出國報告（出國類別：進修）

研習 AI 及資料分析技術於科技偵查及犯罪預防之運用

服務機關：內政部警政署
姓名職稱：警務正黃寶慶、偵查佐宋皇毅
派赴國家：荷蘭
出國期間：113 年 11 月 16 日至 113 年 11 月 29 日
報告日期：114 年 2 月 6 日

摘要

鑒於現今科技犯罪日益複雜，延伸各類數位網路犯罪問題，如詐騙、毒品、槍枝和加密貨幣等犯罪，本（113）年度規劃派員赴先進國家參加公開情資資料分析技術之培訓課程，期以輔助員警各項警政勤（業）務執行，本次為期三天之訓練課程主辦單位為荷蘭 Reuser's Information Services 機構，由荷蘭情報專家 Arno Reuser 親自授課，吸引了多國情資專業人士參與，課程內容涵蓋了公開情資資料分析週期、深網與暗網之應用、搜尋引擎策略及布林邏輯查詢等科技偵查技術，並強調如何系統化尋找問題解決方案和驗證公開資料之可靠性，課程中分組研討促進國際交流與技術學習。另本案亦包含參訪荷蘭國家警察的相關科技偵查等單位，以交流、學習先進國家在網路犯罪和人工智慧應用上的資訊技術及經驗，其中荷蘭國家警察以高科技犯罪組為核心，致力於暗網犯罪調查等領域，其成就為國際所矚目，本署參訓人員藉此了解荷蘭警政資訊科技領域整合 AI 技術與開源情報分析運用之情形，並學習或導入本國警政資訊各項系統運用，預期提升本署犯罪情資料分析能量，並作為本署未來建立系統化的犯罪情資分析課程提供參考，以推動國內治安防護與科技偵查實務之進步。

目錄

圖目錄

表目錄

壹、目的

一、計畫目標

鑒於近年詐騙、毒品、槍砲及幫派組織等犯罪猖獗，新興科技犯罪層出不窮、手法日益翻新（例如區塊鏈、加密貨幣或暗網等），執法機關惟有運用各種資料分析技術拼湊破碎資料才有可能快速及有效的將犯嫌繩之以法，本計畫前往荷蘭海牙參加 Reuser's Information Services 訓練機構舉辦之“Open Source Intelligence Training－Pathfinder Program”課程，該課程學習、訓練如何有效率地收集、分析情資，針對不同目標使用之犯罪情資資料進行網路犯罪分析，並透過與國際專業資料分析人士分享交流，以提升資料分析專業技術及整合運用，充實資料分析人員專業能量。

荷蘭國家警察部隊由 10 個地區單位、中央單位（簡稱荷蘭警政署）和警察服務中心組成，荷蘭警政署直屬內政部及荷蘭皇室，掌理全國警察事務並執行全國性及專業性之警察工作，負責蒐集、建檔、管理、分析及整合各種情資，其中荷蘭國家警察所屬之高科技犯罪偵查單位（Team High Tech Crime, THTC），擁有先進專業的技術能力，專門負責偵查網路和科技相關的犯罪，更因打擊暗網犯罪之成功案例而聞名全球。本計畫將前往荷蘭國家警察或相關執法單位，進行犯罪資料分析之技術交流，透過學習先進國家之犯罪情資分析及運用，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

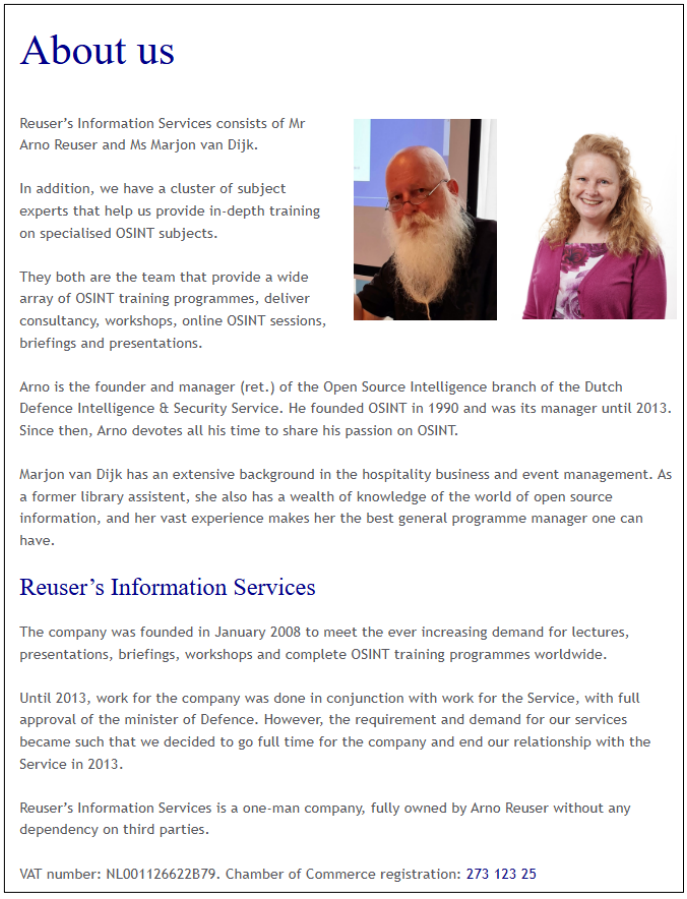
本計畫目的係透過派員參與荷蘭專業情資分析培訓課程，加強培訓本署警政資料分析團隊分析人員資料分析專業能力及資料分析工具運用，以及做為後續規劃及建立我國犯罪情資分析課程之用，並透過與荷蘭執法機關進行犯罪資料分析技術之交流，學習先進國家情資分析模式，以推動科技犯罪偵防，提升治安防護，並借鏡荷蘭國家警察或相關執法單位對於警政 AI 技術之應用情境，作為本署警政 AI 資訊技術之參考。

貳、研習「公開情資資料分析」培訓課程

一、培訓課程及師資介紹

本次派員赴荷蘭參加之培訓課程為由 Reuser's Information Services 訓練機構所舉辦之公開來源情資資料分析課程「Open Source Intelligence Training－Pathfinder Program」，上課地點位於荷蘭海牙，為荷蘭之阿姆斯特丹和鹿特丹之後的第三大城。培訓課程由專業講師 Arno HP Reuser 親自授課，授課講師 Arno 先生自 1990 年即受荷蘭國防情報與安全局（Defense Information System for Security of Netherland, NLDISS）聘請擔任該局培訓教官，從當時網際網路及公開來源情資（Open Source Intelligence, OSINT）未開發的時代建立公開來源情報分析能力。Arno 先生為該國的資訊專業人員，他從網際網路世界的巨量資料中將相關且有用之情資與商業、犯罪及傳統圖書館檢索等資訊結合成為專業的課程內容，並研究遭遇問題時可提供操作的情報方式，這亦是荷蘭軍事

情報和安全局（Militaire Inlichtingen en Veiligheidsdienst, MIVD）邀請 Arno 先生建立該國 OSINT 分析能力之主要原因。講師 Arno 開發了一種系統化、結構化及有計劃的 OSINT 分析方法，用於根據公開來源（開源）的資料尋找可供專業分析人員執行的情報，透過接觸例如 Factiva、Dialog 和 Lexis-Nexis 等國際領先的開源資訊提供者，並掌握這些系統複雜的檢索語言，Arno 先生成功地為問題提供了準確的答案，所以 Arno 先生經常於全球其他情報機構進行分析知識及經驗之培訓，Arno 先生於 2008 年獲得荷蘭政府許可，在 NLDISS 任職期間同時創辦訓練機構「Reuser's Information Services」，投入大量時間從事國際化之 OSINT 研究、寫作、教學、演講、開發課程、培訓計劃、研討會及簡報並提供專業人士諮詢與建議，頻繁與來自政府、國際組織、執法部門、金融部門、私人公司、歐盟、聯合國、北約國際使團或大學等客戶合作，並持續研究網際網路上的資源及 World Wide Web（3W）資源如何與現今的商業資訊提供者做資料勾稽，爰此，本次派員研習之課程報名參加 Reuser's Information Services 機構於 113 年 11 月 26 日至 11 月 28 日舉辦為期 3 日（總時數共計 24 小時）之「Open Source Intelligence Training－Pathfinder Program」專業課程，取得團隊訓練及檢測之認證。



About us

Reuser's Information Services consists of Mr Arno Reuser and Ms Marjon van Dijk.

In addition, we have a cluster of subject experts that help us provide in-depth training on specialised OSINT subjects.

They both are the team that provide a wide array of OSINT training programmes, deliver consultancy, workshops, online OSINT sessions, briefings and presentations.

Arno is the founder and manager (ret.) of the Open Source Intelligence branch of the Dutch Defence Intelligence & Security Service. He founded OSINT in 1990 and was its manager until 2013. Since then, Arno devotes all his time to share his passion on OSINT.

Marjon van Dijk has an extensive background in the hospitality business and event management. As a former library assistent, she also has a wealth of knowledge of the world of open source information, and her vast experience makes her the best general programme manager one can have.

Reuser's Information Services

The company was founded in January 2008 to meet the ever increasing demand for lectures, presentations, briefings, workshops and complete OSINT training programmes worldwide.

Until 2013, work for the company was done in conjunction with work for the Service, with full approval of the minister of Defence. However, the requirement and demand for our services became such that we decided to go full time for the company and end our relationship with the Service in 2013.

Reuser's Information Services is a one-man company, fully owned by Arno Reuser without any dependency on third parties.

VAT number: NL001126622B79. Chamber of Commerce registration: 273 123 25

圖 1、Reuser's Information Services 訓練機構介紹

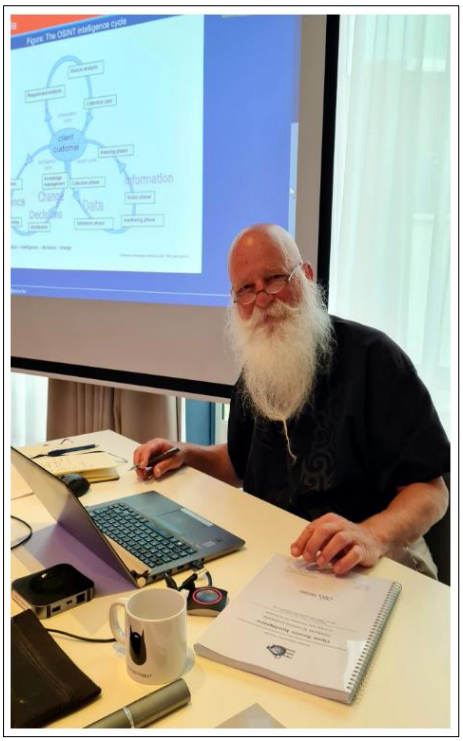


圖 2、本次課程講師 Arno HP Reuser 授課照片

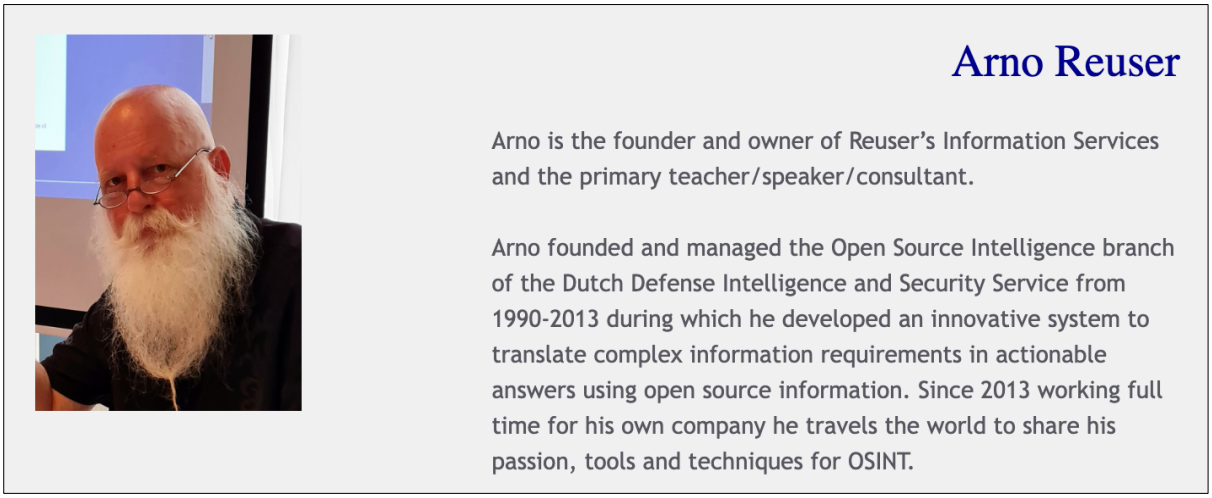


圖 3、本課程講師 Arno HP Reuser 簡介

本（113）年度課程正逢此訓練機構舉辦公開來源情資資料分析課程「Open Source Intelligence Training－Pathfinder Program」的第 50 屆，訓練機構特此盛大舉辦，課程訓練地點於荷蘭海牙的 Bilderberg Hotel 會議廳（Zwolsestraat 22587 VJ Scheveningen, De Haag, Netherlands）舉辦，並於第一天課程晚上舉辦本屆參訓學員及前幾屆學員之學術交流晚宴。本屆參訓的學員共計 14 人，職業涵蓋荷蘭議會資訊人員、丹麥軍方情資分析人員、荷蘭國家銀行的客戶帳戶金流分析人員、英國愛爾蘭學校資訊學科相關教師、私人企業數據分析師、石油公司、荷蘭科技公司資訊科技（Information Technology, IT）人員及與荷蘭警方刑事案件調查合作之顧問公司(Naga Consultancy)主管等，於課程中與國際學員的各階段小組討論、研討時間、實際演練、經驗分享及師生互動，對於荷蘭或其他國家運用公開情資分

析的技術支援及作法有深入的了解，收穫良多，本次研習課程中所做的學習筆記及技術環節，將於本報告下一段內容中詳細說明；另本次課程中的參訓照片，因歐盟嚴格執行一般資料保護規定（General Data Protection Regulation, GDPR），經主辦方及學員要求，如要於任何文件使用，皆須將照片中涉及他人姓名及人臉等個資的地方進行遮蔽處理，以維個資保護。

圖 4、課程環境(一)

圖 5、課程環境(二)

圖 6、課程學員識別證

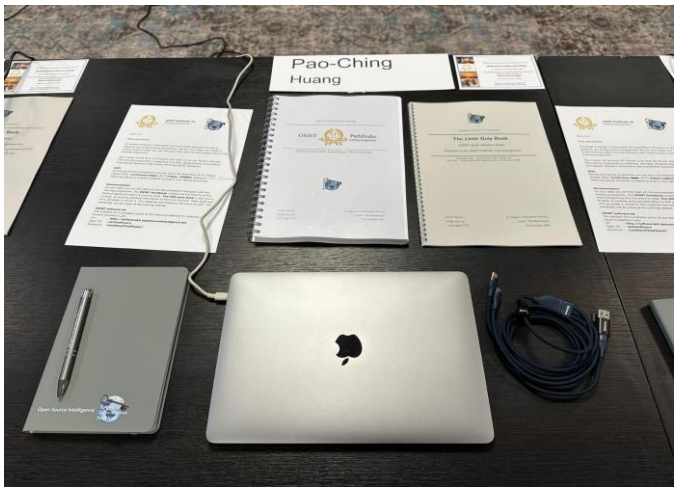


圖 7、課程教材及文件資料

圖 8、課程研討及上課情形(一)

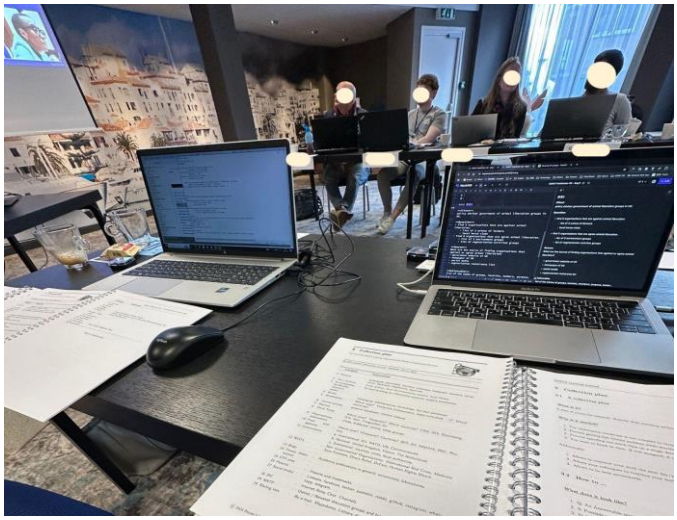


圖 9、課程研討及上課情形(二)

