛技術課程 Neil Algate 教官合影

2. 偵訊攻防訓練課程

犯罪嫌疑人往往會利用自我防衛的否認犯罪或對犯罪事實避重就輕，運用偵訊技巧突破犯罪嫌疑人心房，使其供述實情，是偵查工作最重要也是最困難的部分，偵訊攻防訓練課程由學員針對教官設定模擬之情境，分別扮演犯罪嫌疑人和偵訊人員，嘗試面對犯罪嫌疑人各種卸責之詞，練習如何使犯罪嫌疑人供述真實案件相關事證及情節，進而尋找相關證據，在過程中，教官會與學員討論如何加強偵訊技巧並進行有效偵訊。

圖 10：皮爾中心內部照片

3. 資訊系統訓練課程

Home Office Large Major Enquiry System 福爾摩斯系統(HOLMES)是一個資料庫系統，協助英國警方管理執法機關偵辦管理重大犯罪案件複雜過程，記錄及共享情資的一套「案件管理系統」，通常用於管理偵辦重大謀殺案件，包括連續殺人案件、恐怖攻擊等案件，旨在幫助警方進行大規模調查。警方可以使用該系統來整理並交互利用在重大案件調查中蒐集所有情資，且該系統建置於雲端上，允許多個用戶同時輸入、更新和查閱資訊。英國的所有警察單位都使用 HOLMES 系統，並且能夠將事件連結起來以共享資訊或進行聯合調查。HOLMES 系統的建置是為了滿足不同規模和複雜程度的調查，所有資訊都將被記錄並作為原文件輸入事件庫，工作人員將評估這些資訊，並根據負責調查的官員的政策決定應採取的行動，工作人員將評估何種資訊應該交互運用和索引，以便可以輕鬆地進行後續的研究和檢索。HOLMES 系統第一代開發始於 1986 年，而後英國內政部警政資訊技術機構（Police Information Technology Organization）於 1994 年委派 Unisys 公司優化系統，於 1996 年完成升級改版，即現行福爾摩斯系統第二代 HOLMES 2，該系統可區分為「事件管理 Incident Room」與「災難管理 Casualty Bureau」兩大部分，事件管理系統主要建置目地為：蒐集並管理大量情資、按優先順序處理情資以協助確立調查方向、任務分配與進度管理、圖表化呈現情資分析、產生呈交法院文件。災難管理工具設計上係參考英國高階警官協會（Association of Chief Police Officers）緊急程序委員會負責制定重大災難標準處理程序，當重大災難發生時，所有執行重大災難應變任務之不同單位都須依照此處理程序辦理，系統功能有失蹤人口紀錄、災難資訊紀錄、生還者紀錄、災難生還者與失蹤人口比對、死者鑑定、綜合資訊、失蹤人口電話報案集中處理。

圖 11：皮爾中心上課學員

4. 沉浸式危機模擬(九頭蛇系統，又稱 Hydra 系統)

Hydra 系統係由 Jonathan Crego MBE 教授設計的，該系統是一種沉浸式讓學員身歷其境的互動式訓練模擬環境，目的係透過演練來協助決策者面對突發重大事件可以擬定策略及決策。該演練方式提供了真實事件模擬，使執法人員能即時應對時間緊迫的重大事件，採取最適當的行動及策略。教官會先行將學員分組，每組 3 至 4 人，不同組別分別在不同的模擬情境室進行各項事件情境模擬，教官會撥放模擬實際情況的影片，再由小組成員共同討論面對此情境要如何處置，在設定需作出決策的限制時間內，學員要輸入所作出的決策，教官則會按照各組學員的決策來決境下一段影片的案件內容，模擬情境結束後，教官會在和各組學員討論所作決策及行動並聽取理由，讓每組學員從中獲得經驗，增進決策的全面性及周延性。而我國也有利用相似的概念建置「智慧 XR 警勤訓練系統」，兩者的差異主要為為 Hydra 系統著重於發生重大事件時之決策行為，而智慧 XR 警勤訓練系統著重於面對各類案件的第一線執勤員警，在當下的危機處理及戰術技能，如遇到持刀的歹徒向員警咆哮，員警應立刻拔出警械，這時要選用何種警械也考量員警的危機意識，還有要在哪些時機點即時使用警械才能化解危機，確保自身執勤安全。

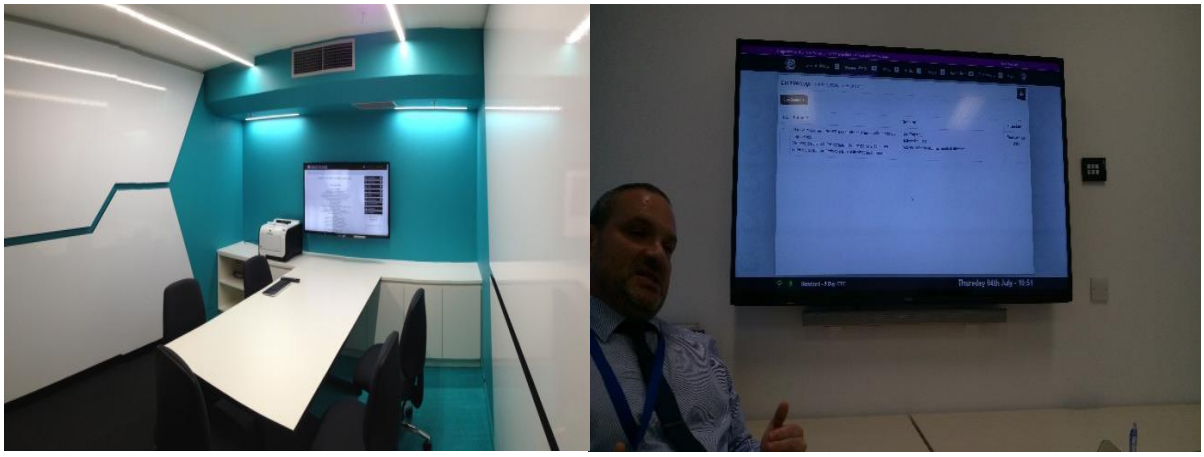

圖 12：模擬情境室照片

圖 13：Hydra 控制中心照片

三、倫敦大學皇家哈洛威學院-法律與犯罪學系(Royral Holloway, University of London)

(一) 學校介紹

倫敦大學皇家哈洛威學院 (Royral Holloway, University of London) 是由兩位知名的社會倡導人士所興建：伊莉莎白里德 (Elizabeth Jesser Reid) 與湯瑪士哈洛威 (Thomas Holloway)。前者於 1849 年興建貝德福特學院 (Bedford College)，此學院為英國第一間開放女性接受高等教育的學府；後者於 1879 年興建皇家哈洛威學院 (Royral Holloway College)，兩所學院於 1900 年正式成為倫敦大學的學院之一，並於 1886 年由維多利亞女王親自舉行揭幕儀式，兩所院校正式合併，成立倫敦大學皇家哈洛威學院。

