出國報告（出國類別：進修）

研習影像 AI 技術及資料分析用於犯罪預防偵查之整合運用

服務機關：內政部警政署
姓名職稱：警務正林品杉、吳柏毅
派赴國家：英國
出國期間：108.06.23~07.06
報告日期：108.10.04

摘要

近年由於新興科技造成犯罪偵查斷點，面對日漸猖獗的毒品及詐欺犯罪集團，執法機關越來越重視運用資料分析技術拼湊破碎資料，以加速案件偵辦，有效地打擊不法組織。英國在倫敦地鐵恐怖攻擊後，各相關治安部門持續著重發展情資整合，並建立先進的犯罪偵防資訊架構與應用模式，本計畫前往倫敦警察廳，進行犯罪情報分析與預測技術之交流，並參加在全球擁有廣大資料分析能量的情報分析師培訓課程「Jane's Open Source Intelligence (OSINT) Training」，透過學習先進國家執法機關之犯罪情報分析模式，期能對我國警察實務推動科技偵查犯罪有所助益；另本計畫亦參訪 Google Deep Mind 研究團隊，針對人工智慧在不同領域上之應用與專家學者交流，以做為本署後續推動警政雲及 AI 警政之參考。

目錄

壹、目的

一、計畫目標

近年由於毒品及詐欺犯罪日漸猖獗，新興科技犯罪層出不窮、手法亦日益翻新，執法機關越來越重視運用資料分析技術拼湊破碎資料，以加速案件偵辦，快速及有效地將歹徒繩之以法。本計畫前往英國倫敦參加 Jane's Open Source Intelligence (OSINT) Training 課程，該課程訓練針對不同目標，使用 OSINT（公開資料源情資分析技術）進行資料分析，學習如何有效率地收集、分析公開資料，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。

倫敦警察廳為英國首都大倫敦地區的警察機關，亦為全英國規模最龐大的警察組織，建立了先進犯罪偵防資訊架構與應用模式，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測之交流，透過學習先進國家之犯罪情報分析、預測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，以及做為後續規劃及建立我國警政資料分析課程之參考，並透過與英國執法機關進行犯罪資料分析與預測之交流，學習先進國家情報分析模式，以推動科技犯罪偵防，提升治安防護，並藉由參訪英國警察廳對於警政影像 AI 技術之應用情境，作為本署規劃及推動 AI 警政之參考。

貳、參訪過程

本次參訪由中華民國駐英國代表處鄭秘書翔徽協助安排及協調參訪行程，並全程陪同參訪事宜。

一、倫敦警察廳

(一)背景介紹

倫敦警察廳（Metropolitan Police Service，簡稱 MET）有近 42,000 名官員和工作人員，是英國最大的警察局（包含 30,302 名警察、警察人員 8,976 人、1,233 名警察社區支援人員及 1,784 特別官員)，該單位由數個主要部門構成，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。

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

1.單位介紹：

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（Operational Command Units，縮寫 OCU）。

2.參訪過程：

本次參訪針對該單位兇殺及重案指揮課（Homicide and Serious Crime Command，SCD 1）所開發之 HOLMES 福爾摩斯系統，雙方並就實務運作、系統設計管理及業務流程等方面交換意見。

3.HOLMES 福爾摩斯系統（Home Office Large Major Enquiry System）

HOLMES 系統是英國警方協助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（如 2005 年倫敦地鐵爆炸事故）等，而其警察資訊架構（PFI framework）通過「全國警察服務改善局（National Policing Improvement Agency）」鑑定，並廣泛應用在英國警方及相關警察單位。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。

圖 1：參訪人員與 HOLMES 系統介紹人員（MET 資訊人員）合影照片

本次參訪係由資訊人員介紹 HOLMES 系統及協助偵辦案件的流程，當發生重大案件時，英國警方會成立此案件的專案偵辦團隊，由數名偵查人員及一名資訊人員組成，並有固定的工作站，此資訊人員負責將團隊蒐集之大量情資（包含各類文件、圖、照片等資料），經確認資料正確性無誤後才輸入至 HOLMES 系統中（每一團隊僅有該名資訊人員具有權限更新該案件的情資，並可查詢整個系統相關資訊），已結案的案件會轉為歷史案件，不再開放編輯，簡言之，HOLMES 系統就是把歷來重大謀殺案件相關資訊彙集而成一個龐雜的知識庫，但僅供全國偵辦重大案件團隊使用，類似本署智慧分析決策支援系統與案件管理系統之結合，並加入大量業務 SOP 後的結果；該系統亦可管理案件偵辦進度，MET 的資訊人員 Teresa 展示系統時，正有 997 件案件(即 997

個專案團隊)正在偵辦中，並可逐一檢視個案件的偵辦進度，另外該系統亦可以圖表化呈現各類資料分析結果，英國司法單位也認同從系統產出移送卷證文件之證據力。

圖 2：參訪人員與兇殺及重案指揮課組長合影照片

(二)反恐辦公室(Counter Terrorism Command)

1.單位介紹：

反恐辦公室（CTC）或稱 SO15 是倫敦警察廳下的一個特殊單位。2006 年 10 月，反恐怖主義部門（SO13）和特別部門（SO12） 合併成立了反恐怖主義辦公室，結合了情報、行動和調查能量形成了一個單一的指揮部。該單位包含 1,500 多名警官和工作人員，以及一些駐外調查人員。該單位的首要任務是維護公眾安全，並通過以下方式瓦解英國境內與海外相關的恐怖主義活動：