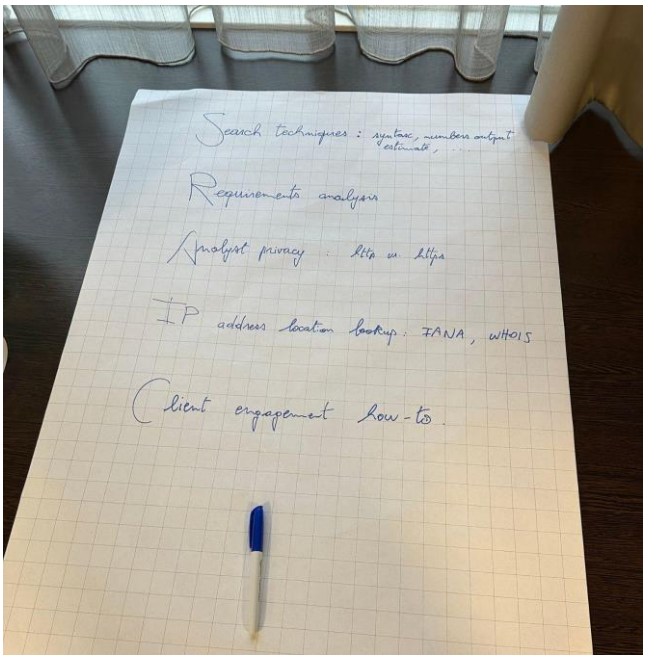


圖 10、分組報告之簡報資料製作

圖 11、與其他參訓學員交流及合影

圖 12、與授課講師 Mr.Arno（創辦人）及該機構總經理 Ms.Marjon 合影

圖 13、本署參訓人員於教室門口合影

圖 14、本署參訓人員通過本課程認證，由講師 Arno 授與證書

圖 15、OSINT 課程訓練合格證書

圖 16、OSINT 課程各屆學員交流晚宴

二、公開情資資料分析課程受訓內容

(一)課程大綱

本次報名參加的情資資料分析課程為 Open Source Intelligence Training 之 Pathfinder 專業課程，課程時間為 113 年 11 月 26 日至 11 月 28 日為期 3 日，每日 9 時至 17 時，共計 24 小時，並需於課程中全程參加實作、分組研討及分組報告，始能通過課程認證並取得該機構所核發之 OSINT Pathfinder 合格證書，本屆相關課程規劃如下：

1.第一天：

(1) 課程開始、OSINT 介紹及課程學習目標：Opening and kick-off of the training programme. Introductions. What is OSINT and what exactly are you going to learn.

(2) OSINT 分析週期：The OSINT Intelligence Cycle.

(3) OSINT 分析週期之系統化、結構化及計畫性的線上研究：OSINT Search Circle for systematic, structured and planned online research.

(4) 網際網路的特徵、使用者、過濾氣泡、趨勢及隱私問題：Internet general characteristics. Who owns the Net, the Filter Bubble, trends, privacy concerns.

(5) 網際網路技術背景及如何運作？網域名稱、IP 位址、whois、ping 及 traceroute 之運用：Internet technical backgrounds. How does it work? Domain names, IP addresses, whois, ping, traceroute.

(6) 需求分析與問題解構、理解研究課題、將模糊問題分解為可回答問題的技術：Requirement analysis and problem deconstruction. Making sense of a research subject. Techniques to break down a vague question into Answerable Questions.

(7) 需求分析（分組練習）：Requirement analysis （exercises）.

*備註：過濾氣泡（英語：filter bubble），又稱為同溫層、個人化資料過濾、篩選小圈圈、資訊繭房、信息繭房（information coccons）等，是一種網站針對個人化搜尋、推薦系統和算法管理篩選後內容的結果所造成的現象。

2.第二天：

(1) 全球 OSINF 格局、開源資料、重複使用之函式庫、文庫資料的附加價值及商業資訊提供商：The global OSINF landscape. Open Sources,Reuser's Repertorium, the added value of libraries, commercial information providers.

(2) 深網，它是什麼、它不是什麼，如何獲得存取權限，並以洋蔥路由器作為深層網路來源的範例：The Deep Web： what is it? What is it not?How to get access. The Onion Router as an example of a deep web source.

(3) 除了網際網路之外，網路上還有什麼：What else is there out there on the Internet that is NOT world wide web? FTP, NNTP, IRC, POP, SMTP.

(4) 蒐集計畫，如何不依賴工具或搜尋引擎，設定研究計畫以獲得控制和結構化資訊：Collection plan; how to setup your research plan to get control and structure without being dependent on tools or search engines.

(5) 搜尋引擎、目錄、單搜尋引擎及元搜尋引擎等，如何找到資料：Search engines. Directories, single search engines, meta search engines, others. The best, the worst, how to find them.

(6) 語義和術語，在資料庫和搜尋引擎中編寫適當的搜尋關鍵字之技術運用：Semantics and terminology. Techniques to compose proper keywords for search in databases and search engines.

3.第三天：

(1) 智慧查詢實現智慧搜尋、建立布林運算查詢邏輯，讓搜尋引擎準確地回答需求：Intelligent queries for intelligent searching. How to construct Boolean queries that will return exactly what you need regardless the search engine.

(2) 布林搜尋運用：陷阱、概念分析及將布林查詢轉換為搜尋引擎指令，並識別錯誤的規則。Boolean searching：pitfalls, traps, concept analysis and how to translate Boolean queries to a search engine. Rules to recognize errors and failures.

(3) 搜尋策略一，透過系統化方法建構搜尋模組，將數百萬次搜尋結果量降低到具有高相關性的數量：Search strategies. Building Blocks for a very systematic approach, Successive Fractions to bring down millions of hits to a normal number with high relevance.

(4) 搜尋策略二，連續的分數將數百萬個結果減少到幾百個，相關性更高：Search Strategies. Successive fractions to bring down millions of results to a few hundred with much higher relevance.

(5) 分組和個人練習時間，將 LOG 技術應用於搜尋策略：Group and individual exercises applying Arno's LOG techniques to the search strategies.

(6) 以驗證方式和驗證技術建立資訊的可靠性和可用性：Validation and validation techniques, things to do to establish reliability and usability of information.

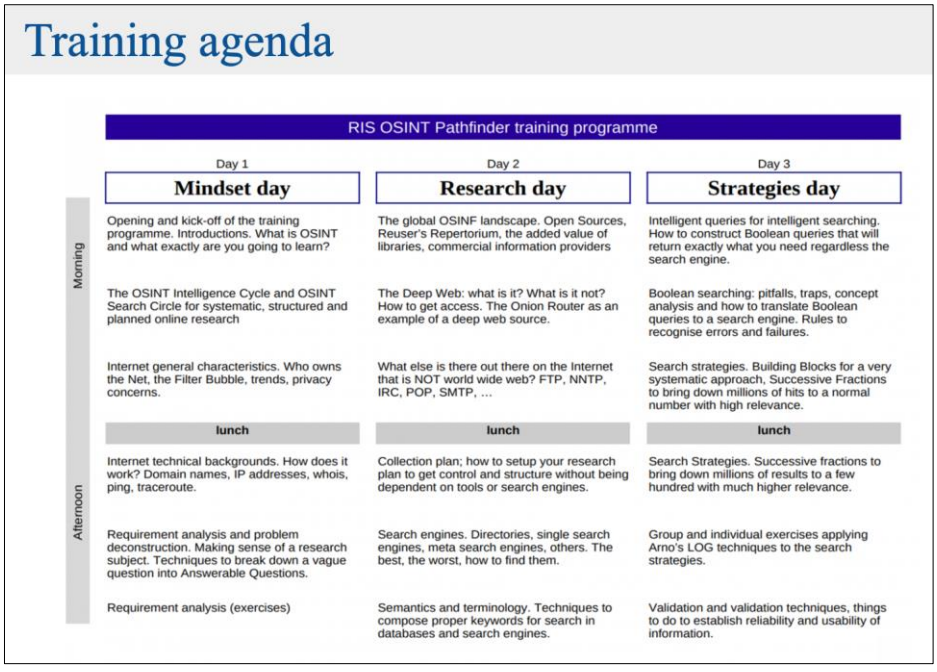


圖 17、本次 OSINT 培訓課程表

(二)課前準備

1.電腦環境建置：

本課程個人電腦所需作業系統環境為 Windows，如為使用 Mac OS 作業系統之學員需先於 APPLE 電腦完成虛擬機（Virtual Machine, VM）建置後安裝 Windows 作業系統，因本署參訓人員皆使用 Mac OS 作業系統，爰分別以 VMware Fusion Pro 及 Parallels 建立所需之主機虛擬環境，並安裝 Windows 11 使用。

2.課程軟體安裝及教材預習：

因本次 OSINT 課程所需之電腦環境及需操作的專業軟體較多，主辦單位課前以電子郵件提供相關軟體、硬體安裝及研讀資料，為使培訓課程供學員做最佳準備，請參訓人員務必於課前進行軟、硬體安裝及預習相關課程內容。經下載主辦方所提供之 ZIP 檔案（OSINT Package）解壓縮後執行目錄 start.exe 檔案及軟體並透過電腦虛擬環境安裝，並於虛擬機佈署 Windows 11 作業系統執行運算；另主辦方亦提供了一些必要的工具，例如將於暗網（Dark Web）使用的 Tor Browser 瀏覽器、XMind Portable 心智圖解決方案軟體等，將於為期 3 日的課程中使用。

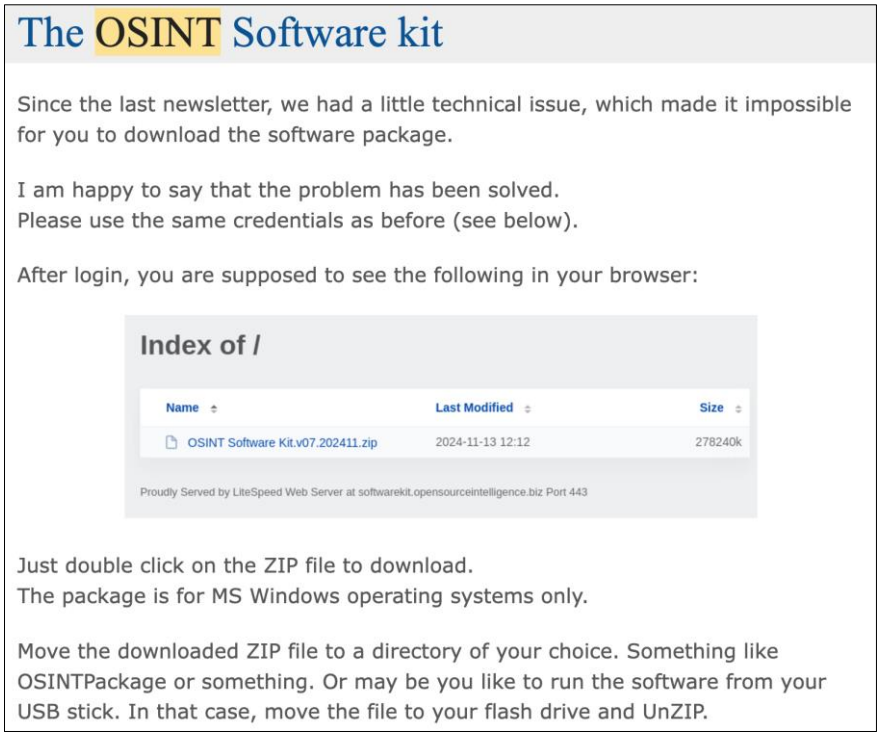


圖 18、課前準備安裝之軟、硬體環境

主辦方式預先提供幾篇有關公開來源情報分析之論文資訊，預先說明開源情報及用途，另提供相關影片供學員事先瀏覽，俾利初步了解本次課程內容：

(1)「The RIS Open Source Intelligence Cycle / Arno H.P. Reuser」（RIS 開源情報週期/Arno HP Reuser）

(2)「Journal of Mediterranean and Balkan Intelligence.- Vol.10, no.2（2017）.-p.29-43」（地中海和巴爾幹情報雜誌。卷 10、第 2 號-2017、p.29-43）：解釋什麼是 OSINT 以及它如何在 OSINT 情報週期中應用。

(3)「Open Source Intelligence：so what? / Arno Reuser」（開源情報：那又怎樣？/Arno Reuser）：在德國亞琛為 P3 Group 進行的關於 OSINT 實踐方面的演講。

(4)「The role of OSINT in intelligence research / Arno Reuser」（OSINT 在情報研究中的作用/Arno Reuser）：在美國德克薩斯厄爾巴索的公立大學之情報安全研討會上的演講。

(5)「OSMOSIS Quick Hits：episode 3 Arno Reuser」（OSMOSIS 快速點擊：第 3 集/Arno Reuser）：我們將在接下來重點介紹 2021 年加州聖地亞哥會議上的一些演講者。本週，我們迎來了 Arno Reuser。Arno 不是典型的 OSINTER。他來自荷蘭，擁有廣泛的研究背景。Arno 開發了一個系統，幫助您確保向客戶提出正確的問題，從而獲得最佳結果。

(6)「Let's talk about Open Source Intelligence（OSINT）- Out of BandInterview on the role of OSINT in cybersecurity」（讓我們來談談開源情報 OSINT，關於 OSINT 在網路安全中的採訪）

(7) 開源情報網站（https：//opensourceintelligence.biz/）

(8) OSINT 資料書（http：//rr.reuser.biz）

(9) OSINT 參考書目（https：//bib.opensourceintelligence.biz/）

(10)培訓計劃（http：//www.reuser.biz）

(三)參訓課程內容

1.第一日

(1) 大綱：搜尋語法技巧、分析隱私權、IP 查找、客戶（問題）目的確認及需求分析，講師 Aron 特別於 Google 搜尋引擎之運算列出以下建議，並提醒在執行公開情資蒐集任務前，務必釐清所需調查的問題及所欲達成的目標：

A. Aron's law one：Check the number of results.

B. Aron's law two：Is there a match between result page and query.

C. Aron's law three：Use parenthesis for every set.

(2) 研習內容：

A. OSINT 定義：

開源情報是一個協作、整合的方法論及產出的過程，透過為客戶提供有價值的情報，來滿足客戶的情報需求，這些情報是透過全面性的研究過程而產生。換言之，OSINT 是指任何合法且符合道德標準的資訊，任何人在任何時間、地點都可以取得這些資訊。OSINT 幾乎包含所有資訊，除了少數限制，例如版權、

許可和智慧財產權。從本質上講，OSINT是所有公開的資料和資訊。講師於課堂中提及，雖然網路是 OSINT 之重要來源，但它不應該被視為唯一的來源，其他亦可包括：

●印刷來源：書籍、報紙、期刊、手冊、參考書籍、目錄。

●電子來源：電視、廣播、網站、網路攝影機。

●線上來源：電子郵件、電話、線上論壇、桌面電腦、物聯網。

●數位來源：社群媒體、資料庫、商業資訊提供者。

B. OSINT 週期：

情報週期包括準備、蒐集、整理、分析、報告，是一個從資料到資訊、情報、決策和變化的過程。在這個過程中最重要的一步也就是「準備」階段，在此階段需要明確、清楚地知道「客戶」的情報需求，必須釐清客戶提出的所有需求，以及客戶所預期的交付成果，避免存在不明確的需求，例如：客戶提出「請給我一份廣為人知的野生動物救援團體清單」，此時我們必須去釐清何謂「廣為人知」的定義?清單內需要有幾筆資料?等問題，透過釐清、明確化客戶的需求後，才能進一步的去識別、評估相關資訊的來源，並制定蒐集所需所有資訊的計畫。

當開始進行資料蒐集時，我們必須先知道「資料」是未經處理的事實和觀察結果，資料需要經過處理和分析才會變成「資訊」，換言之，資訊是經過組織和結構化的資料，提供特定主題的洞察結果。

透過不斷地蒐集、組織、索引、融合、監控、驗證的過程，資訊將會越來越清晰，並經過評估和解釋，變成可作為提供機會、趨勢或潛在威脅的「情報」。最後，透過報告階段，將客戶所需的情報進行反饋，客戶即可根據情報進而作出具策略性、戰術性、行動性的決策並實施變革。OSINT 情報週期是一個強大的框架，用於蒐集、分析、產出來自公開來源的情報，透過遵循 OSINT 週期的每個階段，客戶將可以獲得有價值的洞察情報，以了解各種問題，做出明智的決策，並有效應對新出現的挑戰。