英國女王之女，安妮長公主 (The Princess Anne, Princess Royal) 為現任倫敦大學的校監，經常於大學參加相關典禮儀式，使大學與英國皇室保有良好的關係。於 2014 年學院的音樂學系欽定為慶祝伊麗莎白二世女王鑽禧紀念典禮，為過去一世紀年間，僅有的兩次特殊榮譽。

創校至今，皇家哈洛威學院已成為英國研究型大學的先驅之一，擁有卓越的科研成果，其中科學、藝術、商學、經濟、法律等領域皆於全球占有領先的地位。學院秉持教學與研究可改變人生、拓展思維的辦學理念，致力於協助未來的領導者發掘自身潛力，同時培養社會責任，藉以栽培優秀的領導人才。學院每年招收逾一萬名學生，包含兩千名的國際學生，以多元的學習為基礎，建立一處國際且多文化的學習環境。

圖 14：倫敦大學皇家哈洛威學院外觀照片

(二) 參訪內容

皇家哈洛威學院(Royal Holloway, University of London)的法律與犯罪學系（Department of Law and Criminology）是該大學的一個學術部門，專注於

法律和犯罪學相關的教學和研究。

該系所提供各種與法律和犯罪學相關的課程，包括法學學士（LLB）、法學碩士（LLM）、犯罪學碩士（MSc in Criminology）等學位課程。這些課程旨在培養學生對法律體系和犯罪問題的理解，以及提供他們所需要的技能和知識。在教學方面，教師和學者們擁有豐富的專業知識和經驗，能夠為學生提供專業指導和支援。同時，學生還可以通過實習和實踐機會來應用所學知識，培養他們的實踐能力。在研究方面，該系所致力於推動法律和犯罪學領域的研究，涵蓋了各種主題，如刑法、民法、國際法、犯罪學理論、刑事司法等。研究的成果不僅能夠豐富學術界的知識庫，還能夠為社會和政府決策提供重要的參考依據。整體而言，皇家哈洛威學院的法律與犯罪學系是一個致力於法律和犯罪學研究和教育的學術機構，為學生提供了廣泛的學習和發展機會。

本次參訪法律與犯罪學系教授 Dr Mohammad，透過簡報方式介紹法律與犯罪學系，雙方就分享如何運用所學的知識結合未來實務應用，並針對以下議題進行討論。

- 法律與犯罪學術知識與警務工作之連結

  法律與犯罪學術知識與警務工作之間存在著密切的關聯性，歸納以下重點：

  (1) 法律遵從：警務人員需要了解法律和法規，以執行與犯罪相關的職責。法律與犯罪學術知識可以提供他們對相關法律的理解和應用，並確保他們的行動符合法規。

  (2) 犯罪學：警務人員對於犯罪學的知識能夠幫助他們了解犯罪的原因、模式和動機，從而更好地預防犯罪和制定有效的執法策略。

  (3) 證據蒐集和刑事司法程序：警務人員需要具備對證據的蒐集和保護的知識。他們需要了解適用的刑事司法程序和要求，以確保證據能夠在法庭上有效使用。法律與犯罪學術知識可以幫助他們了解這些程序以及與其相關的法律原則。

  (4) 犯罪分析和預防：警務人員利用犯罪學的知識進行犯罪分析，

以了解犯罪的模式、趨勢和特點。這樣他們可以更好地制定和實施犯罪預防策略，提高公眾的安全。

(5) 依法行政：警務人員在執法過程中需要平衡執法權力和保護公民權利之間的關係。法律與犯罪學術知識可以幫助他們理解這一平衡，確保他們的行為符合法律規定，同時尊重和保護公民的權利。

■ 運用犯罪統計數據進行深度分析

用實務上的犯罪相關統計數據進行更進一步的分析可以幫助警務人員深入了解犯罪模式、趨勢和特徵。歸納以下重點：

(1) 犯罪率和地理資訊系統（GIS）：犯罪率統計數據可以用於分析不同地區的犯罪趨勢。通過將這些數據與 GIS 地圖相結合，可以發現犯罪熱點區域和高風險地帶。這可以幫助警務人員更聚焦地設計和部署執法資源。

(2) 時間和季節效應：分析犯罪統計數據時，可以了解到犯罪率在不同時間和季節的變化。例如，特定類型的犯罪可能在特定季節暴增。這些洞察可以幫助警務人員規劃和調整執法策略。

(3) 犯罪類型和特徵：犯罪統計數據可以提供各種犯罪類型和特徵的洞察。警務人員可以將這些數據用於分析犯罪模式，例如哪些行為特徵可能與特定犯罪有關聯。其分析結果以助於警務人員制定更有針對性的執法策略和預防措施。

(4) 社會和經濟因素：除了犯罪數據外，還可以將其他社會和經濟因素納入分析。例如，通過研究人口結構、經濟狀況和教育水平等因素，並了解這些因素與犯罪之間的關聯。以助於警務人員制定更全面和有針對性的犯罪預防措施。

(5) 數據分析工具和技術：利用數據分析工具和技術，可以更有效地處理和分析大量的犯罪統計數據。這些工具可以幫助蒐集數據中的模式和趨勢，並進行視覺化呈現，以便更好地理解和利用這些數據進行決策，如警政署的智慧分析決策支援系統就是很好的案例分享。

圖 15：參訪皇家哈洛威學院模擬法庭照片

圖 16：參訪人員與法律與犯罪學系教授 Dr Mohammad 合影

四、英國倫敦警察廳

(一) 背景介紹

倫敦警察廳由數個主要部分構成，每個部門各司其職。主要的部門有地區巡邏部（Territorial Policing Directorate）、專門刑事部（Specialist Crime Directorate）、特殊行動部（Specialist Operations）、中央行動部（Central Operations），及行政暨支援（administration and support）。每個部門皆由警察廳助理總監（Assistant Commissioner）負責監督。管理委員會則由警察廳總監（Commissioner，即廳長）、副總監（Deputy Commissioner，副廳長）及各部門領導人組成

■ 地區巡邏部（Territorial Policing）

地區巡邏部(縮寫 TP)負責大倫敦地區內部每日的地方性巡邏，巡邏範圍組成了倫敦警察廳警區，被劃分為 32 個自治市行動指揮隊（Borough Operational Command Units，縮寫 BOCUs），每個行動隊皆有負責巡邏、處理緊急狀況的警員。社區守望相助隊由警員及警方社區支援員組成，負責在某行動隊轄下的特定區域內巡邏。刑事偵緝科（Criminal Investigation Department，即 CID）的刑警亦附屬於各個行動組，執行調查工作。另外，皇家公園行動指揮隊（Royal Parks Operational Command Unit）及交通安全行動指揮隊（Safer Transport Command）同樣也是地區巡邏部的下轄單位。