(1)尋找、調查和預防恐怖攻擊威脅和脈絡。

(2)政府間跨單位合作，以獲取和使用有關恐怖主義和極端主義的情報和證據。

(3)確保集中力量打擊恐怖主義活動，以實現物有所值、提高生產力及有效率地利用政府資源。

(4)中央與地方及跨國間合作，互相分享相關情報、技術與經驗，以共同打擊恐怖主義威脅。

(5)與民間企業及合作夥伴、機構、團體等合作，提供建議和支持，以瓦解導致恐怖主義和極端主義的意識形態。

(6)透過支援、分工合作以維持國家反恐網脈，以完成英國的反恐警務。

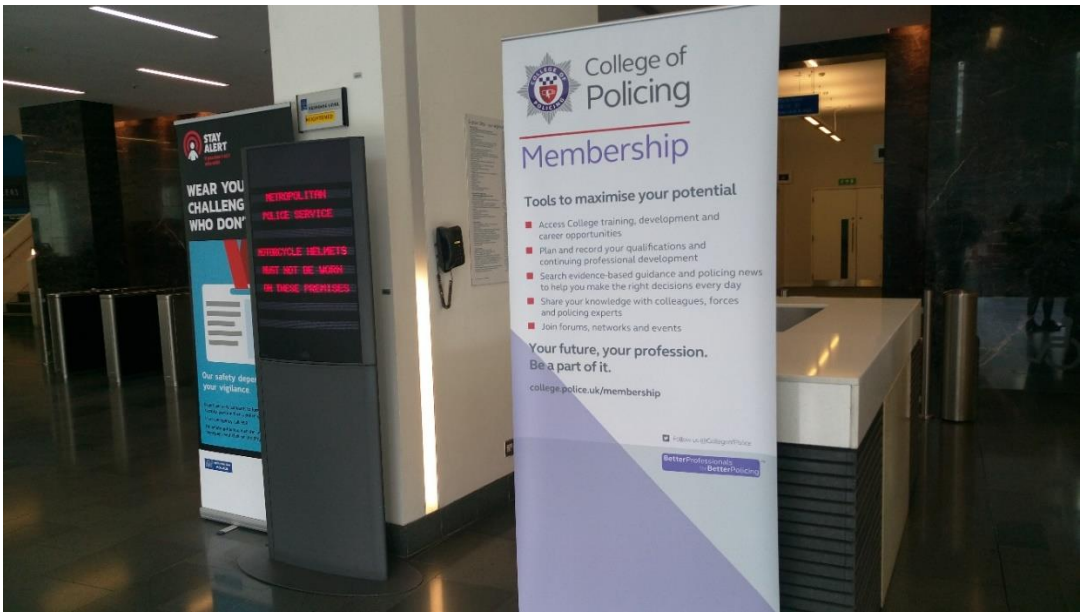

圖 3：反恐辦公室大廳

2.參訪過程

本次參訪由 Conrad Wiid 先生接待，除了介紹該單位的任務之外，也介紹了目前對於該國反恐任務中相當重要的影像辨識系統 DBEU（Digital Biometric Exploitation Unit），雙方並就實務運作、影像來源、使用技術等方面進行交流。

該系統提供國家數位開發服務 NDES(National Digital Exploitation Service)，包含下列功能：

-通信數據開發 communications data exploitation

-數位媒體開發 digital media exploitation

-技術創新與發展 technical innovation & development

-開源軟體開發 open source exploitation

-依法攔截 lanful intercept

-數位生物辨識開發 digital biometric exploitation

該系統的影像來源大多來自廣泛設置於各交通樞紐（如地鐵、車

站）等人潮眾多的地方所架設的超高清監視攝影鏡頭（CCTV），鏡頭則專門針對人臉及人體進行拍攝，其主要目的在於避免及預防恐怖攻擊的發生；與我國不同的是，該國為了反恐任務，特別由專人就各 CCTV 所拍攝到的影像進行截圖上傳，除了最基本的人臉以外，亦包含了受關注對象的手提包、背包、鞋底圖案、錢包或信用卡外觀、嘴唇、手部青筋、鬍子、痣或疤痕等清晰截圖（部分資料來自刑事案件破案後嫌犯的相關資料，及民眾自行上傳提供之資料），提供「小物辨識」功能使用。因英國人民沒有身分證，且受限於個人資料保護等法規，該系統的辨識基礎影像比對來源為前述警方自己所收集、上傳之資料，且不提供即時影像辨識功能；該系統結合了 NeoFace、Cognitec 及 Micro Focus 等三種辨識引擎，分屬不同公司的三種演算法同時進行比對，針對比對目標，會分引擎依序列出相似度最高的前 500 張圖片原始檔供參考。

圖 4：英國 Liverpool 地鐵站某出口監視器

受限於該國高度保護人民基本隱私權益的法規，該國執法單位無法自行使用影像辨識系統，全英國僅該辦公室 12 人擁有權限，執法人員可依規定向反恐辦公室提出影像辨識需求申請，由專人接受申請後，將欲比對的圖片經由系統比對並判斷後，會將比對結果告訴申請單位，且該比對結果僅能做為參考，無法做為直接證據，不受司法單位認同。