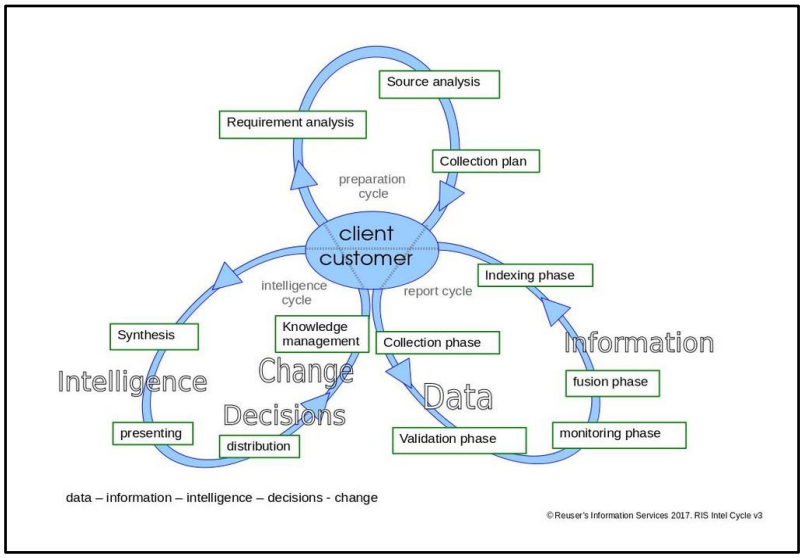


圖 19、OSINT 運作流程（針對 Client 端）

C. 過濾氣泡：

係指搜尋引擎和社群媒體平臺會根據使用者的搜尋歷史、位置和其他個人資料，將搜尋結果個人化的現象。這可能會導致使用者只接觸到與其現有觀點較為相符的資訊，而無法接觸到不同的觀點。搜尋引擎使用複雜的演算法來分析使用者的行為，包括：

- 搜尋歷史。
- 瀏覽歷史。
- 地理位置。
- 社群媒體活動。

根據上述這些資訊，搜尋引擎會調整搜尋結果，以便優先顯示使用者可能感興趣的內容，這可能會導致使用者陷入一個「資訊迴音室（Echo Chamber）」，只接觸到與其現有觀點相符的資訊，過濾氣泡的影響：

- 限制了使用者接觸到不同的觀點。
- 加劇了社會的極化和分裂。
- 讓使用者更容易受到假資訊和宣傳的影響。

過濾氣泡的爭議係有些人認為過濾氣泡並不存在或認為其影響被誇大了。David Graus 博士亦在 2018 年 3 月的「LOGIN IP Lezingen」（VOGIN IP Lecture 是為資訊專業人士舉辦關於搜尋等領域的年度會議）會議上表示：不存在網路過濾氣泡這種東西。那應該如何避免過濾氣泡呢？

- ●使用不同的搜尋引擎：嘗試使用 DuckDuckGo 等不追蹤使用者搜尋歷史的搜尋引擎。
- ●清除搜尋歷史：定期清除搜尋歷史記錄，可以減少過濾氣泡的影響。
- ●主動搜尋不同的觀點：有意識地搜尋與自己觀點不同的資訊，可以幫助打破過濾氣泡。

D. Google 搜尋技巧：

在使用網路搜尋資料前，需要了解以下幾點可能影響搜尋結果的因素：不同的搜尋引擎（例如 Google、Bing）、所使用的地區網域（例如.com、.tw）、語言設定及是否使用 VPN 等，這些因素會影響搜尋結果的排序與內容呈現。

另外可以嘗試使用 google.com/ncr，是 Google 的一個特殊網址，其中 ncr 代表"No Country Redirect"（不進行國家跳轉），當你訪問這個網址時，它會將你定向到 Google 的全球版本，不因你的地理位置而自動跳轉到當地的 Google 網站（例如 google.com.hk、google.com.uk 等）。以Google 瀏覽器為例，以下介紹常用之搜尋技巧（不同瀏覽器搜尋語法會有所不同）：

a.善用搜尋運算符號：

- 「AND」：表示「同時包含」，使用 AND 將搜尋字詞連接起來，表示我們要搜尋同時包含所有這些字詞的文件。例如搜尋「詐騙手法 AND 假投資」將會找到同時包含「詐騙手法」和「假投資」的文件。

  備註：[空白格(space)]視為 AND，爰搜尋「詐騙手法 AND 假投資」等於搜尋「詐騙手法 [空白(space)] 假投資」。

圖 20、課程研習內容實作圖(一)

- 「OR」：表示「至少一個」，使用 OR 將搜尋字詞連接起來，表示我們要搜尋包含至少一個這些字詞的文件，例如搜尋「詐騙手法 OR 空軍」將會找到包含「詐騙手法」或「空軍」或同時包含兩者的文件。

圖 21、課程研習內容實作圖(二)

- 「-」：表示「排除」，使用減號符號「-」排除特定字詞，例如搜尋「警政署 -165」將會找到包含「警政署」但不包含內容有「165」的文件，而如僅搜尋「警政署」則有可能會看到搜尋結果中有「165」之內容。

圖 22、課程研習內容實作圖(三)

圖 24、課程研習內容實作圖(四)

b.使用引號精準匹配：

- 將搜尋字詞放在引號符號「” 」中，表示我們要搜尋完全相同的詞組，例如搜尋「”National Police Agency” 」將會於搜尋結果找到包含「National Police Agency」這個完整詞組的文件，而不是包含這些單字但順序不同的文件。

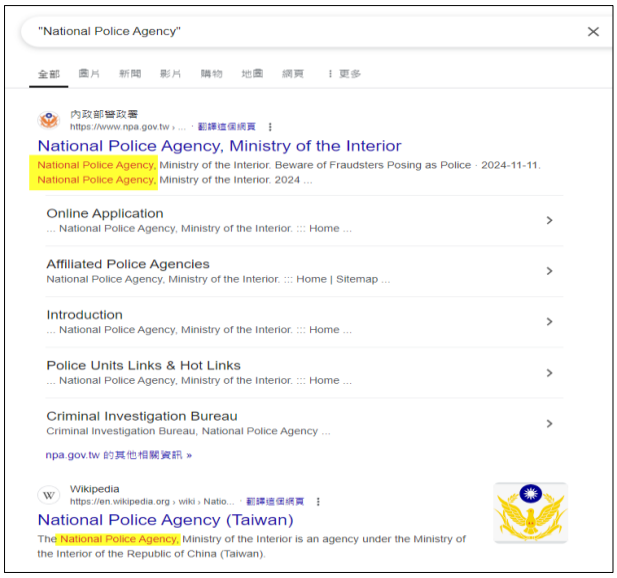


圖 24、課程研習內容實作圖(五)

c.使用星號作為萬用字元：

- 星號符號「*」可以代表任何字元或字元序列，例如搜尋「” 保安警察*總隊” 」將會找到包含「保安警察第一總隊」、「保安警察總隊總隊」、「保安警察單位，總隊」，其中星號位置由任意字詞填充等文件。

圖 25、課程研習內容實作圖(六)

d.使用 site 進行特定網站搜尋：

- 「site」可以用來限制搜尋結果僅顯示來自「特定網站」或「網域」之內容，這對於過濾資訊、進行精確搜尋或研究特定網站內的內容非常有用，例如如果今天要執行「在刑事局官網中搜尋有關科技偵查」的相關內容，即可使用搜尋指令「 “科技偵查” site：cib.npa.gov.tw」進行搜尋，搜尋結果將只會顯示於刑事局網站中有關科技偵查之內容。

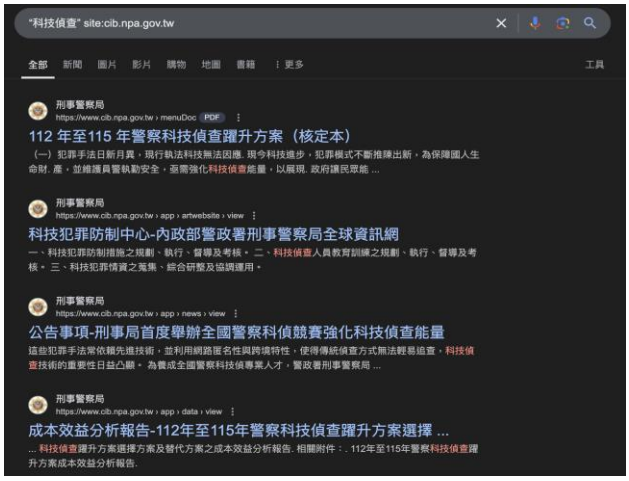


圖 26、課程研習內容實作圖(七)

e.使用 filetype 進行檔案類型搜尋：

- 「filetype」可讓使用者限定搜尋結果為特定類型的檔案，例如 PDF、DOCX、PPT 等，這對於需要查找特定格式文件的人非常實用，例如研究學術文章、下載簡報或尋找專業文件等情境。

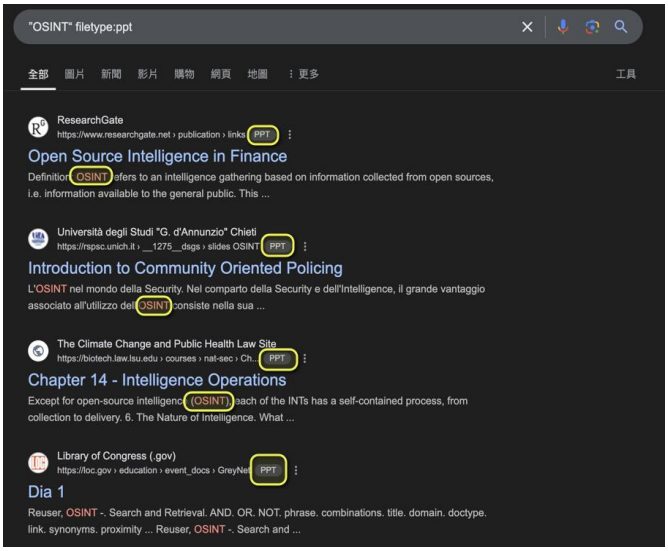


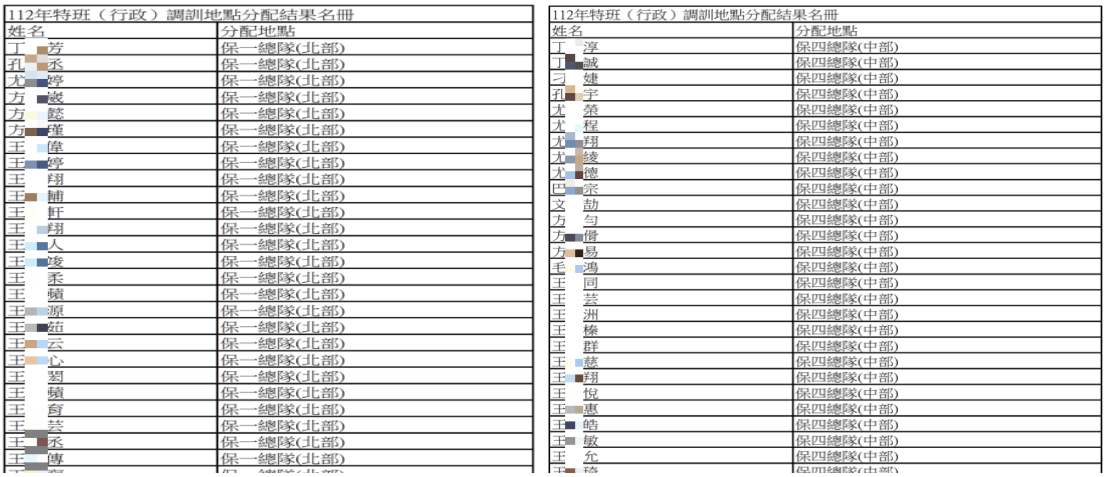
圖 27、課程研習內容實作圖(八)

f.實際運用

- 假設我們想知道 112 年特班人員相關資訊，在已知事實中，我們知道關於四等特考班的受訓事宜“可能”是由警專、保一、保四或保五總隊負責代訓，先以警專為標的，在警專行政單位中為教務處所負責的可能性最大，所以我們的目標是「在警專教務處網站中搜尋有關特考班相關 PDF 文件檔案」，即可使用以下搜尋語法「“112 年特班” site：educate.tpa.edu.tw filetype：pdf」，搜尋結果將會顯示在警專教務處網站中與 112 年特班有關的 PDF 檔案。

圖 28、課程研習內容實作圖(九)

- 搜尋結果我們得到兩份 112 年特考班人員調訓地點名冊（名冊中因含姓名個資已遮蔽處理）。



112年特班（行政）調訓地點分配結果名冊

姓名	分配地點
丁[redacted]芳	保一總隊(北部)
孔[redacted]丞	保一總隊(北部)
尤[redacted]婷	保一總隊(北部)
方[redacted]崴	保一總隊(北部)
方[redacted]懿	保一總隊(北部)
方[redacted]瑾	保一總隊(北部)
王[redacted]偉	保一總隊(北部)
王[redacted]婷	保一總隊(北部)
王[redacted]翊	保一總隊(北部)
王[redacted]博	保一總隊(北部)
王[redacted]軒	保一總隊(北部)
王[redacted]翊	保一總隊(北部)
王[redacted]人	保一總隊(北部)
王[redacted]俊	保一總隊(北部)
王[redacted]柔	保一總隊(北部)
王[redacted]頡	保一總隊(北部)
王[redacted]源	保一總隊(北部)
王[redacted]茹	保一總隊(北部)
王[redacted]云	保一總隊(北部)
王[redacted]心	保一總隊(北部)
王[redacted]潔	保一總隊(北部)
王[redacted]頡	保一總隊(北部)
王[redacted]育	保一總隊(北部)
王[redacted]芸	保一總隊(北部)
王[redacted]柔	保一總隊(北部)
王[redacted]博	保一總隊(北部)

112年特班（行政）調訓地點分配結果名冊

姓名	分配地點
丁[redacted]淳	保四總隊(中部)
丁[redacted]誠	保四總隊(中部)
弓[redacted]婕	保四總隊(中部)
孔[redacted]宇	保四總隊(中部)
尤[redacted]榮	保四總隊(中部)
尤[redacted]程	保四總隊(中部)
尤[redacted]翔	保四總隊(中部)
尤[redacted]綾	保四總隊(中部)
尤[redacted]德	保四總隊(中部)
巴[redacted]宗	保四總隊(中部)
文[redacted]勛	保四總隊(中部)
方[redacted]勻	保四總隊(中部)
方[redacted]儒	保四總隊(中部)
方[redacted]易	保四總隊(中部)
毛[redacted]鴻	保四總隊(中部)
王[redacted]同	保四總隊(中部)
王[redacted]芸	保四總隊(中部)
王[redacted]洲	保四總隊(中部)
王[redacted]榛	保四總隊(中部)
王[redacted]群	保四總隊(中部)
王[redacted]慈	保四總隊(中部)
王[redacted]翔	保四總隊(中部)
王[redacted]悅	保四總隊(中部)
王[redacted]惠	保四總隊(中部)
王[redacted]皓	保四總隊(中部)
王[redacted]敏	保四總隊(中部)
王[redacted]允	保四總隊(中部)

圖 29、課程研習內容實作圖(十)

E. 需求分析與問題解構：

本項的重點為理解所需情報主題並將模糊問題分解成可回答的問題。在進行開源情報（OSINT）研究時，需求分析和問題解構是至關重要的步驟。這些步驟能幫助研究人員釐清客戶的需求，並將模糊、籠統的問題轉化為可回答的具體問題，以確保研究的效率和準確性。

a. 理解研究主題

- 主題的背景和範圍：確定研究的具體領域，並了解其相關的歷史、現狀和發展趨勢。
- 客戶的具體需求和目標：確定客戶希望透過研究獲得哪些資訊，以及這些資訊將如何被使用。
- 可用的資料來源和資訊類型：評估可用的公開來源，例如新聞報導、社交媒體、學術期刊、政府文件等，並確定哪些來源最有可能提供所需資訊。
- 時間限制和資源分配：確定完成研究的時間限制，並分配必要的資源，例如人員、資金和工具。

b. 問題解構技巧

當客戶需求模糊不清時，可以使用以下技巧將其分解成可回答的具體問題：

- 問題細分：將一個大的、模糊的問題分解成多個較小、更具體的子問題，逐步縮小研究範圍，例如可將「分析中輟生比例與失蹤人口關係」這個模糊問題細分為「哪些年齡段的中輟生被通報失蹤人口數量最高？」、「中輟生失蹤的原因有哪些？」、「中輟生的失蹤與犯罪集團招募等問題是否存在關聯？」、「中輟生涉及犯罪之人數？」、「中輟生涉及犯罪之