■ 專門刑事部（Specialist Crime Directorate，SCD）

專門刑事部（縮寫 SCD）是倫敦警察廳的調查部門，負責針對重大案件、有組織犯罪及特殊犯罪等案件的調查工作，有時也會介入刑事偵緝科無權偵辦的案件。該部門由一名助理總監統率、四名高級警官領導內部的基層行動指揮隊，專門刑事部單位如下：

(1) 兇殺及重案指揮課（Homicide and Serious Crime Command，SCD 1）：負責謀殺、謀殺未遂及殺嬰等殺人案件的偵辦，調查工作由其下轄的謀殺調查組（Murder Investigation Team）進行。該調查部也負責偵辦當事人生命可能受到威脅的失蹤及綁架案件。

(2) 強姦及性犯罪課（Rape and Serious Sexual Offences，SCD 2）：偵辦涉及強姦罪及各種性犯罪的案件。

(3) 指紋部（Fingerprint Services）：負責居於英國境內人士指紋的蒐集及歸檔作業。此外，當某些人士欲進入需要行為良好證明才准許入境的國家時，則是由該單位提供入境許可證明書。

(4) 刑事鑑識課（Forensic Services Command Unit，SCD 4）：負責為倫敦 32 區的自治市行動組及其他警備單位提供隨叫隨到的司法科學鑑定。

(5) 虐童調查隊（Child Abuse Investigation Team，SCD 5）：負責偵辦

針對未成年人進行肉體、精神或性等虐待的犯罪事件。

(6) 經濟及特殊犯罪課（Economic and Specialist Crime Command，SCD6）：負責針對重大案件及經濟犯罪案件的調查。

(7) 三叉戟團伙犯罪指揮中心（Trident Gang Crime Command，SCD 8）：負責調查倫敦黑人社區內槍枝犯罪的單位，是倫敦警察較為著名的單位之一。

(8) 重案及組織犯罪課（Serious and Organised Crime Group，SCD 7）：負責調查重大案件、組織性犯罪危及人類生命的案件。

(9) 秘密警務情報課（Covert Policing/Intelligence，SCD 10）：負責為其他警務部門提供人力對嫌犯或犯人進行暗中監控工作。

■ 中央行動部（Central Operations，CO）

中央行動部（縮寫 CO）負責為警察廳其他部門提供專門的職務及行動支援。

■ 特殊行動部（Specialist Operations，SO）

特殊行動部（縮寫 SO）是倫敦警察廳負責執行特殊勤務的部門。目前該部門被分為以下三個單位：

(1) 警備指揮科（Protection Command）：分為要員保護組、皇室成員保護組、外交保護組。

(2) 反恐指揮科（Counter Terrorism Command，SO15）：首要任務是維護公眾安全，及防止倫敦成為適合恐怖主義發展的環境。勤務內容包含：將恐怖活動及非法行動的參與者繩之以法、預防或瓦解恐怖活動、蒐集並運用倫敦地區恐怖主義或極端主義的相關情報。

(3) 保安指揮科（Security Command）：分為西敏寺課及航空保安課。

(二) 參訪內容

本次參訪了解英國在反恐及維護治安等任務中扮演舉足輕重的角色的影像辨識系統 Digital Biometric Exploitation Unit，該系統影像來源係從大眾運輸交通樞紐等重要道路且人潮眾多的地方所架設之 CCTV，並由專門處理影像人員將 CCTV 所拍攝的人臉、身體特殊特徵(如嘴唇、鬍子、疤

痕、刺青)及判斷有異常行為對象的包包、鞋子(包含鞋底圖案)等影像進行後製截圖，可提供後續物品辨識功能作使用。該系統辨識影像比對來源為警方透過刑事案件所蒐集或上傳之影像，較為特別的是倫敦警察廳於特定地點部署了即時人臉辨識監視器，並設置獨立系統加以辨識比對，該系統不會介接其他的 CCTV 影像，系統內會加入通緝犯、嚴重犯罪案件(嚴重暴力、槍枝犯罪、兒童性剝削)對象的相片作為比對之用，但礙於英國對於個人資料的保護及議員、資料保護組織和人權組織的質疑，仍面臨了正確保障及部署地點、數量的透明度等考驗。

圖 17：英國倫敦警察廳正門外觀照片

五、歐洲資訊安全應用展覽會(2023 Infosecurity Europe)

(一) 展覽簡介

Infosecurity Europe 是歐洲最大的資訊安全展覽會之一，每年都吸引著全球資訊安全領域的專業人士、企業和組織參與。今年度 Infosecurity Europe 於英國倫敦舉辦，參展商和參與者為全球各地的資訊安全供應商、技術公司、諮詢機構、研究機構和相關組織參展。觀展者包括資訊安全

專業人士、企業高階主管、政府代表、學術界人員以及對資訊安全感興趣的對象，本次看展人數 3 天內達 13,800 以上，提供約 380 個技術創新或解決方案。展覽主題涵蓋資訊安全領域的各個方面，包括網路安全、資料保護、身分驗證、風險管理、合規性、威脅情報、安全意識和教育等。展覽內容包含參展商展示他們的技術創新、網路安全工具、資料保護解決方案、風險評估服務等。此外，展會還包括技術演示、專家演講、圓桌討論會議、工作坊和培訓課程等豐富的活動內容。

(二) 觀展過程

本次參展了解歐洲資訊安全最新趨勢、網路安全相關技術之應用，觀展廠商如下：

- Netscout Systems 公司

  Netscout system 總部位於美國，是一家網路安全和網路性能管理解決方案廠商。該公司成立於 1984 年，其產品和服務旨在提供企業或組織監測、保護和優化其網路和應用程式的性能。

- Cisco systems 公司

  Cisco systems 是一家全球領先的科技公司，總部位於美國 San Jose, Carfornia。成立於 1984 年，思科致力於為全球的組織、企業和個人提供創新的網路技術和解決方案，主要為開發、製作和銷售網路硬體、軟體、通訊裝置等高科技產品及服務。

- Juiper Network 公司

  Juniper Networks 總部位於美國加州，是一家網路設備和解決方案廠商。該公司成立於 1996 年，其產品主要包含路由器、交換機和防火牆等領域。並致力於為企業和服務提供者提供高性能、可靠和安全的網路基礎設施，以滿足不斷增長的網路需求。

- F5 Networks 公司

  F5 Networks 總部位於美國華盛頓州，是一家網路應用層服務和應用交付網路解決方案廠商。該公司成立於 1996 年，在全球各地設有開發、製造和行政辦事處。其產品涵蓋應用加速、應用安全、阻斷服務攻擊防禦和負載均衡等領域。公司致力於幫助