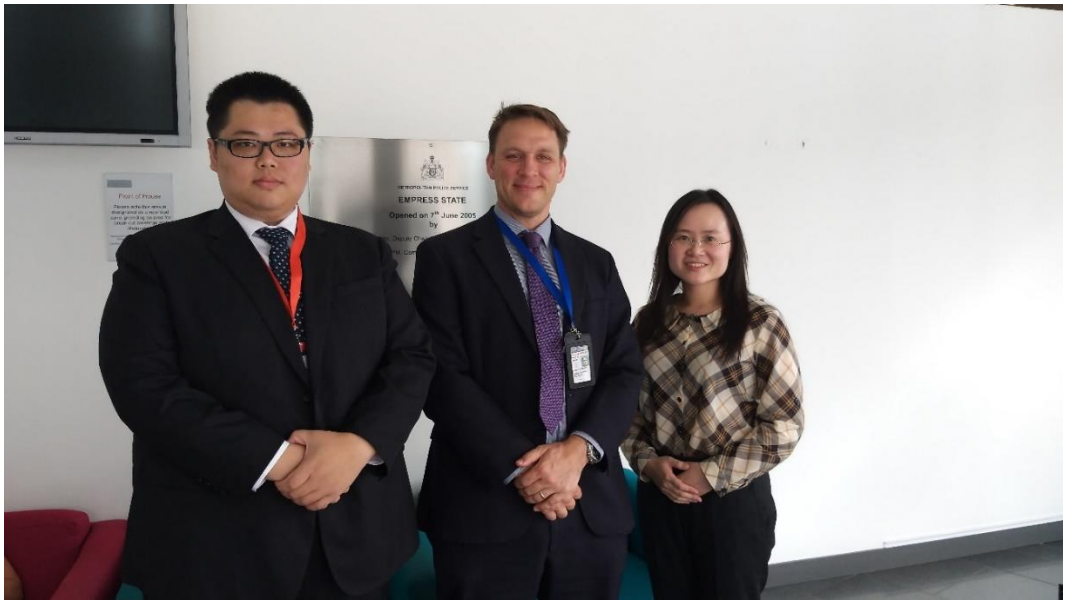

圖 5：參訪人員與反恐辦公室 Conrad Wiid 合影照片

(三)皮爾中心-亨登警察學院（Peel Centre - Hendon Police College）

1.單位介紹：

亨登警察學院隸屬倫敦警察廳下，做為大倫敦地區的警察培訓中心。該單位目前的正式名稱是皮爾中心（Peel Centre），但在警界仍習慣使用舊名，通稱為 Peel House，並以「Hendon」做為簡稱。

該中心由培訓主任和協調員管理，負責監督新進警察人員培訓。Hendon 做為三個地區培訓中心之一，新進警察人員必須參加該培訓中心為期 13 週的課程（以有給薪實習生身份參加）。此外，所有特別警察（Special constables，類似我國義勇警察，為民眾自願參加，經過訓練後，可以在一定程度上可以協助警員執行各項勤務，並能獲得政府給予的少量津貼補助)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）中完成剩下的 23 天課程（可於一般上班日密集訓練，或選擇於假日受訓）。該中心設計許多有關警察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。此外，在職員警也必須定期返回中心接受訓練以精進相關執法技能。

圖 6：皮爾中心正門外觀照片

2.參訪過程：

本次參訪該訓練中心，由多位負責不同課程的主管分別介紹各類訓練項目，包含資訊系統訓練、專業資訊人員培訓、駕駛技術訓練、偵訊攻防訓練、九頭蛇系統（Hydra）等，雙方並就實務運作及訓練等交換意見。

資訊系統訓練(包含前面提到的 HOLMES 系統，在參訪過程中正好有該系統的訓練課程在進行中)，類似我國各類警政資訊系統常年訓練，而專業資訊人員培訓亦類似我國目前正在辦理資料分析專業課程，針對警察資訊人員進行更專業化的培訓。

偵訊攻防訓練係由各學員針對教官指定的情境，分別扮演嫌犯及偵訊人員，來嘗試各種在實務上會遇到的狀況以練習如何進行有效的偵訊，增進偵訊技巧，教官會在一旁記錄所有過程，並於事後與學員進行討論。該訓練亦與專業表演公司合作，聘請專業演員扮演受偵訊人員，以提升訓練效果。

而由 Jonathan Crego MBE 教授設計的 Hydra 系統，是一種身臨其境的互動式培訓模擬環境，可提供演練以幫助決策者更好地管理重大事件。該方法提供了高度真實的事件模擬，使執法人員能夠實時響應緊迫的重大事件，並探討事件發生時採取的行動及策略，對機關及大眾的影響。教

官們將學員不分階級、機關及專業領域，以每組 3-4 人進行分組，分別在不同的模擬情境室（Syndicate Room）進行模擬，教官會在控制中心播放由專業演員模擬實務狀況的影片，由各分組學員討論遇到此情形時要如何處理，在有限的時間內取得共識後，在模擬情境室即時輸入決策作為，控制中心的教官會依照各組學員的應答方式，來決定下一個影片片段改變案件走向，於大約 45 分鐘的過程中結束該次訓練主題，並再次召集所有學員到教室中討論每一組學員的應對方式及理由，以共同精進。此過程不僅能夠記錄各種困難且即時的決定，亦可分享各種不同階級及領域的學員豐富且詳盡的經驗，且訓練有素的教官在情境模擬練習中，也可以透過麥克風即時對話，進一步討論過程中如何進行決策。