類型？」、「中輟生的性別是否會影響其失蹤的可能性？」等子問題。

- 識別假設：明確研究過程中所做的假設，並檢驗這些假設的合理性。例如「假設中輟生失蹤與其缺乏社會支持和家庭關懷有關」，研究人員需要檢驗這個假設是否成立，並尋找支持或反駁它的證據。
- 重新定義模糊詞彙：將模糊的詞彙或概念重新定義為更精確、可量化的指標。例如：
  - 「中輟生定義」：依據國民小學與國民中學未入學或中途輟學學生通報及復學輔導辦法第二條規定：「中途輟學學生（以下簡稱中輟生）：指國民小學及國民中學學生有下列情形之一者：（一）未經請假、請假未獲准或不明原因未到校上課連續達三日以上。（二）轉學生因不明原因，自轉出之日起三日內未向轉入學校完成報到手續。」，由此可知中輟生的年齡區段位於 6 歲至 15 歲。
  - 「失蹤人口定義」：依據失蹤人口查尋作業要點第二點規定：「本要點查尋之失蹤人口，指在臺設有戶籍，並有下列情形之一且行方不明者：（一）隨父（母）或親屬離家。（二）離家出走。（三）意外災難（例如海、空、山等災難）。（四）迷途走失。（五）上下學未歸。（六）智能障礙走失。（七）精神疾病走失。（八）失智症走失。（九）天然災難（例如水、火、風、震等災難）。（十）其他原因失蹤。」，由此可知，在分析中輟生與失蹤人口關係時，可針對 10 項失蹤原因進行更進一步的分析。
- 設定限制條件：為研究問題設定時間、地域、資料來源等限制條件，以提高研究的針對性和可行性。
  - 時間限制：例如分析過去五年或十年內的中輟生失蹤數據。
  - 地域限制：例如針對特定直轄市、縣市、離島區域進行分析。
  - 資料來源限制：例如使用官方統計數據、新聞報導、學術研究等特定資料來源。

c. 將模糊問題轉化為可回答的問題

透過上述技巧，可將模糊問題轉化為下列可回答之問題類型：

- 封閉式問題：可以透過明確的答案來回答的問題（例如「是」或「否」）。

- 開放式問題：需要提供更詳細、解釋性答案的問題。
- 量化問題：可以用數值或統計數據來回答的問題。
- 比較問題：比較兩個或多個對象之間的差異或相似性的問題。

d. 範例說明

以下是一些將模糊問題轉化為可回答問題的範例：

模糊問題：員警非因公務查詢案件數量是否正在增加？
可回答的問題：

- 在特定時間範圍內（例如過去 5 年），[某警察機關]員警使用警政資訊系統非因公務查詢案件的數量是否有增加？
  - 透過設定時間範圍及警察機關，具體化了模糊問題。
- 與[基準年]相比，[特定年份][某警察機關]的員警非因公務查詢而受到處分的案件數量是多少？
  - 透過設定「比較基準」和「具體指標」，這個問題將模糊問題轉化為可量化問題。
- 哪些因素導致[某警察機關]的員警冒險進行非因公務查詢資訊系統？
  - 探討了造成非因公務查詢情形的潛在原因、動機、誘惑，以引導更深入的調查。
- 各警察機關執行非因公務查詢系統之稽核方式及查處作為相比，是否影響非因公務查詢案件之數量？
  - 透過比較不同機關的稽核方式及查處作為，探討了與非因公務查詢案件發生數量的關係，找出可能可降低員警非因公務查詢的解決方案。

透過以上範例，可觀察到下列技巧被運用於將模糊問題轉化為可回答問題：

- 設定明確的時間範圍及標的：避免「正在增加」此模糊的時間概念，並指明具體的警察機關為何。
- 定義關鍵詞：闡明「非因公務查詢」的定義，例如使用警政資訊系統查詢與偵辦案件無關之資訊。
- 使用可量化的指標：例如查詢次數、處分案件數量等，以利於資料追蹤和比較。
- 探究原因和影響：分析造成非因公務查詢的因素，以及這些查詢可能帶來的後果。
- 比較分析：將各警察機關之稽核方式及查處作為進行比較，以評估問題的嚴重性和尋找解決方案。

2.第二日

(1) 大綱：針對OSINT策略擬定、深網（Deep Web）、暗網（Dark Web）、全球各種公開來源情資網站搜查技巧、Tor Browser於暗網之資料分析、ChatGPT情資分析運用、分組研討及報告。

(2) 研習內容：

A. 深網（Deep Web）

深網係指於網際網路中無法被標準的搜尋引擎索引到的部分，換句話說，深網是搜尋引擎「看不到」的網際網路部分。這與我們日常使用的「表面明網」不同，表面明網的內容可以被Google、Bing等搜尋引擎輕鬆搜尋到。深網包含了各式各樣的資訊，通常需要特殊的權限才能存取，因此裡面的資訊不會被公開索引，例如私人資料庫、學術研究、政府文件、企業內部網路、醫療紀錄或金融交易紀錄。

B. 暗網（Dark Web）

暗網常被誤解為一個充滿犯罪活動的隱藏網路世界，雖然暗網確實有一部分被用於非法、犯罪等活動，但它同時也具有合法用途，例如保護隱私和言論自由。暗網本質上亦是網際網路的一部分，但其內容無法被標準搜尋引擎索引，這意味著使用者無法透過 Google 或 Bing 等一般使用者所使用的搜尋引擎找到暗網上的資料。但暗網並非均無法存取，只是其資料內容未被索引，爰使用者需要透過特殊的軟體和技術，例如 Tor 瀏覽器才能進入暗網，其資料規模遠超過我們日常使用的表面明網。據估計，暗網的內容可能比表面明網多出數百倍甚至數千倍。此外，暗網也具有合法用途，例如一些受到政府審查的言論可以在暗網上找到表達的空間，另有部分注重隱私的個人和企業組織則利用暗網來保護其資訊安全。

暗網的使用及存取存在一定的風險，唯有深入了解其特性，可幫助我們在OSINT過程中更安全的使用這個資源：

- 安全風險：暗網上存在許多惡意軟體和網路釣魚網站，使用者需要小心謹慎，避免受到攻擊。
- 法律風險：暗網上的一些活動可能涉及非法、犯罪等行為，使用者需要了解相關法律規範，避免觸犯法律。
- 道德風險：暗網上的一些內容可能具有攻擊性或有害性，使用者需要保持批判性思維，避免受到負面影響。

C. OSINT策略擬定

沒有做好計畫，就是計劃要失敗（Failing to plan is planning to fail）。因此我們在進行OSINT過程前，最重要的事情就是「策略擬定」，資訊環境太複雜，如果沒有計畫就無法開始進行調查，包含前面所說的，需要充分理解客戶需求、期待且可交付項目，這都攸關 OSINT 的策略擬定，好的策略可以防止你在蒐集資料的過程中迷路，也可以避免在單一細節上花費太多的時間，如果策略擬定得當，它會告訴你何時應該停止搜尋。此外，完整的計畫可以讓你在搜尋工作暫停後，在對

的地方繼續開始，也能將工作分配給其他人繼續執行。蒐集計畫主要有三個核心項目：

- Q (Question)：一個可回答的問題。
- S (Source)：可能的資料來源。
- D (Deliver)：所需交付的成果。

我們在制定 OSINT 蒐集計畫時也應該考慮下列各項因素，舉例如下：

- 客戶的是對什麼感興趣?
- 這是真正的問題嗎?
- 主題是否明確?
- 問題是否完整?
- 問題是否存在謬誤?
- 有什麼前提假設?
- 定義不明確的字句?
- 這些資訊將用於什麼目的?
- 客戶的職業、專長、背景?
- 所需答案的專業水平?
- 需要多少資訊?
- 所需要的時間範圍?
- 所需要的資訊類型?
- 有何限制?

表 1、本次課程進行 OSINT 策略擬定之實作範例

<table>
<tr><th>類別</th><th colspan="2">範例</th></tr>
<tr><td rowspan="3">報紙</td><td>Q
(Question)</td><td>建立一份 2022 年至 2023 年間，關於英格蘭和威爾斯之動物解放組織之暴力行為的 15 篇報導清單。</td></tr>
<tr><td>S
(Source)</td><td>《 Guardian 》 《 Times 》《Financial Times》《Sunday Telegraph》《Independent》</td></tr>
<tr><td>D
(Deliver)</td><td>標題、作者、報紙、出版日期、URL、全文</td></tr>
<tr><td>所屬機構資料庫</td><td colspan="2" rowspan="5">執行
Q、S、D</td></tr>
<tr><td>圖書</td></tr>
<tr><td>期刊</td></tr>
<tr><td>智庫</td></tr>
<tr><td>組織、協會</td></tr>
</table>

項目
非政府組織
社群媒體
地圖
照片
影片
遊戲論壇
Podcasts

D. 全球各地公開來源情資網站的搜尋技巧

關鍵在於制定完善的搜尋策略，並熟悉各種搜尋引擎和資料庫特性，課程講師於課程上分享一些實用技巧，分述如下：

a. 精準定義問題：

- 在開始搜尋前，花時間釐清你的目標和所需要的資訊。
- 避免使用模糊的詞彙，盡可能具體的關鍵詞和日期範圍。
- 確定所需要的資訊類型，例如新聞文章、學術論文、社交媒體貼文、公司報告等。

b. 善用多樣化的搜尋引擎

不要只仰賴 Google，請多嘗試使用其他搜尋引擎，例如：

- DuckDuckGo（注重隱私，減少垃圾廣告）
- Shodan（能檢測連接到網際網路的各種設備，並顯示其 IP 地址、地理位置、開放埠、所使用的軟體版本等）
- Bing
- Baidu

c. 尋找專業資料庫

許多專業資料庫提供特定領域的深入資訊(料)，不過通常需要付費訂閱始能使用，例如：

- Lexis-Nexis（法律法規、稅務及商業資訊服務提供商）
- ProQuest Dialog（國際最大的情報檢索系統）
- Factiva（商業、金融及新聞資訊）

d. 活用進階搜尋技巧

善用搜尋引擎提供的進階搜尋功能，這些功能可以幫助我們更精準地找到所需的資訊，並減少無關結果的干擾，例如：

- 限定語言、地區、時間範圍。
- 依檔案類型、網站、作者篩選。

- 使用特定語法，例如「site：」、「filetype：」或「intitle：」等。

e. 驗證資訊來源

- 務必仔細檢查資訊來源的可靠性和可信度，特別是在網路上所蒐集的資料。
- 參考多個來源，比較不同觀點，避免陷入資訊繭房或認知偏差。
- 注意資訊發佈的時間，確保資訊的時效性。
- 使用事實查核工具或網站，驗證資訊的真實性。

f. 持續學習與精進

OSINT 是一個不斷發展的領域，新的工具和技巧不斷推陳出新，提供一些建議如下：

- 積極參與相關社群，例如 OSINT 研討會、線上論壇、社交媒體群組等，與其他專業人士交流學習。
- 閱讀相關書籍、文章或報告，以掌握最新的趨勢和發展。

綜上，老師於課程中給予鼓勵：成功的 OSINT 調查需要結合技巧、策略和批判性思維，唯有透過不斷的學習和精進，我們才能夠更有效率的從全球這麼龐大的公開來源情資網站、資源(料)中獲取有價值的情報。

3.第三日

(1) 大綱：總結 OSINT 過程、分組研討及報告、結業式。

(2) 研習內容：

A. OSINT Process 心智圖

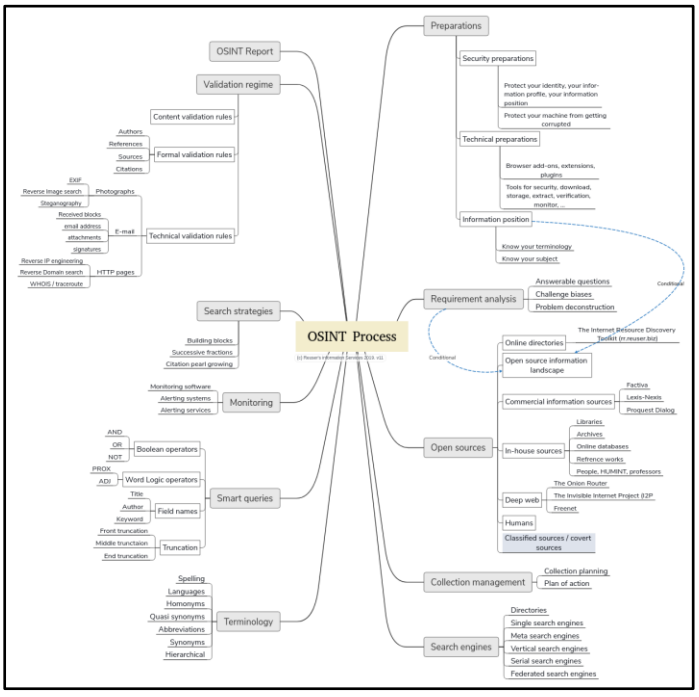


圖 30、OSINT Process 心智圖

a. 準備階段（Preparations）
   - 安全準備（Security preparations）
     - 保護自身身份、個人資訊及位置。
     - 防止所用設備遭到入侵、破壞。
   - 技術準備（Technical preparations）
     - 瀏覽器運用各種插件功能。
     - 使用虛擬機(VM)建立安全的 OSINT 調查環境。
   - 資訊定位（Information position）
     - 了解調查主題。
     - 了解主題所涉及的相關術語。

b. 需求分析（Requirement analysis）
   - 可回答的問題。
   - 避免資訊偏見。
   - 進行問題解構。

c. 公開資源（Open sources）
   - 印刷來源：書籍、報紙、期刊、手冊、參考書籍及目錄。
   - 電子來源：電視、廣播、網站、網路攝影機。
   - 線上來源：電子郵件、電話、線上論壇、桌面電腦、物聯網。
   - 數位來源：社群媒體、資料庫、商業資訊提供者。
   - 商業來源：Factiva,Lexis-Nexis,Proquest Dialog。
   - 深網。
   - 暗網。
   - 專家人員。

d. 蒐集管理（Collection management）
   - 蒐集計劃

e. 搜索引擎（Search engines）
   - Google
   - Bing
   - 百度
   - DuckDuckGo

f. 智能查詢（Smart queries）
   - 使用布林運算符(Boolean algebra)
     - AND
     - OR
     - NOT
   - 字詞邏輯運算符
     - site

        - filetype
        - intitle
        - inurl
        - intext
    - 術語
        - 拼寫
        - 語言
        - 同義詞
        - 近似詞
        - 縮寫

g. 驗證規範（Validation regime）
    - 內容驗證
        - 作者、參考資料、來源、引用。
    - 技術驗證
        - EXIF、圖像搜索。
        - 電子郵件地址。
        - WHOIS、Traceroute。

h. OSINT 報告
    - 產製及運用。

參、參訪過程

荷蘭警察機關簡要概述：荷蘭國家警察總隊（荷蘭語：Korps Nationale Politie），另稱荷蘭國家警察或國家警察部隊，荷蘭警察機關分為十個地區單位、兩個國家單位、警察學院、警察服務中心和國家調度合作中心，這些機構的執法目的是調查涉嫌犯罪活動、將調查結果提交法院以及在司法行動期間暫時拘留涉嫌犯罪分子，不同層級的政府和不同機構的執法機構也普遍擔負著威懾犯罪活動和防止犯罪成功實施的責任。下圖為荷蘭國家警察徽章，所有穿警察制服的員警都需戴著國家警察徽章標誌，其中標誌中的菱形代表法律之書、帶有火焰的手榴彈代表警惕。

圖 31、荷蘭國家警察徽章

一、地區及中央警察機關

(一)烏特勒支無人智慧警局

荷蘭的烏特勒支（Utrecht）是荷蘭第四大城市，為烏特勒支省省會及人口最多的城市，包含周圍的宰斯特、尼沃海恩、菲亞嫩等城鎮，總人口達 45 萬 7,746 人。本次參訪行程第一站為該國從 2024 年 9 月開始運作的「荷蘭第一間沒有警察的警察局」，該國又稱「智慧警局」，走出烏特勒支中央車站（Utrecht Centraal）位於 Hoog Caterijne 入口左側，即可看見座落於連棟建築之其中一間，開放時間為週一至週三上午 8 點至晚上 8 點、週四和週五上午 8 點至晚上 10 點、週六上午 9 點至晚上 10 點及週日上午 9 點至晚上 7 點。