企業提供高性能、可靠和安全的應用程式交付，以滿足不斷變化的業務需求和安全挑戰。

- 趨勢科技(Trend Micro)公司

  趨勢科技為網路資安全球領導廠商，致力建立一個安全的資訊交換世界。憑藉著數十年的資安專業、全球威脅研究以及持續不斷的創新，該公司跨雲端、網路、裝置及端點的網路資安平臺隨時守護著全球 50 多萬家企業機構及 2.5 億以上的一般使用者，提供各種強大的進階威脅防禦技術，專為如 AWS、Microsoft 及 Google 的環境提供最佳化，集中掌握及更快更有效的偵測及回應威脅。

圖 18：2023 Infosecurity Europe 展覽中心入口

圖 19：2023 Infosecurity Europe 展覽內部

參、倫敦警察廳經濟和網路犯罪學院「揭密網路犯罪」課程

一、課程起源與介紹：

經濟和網路犯罪學院在打擊經濟犯罪方面發揮著關鍵作用。作為英國國家詐欺和網路犯罪偵查領導機關，倫敦警察廳是培訓執法人員和反詐欺組織的中心。自 2012 年以來，經濟和網路犯罪學院為國家和國際政府單位、私人企業部門組織和個人提供培訓課程，由合格專業的調查員培訓團隊為所有政府、私人企業、第三方組織及其他警察單位提供各個級別的各項主題培訓課程。

二、參訓地點：

本次課程由英國倫敦警察廳主辦，課程地點位於 etc.venues Moorgate Bonhill House，etc.venues 公司在英國各地提供了極具舒適體驗的會議室、活動、培訓室場館。

圖 20：etc.venues Moorgate Bonhill House 外觀及前台

三、課程成員介紹：

本次課程由 Mark Johnson 擔任講師，Mark Johnson 是經過註冊的 IT 專業人員及網路詐欺和公開情資分析培訓師，曾經領導及協助邁阿密港和金斯頓港的緝毒行動，也曾擔任大東電報局在詐欺控制系統的 EMEA 地區主管，代表歐洲刑警組織和歐盟委員會向歐盟各地的金融情報機構提供社群媒體風險和調查培訓。專業教學領域包含網路犯罪、數位詐欺、加密貨幣犯罪風險和開源公開情資分析。

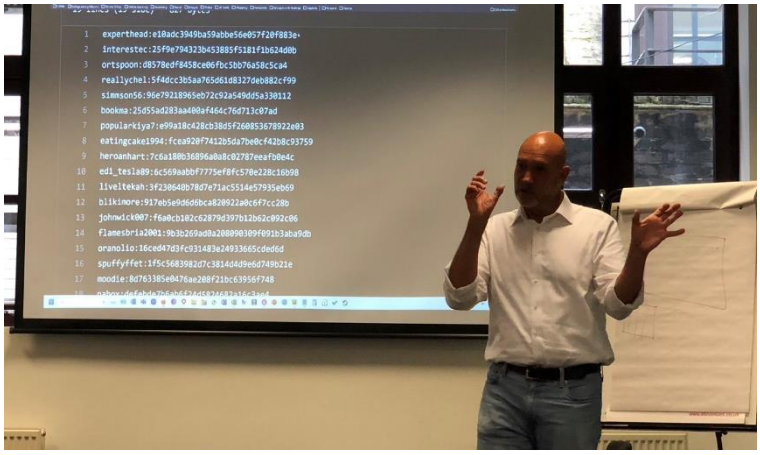

圖 21：揭密網路犯罪課程講師 Mark Johnson

本次參加課程學員共計 8 人，除筆者外，還有來自英國不同執法機關的執法人員，分別有聯合國際犯罪中心 JICC、倫敦警察廳及各地方警察機關之警務人員，其他少數來自民間企業專責處理網路犯罪和詐欺等人員，學員背景廣泛。

圖 22：參訓學員上課情形

四、課程內容：

(一) Demystifying Cybercrime 課程介紹

該課程主要讓上課學員充分掌握現代網路和設備技術的基礎知識，揭開新型態資通訊技術的神秘面紗，並提供易於理解的模型來調查相關網路犯罪案件。

(二) Demystifying Cybercrime 課程總計三天，課程內容主要分為 5 個主題，各主題內容依序簡要說明如下:

1. Real or Fake-Deep fake

深偽技術（英語：Deep fake）又稱深度偽造，是英文「deep learning」(深度學習)和「fake」(偽造)的混成詞，指的是基於人工智慧的人體圖像合成技術的應用，Deep fake 技術可將已有的圖像或影片疊加至目標圖像或影片上。傳統上是採用基於 3D 模型重建追蹤技術，較新的技術則是採用深度學習來達到換臉效果，為了解決深度學習的訓練難度和生成品質，又進一步融合了生成對抗網路技術。表情偽造是將其他人臉圖像的表情替換到目標人臉上，從而達到目標人物做指定表情的目的。此外，換臉偽造和表情偽造還常常結合語音偽造技術，透過文字到語音合成和語音轉換技術來製作虛假語音。

Mark 講師一開始先放上幾張人臉的照片，請大家分辨真實的照片和透過 Deep fake 所生成的照片，在學員討論的過程中，Mark 提示在辨別的過程中可以透過觀察照片中人物的眼距和眼睛幅度來分辨真假，另透過 AI 的 Deep fake 軟體可以利用所匯入龐大的照片資料來作訓練，進而創造出不存在的人物的照片，甚至使用者可以事先設定性別、年齡或特徵等，產出所設定條件的人物照片。

要發現深度偽造的影片或照片不是件簡單的事，有些影片的製作非常精緻，有幾個關鍵有助於確認眼前所看的，是否為非常具有說服力的深度偽造影片。若是影片中有人物臉孔出現，請特別注意臉部部分，並可試著尋找以下特徵：

(1) 明顯的視覺瑕疵

若要判斷是否為深偽影片，影像疊加部分的接合處是否有明顯瑕

疵為重要的判斷依據，也可觀察臉部輪廓的邊緣是否有出現不自然的紋理。即使是製作精緻的深偽影片，在背景區域或是影片跨幀時，人物的輪廓都有可能產生模糊或是失真的情形出現。