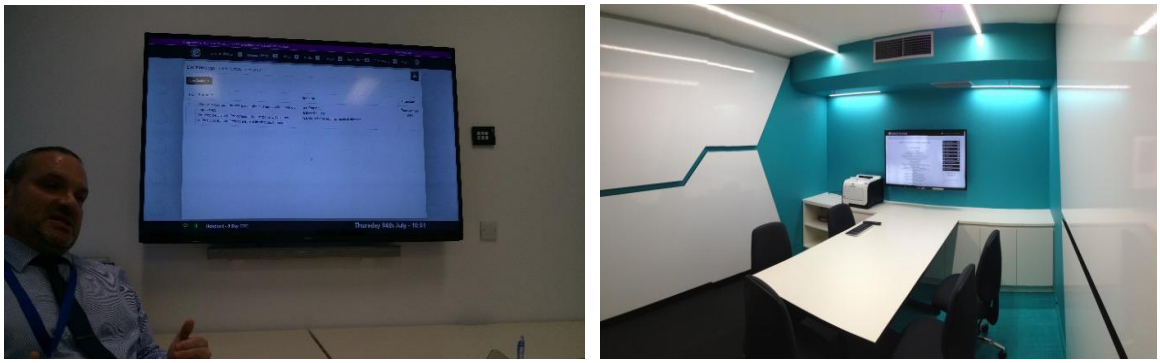

圖 7：模擬情境室（Syndicate Room）照片

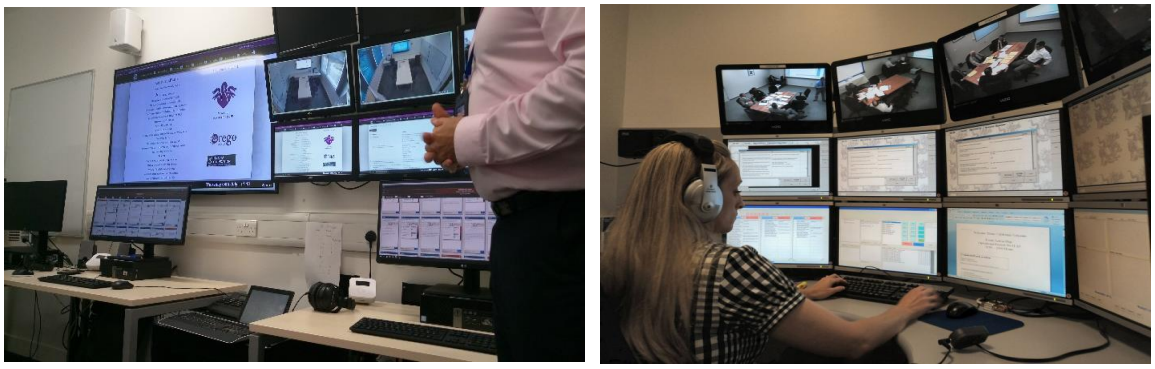

圖 8：Hydra 控制中心照片

Hydra 方法已經發展了 25 年多，最新版本的「Hydra in the Cloud」（HITC）提供了許多附加的學習方法和遠端功能。由於網路化的關係，它幾乎可以在任何可以連網的地方進行訓練，從而實現 Hydra 這種沈浸式教學方法的全球化。

Hydra 最初旨在協助英國境內的警察和消防部門處理重大事件。Hydra Foundation 從過去到未來都將繼續免費提供 Hydra 軟體、所有更新及客戶服務給英國警察及消防部門。對於其他機構，則會收取技術支援和培訓費用。

圖 9：參訪人員與皮爾中心主管合影照片

二、國家詐騙情資局（National Fraud Intelligence Bureau）

(一)單位介紹

國家欺詐情資局是英國專責打擊詐欺的警察部門，負責收集和分析有關欺詐和經濟犯罪的網絡犯罪情報。NFIB 成立於 2006 年，由倫敦金融城警察局管理並監督，為該國經濟犯罪調查領導者之一。

NFIB 分析的資料來源來自公共部門和私人企業的許多單位，包括工業、商業和政府單位。執法部門和私人企業背景的調查人員分析了欺詐活動和行為的不同模式的原始資料。當發現一定模式時（例如找出持續犯罪者或相關活動），其情資報告將發送給相關地區的執法單位進行調查，除了英國國內，甚至也包含海外調查。企業和警方可以使用名為「Action Fraud」的國家欺詐通報服務向 NFIB 舉報欺詐犯罪行為，而目前大約有 90 名非警職的調查員在倫敦金融城的 NFIB 工作。

(二)參訪過程

國家詐欺通報服務中心（Action Fraud）是英國針對欺詐和財務驅動的網絡犯罪的國家通報服務，類似本署 165 反詐騙平臺，該服務由倫敦

金融城警察局與國家欺詐情資局（NFIB）共同運作。本次參訪由 Action Fraud 的 Emma Brown 女士進行接待，介紹了國家詐騙情資局與國家詐欺通報服務中心對於詐欺案件的合作模式，與本國 165 反詐騙平臺與各警察機關間運作的模式極度類似，雙方就實務運作及服務中心與警察單位合作模式交換意見。