圖 32、無人智慧警局外觀

本次參訪由荷蘭警政單位 2 名人員的引導及介紹，讓我們深入了解這個智慧警局的運作機制及操作，並向我們說明了原本會有警員在值班臺的傳統警察局與這間無人智慧警局的差異，經詳細說明，民眾如有報案需要或問題詢問，可用位於建築內左側具備隔音的私人空間內的機器與智慧化虛擬警員進行對話，或選擇更進一步的視訊或語音通話，操作時十分顧及個人案件之隱私，藉由把案件情況描述給員警知道，如此一來，民眾不需要預約，即可進行警政資料的詢問、檢舉、報案（例如失竊、傷害等）；另外，如果發生嚴重事件，按下房間內另外一個通話鈕亦可與該地區的真正執勤警察進行遠端視訊通話，由警察判斷如何進一步協助；惟如涉及重大案件，該國警政人員表示，仍需循真正員警的報案管道較為妥適，避免影響個人的權益。

除了於無人智慧警局提供室內休息區可供民眾暫時休息之外，這個無人智慧警局內另建置有互動電子看板設備，可以由該資訊系統設備提

供警政資訊、警政互動小遊戲及填寫電子建議表單等功能，拉近警察與民眾距離，亦讓警局（派出所）不再只是單純報案的地方。

圖 33、可與智慧化虛擬警員進行對話且具備隔音及隱私的報案空間

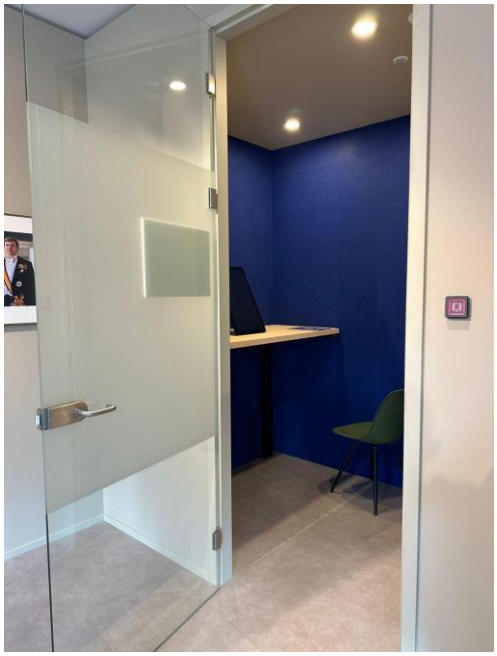


圖 34、智慧化報案空間一隅

圖 35、無人智慧警察局民眾休息區一隅

圖 36、模擬操作智慧設備

圖 37、模擬操作報案資訊系統

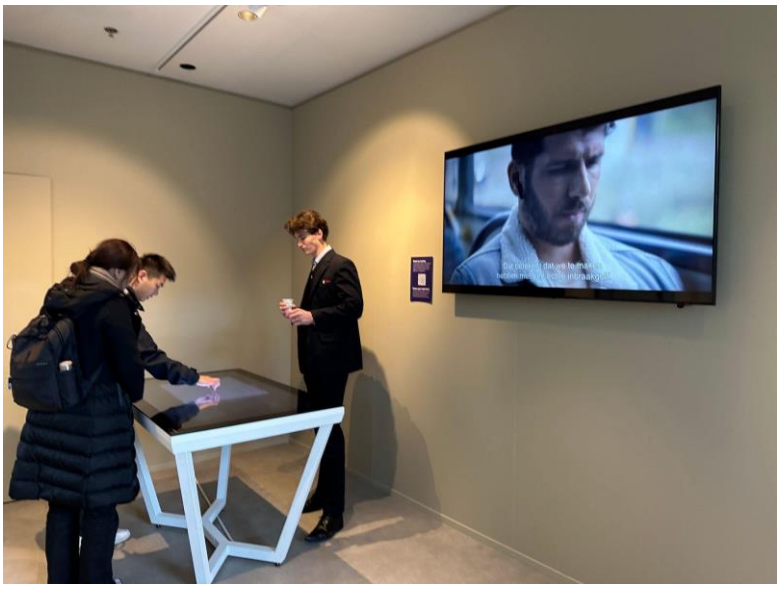


圖 38、該局人員向我們介紹警政互動資訊系統設備

圖 39、實際操作該局警政互動資訊系統設備

圖 40、該局人員向我們說明智慧警局其他業務

圖 41、致贈本國禮品予該國人員

圖 42、致贈本國禮品予該國人員

(二)荷蘭烏特勒支（Utrecht）警察局

烏特勒支是荷蘭的重要城市之一，也是該國交通和文化的重要樞紐，荷蘭國家警察分為 10 個地區，統稱「荷蘭國家警察（Nederlandse Politie）體系」，每個地區再細分為數量不等的地方警局，本次參觀的烏特勒支警局（Utrecht Police Office Paardenveld）即是荷蘭國家警察的區域分部之一、烏特勒支省的地方執法機構之一，烏特勒支警局負責的範圍包括烏特勒支市以及周邊的城鎮和村莊，其地理位置附近有烏特勒支中央車站（Utrecht Centraal），交通便利，位於荷蘭烏特勒支市中心、Paardenveld 公園旁，是一座結合現代化設計及社區公共服務功能的建築，也是烏特勒支城市警政業務運作的核心之一，經分享本國警政運作狀況，並向該局人員請教該局的警政相關作為及科技偵查執行的狀況，使得本次行程更加瞭解烏特勒支的警政運作及治安狀況，惟因該局人員嚴格執行該局辦公區域不得拍照的規定，無法取得相關細節照片或合照呈現於本報告中。該局周邊有許多商業區和公共設施，因此該局在維護城市秩序和公共安全方面發揮了至關重要的作用，相關內容分別描述如下：

1.該局建築物的架構雖然看似低調卻也維持半開放式的設計，並提供大廳開放環境予民眾可以與警政人員接觸之接待區，建築內部設有多功能辦公區域、會議室、拘留設施等，滿足警察業務工作的需要。

2.該局負責烏特勒支市中心及周邊區域的治安、巡邏和犯罪預防等警察工作，執勤重點涵蓋：

(1)社區警務：與轄區民眾、企業及其他政府部門建立溝通聯繫，以利預防性措施施行、降低犯罪率。

(2)交通管理：該局位於該地區的交通樞紐，行經車輛眾多，爰處理交通事故、疏導交通等工作十分重要。

(3)緊急勤務：該局為烏特勒支市區的主要警察局之一，經常處理各類緊急事件，包括暴力犯罪、公共安全、自然災害問題等案件。

(4)社區參與：該局近期強調與當地社區的互動，除了設置民眾服務中心，為民眾提供法律諮詢、報案服務和其他警政服務項目，並定期舉辦交通安全講座和社區座談等，增強民眾對犯罪預防工作的支持，並針對特定社會問題（例如青少年犯罪或毒品濫用）提供解決方案。

3.該局的運作也結合了荷蘭國家警察體系下所運用的警察科技技術，如數位化辦公系統（例如視訊互動等）、監控設備（門禁）以及行動應用程式，用於提高警察人員工作效率；另該局於犯罪執法方面亦利用科技偵查提升執法效率，以應付日益複雜的公共安全挑戰：

(1)科技偵查相關技術運作：該局在偵查工作中，運用人工智慧、數據分析和物聯網技術，以執行犯罪預防和偵查，分述如下：

(2)數據分析：該局使用地理資訊系統（Geographic Information System, GIS），讓執勤警察可更有效地安排巡邏路線，並針對高風險區域進行快速及精準之部署；另以犯罪資料庫進行犯罪熱點分析，透過過去的案件資料和地理資訊，建立犯罪風險地圖。

(3)監控影像：惟閉路電視監控系統（Closed-Circuit Television, CCTV），因該局需考量歐盟嚴格的一般資料保護規定（General Data Protection Regulation, GDPR），在市區監控攝影機的運用有諸多的限制（尤其人臉辨識技術），部分結合人工智慧（AI）分析軟體，進行異常行為檢測，例如肢體衝突、車輛違規停放或可疑行為模式等。

(4)使用物聯網（Internet of Things, IoT）設備：透過建置於市區內個基礎設施上的物聯網感測器，該局能即時監測城市中的重要基礎設施，例如橋樑、車站和商業中心，並對異常情況（如可疑包裹或突發事故）做出快速反應。

(5)數位化偵查工作流程：該局藉由將部分工作轉以數位化工作流程，提升偵查工作效能：

A.案件管理系統：使用中央化的系統平臺記錄各類案件資訊，所有數據依照系統權限可以共享，以利不同部門間協作。

B.行動設備應用：警員隨身可使用之行動設備，內建犯罪數據庫和即時通訊功能，以利現場執法和資料調閱。

C.數位證據蒐集：導入數位取證工具，可用於蒐集並分析犯罪現場取得的手機、電腦或其他數位設備的證據，尤其運用在網路犯罪偵查。

4.網路犯罪偵查：隨著網路犯罪案件的增加，該局亦設置了處理數位相關犯罪的部門，並依照發生之案件與荷蘭國家警察之高科技犯罪組（將於後面前往參訪之內容詳述）合作偵辦，可能涉及的案件有：

(1)深網與暗網偵查：利用專業工具追蹤非法交易和資料洩露來源。

(2)社交媒體分析：利用演算法搜尋公開的社交媒體數據，偵測可能的犯罪模式，如恐怖襲擊或欺詐活動。

(3)勒索病毒應對：協助受害企業和市民應對網路勒索軟體攻擊，並伺機追蹤犯罪者。

5.社區參與與透明度：該局另一個科技運用是與結合了"Veilig Utrecht"（安全烏特勒支）的手機應用程式之運用，並可與市民互動，該 APP 係由烏特勒支市市政府單位所開發，用於報告垃圾、綠化、交通、滋擾、街道騷擾、路面損壞、燈柱故障等問題，除了透過警局網站、電話和 WhatsApp 報案的方式，多了一個 APP 的使用管道，使報案變得更加容易，例如實時舉報可疑活動、獲取犯罪熱點信息、接收警方發布的緊急通知，這種數位 APP 的推廣和運用提升警民合作的參與度，也增強了警局與社區之間的信任關係。

圖 43、烏特勒支警局（Utrecht Police Office Paardenveld）外觀

圖 44、於該局大門口留影

(三)荷蘭鹿特丹（Rotterdam）警察局

鹿特丹是荷蘭第二大城市，位於荷蘭的南荷蘭省，新馬士河畔，擁有世界著名的港口，因此警察局面臨的治安挑戰包括國際犯罪、毒品走私、以及多元文化背景下的社會管理，鹿特丹警察局（Rotterdam Police unit）是荷蘭國家警察（Nederlandse Politie）的分區之一，該分區以鹿特丹市為核心，涵蓋周邊的都市群（Rijnmond 地區），該局建築物分為兩棟高大的建築，第一棟綠色建築物為警察同仁及職員專用的辦公處所，無提供民眾洽公服務，另外一棟位於綠色建築物的右側，是對外開放之警察局，提供荷蘭警方受理民眾報案、案件處理等處所，周圍停放了許多勤務使用的警車，且有許多警察進出大門，負責運作該局轄區的各項警政服務。

圖 45、鹿特丹警察局（Rotterdam Police unit）警察同仁專用之辦公大樓外觀

圖 46、鹿特丹警察局（Rotterdam Police unit）勤務處所外觀

經向該局負責對外接洽的執勤員警 Mr. Gieas 請教，Gieas 警官十分熱心，於值班臺向我們介紹了該局各項警務運作及責任範圍等該國的警察業務相關資訊，轄區位置介紹、部門分布狀況、無線電通訊頻道切換機制、勤務派遣、受理報案系統運用、巡邏人數、支援警力及到場時限等內容，作為本次參訪期間對於荷蘭警方的資訊系統及通訊系統運用於基層員警勤務有初步了解，十分受用，經綜整說明如下：

1.組織架構：該局組織結構包括多個部門，負責鹿特丹及其周邊地區的治安與執法工作：

(1) 治安巡邏部門：負責日常巡邏、突發事件應對以及維護公共秩序。

(2) 刑事調查部門：集中處理重大案件，如謀殺、毒品犯罪、黑幫活動，以及國際犯罪。

(3) 交通管理部門：管理交通安全，調查交通事故，監控港口和高速公路物流。

(4) 社區警察：協助居民解決社區安全問題，加強警民聯繫。

(5) 特種部隊與專業單位：包括防暴警察、反恐小組、網絡犯罪部門及港口安全相關的團隊。

2.該局主要任務與挑戰：因為該市是世界最大港口之一，涉及複雜的國際物流和跨國犯罪，鹿特丹警察工作有其特殊性，任務分別概述如下：

(1) 打擊跨國犯罪：鹿特丹港是犯嫌走私毒品的重要通道，因此 Gieas 表示該局經常與歐洲刑警組織（Europol）及其他國際機構合作。

(2) 社區治安：鹿特丹是一個多元文化城市，該局重視種族和文化差異對治安的影響，盡可能的維持警察與社區的聯繫並致力促進社會和諧。

(3) 應對恐怖威脅：作為重要的國際城市，鹿特丹的公共場所和基礎設施面臨潛在恐怖主義威脅，爰需要有標準的勤務應對方式，例如反應時間。

(4) 港口安全：保護港口基礎設施，確保港務物流系統的運行。

(5) 青年犯罪預防：通過協助社會計劃和教育活動，並結合警察服務以降低青少年犯罪率。

3.該局有採用現代科技技術提升執法效率和安全性：

(1) 智慧影像與監控系統：監控港口與城市公共場所等敏感地區，惟因歐盟嚴格的一般資料保護規定（General Data Protection Regulation, GDPR），仍需有一定的使用限制。

(2) 數據分析模式：案件資料匯集，並用於犯罪模式分析和觀察治安狀況。

(3) 警政資訊系統應用：提供員警便利的線上服務，包括案件紀錄、案件報告及報案平臺等。

於本局行程的最後，Gieas 警官與我們互換警察的臂章作為紀念，也是此行獲得荷蘭警察所致贈的該國警徽 Politie 臂章，惟因該局勤務關係 Gieas 警官無法離開值班處所且該警局不允許於建築物內拍照，爰於警察局大門口與荷蘭警察所致贈的該國警徽 Politie 臂章合影紀念，以及與該局執勤員警於警局旁可拍照處留影。

圖 47、於該局辦公大樓前留影

圖 48、於該局勤務處所與 Gieas 警官致贈的警徽 Politie 臂章合影

圖 49、與該局執勤員警互贈警徽臂章，並於該局可拍照處合影

(四)荷蘭國家警察高科技犯罪組（NHTCU）

荷蘭國家警察總隊，又稱荷蘭國家警察或國家警察部隊，分為十個地區單位、兩個國家單位、警察學院、警察服務中心和國家調度合作中心，本行程參訪的單位為隸屬荷蘭國家警察的「高科技犯罪組」（National High Tech Crime Unit, NHTCU），本次參訪經本國駐荷陳警察聯絡官逸明的努力促成之下，由該組犯罪情資分析部門主管 Gea Wind 女士，帶領專員 Sven Terhürne 先生、專員 Arthur van Bunningen 先生為我們介紹有關荷蘭警察體系概況及該單位所發展的高科技犯罪運作，並從資訊技術面與本國參訪人員研討各種犯罪情資、網路犯罪調查及科技偵查應用等主題，這也是本署第一次前往該國的高科技犯罪偵查單位內部進行座談及研討相關警政議題，本署參訪團為求慎重，於參訪前業準備相關訪談議題，希望於會面的過程中能與該單位專業人員有更好的交流和分享，十分具有意義，本次參訪目的及與高科技犯罪組之參訪議題分別如下（中英文對照）：

1.參訪目的：

(1) 本次本署派員參加 AI 資料分析及公開來源情資（Open-Source Intelligence,OSINT）等專業情報分析培訓課程訓練，加強培訓本署警政資料分析團隊分析人員資料分析專業能力及資料分析工具運用，以及做為後續規劃及建立我國犯罪情資分析課程所用。

（To participate in professional training courses on AI data analytics and Open-Source Intelligence （OSINT） for intelligence analysis, thereby enhancing the data analysis skills and tool usage of our police data analysis team. The insights from this training will also contribute to the

planning and development of our national crime intelligence analysis programs.）

(2) 透過與荷蘭國家警察或相關執法單位進行犯罪資料大數據運用及分析技術之參訪交流，學習先進國家情報分析模式、犯罪情資運用及系統規劃，對我國警察實務推動科技偵查犯罪及 AI 警政有所助益，以作為本署警政資訊技術及提升治安防護之參考。