(2) 被改變的非臉部特徵

可以試圖使用此人物的其他圖像進行兩者相互比較。觀察主要臉部以外的特徵有無被改變，例如：手部、頭髮、體型。

(3) 不自然的肢體動作

如果影片人物的身體和頭部連結起來感覺生硬，可能表示影片的只有讓 AI 將圖像合成到人物的臉上，而沒有處理其他有關肢體動作的部分。

(4) 難以令人信服的聲音

深度偽造的創造者如果想讓對象人物說話，必須使用人工智慧生成的聲音，或是使用模仿對象人物聲音的演員。因此將影片音訊與該對象人物的聲音作比較，可能會聽出一些差異。

圖 23：Deep fake 辨識介紹

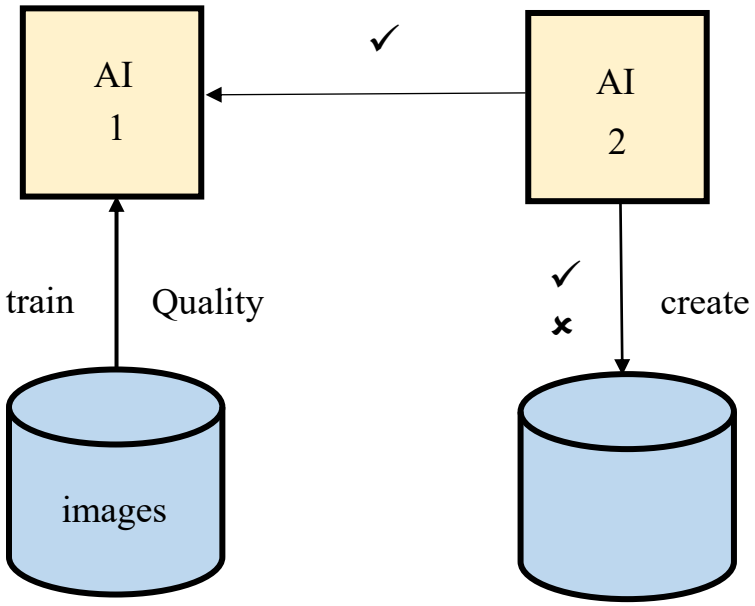

圖 24：Deep fake 深度學習示意圖

2. OSINT

公開來源情資（OSINT）被定義為透過蒐集、評估和分析公開來源情資而產生的結果，目的是為了得到特定所需的情資。

(1) OSINT 來源

- 公共紀錄
- 新聞媒體
- 圖書館
- 社群媒體平臺
- 圖片與影像
- 網站
- 暗網

(2) OSINT 使用者

- 政府單位
- 執法機關
- 軍事單位
- 記者
- 人權調查人員
- 私人偵探

- 律師事務所
- 資訊安全
- 網路威脅
- 滲透測試
- 社交工程

(3) 情資週期

- 準備(Preparation)

  評估需求和要求，確定任務目標及篩選資料最佳來源。

- 蒐集(Collection)

  儘可能從較多的相關來源蒐集資料和資訊。

- 處理(Processing)

  分類、組織所蒐集的資料。

- 分析(Analysis and Production)

  對所蒐集的資料形成可理解的解釋，得出結論並建議後續步驟。

- 呈現(Dissemination)

  公開來源情資調查結果的呈現和交付，例如：書面報告、時間表、建議等。

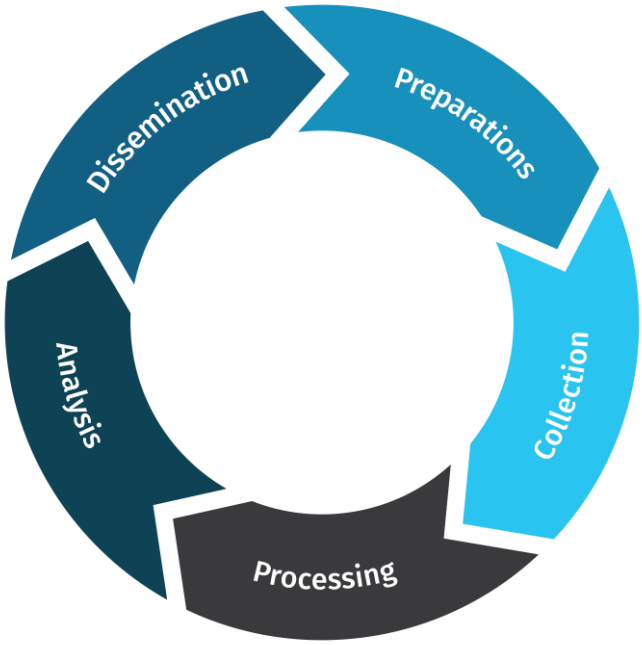

圖 25：情資週期示意圖(引自 SANS)

(4) OSINT 優點

- 可獲得公開資料

  OSINT 蒐集公開且合法獲取的資料，不必依賴機密或受限的資料來源。

- 來源廣泛

  公開來源情資可以從多種來源蒐集，包括社群媒體、新聞文章、政府公開資料和學術論文。

- 具有及時性

  由於公開來源情資多來自於公開資訊，可快速、實時地蒐集資料。

- 具成本效益

- 公開來源情報比其他形式的情資蒐集更具成本效益，因公開來源情資源自於公開資訊，不需要專門的設備或人員。

- 透明度高

  OSINT 具透明性，可簡易迅速驗證情資正確性。

(5) OSINT 相關技巧

- 搜尋引擎

  Google、Bing 和 Yahoo 等搜尋引擎是蒐集 OSINT 的有效工具，透過使用進階搜尋指令，可快速過濾和縮小搜尋結果以查找相關資料。

- 社群媒體

  可透過監控和分析 Twitter、Facebook 和 LinkedIn 等社群媒體平臺來取得更多面向的資料。

- 公共紀錄

  法院訴訟資料、財產紀錄和商業登記檔案等公共紀錄可蒐集有關個人、組織的資料。

- 新聞來源

  報章雜誌和網路新聞媒體等新聞來源可深入了解當前事件和趨勢。

- 網頁擷取

  網頁擷取需使用軟體或工具從網站中擷取資料，透過從多個網站擷取資料可快速有效地蒐集巨量資料。

- 資料分析工具

  Excel、Tableau 和 R 等資料分析工具對於分析巨量資料集非常有效率，可識別資料中的模式、趨勢和關係。

3. Dark Web

暗網，是由深網的一小部分所構成的，只能用特殊軟體、特殊授權、或對電腦做特殊設定才能訪問，構成暗網的隱藏服務網路包括 F2F 的小型對等網路以及由公共組織和個人營運的大型流行網路，如 Tor、自由網、I2P 和 Riffle。Tor 暗網可以稱為洋蔥區域（onionland），其使用網路頂級域字尾.onion 和洋蔥路由的流量匿名化技術。

3 Parks	資料量	說明
第一層明網 (Surface Web)	約4%~5%	能被任意搜尋引擎發現，並建立index區域，例如公開開放瀏覽網站
第二層深網 (Deep Web)	約90%~91%	網際網路上無法透過搜尋引擎搜索到的任何資訊。包含大多數良性網站或是需要帳號密碼登入後，才能檢所的資料、各類需要登入電子郵件資訊(例如Gmail)、不對外內部資訊系統(例如EMS)
第三層暗網 (Dark Web)	約4%~5%	也可以說，暗網是深網的一部分延伸，暗網中的網站的特點是使用加密軟體，普通搜尋引擎也無法訪問到的部分網路、被竊取的外洩資料，這些資訊的建立者或散布者希望將其隱藏，提供有需要的人存取。無法通過普通的谷歌瀏覽器或Safari瀏覽器訪問暗網