在國家欺詐管理局於 2014 年 3 月關閉後，相關業務被轉移到倫敦市警察局，Action Fraud 有一個公開給民眾的網站和服務中心，提供各種不同類型的欺詐諮詢與預防建議。個人和企業可以在其網站上或通過電話向 Action Fraud 尋求諮詢幫助（例如將電子郵件轉發給 Action Fraud 確認是否為詐欺內容），該諮詢服務亦有提供多國語言專人服務。Action Fraud 只處理正在進行中的詐欺行為，意即，民眾一旦受騙、有財產損失時，便已超出 Action Fraud 的業務範疇，只能去警局報案，與本國 165 專線處理模式相同，平均每個月都有超過 40,000 筆通報詐欺紀錄。較為先進的是，當英國民眾向 Action Fraud 諮詢時，將獲得犯罪參考編號（類似報案編號），並將其案件轉交給國家欺詐情資局，受理後 28 天內民眾可透過登入網站帳號，得知所通報案件的處理進度，受理超過 28 天的案件才接受電話詢問。

圖 10：參訪人員與 Action Fraud 人員 Emma Brown 合影照片

三、刑事紀錄局(ACRO Criminal Record Office)

(一)單位介紹

ACRO 刑事紀錄局是為了提供更安全社區工作而設立的國家警察部門，該局成立於 2006 年（前身為 ACPO 犯罪紀錄辦公室），目的是建立一個以業務為重點的單位，以組織犯罪紀錄資料的管理，並改善犯罪紀錄和生物資訊之間的關聯。

自那時起，該部門發展迅速，目前擁有 300 多名員工。ACRO 於 2017 年被英國女皇的警察監察局認可，為英國警察部門提供「優秀」和「至關重要」的服務，其工作被認為是社區安全的基礎。

作為該國犯罪紀錄和生物識別資訊領域的領導者，ACRO 刑事紀錄局提供一系列服務，包含為執法和公共保護單位提供幫助、協助將違法者繩之以法，及滿足公眾的合法資訊和管理需求。ACRO 任務如下：

-提供有效和國家認證的犯罪紀錄資訊服務

-開發、擴展和推廣相關的服務及其新增需求

-領導犯罪紀錄資料服務領域，提供專家建議、指導和支援

(二)參訪過程：

本次參訪由刑事紀錄局 Michael Scott 介紹該國刑事犯罪紀錄業務及系統，雙方並就實務運作與系統設計進行交流。

ACRO 負責管理英國刑事紀錄交換中心（UKCA-ECR），該機構與其他歐盟成員國家交換判決確定之犯罪紀錄資料。在歐盟以外，則通過國際刑警組織管道與所有非歐盟國際刑警組織國家交換重要犯罪紀錄（如性侵嫌犯資料）。

ACRO 也向一般民眾提供服務，包括提供如 DVS、ICPC 等警察證明，以及紀錄刪除請求等服務。對於非警察機構，則提供調查和起訴的國家警察犯罪紀錄（Police National Computer services，PNC）服務。並確保 PNC 隨時更新當前的犯罪紀錄資料，警察人員可以查詢和使用這些資料來調查犯罪並保護公眾。

圖 11：參訪人員與刑事紀錄局 Michael Scott 合影照片(左一為鄭秘書翔徽)

四、波蘭警察成立 100 週年酒會

本次很榮幸受邀參加於波蘭駐英國大使館之波蘭警察成立 100 週年酒會，英國各警察單位亦有派員參加。活動開始時，由波蘭大使、警察最高領導人及警察代表進行致詞，同時播放員警因公殉職基金會募款影片，該基金會提供因公殉職的員警配偶及子女們心理諮詢、教育補助等協助，並定期舉辦各類活動，而其資金來源則來自民眾捐款及各種活動的募資。

隨後進行相關宣示並完成典禮儀式，之後於餐會中與多名英國各警察單位人員就雙方許多業務、行政流程進行交流。

圖 12：參訪人員參加活動照片

圖 13：波蘭警方代表致詞

圖 14：參訪人員與倫敦警察廳高階警官合影照片

五、Google Deep Mind 團隊

(一)背景介紹

1.Google Deep Mind 團隊是一個由科學家，工程師，機器學習專家等組成的團隊，共同致力於推動人工智慧領域的發展。其技術用於廣泛的公共利益和科學發現，並與其他人就重大挑戰進行合作。

圖 15：Google 公司位於倫敦分部及一旁正在新建的 Google 大樓照片

該團隊非常重視大數據資料，並認為它有能力用來解決問題、發現創意，並創造科學突破，構建今天生活的世界。以下引用該團隊的發言，可生動了解該團隊的核心精神：「目前仍有許多尚未發現的新知識新方法等待著我們，對改善人們福祉和環境的諸多挑戰也不小。就像哈伯望遠鏡可以幫助我們更深入地了解太空一樣，我們的目標是建立先進的人工智慧（AI，有時也稱為 Artificial General Intelligence-AGI）以擴展知識並找到新的解決方案，相信可以幫助人們解決成千上萬的問題。」