（To exchange knowledge with the Dutch National Police and related law enforcement agencies on big data applications and analysis techniques in crime data. This will enable us to learn from advanced intelligence analysis models, criminal intelligence applications, and system designs, benefiting the practical implementation of technology in police crime investigation and AI-assisted policing. This experience will serve as a reference for advancing our police information technology and improving public safety measures.）

2.參訪議題：

(1) 貴國警察機關針對警政或犯罪資料之大數據分析應用現況。（Current applications of big data analysis in police work or crime data by the Dutch police.）

(2) 有關科技偵查犯罪實務，是否建有相關資訊系統輔助員警運用?（Availability of information systems supporting practical applications of technological crime investigation.）

(3) 如發生刑事案件，貴國警察人員如何運用相關犯罪資料進行偵查分析？（Methods by which Dutch police utilize relevant criminal data in investigation and analysis during criminal incidents.）

(4) 貴國警察於犯罪資料分析過程中，是否曾運用公開來源情資分析技術進行偵查?或使用何種專業分析技術及工具?（Use of open-source intelligence analysis techniques by the Dutch police in criminal data analysis, including any specific professional analysis tools and technologies.）

(5) 現今AI科技進步迅速，貴國警方是否運用AI科技於警政相關領域?（The use of AI technology by the Dutch police in policing.）

(6) 欲了解貴國對於科技犯罪偵查之人才培訓規劃安排及制度。（An overview of talent training programs, arrangements, and systems in the Netherlands for technological crime investigation.）

圖 50、荷蘭國家警察高科技犯罪組（NHTCU）簡報首頁歡迎畫面

本日正逢荷蘭初雪，外面天氣由下雨轉為下雪，十分寒冷，本署駐荷蘭警察聯絡官及本署參訪人員抵達荷蘭國家警察之「高科技犯罪組」部門，該單位建築物旁僅有一個接待處且戒備森嚴，只有經接待處人員與內部人員聯繫之後，由內部人員前來帶領始可進到下一個門禁關卡，從大門口到該單位內部會議室至少經過了 3 道管制站，且需要內部人員的識別證感應卡及訪客人員換證之後的感應卡同時於門禁設備感應，才能開啟隔離門，人員管制嚴格。本次拜訪由該組犯罪情資分析部門主管 Gea Wind 女士、專員 Sven Terhürne 先生、專員 Arthur van Bunningen 先生接待。參訪會議的一開始，由該組犯罪情資分析部門主管 Gea Wind 女士開場及介紹該國高科技犯罪組的組織及運作，中間則由專員 Sven Terhürne 先生、專員 Arthur van Bunningen 先生為我們說明科技偵查及資訊技術的應用，相關研討內容，分述如下：

1. 荷蘭警察隸屬於司法部，下轄十個區域單位及中央單位：
   (1) 區域單位：荷蘭全國劃分為十個區域，每個區域都設有獨立的警察單位，負責處理該區域內的治安事務。阿姆斯特丹是首都，擁有最大的區域單位，而其他區域則相對較為鄉村。
   (2) 中央單位分為專業知識與營運單位：負責提供特定領域的專業知識和技術支持，例如警犬、警馬、直升機、警察學院、緊急電話行動小組、網路安全、鑑識科學、數據分析等。
   (3) 調查與干預單位：專門負責特定犯罪領域的專門小組，例如高科技犯罪、兒童剝削、環境犯罪和經濟犯罪。
2. 本次參訪之高科技犯罪組（National High Tech Crime Unit, NHTCU）是荷蘭國家警察局內負責調查高科技網路犯罪的專業團隊，致力於調查先進的網路犯罪，包括勒索軟體、加密貨幣和暗網市場等犯罪調查，該部門成立於 2013 年，最初只有 35 人，目前已發展到超過 250 人，

並持續增加中。該單位積極參與國際合作，並自行發展一套 CSAE 模型用於處理各種網路犯罪調查，且頗有績效。

圖 51、該組單位主管（Gea Wind 女士）為我們介紹組織編制

3. 國際合作策略：NHTCU 根據國家的戰略重要性、法律協調性、行動一致性和組織整合度來選擇合作夥伴，並定期舉行會議，討論案件進展和合作策略，亦積極參與國際刑警組織等國際組織的活動，與全球各地的執法單位合作共同打擊網路犯罪。此外，他們還會利用歐盟的制裁制度來制裁網路犯罪分子。會議中介紹了幾個 NHTCU 參與案例：
   (1) AlphaBay&Hansa Market：AlphaBay 是一個曾經在美國盛行的暗網交易平台，後來被美國聯邦調查局（FBI）與泰國當局共同查封。然而，AlphaBay 的用戶隨後轉移到另一個名為 Hansa 的暗網市場。NHTCU 掌握了這個契機，秘密滲透並接管了 Hansa Market 的伺服器，並暗中監控平台上的犯罪活動長達一個月之久，並使全球執法團隊能夠深入了解數千名網路犯罪分子。
   (2) Emotet & Operation Endgame：Emotet 是一個曾經肆虐全球的大型殭屍網路，主要是感染電腦系統並竊取敏感資訊，常被用作其他網路犯罪活動的初始入侵工具，利用社交工程技術誘使使用者點擊，一旦感染，可以下載其他惡意軟體，如勒索軟體，為有效打擊勒索軟體攻擊，歐洲刑警組織與美國、英國等多國合作發起了「OPERATION ENDGAME」行動，目標是針對勒索軟體攻擊鏈中的「初始入侵」環節進行干預，並成功瓦解了 Emotet 殭屍網路。然而，犯罪集團僅花了六個月的時間就重建了 Emotet，儘管新版本沒有原先版本那麼成功，但這個案例突顯了打擊網路犯罪的長期性和複雜性。下圖即為該單位成功瓦解網路攻擊等案件時的標語，告訴大家「透過終局之戰行動的國際合作，採取了一系列協調行動來拆除網路犯罪服務。執法機構查獲了與該領域相關的資料庫

和其他資訊。任何操作或使用這些網路犯罪服務的人都會受到調查和起訴。」

圖 52、該單位成功瓦解網路攻擊等案件時所使用之標語

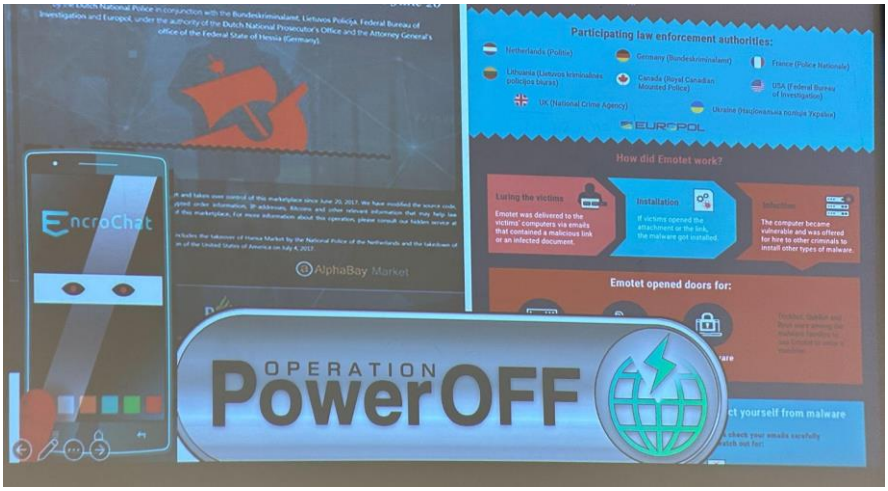


圖 53、破獲並成功關閉（Power Off）許多犯罪集團惡意網站

4. CSAE 模型運用：

CSAE 框架，其英文字由 Collect、Store、Analyze、Engage 的第一個字母組成，該模型的四個階段分別表示「蒐集資料」、「儲存資訊」、「分析情資」、「案件行動」。目的在解決執法機構於調查有組織犯罪的過程中面臨的挑戰，特別是在現今大數據時代下，如何有效地處理大量證據並將其轉換為可操作的情報。傳統調查方法在處理當今犯罪的規模和複雜性方面捉襟見肘，犯罪者利用各種技術手段來隱藏他們的活動，使得執法機關難以追蹤和蒐集證據，該單位以 CSAE 模型強調以資料科學方法來應對這些挑戰，並強調執法機關間之技術協調的必要性，技術協調意味著各機關應採用共同的標準、執行流程

和統一工具來處理證據，才能有助於提高調查效率及避免遭特定資訊系統服務供應商（或系統開發商）所侷限。CSAE 模型的四個階段形成一個循環的流程，引導執法機關從資料蒐集到最後採取行動的全過程，CSAE 模型能在現在大數據時代有效應對組織犯罪，通過結合資料科學方法、政策制定和多方合作，有助於提升犯罪調查效率和有效性，值得我國於犯罪情資分析的資料運用作為借鏡。

圖 54、CSAE 模型四階段（蒐集、儲存、分析、行動）

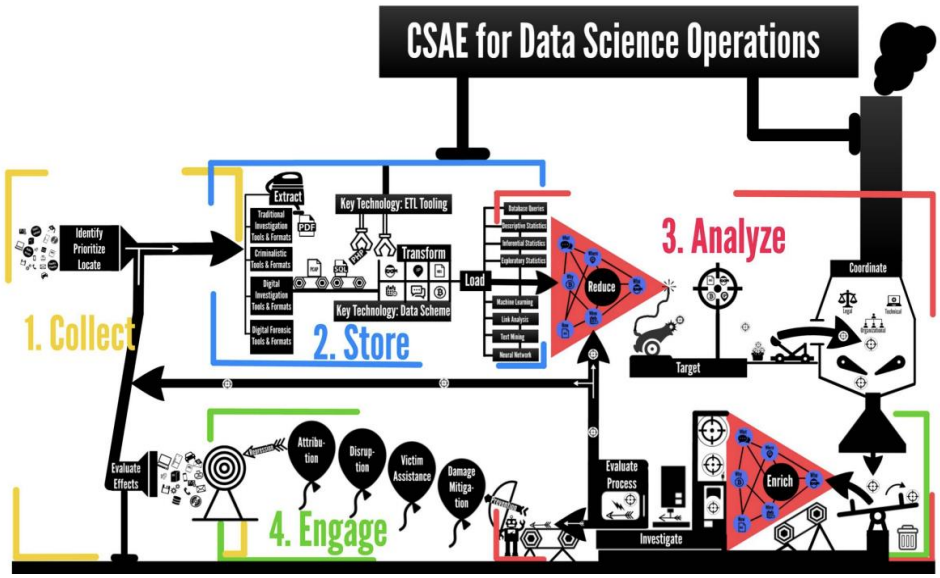


圖 55、CSAE 模型應用於資料科學之整體流程

圖 56、專員 Sven Terhürne 先生說明 CSAE 模型四階段之應用

(1) 蒐集（Collect）：識別與犯罪相關的資料來源，強調資料之質量而非數量，資料來源可能包括從手機、電腦、伺服器、加密通訊平台、社群媒體、道路攝影機及警政系統中所蒐集與犯罪活動有關資料。

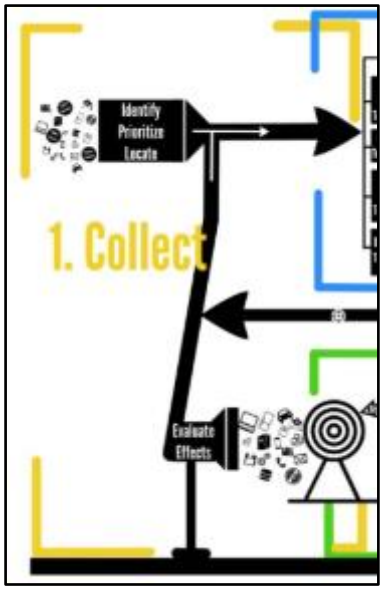


圖 57、CSAE 模型之蒐集（Collect）步驟

(2) 儲存（Store）：將蒐集到的資料轉換為資訊，即將資料歸納並賦予資料意義，使其更具相關性和目的性，採用 ETL 流程：擷取（Extract）、轉換（Transform）、載入（Load），將資料清理、標準化，轉換為統一的格式，建立一個結構化的數據倉儲，並使用分散式搜尋和分析引擎 Elasticsearch，以便於後續的分析和使用，其中 Elasticsearch 是一個基於 Lucene 程式庫的搜尋引擎（主要用於全文檢索和搜尋之開放原始碼程式庫），它提供了一個分散式、

支援多用戶的全文搜尋引擎，且具有 HTTP Web 介面及可使用 JSON 文件，Elasticsearch 是用 Java 開發的，官方客戶端在 Java、.NET（C#）、PHP、Python、Apache Groovy、Ruby 和許多其他語言中都是可用的，在科技技術的領域 Elasticsearch 是最受歡迎的企業搜尋引擎。

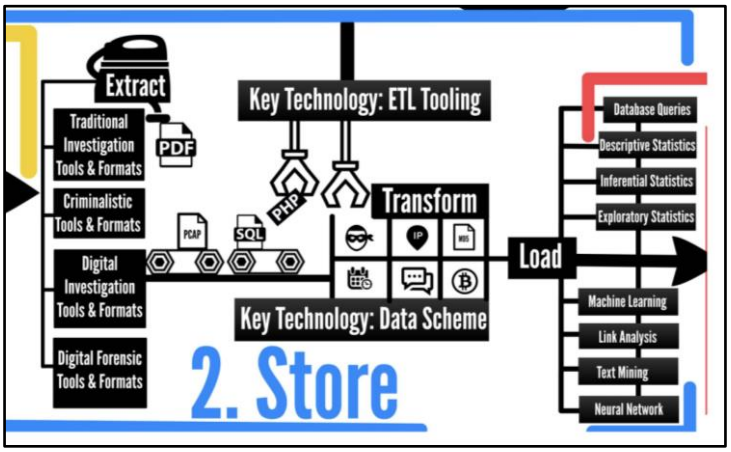


圖 58、CSAE 模型之儲存（Store）步驟

(3) 分析（Analyze）：將蒐集及整理過並儲存之資訊（資料）透過因果、邏輯關係及犯罪領域的知識與經驗互相結合，轉換為可用情資，形成對犯罪活動的洞察和理解，例如使用社交網絡分析（Social Network Analysis, SNA）演算法技術來識別犯罪網絡中之關鍵節點（node）和關係（relation），進一步識別犯罪模式、犯罪趨勢和犯罪參與者為何，作為後續偵查行動之依據。其中分析流程更包含了協調（Coordinate）及豐富（Enrich）的環節，分別執行資料態樣的限縮，避免無限發散，以及資料的整合，串連有用的情資，讓偵查資料延伸更多可供利用的關係，供偵查人員查找細節。

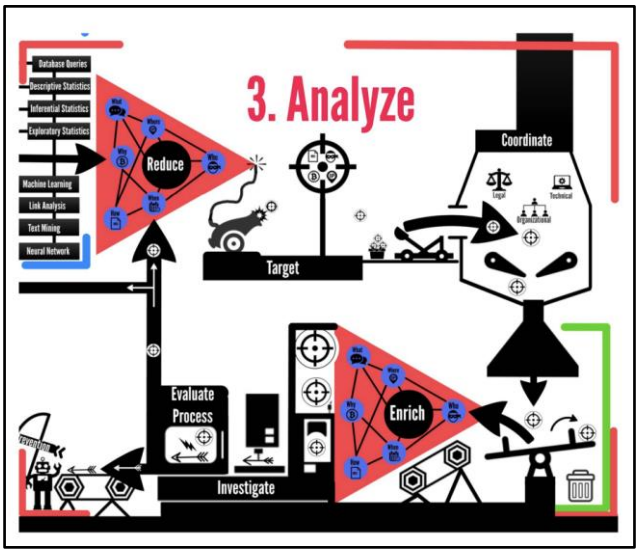


圖 59、CSAE 模型之分析（Analyze）步驟

(4) 行動（Engage）：根據分析結果採取案件行動，並強調多樣化的干預措施，而不僅僅局限於逮捕和起訴。例如為受害者提供心理輔導和法律援助、依據識別犯罪組織的關鍵成員，並將其作為逮捕目標，或是根據分析結果來定位和破壞犯罪分子使用的伺服器和其他基礎設施，更包含了犯罪集團的上、下游共犯連結。