圖 16：網路分層架構

(1) Tor 介紹

- 可以透過 Tor 連結 Internet (明網)
- 允許連結匿名 Web 服務器，也允許使用者自建託管匿名 Web 服務器
- 服務器需要持續維持上線狀態
- 可被阻斷攻擊(利用阻斷攻擊來達成管制)
- 洋蔥網路已成功被多國國家封禁

- 最成熟具備許多用戶和開發人員
- 核心是 Mozilla 的 Firefox 瀏覽器
- Tor Network 運行隱匿活動
- Onion 網站可使用一般瀏覽器瀏覽

在洋蔥網路上，有個 Tor2web 技術，讓網際網路使用者不需要使用 Tor 瀏覽器也可以 Access Tor Onion 服務。透過 Tor2web 運營商就可以達成這樣的閱覽分析，但是 Tor2web 只保護洋蔥網站訊息發布者，而不是使用者，換言之，這樣的服務對 End User 並不安全。tor2web proxy 就像一個標準的網路基礎服務。Proxy 不檢查或修改內容，只是來回傳遞資訊。

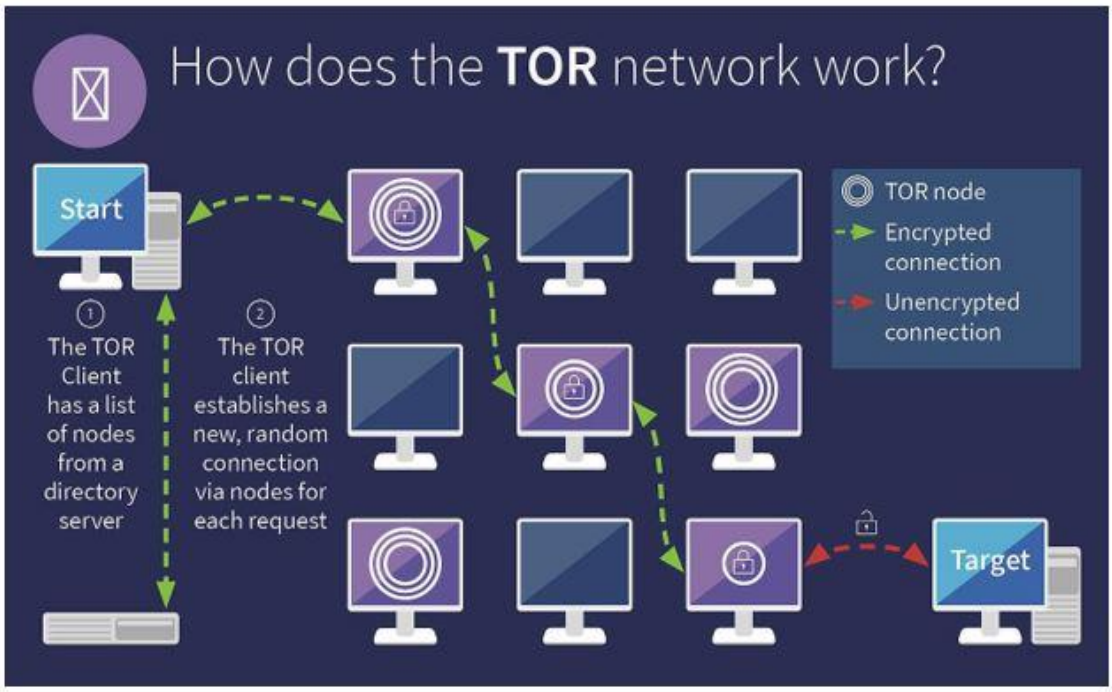

圖 27：Tor Network 架構示意圖

(2) I2P 介紹

- 可以透過 I2P 連結 Internet (明網)。
- I2P 是在明網基礎內運行的封閉網路。與 VPN 和 Tor 不同截
- 然不同，設計本質上是 outproxy 網路，專為與互聯網的匿名和
- 私人通信而設計，I2P 被設計為點對點網路。
- I2P 網路節點可以託管暗網服務的伺服器，也可以 access 其他

- 節點託管的伺服器和服務的用戶端。
- I2P 中的每個用戶端/伺服器都自動成為一個中繼節點，Data 通過哪一個特定節點路由取決於頻寬。
- I2P 中沒有互聯網，因此該網路由自己的匿名和隱藏網站組成，稱為 eepsites。
- I2P 採用 Java 環境。
- 全球約 5 萬多臺志願者電腦，無法進行第三方監控。

4. Dark Web

ChatGPT，稱為聊天生成預訓練轉換器（英語：Chat Generative Pre-trained Transformer），由 OpenAI 開發的人工智慧聊天機器人程式，於 2022 年 11 月推出，該程式使用基於 GPT-3.5、GPT-4 架構的大型語言模型並以強化學習訓練。技術面而言，ChatGPT 是「生成式預訓練轉換器」（Generative Pre-Trained Transformer）技術的最新發展，採用深度學習（deep learning），根據從網路上獲取的大量文本樣本進行訓練。ChatGPT 目前仍以文字方式互動，而除了可以用人類自然對話方式來互動，還可以用於甚為複雜的語言工作，包括自動生成文字、自動問答、自動摘要等多種任務。如：在自動文字生成方面，可以根據輸入的文字自動生成類似的文字（劇本、歌曲、企劃等），在自動問答方面，可以根據輸入的問題自動生成答案。還有編寫和除錯電腦程式的能力。

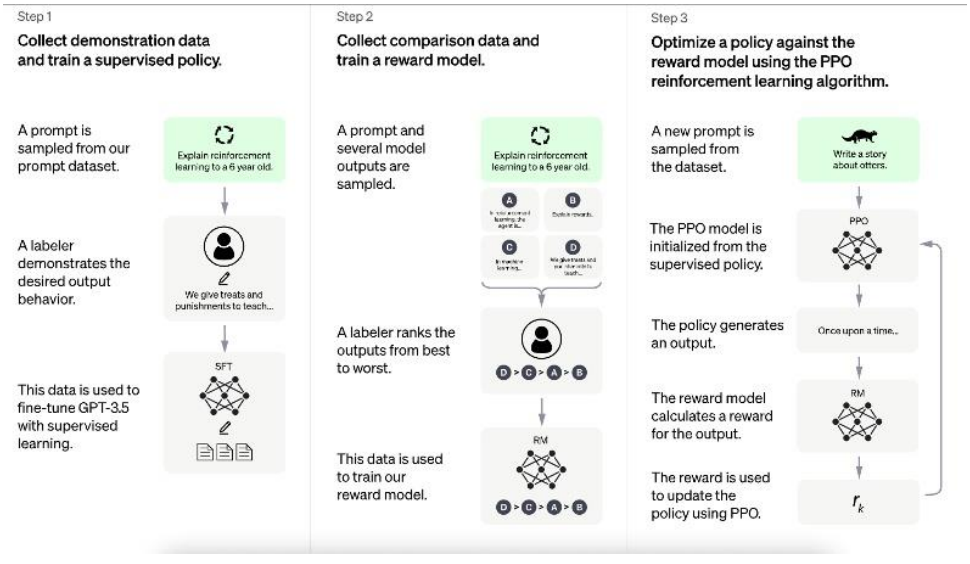

圖 28：ChatGPT 採用深度學習示意圖

課程中 Mark 講師展示如何利用 ChatGPT 設計出一個用 Python 程式語言撰寫的商業網站，並利用 GPT token encoder and decoder 編譯 ChatGPT 所產出的程式。