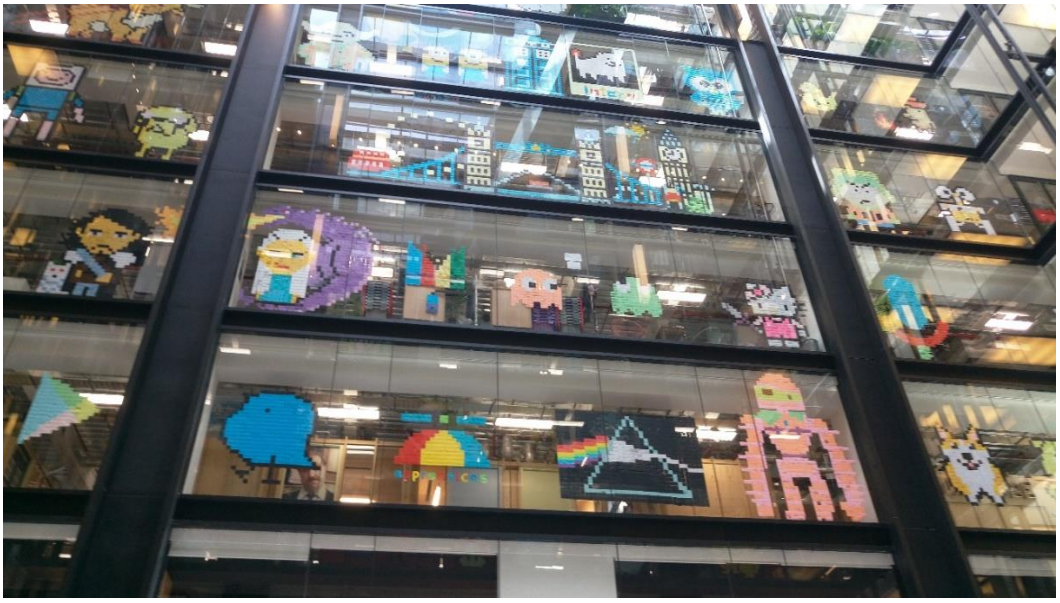

圖 16：Google 公司倫敦分部大廳照片

2.最新的研究成果：

(1)科學突破

這些產品建立在自然，科學和其他科學相關期刊上發表的突破上。相較於許多尚未解決的研究問題，該團隊較為注重的是強化系統自我創造力，以及自身於解決問題能力方面取得的進展。

(2)現實生活的影響

該團隊經常與各領域專家合作，挑戰將進階應用於現實生活的方法。到目前為止，該團隊已經建置了一些系統來幫助如節約能源，辨識眼睛疾病等能解決民眾重要議題的系統，致力於加速科學發展，並持續改進世界各地的 Google 產品。

(3)最新研究

Deep Mind 致力於解決電腦科學中一些最複雜的挑戰，擁有一系列包括神經科學、機器學習、機器人、程式語言、影像辨識等相關研究和出版物，如聞名全球的 AlphaGo（擊敗專業棋士的阿爾法圍棋電腦）及 AlphaStar（知名即時戰略遊戲《星海爭霸2》的 AI 核心引擎）。

(二)參訪過程：

本次參訪由中華民國駐英國代表處科技組吳組長俊輝陪同，與 Google Deep mind 團隊進行雙方人工智慧之深度強化學習、類神經網路等技術及應用進行交流，以做為我國發展警政 AI 的參考。

圖 17：與 Google Deep Mind 團隊成員合影照片（左一為吳組長）

參、Jane's OSINT 公開情資資料分析培訓課程

一、課程起源與介紹：

Jane's 在分析研究航空、國防和安全方面領域擁有超過 100 年的豐富經驗。該團隊著名的國防專業知識可幫助企業優化運營並降低商業風險，從而做出更具影響力的決策。

Jane's 在全球擁有 200 多位分析師和內部的 2,000 多位專業領域專家，並借助 34 個國家及地區的 15,500 多名 IHS Markit 同事的專業知識，提供了國際視野和第一手的資料蒐集及分析服務。

二、參訓地點：

本次課程由 Jane's 主辦，訓練地點係位於英國倫敦 Ropemaker Street 的 IHS Markit 總公司。

圖 18：IHS Markit 公司大樓外觀及前台

三、課程成員:

本次參訓課程由 Terry Pattar 先生擔任講師，Pattar 先生為 Jane's 情報部的副主任，該部為國家安全和政府單位提供威脅評估、視野掃描、能力分析和公開情資（OSINT）建議。

Pattar 先生負責管理 Jane's 的 OSINT 和情報分析培訓課程的計劃設計與交付。他在各種調查和諮詢職位上擁有 17 年的經驗，其中包括為國家安全和政府單位提供 Jane's 定制的分析產品和培訓服務長達 10 年，以及一年作為海灣地區顧問進行盡職調查的經驗。Pattar 先生專門研究分析對地區穩定

和全球安全的新威脅，並協助發展軍事和安全部隊的能力。他的專長是反恐情報分析，並在中東、北非和南亞擁有特定的地區專業知識。在埃克塞特大學期間，他閱讀阿拉伯語言和文學，以及中東和北非的政治和歷史。並擁有英國倫敦大學東方與非洲研究學院的近東和中東研究文學碩士學位。

圖 19：參訓人員與講師 Terry Pattar 合影

本次參加課程學員共計 16 人，除筆者 2 人外，還有英國當地不同政府單位資料分析師、來自美國執法機關的資料分析人員，還有其他來自民間企業如 Google 分析師、情資分析人員及跨國公司老闆等，學員背景廣泛。