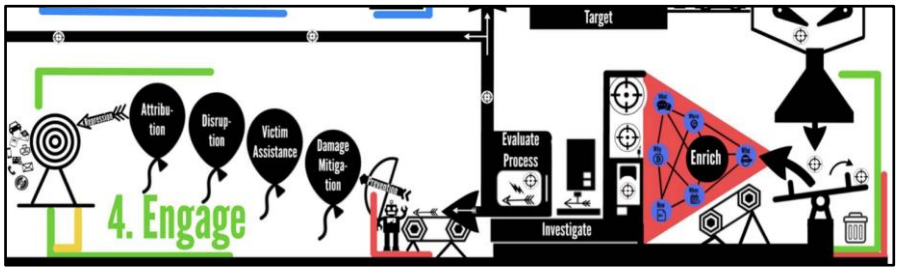


圖 60、CSAE 模型之行動（Engage）步驟

圖 61、參訪會議與該國專業人員之討論過程

圖 62、致贈本署紀念禮品予該單位人員

圖 63、本次參訪人員與該組人員合影 1

圖 64、本次參訪人員與該組人員合影 2

圖 65、雙方互贈參訪禮品並合影留念

圖 66、該單位公布欄一隅之「荷蘭網路犯罪預防計畫」

（荷蘭語標語：Hack Right - Talent winnen & Recidive voorkomen；贏得人才&防止累犯）

(五)參訪荷蘭哈倫（Haarlem）警察局及該局國際執法合作中心

哈倫（荷蘭語：Haarlem）是位於荷蘭西部北荷蘭省的中型城市，也是該省的首府，位於阿姆斯特丹以約西 20 公里，人口約 16 萬人，它也是美國紐約市著名的街頭文化區域哈林區（Harlem）的名字來源。哈倫是一個繁榮的城市，擁有大量的紡織工業、造船廠和啤酒廠，也曾是著名的銀製手工藝品之城，特別是鬱金香的種植和出口而聞名，享有「花城」的盛譽；另哈倫也是一座觀光資源豐沛的城市，擁有許多歷史建築與博物館。每一年哈倫大約會有至少 70 萬人次到訪，僅次於荷蘭四大城市（阿姆斯特丹、鹿特丹、海牙及烏得勒支），因哈倫警察局是位於北荷蘭省哈倫市的主要執法機構，負責維護該市及周邊地區的公共安全與秩序，作為荷蘭國家警察（Nederlandse Politie）的一部分，哈倫警察局不僅致力於日常的治安管理，還肩負著與當地社區緊密合作、推動犯罪預防的責任，轄區的治安、交通等勤（業）務日趨繁重，主要的警政工作包括處理治安問題，亦涉及旅遊相關的安全管理。

圖 67、哈倫（Haarlem）警察局外觀 1

圖 68、哈倫（Haarlem）警察局外觀 2

本次參訪經本國駐荷陳警察聯絡官逸明的聯繫及接洽，由哈倫警察局國際執法合作中心（International Rechtshulp Centrum, IRC）的警官 Willam 於該局會議室與我們分享及討論該局相關跨國合作案件的偵辦與應用、情資相關交流及該局警政運作概況等內容，Willam 警官更特別提及近期臺灣與比利時國際毒品案，透過他本人及荷蘭警方聯合共辦國際毒品案件（古柯鹼）毒品證物移交等跨國勤務，對於荷蘭賡續與本國檢警有密切跨國合作，表達期盼與肯定，並於拜訪後前往警局附近的餐廳進行午餐餐敘及心得交流。經 Willam 警官與我們分享該局的勤（業）務職責，經本國參訪人員針對 Willam 警官於座談時的口述，摘要如下：

1. 治安維護與犯罪預防：該局員警需編排經常性勤務於市區進行巡邏，特別是在哈倫市中心的熱門地區，如格魯特馬克特廣場（Grote Markt）和哈倫大教堂（St. Bavo’s Cathedral）周邊；另則透過規劃執行的社區警政計畫，與當地居民和企業建立聯繫管道，並有相關資訊系統可收集基層情資建檔，經數據運用之後藉以關注潛在犯罪事件發生情形。
2. 交通管理與執法：哈倫市是一個重要的交通樞紐，該警察局交通相關部門負責城市之交通管理，尤其在荷蘭自行車眾多，需有員警不定時編排勤務於自行車及汽車共用的道路上執行交通執法，更特別針對行人與自行車密集的區域，設立專項巡邏，確保民眾行車安全和秩序。
3. 旅遊與活動安全：哈倫是荷蘭一個著名且古老的旅遊城市，近幾年吸引了大量國內、外遊客，該局在主要旅遊景點提供警政服務站點，內有多國語言服務，讓遊客需要時得以利用；另外大型活動（例如文化節、國王節慶祝活動等）期間，員警需協助維持民眾秩序、提升治安層級，並與其他緊急應變的警察單位合作應付各種突發治安事件。

4. 網路犯罪與刑案偵查：該局設有專門的數位犯罪部門，循荷蘭國家警察的荷蘭網路犯罪預防計畫，著手處理該局轄區內之網路詐騙、身份盜竊等案件，目前刻正逐步提升網路資安的意識。
5. 現代化設施與科技應用：該局藉由資訊科技的應用提高員警執法效率和橫向溝通便利性，目前更規劃擴大網路犯罪偵查能力，以應對數位化的犯罪挑戰，例如：
   (1) 數位化案件管理系統：所有案件和偵查流程均在中央資訊平臺上進行記錄與管理，方便內部員警之間的協作、共辦並提升辦案效率。
   (2) 監視器系統：在轄區內部分主要路口和公共空間安裝了監視器系統，結合 AI 技術進行行為模式分析，能快速檢測和預警異常活動，惟因歐盟嚴格的一般資料保護規定（General Data Protection Regulation, GDPR）限制，目前在相關監視器系統的使用上仍有一定的限制。
   (3) 隨身攝影機（Bodycams）：哈倫警察在執行任務時需配備隨身攝影機，以提高透明度並保障執法人員與民眾的安全，此項與本國員警執勤的配備相同。
   (4) 應用程式平臺：當地居民可透過於Google Play或APPLE APP Store的Politie - Nederland專頁，下載一款「112NL」APP，以哈倫政府相關單位之官方應用程式舉報可疑行為、查詢案件進展，甚至與警方進行即時聯絡。此APP是荷蘭緊急服務警察、消防隊、救護車等官方應用程式，在緊急情況下可透過APP使用，系統將資料傳送至控制室使得警察單位、消防單位或醫療單位能夠更快、更好地提供幫助，另外則包含無法正常說話、無法聽清楚或與服務人員聯繫不順利時，手機會自動與控制室共享您的位置。

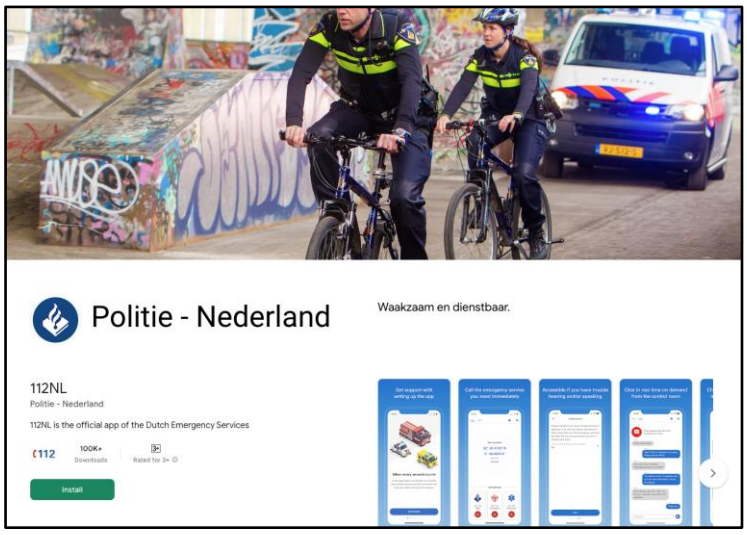


圖 69、於 Google Play 之 APP 頁面

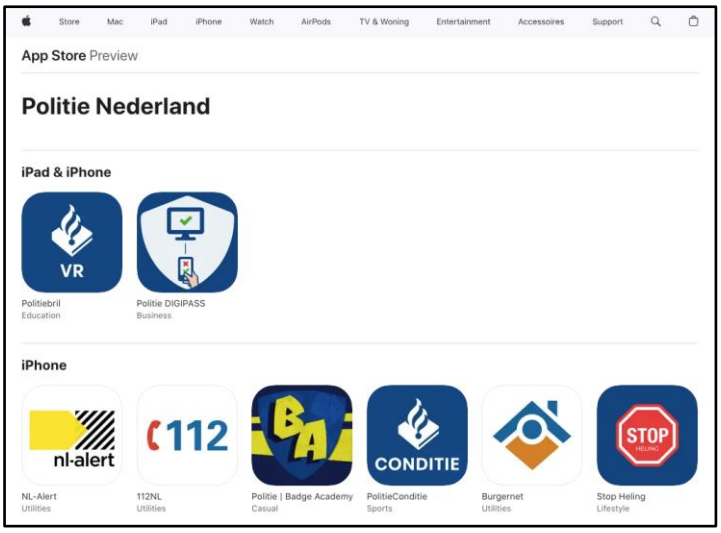


圖 70、於 APPLE APP Store 之 APP 頁面

6. 社區參與與透明警政：該局的警政工作及策略非常注重與該城市內社區的互動，強調民眾與警察之間透明與信任的重要性，例如：
   (1) 社區會議：定期舉辦座談會，與當地居民討論近期治安問題並開放建議回饋。
   (2) 警局開放日活動：邀請市民參觀警察局，展示執法工作內容並伺機提供治安及交通等教育。
   (3) 加強與社交媒體互動：該局使用社群媒體等平臺，分享民眾安全提示、常發生之治安狀況宣導及任何需要的警察通知。
7. 加強與其他執法機構的合作：針對跨區域犯罪和恐怖主義威脅。
8. Willam 警官也跟我們分享，荷蘭警方於受理報案時需要預約，並不會即時處理發生的案件，即使是受傷的案件，亦需要先行就醫再依據報案的預約情形前往警察單位辦理後續的報案程序，與本國可以直接進到派出所等警察單位報案的方式十分不同；另該局正持續推動環保和可持續性的執法策略，例如採用電動巡邏車供員警執行勤務。

圖 71、本署人員與哈倫警察局警官 Willam（右 1）於接待大廳合影

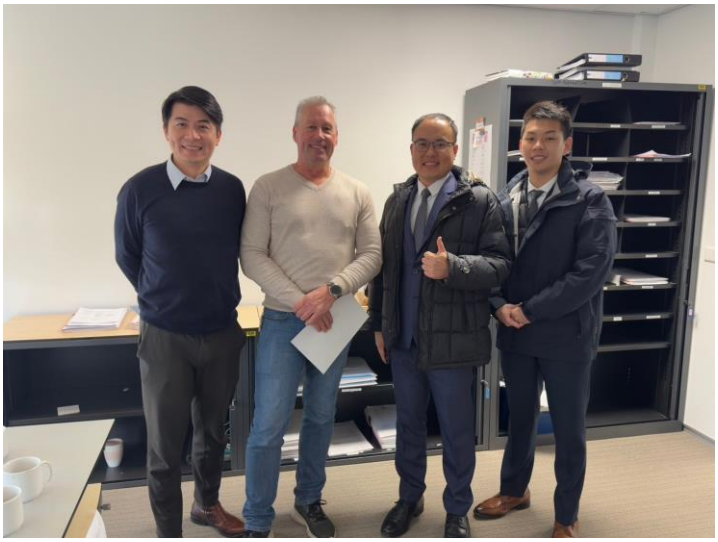


圖 72、本署人員與該局警官 Willam（左 2）合影

圖 73、本署人員於該局國際執法合作中心（IRC）辦公室

圖 74、參觀該局與國際各執法單位交流之紀念品展示櫥窗

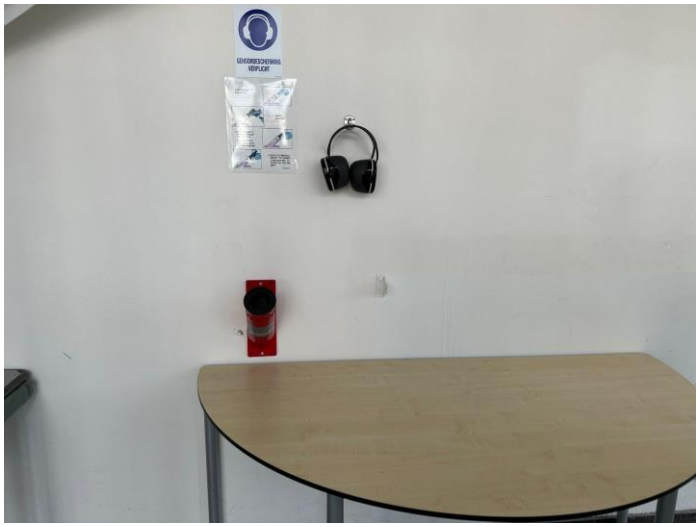


圖 75、參觀該局執勤員警清槍桶等安全設備

圖 76、與該局警官 Willam（右 1）參訪後餐敘合影

二、海牙資安三角洲（HSD Campus）

海牙資安三角洲（The Hague Security Delta,HSD）公司位於荷蘭海牙，是歐洲最大的資訊安全相關之聚落，旨在促進荷蘭資訊安全產業的發展，自從2013 年超過 300 家公司、政府機構、知識機構，透過 HSD 共同合作開發創新的安全解決方案，並為荷蘭許多新創科技公司提供發展的空間與資源。HSD 的宗旨包括增進各相關組織的知識、開發特定計畫、支持市場進入及提供資金和人才支持。

圖 77、海牙資安三角洲（HSD Campus）位於海牙的總部外觀

本次接洽 HSD 公司安排與科技犯罪偵查及情資蒐集等相關議題的資訊科技公司辦理參訪工作，最後確定由與本案研習計畫相關的 CFLW 科技公司參訪，該公司全名為 CFLW CyberStrategies，成立於 2019 年，由荷蘭應用科學研究組織成立的新創公司（荷蘭語：Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO），CFLW 公司針對加密貨幣及暗網等技術領域有深入的研究，尤其核心產品為 Dark Monitor，主要用於暗網檢索的工具，就像暗網的 Google 一樣，目前該國或國際的政府單位或情資單位亦使用該公司相關技術進行資料蒐集及偵查，CFLW 公司的主要業務和商業模式專注於網絡情報服務，主要客戶為全球的執法機構，其商業模式提供整個機構以單一價格取得授權，例如整個警政單位使用者 1 年只需支付 25,000 歐元，即可讓全國員警使用 Dark Monitor 進行暗網的資料蒐集及偵查，此商業模式能讓 CFLW 公司接觸到更多潛在使用者，並透過使用者間的口碑來擴大影響力，其中使用 Dark Monitor 的使用者無需建置進入暗網所需要的各種安全環境，不需要具備

深入的資訊技術能力，即可透過 CFLW 公司維運的平臺接觸暗網或深網的世界，讓員警克服進入暗網或深網的前置作業，提升使用者入門門檻；另 CFLW 公司也提供其他服務，例如加密貨幣分析和反釣魚工具，並透過 API 讓客戶可以將這些工具客製化整合至自行開發的資訊系統中使用。

圖 78、海牙資安三角洲（HSD Campus）簡報介紹

經於參訪過程中深入了解，CFLW 公司的團隊和合作夥伴主要由 IT、數據分析、AI 和資料庫開發人員組成，位於亞洲的部分開發團隊位於越南，該公司與大學、研究機構和國際組織合作進行研究和開發，例如阿姆斯特丹大學、TNO、奧地利 AIT 和西班牙等，也積極參與歐盟項目，並與歐洲刑警組織和歐洲警察署保持密切關係。經循 CFLW 公司與本國的關係，於 2024 年 10 月 22 日曾由數位發展部數位產業署率領 5 家臺灣資安業者參加荷蘭 ONE Conference 系列活動，並促成荷蘭資安研究機構 CFLW、資安創新平臺海牙資安三角洲（HSD）與臺灣 5 家業者共同簽署合作備忘錄，深化臺荷資安產業合作，CFLW 公司計劃於明（115）年 4 月參加臺灣資安大會，並期望與本國相關單位未來有更多的合作機會並進行Dark Monitor 產品分享與提供試用。以下針對參訪過程中CFLW所分享之暗網網路監控系統，說明如下：