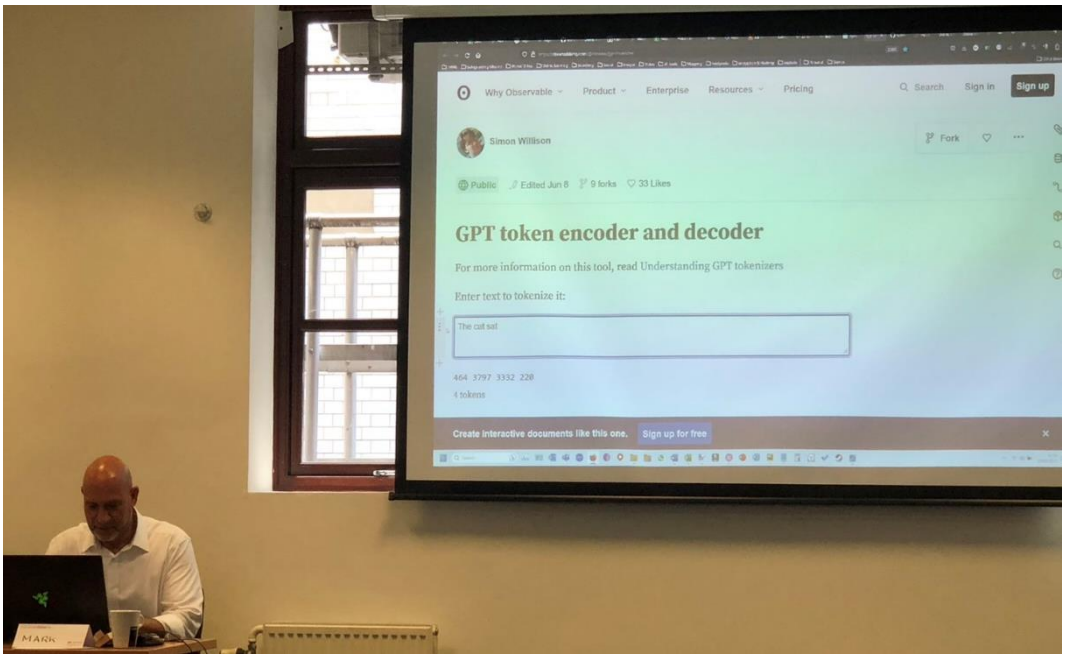

圖 29：ChatGPT 展示

5. Malware

惡意軟體（英語：Malware, malicious software），指通過網路、可攜式儲存裝置等途徑散播的，故意對個人電腦、伺服器、智慧型裝置、電腦網路等造成隱私或機密資料外洩、系統損害、資料丟失等非使用預期故障及資安問題，並且試圖以各種方式阻擋使用者移除它們。

(1) 惡意程式種類

- 病毒

  開機型病毒(Boot Strap Sector Virus)

  藏匿在開機磁區(BootSector)，藉由開機動作觸發，在作業系統還沒被載入之前就先被載入記憶體中，針對 DoS 的各類中斷(Interrupt)得到完全的控制，進行傳染和破壞，造成系統崩潰、資料破壞。

  檔案型病毒(File Infector Virus)

通常寄生在可執行檔(*.com , *.exe 等)，潛伏、特定條件執行，當檔案被執行時，病毒程式跟著被執行，依傳染方式不同區分常駐型與非常駐型，造成文件或資料被破壞、占用效能或儲存空間等。

- 巨集病毒

  利用(office)軟體的巨集功能執行，感染 Word、Excel、PowerPoint、Access 檔案，造成大量寄信(Outlook)、破壞文件資料、跳出對話框。

- 間諜程式(Spyware)

  未經授權安裝在個人電腦，蒐集關於使用者、電腦或瀏覽習慣的資訊，追蹤每一次操作，將結果發送給遠端使用者，也可以從網路上下載其他惡意程式並安裝在電腦上，造成資料洩漏、進行其他後續惡意活動。

- 特洛伊木馬(Trojan Horse)

  不屬於病毒，是看似正常的程式，但會進行惡意的活動，不會自我複製，會在電腦上留後門，讓惡意程式存取系統，竊取機密或個人資訊，造成資訊被蒐集往外送、外部 IP 傳送或接收資訊。

(2) Cyber Kill Chain

- 偵查(Reconnaissance)

  攻擊者蒐集目標對象的資料，如電子郵件信箱、社群平臺的資料，以找到可以下手的弱點，或透過工具，掃描目標對象的網站、系統，得知使用的系統種類、版本。

- 武裝(Weaponization)

  攻擊者使用現成的開源工具或是自行開發專屬的惡意程式。

- 遞送(Delivery)

  攻擊者將攻擊武器送入目標的系統內，例如透過釣魚信件裡的連結、夾帶木馬程式的盜版軟體、隨身碟。

- 漏洞利用(Exploitation)

確保遞送的惡意軟體，藉由目標對象的系統漏洞，得以順利開啟，並使攻擊者獲得控制權。

- 安裝(Installation)

  攻擊者確保自身可以長期控制目標的系統內，以有足夠的時間進行後續環節

- 發令與控制(Command & Control)

  攻擊者潛伏在目標的系統內，蒐集資料，探索環境，以便審慎規劃後續行動。

- 行動(Actions)