(一)CFLW 公司暗網網路監控系統（DWM）是一款開源情報（OSINT）解決方案，可洞察源自於濫用暗網網路和加密資產的犯罪和詐欺活動。暗網網路，如洋蔥路由器（Tor）或隱形網際網路計畫 （I2P），已成為犯罪分子利用技術匿名性的避風港。他們的非法活動範圍從虐待兒童和販毒到大型金融犯罪，影響網路空間和現實世界。此類型非法活動受到日益先進的網路服務的加持，提供以單一供應商商店、暗網市場、搜尋引擎或暗網網路索引等形式出現。鑑於此機會主義活動的性質日益複雜，執法機構、網路安全機構、金融機構和安全產業的安全專業人員普遍需要更強大的暗網網路監控

能力。CFLW 公司的先進分析工具為專業人員提供有關可疑活動的威脅情報，使他們能夠適當鎖定調查範圍、追蹤和逮捕嫌疑人，並破壞和起訴其犯罪基礎設施。DWM 最初由荷蘭應用科學研究組織（TNO）構思和開發。當概念達到足夠的技術成熟度後，它被轉移到 CFLW 公司進行進一步完善和成熟解決方案，目標是擴展到全球使用並實現預期影響。

(二)DWM 具備以下獨特功能：

1. 暗網網路的 Google：DWM 通過整合來自 Tor、I2P、Zeronet 等平臺的暗網網路服務，提供暗網網路的鳥瞰圖。它提供對源自暗網網路的大量數據集的存取權，這些數據集已分類並呈現每個索引和可搜尋的網域。此方法導致每天監控超過 100 萬個暗網網路網域，截至發佈日期，目前有超過 300,000 個網域處於活動狀態。
2. 原始資料存取：DWM 授予對完整時間戳記、爬取的 HTML 頁面儲存庫的存取權，使調查人員和研究人員能夠將其發現置於未處理資料的原始上下文中。這種方法避免了對解釋或系統生成的見解依賴，確保對資訊的準確理解。
3. 時光機：DWM 提供對從暗網網路收集的大量索引數據集的存取權，該數據集的功能類似於時光機，用於調查離線暗網網路網域的歷史記錄。該數據集包含廣泛的網域，其中一些網域包含爬蟲程式重複下載的多個頁面。每次爬蟲程式檢查特定網域的 HTML 內容時，它都會通過保存 HTML 檔案及其標頭來建立快照。然而 DWM 將當前下載內容與先前下載內容進行比較以識別任何更改。檢測到更改時，會生成新版本，使用戶能夠輕鬆有效地監控網域歷史記錄。
4. 以基礎設施為中心的方法：DWM 關注於最終收集暗網網路網域，因此關注於識別非法活動的入口點，與其他暗網網路監控解決方案相比，DWM 方法的隱私侵入性明顯更低，其他解決方案通常優先考慮個人或嫌疑人作為起點。這種區別導致 CFLW 公司在鎖定市場時撒下更大的網，更多地關注威脅基礎設施而不是個人。

圖 79、由 CFLW 公司執行長Mark 先生進行簡報說明 1

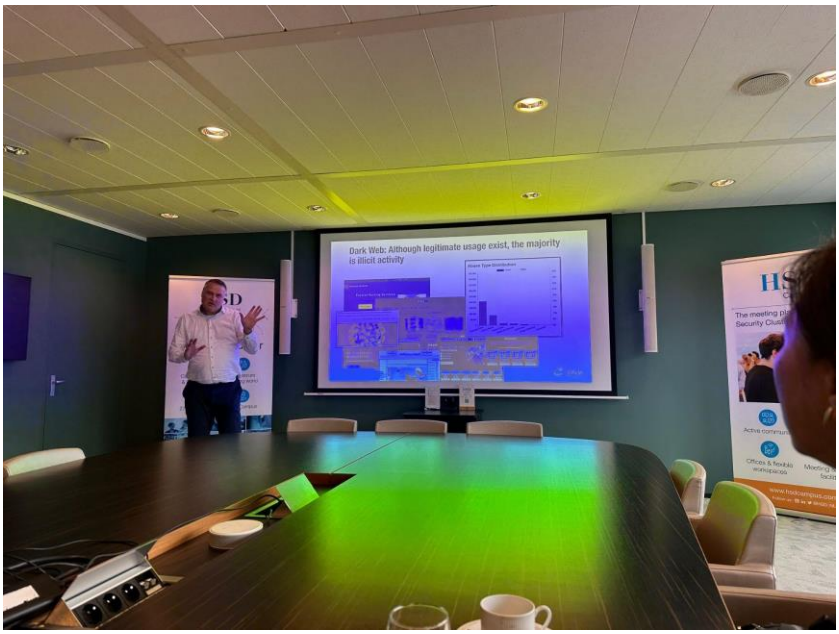


圖 80、由 CFLW 公司執行長Mark 先生進行簡報說明 2

圖 81、意見交流 1

圖 82、意見交流 2

圖 83、致謝及致贈紀念品 1

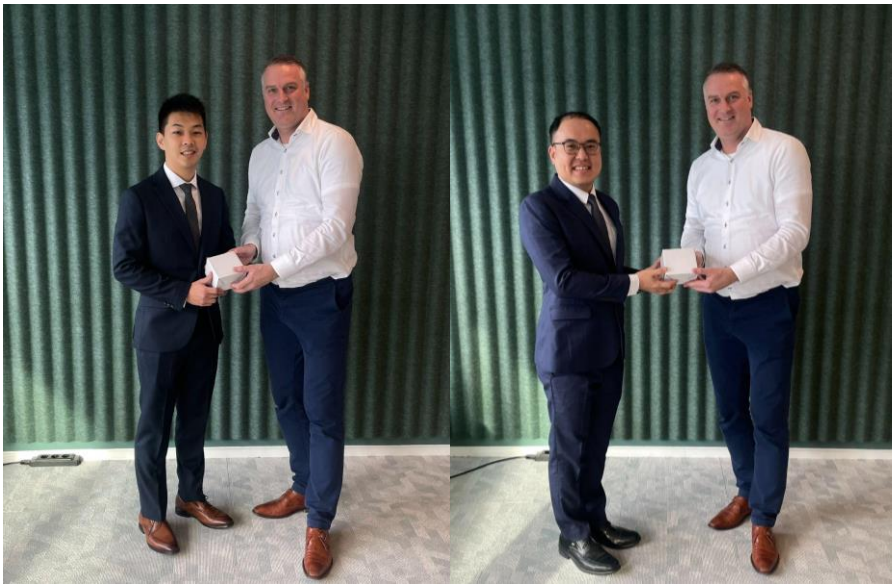


圖 84、致謝及致贈紀念品 2

圖 85、拜訪後與 CFLW 公司執行長合影

三、駐荷蘭台北代表處

「駐荷蘭台北代表處」是中華民國（臺灣）設於歐洲的外交官方機構，負責在本國與歐洲各國的國際事務及各種交流活動協助，包括外交、經濟、文化、警政和教育等領域，由於臺灣的國際地位特殊，駐外單位多以「台北代表處」名義運作，而非傳統的「大使館」或「領事館」。代表處內涵蓋外交部、移民署及警政署等人員進駐，各司其職，其主要職責有領務服務：提供護照申請、簽證發放、文件認證等服務，協助臺灣公民在荷蘭的需求。經濟合作：推動貿易、投資與科技合作，促進雙方的經濟發展。文化交流：舉辦展覽、演出和講

座，推廣台灣文化。教育合作：促進學術交流與學生交換計畫。僑務服務：協助僑民活動並支持台灣僑民組織。本次本署於荷蘭等地之參訪行程主要由駐荷蘭台北代表處之本署刑事警察局國際刑警科陳聯絡官逸明協助接洽，前往荷蘭相關警察單位了解警政資訊或科技偵查等面向之研討，爰於本次參訪期間特別拜會本國駐荷蘭台北代表處，分享本次荷蘭研習進修課程內容及拜訪該國專業警察單位之目的，並向聯絡官請教荷蘭與臺灣之警政合作夥伴之間的關係，協助我們深入了解荷蘭當地的風俗民情、天氣及生活習慣。

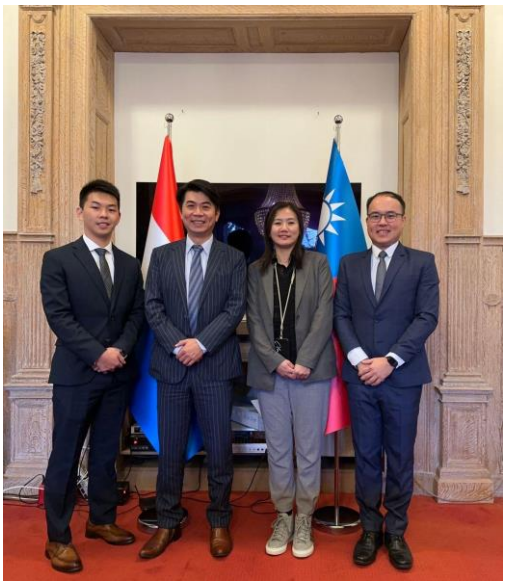


圖 86、與本署派駐歐洲之警察聯絡官於駐荷蘭台北代表處合影

圖 87、於本國駐荷蘭台北代表處前合影

肆、心得及建議

一、參訓(訪)心得

本次參加荷蘭 Reuser's Information Services 機構舉辦的公開情資資料分析（OSINT）訓練課程，不僅是一次深具專業價值的學習機會，更是開拓視野、學習國際公開情資資料分析技術的重要經驗，課程由資深資料分析專家 Arno HP Reuser 親自授課，課程內容系統性地涵蓋 OSINT 的基礎理論、實務操作及工具運用，課程內容之完整性和深度令人參訓人員印象深刻，其中透過課程中的系統化教學方法，例如布林查詢公開情資之運算、深網資料蒐集與分析技巧及需求分析與問題解構之應用，提升了本署資料分析人員面對龐大公開資料時的篩選與驗證能力，且能進一步運用這些技術針對特定議題進行深入調查及分析，除此之外，尤其在與來自不同國家背景的學員進行分組討論和實際演練時，發現不同文化和行業背景在解決問題上的多元思考方式，啟發我們處理犯罪情資分析工作的思維。此外，課程中使用的軟、硬體，例如暗網瀏覽器 Tor、XMind 等工具應用，以及課前虛擬環境的建置，體現了主辦方對技術細節的重視及課程內容能顧及不同職業領域之參訓學員的用心。

此次參訪荷蘭部分地區或中央的警察機關，深入了解其警政體系與智慧化運作。烏特勒支智慧警察局運用虛擬警員與視訊系統，提供隱私保護的報案及諮詢服務，展示科技應用提升警政效率的典範；烏特勒支警局則強調社區警政與數據分析，透過科技應用掌握轄區報案案件地理位置或熱點分布，並結合員警派遣、巡邏及調度的應用，提升犯罪偵查與治安維護成效；鹿特丹警局因地理位置涵蓋交通及港口轉運重要地點，在跨國犯罪防治、港口安全與社區治安方面具有挑戰，並已採用類似我國案件管理系統之案件控管及跨系統情資整合，以應對複雜治安問題；荷蘭國家警察高科技犯罪組展示了荷蘭在網路犯罪偵查、實務案例及 AI 情資分析方面的領先能力。雖然我國在犯罪情資整合上較荷蘭容易，但荷蘭執法機關對情資運用程度卻較為進步，常可看到情資整合中心(Intelligence Fusion Center)或情資單位(Intelligence Analysis Unit)，偵查人員蒐集現場資訊後即可交由犯罪情資分析人員分析，並依據分析的建議進行後續行動，惟我國偵查人員仍習慣傳統案件偵查模式，大多用於逮捕前或逮捕後的資料查證部分，會適時著手運用情資分析技術的偵查人員仍佔少數，但隨著科技發展及犯罪手法日新月異，傳統偵查方式已出現許多偵查斷點，因此如何使我國偵查人員了解並善用情資分析技術或建立專責情資分析單位，確實是我國仍需向荷蘭警察機關學習之處，本次參訪加深了對荷蘭警察數位化與科技應用的認識及啟發。

一、建議事項：

(一)加強培訓公開情資資料分析專家，納入本署犯罪情資資料分析課程內容：為打破刑案犯罪斷點、落實跨縣市刑案情資協作，本署每年皆舉辦犯罪情資分析基礎及進階課程（各 2 梯次，每梯次 5 日），培養各警察機關執行刑案情資資料分析人才，由各警察機關遴派於實務辦案績效良好及專精資料分析之人員參訓，並規劃學員結業後擔任各警察機關資料分析團隊之種子教官，並

負責刑案協作平臺資料分析員。本次參訪學習公開情資資料分析（OSINT）技術及軟體應用，可加入本署資料分析課程內容，並參考參訓機構之課程教學方式，提升員警學習效果。

(二)強化本署既有警政大數據資料庫，導入大數據 AI 運算之框架技術：傳統調查方法在處理當今犯罪的規模和複雜性方面捉襟見肘，犯罪者利用各種技術手段來隱藏非法活動，使得執法機關難以追蹤和蒐集證據，荷蘭國家警察高科技犯罪組於大數據資料處理系統導入 C.S.A.E.框架模型，模型四個階段分別表示蒐集資料（Collect）、儲存資訊（Store）、分析情資（Analyze）、案件行動（Engage），並運用 Elastic Search 分散式搜尋及分析引擎於 AI 平臺中，強調以新興的資料科學方法來應對犯罪挑戰，目的在解決大數據時代如何有效地處理大量犯罪資料並將其轉換為可用情資。本署犯罪情資資料庫未來可將既有 Elastic Search 搜尋引擎強化為 Elastic Search AI Platform 引擎，透過 AI 技術強化人、車、案、物等事件關聯之情資網脈運算效能，以應付日趨龐大之各種犯罪情資及公開來源情資之資料分析和運用，期能提升員警使用警政系統之刑案偵辦效能。

(三)強化暗網犯罪偵查工具，縮短員警進入暗網技術門檻：面對詐欺犯罪專業分工、毒品犯罪組織扁平化、跨國犯罪證據移轉、黑道組織利益合流等新型態治安問題，暗網涉及之犯罪態樣愈加普遍及多樣，已成為新型態犯罪溫床。由荷蘭應用科學研究組織成立並與荷蘭學術研究機構或國際組織（例如歐洲刑警組織等）有密切關係的 CFLW CyberStrategies 資安研究機構，主要專注於提供網絡情資分析服務，針對加密貨幣及暗網等技術領域有深入的研究，目前國際政府或情資單位亦使用該機構相關技術進行資料蒐集及偵查，其 Dark Web Monitor 核心技術主要用於暗網檢索，提供使用者不需具備專業資訊能力且無需建置進入暗網所需之各種安全環境，即可透過 Dark Web Monitor 平臺接觸暗網內部資訊。本署相關科技犯罪偵查工作未來可強化並導入暗網犯罪偵查工具，讓員警能克服暗網使用門檻，全面提升員警於暗網犯罪資料蒐集及偵查效能。

伍、參考資料

一、Reuser's Information Services 機構 OSINT 網站（https：//opensourceintelligence.biz/）

二、開源情報最重要來源的參考書目資料庫（https：//bib.opensourceintelligence.biz/

三、資料分析及處理文獻 1－CASE 模型（https：//cpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2021/03/White-Paper-Towards-Data-Scientific-Investigations.pdf）

四、資料分析及處理文獻 2－如何實現可信任數據執法管理？（https：//www.europarl.europa.eu/cmsdata/240167/vanBunningenTrustDM.PDF）

五、公開情資資料分析 OSINT 工具書（http：//rr.reuser.biz）

六、荷蘭網路犯罪預防計畫（https：//portswigger.net/daily-swig/hack-right-dutch-cybercrime-prevention-program-comes-of-age）

七、荷蘭國家警察（National Police Corps of Netherlands - WikiPedia）https：//en.wikipedia.org/wiki/National_Police_Corps_（Netherlands）

八、荷蘭國家警察所屬高科技犯罪單位（Team High Tech Crime, THTC）（https：//kombijde.politie.nl/vakgebieden/ict/cybercrime-aanpakken）

九、荷蘭烏特勒支無人警察局（https：//www.iotm2mcouncil.org/iot-library/news/smart-cities-news/utrecht-opens-smart-police-station/）

十、HSD Compus（海牙資安三角洲）（https：//securitydelta.nl/about/hsd-campus）

十一、工商時報－歐洲最大資訊安全聚落海牙安全三角洲來臺（https：//www.ctee.com.tw/news/20240528700616-431202）

十二、CFLW 資安研究機構（https：//cflw.com/）