  根據攻擊者的最終目標，採取行動，如破壞系統、竊取機密資料、勒索目標對象。

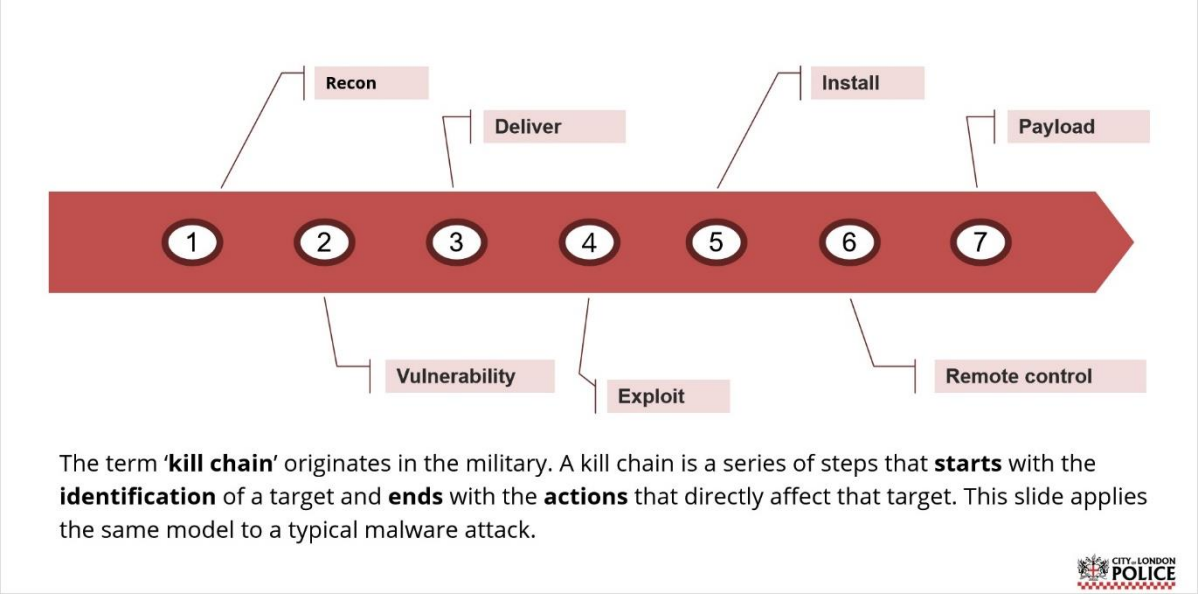

圖 30： Malware「Kill Chain」

肆、心得及建議

一、強化數位情資資料庫，提升辦案效率

本署於 105 年建置智慧分析決策支援系統，並於 106 年上線供各警察機關偵辦刑案使用，利用巨量資料分析串聯人、車、案，取得案件脈絡分析、犯罪手法、通聯習性等情資，但本次參訪英國 JICC 發現跨國犯罪件數日益增加，越來越多的犯罪者擅長利用新興科技犯罪或躲避警察單位追緝，建立犯罪者數位身分與真實身分分析比對已為執法單位刻不容緩的任務，因此可建置數位情資科技偵查平臺，強化數位情資資料庫，提供數位身分比對與辨識、社群互動行為分析、交易圖譜分析，縮短員警辦案需瀏覽以及分析之時間，輔助員警在複雜繁多的資訊中，快速取得重要參考情資，加速辦案進展。

二、加強安全駕駛訓練，增進執勤安全

本次至皮爾中心-亨登警察學院體驗安全駕駛技術課程，該課程內容主要針對員警在駕車追緝嫌犯時之安全駕駛訓練課程，課程為期 3 週，目的在提升員警在高速追捕和逮捕逃犯時的駕駛技巧和安全意識，學員必須通過本課程實際模擬駕車追緝嫌犯測驗後才得以擁有路上駕車執法的資格，未來可仿照英國安全駕駛技術課程，研擬在合適的道路範圍進行安全駕駛技術課程，讓員警實際擁有道路駕駛經驗及具備相關道路安全意識，避免許多第一線剛分發單位員警只具備基本汽車駕照，在駕駛警車於道路上執法時才開始熟悉駕車技巧，發生事故頻傳，往往危及員警或用路人安全，亦可擴大辦理相關安全駕駛課程，讓更多員警藉著參訓機會增進安全駕駛技巧，減少事故發生，提升執勤安全，避免事故傷亡。

三、建置教育訓練平臺，培養科技偵查人才

本次參訪英國有關英國 HOLMES 系統資訊系統訓練，發生重大案件時，警方會成立該案件的專案小組，由偵查人員及資訊人員組成，此時資訊人員負責將專案小組所蒐集的情資，經檢核資料正確性後才輸入至 HOLMES 系統中，HOLMES 系統將歷年來的重大案件相關資訊匯入知識庫，僅提供全國偵辦重大案件使用，因此英國各警察單位會定期實施針對資訊人員之教育訓練，以因應日新月異的犯罪偵查情資。因此面對新興毒品犯罪、不斷演化的新型態詐欺犯罪，可研擬建置數位情資科技偵查教育訓練平臺，在全國各警

察機關開辦科技偵查相關教育訓練後，可將課程教材、試題、問卷等課程資訊匯入該平臺上，讓全國員警可以不受時空場地侷限，在平臺上學習最新的數位情資科技偵查課程，不論是虛擬貨幣追蹤、社群帳號分析、公開網路情資蒐集等，能針對新形態犯罪所使用的技術進行系統化學習，未來能有效運用在科技偵查實務工作上。

四、強化車牌影像辨識系統，提升影像正確辨識率

英國影像辨識系統資料來源龐雜，不只使用一套辨識引擎辨識所擷取之影像，而是同時用三家不同公司所開發的辨識引擎進行影像辨識。現今各縣(市)警察機關犯罪偵查所使用的路口監視器車牌辨識系統皆為各縣(市)自行建置，因此使用之辨識引擎皆出自於不同家公司，不僅未作整合，亦導致辨識結果正確率高低不同，建議未來本署可強化車牌辨識系統所使用之 AI 辨識引擎，將全國各縣(市)警察機關所匯入本署資料庫之路口監視器影像檔案，藉由本署強化的 AI 辨識引擎加以辨識，並解決低光源、高曝光度、高傾斜角度、遮蔽影像 所導致影響辨識正確率的問題，提升各縣(市)警察機關車牌辨識正確率，讓員警遇案需使用車牌辨識系統功能時，能有效掌握目標車輛行蹤，並提高案件偵破率。

伍、參考資料

一、聯合國際犯罪中心

https://www.nationalcrimeagency.gov.uk/news/joint-international-crime-centre-launches

https://www.policeprofessional.com/news/uk-sets-up-new-specialist-unit-to-target-international-crime/

二、倫敦警察學院

https://en.wikipedia.org/wiki/Hendon_Police_College

https://www.london.gov.uk/press-releases-5613

三、倫敦大學皇家哈洛威學院

https://www.royalholloway.ac.uk/

https://www.royaledu.net/index.php?cmsid=625&id=88

https://zh.wikipedia.org/zh-tw/%E5%80%AB%E6%95%A6%E5%A4%A7%E5%AD%B8%E7%9A%87%E5%AE%B6%E9%9C%8D%E6%B4%9B%E5%A8%81%E5%AD%B8%E9%99%A2

四、英國倫敦警察廳

https://www.met.police.uk/

https://zh.wikipedia.org/wiki/%E5%80%AB%E6%95%A6%E8%AD%A6%E5%AF%9F%E5%BB%B3%E6%9E%B6%E6%A7%8B

五、歐洲資訊安全應用展覽會

https://www.infosecurityeurope.com/

六、Hydra Foundation

http://hydrafoundation.org/

https://www.pureav.co.uk/

七、The City of London Police Economic and Cyber Crime Academy

https://academy.cityoflondon.police.uk/

https://academy.cityoflondon.police.uk/demystifying-cybercrime-for-non-technical-audiences/