圖 20：參訓學員

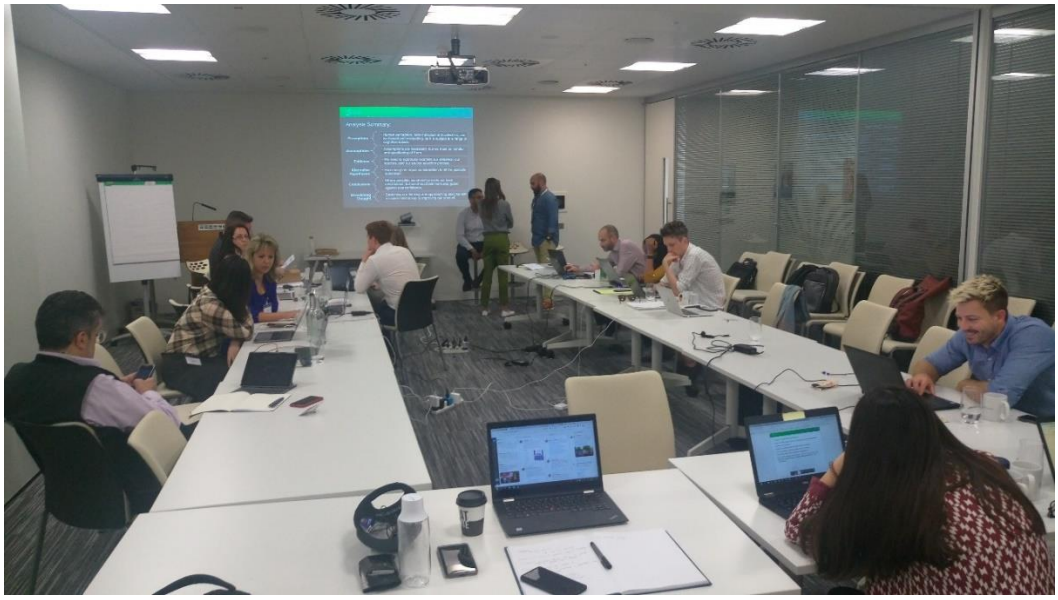

圖 21：OSINT 分組討論實況

四、課程內容：

(一)OSINT 的定義

- 情報 Intelligence：收集、匯整、評估並用於回答特定問題的資訊。
- 開源軟體 Open Source：公開訊息。

OSINT 不僅僅是簡單的研究和分析。該術語意味著達成進行不透露正在收集該資訊研究的目的。OSINT 還意味著研究活動是更廣泛的情報過程的一部分。

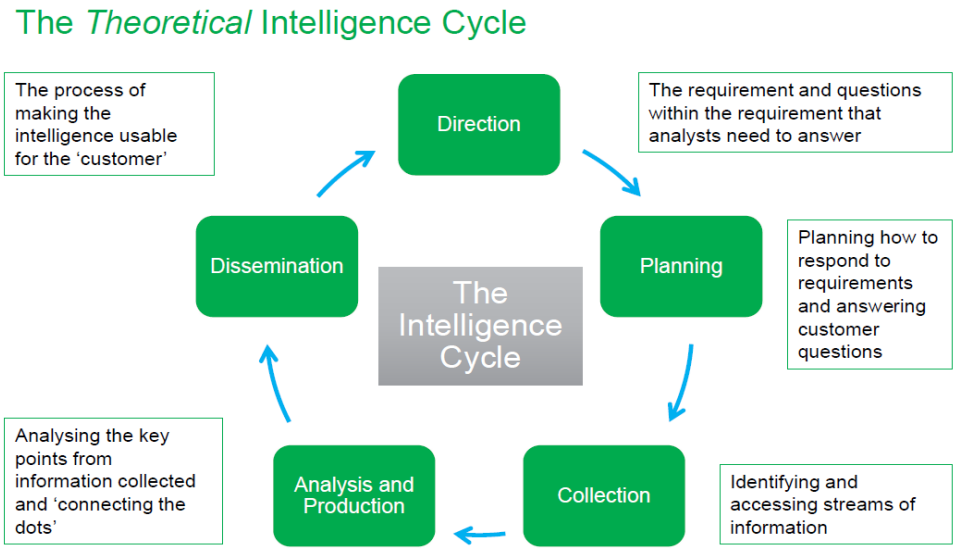

圖 22：情報理論分析循環

(二)OSINT 公開情資資料分析課程總計三天，課程內容主要分為 8 個章節，各章節內容依序簡要說明如下:

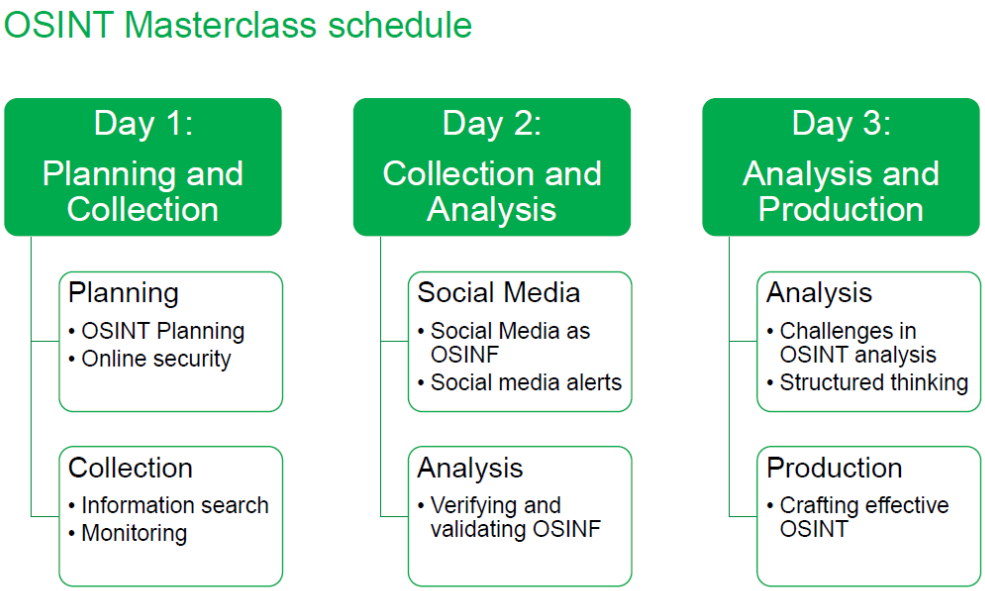

圖 23：Jane's OSINT 公開情資資料分析培訓課程表

1.規劃 Planning

(1)標的：

●練習創建有條理的計劃以提高 OSINT 流程的效率。

●分解要求以確保為特定客戶回答正確的問題。

●確定初始來源以準備資訊收集。

●練習使用計劃清單。

(2)規劃階段的三大步驟：

●客戶 Customer：

※誰是客戶？

※他們要求什麼？

※他們想要問什麼？

※截止日期？

●需求 Requirement：

※需要解決什麼問題？

※希望產出的結果模式為何？

●來源 Sources：

※那些資訊是我們需要的?

※要從哪裡取得這些資訊?

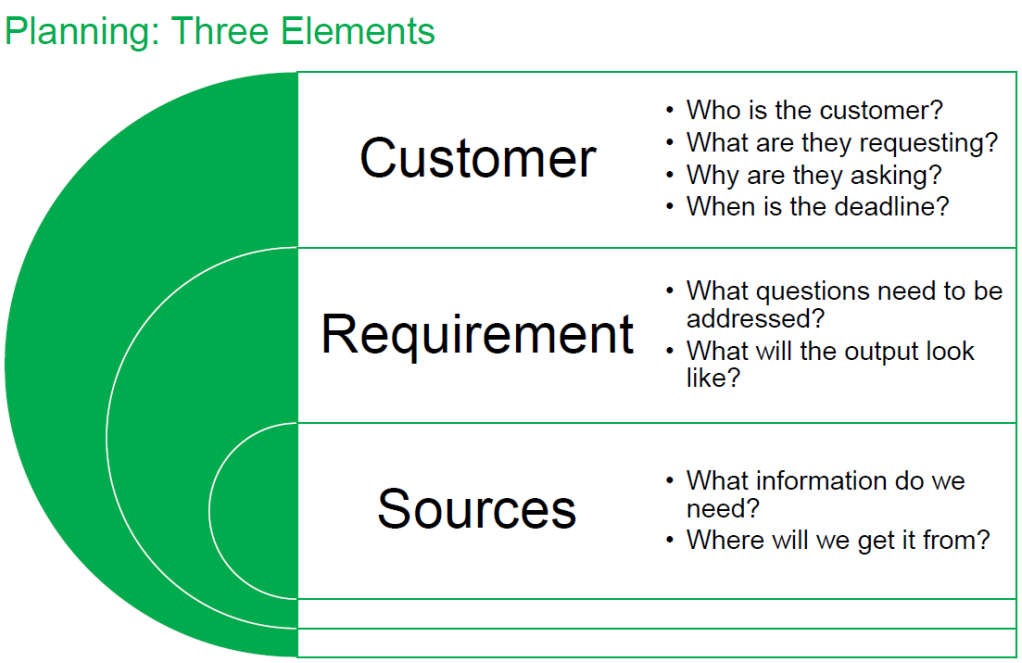

圖 24：規劃階段的三大步驟

(3)A 計畫-了解客戶：

為了幫助塑造我們的 OSINT 研究和分析過程，分析師可以從建立需求的背景中受益。我們應該向客戶詢問以下問題，以便為我們提供更多背景資訊：

●最終用戶：誰提供資訊？

●發動者：是什麼促使了這個需求？

●目標：需求的目的是什麼？

●格式：應該採用什麼格式？

●詳情：他們需要什麼級別的細節？

(4)B 計畫-做出聰明的假設

在不受特定客戶指導的情況下，我們需要對客戶做出聰明的假設，以產出最終報告或簡報。考慮以下問題會很有幫助：

●誰將閱讀此報告？

●他們可能會根據報告的結論採取什麼行動？

●報告中需要解決哪些關鍵問題，以幫助接受資訊的人員採取適當的行動或做出決定？

●他們可能會花多少時間吸收這份報告上資料？

有時我們無法回答以上所有問題，但對接受資訊的人員及其要求的理解越清楚，我們的研究方向就越明確。

(5)了解需求

除了定義客戶或接受資訊的人員之外，我們還需要關注需求的細節：

●客戶真正想知道什麼？

●要求中的定義是否有認知上的不同？

●他們的要求可行嗎？

●他們的要求是否已經在其他地方得到解決？

我們的目的是澄清任何認知上的不同，並更明確地定義要求的範圍，以進一步集中我們的研究工作。我們還應該記下我們所做的任何假設。

(6)創造子問題

將已識別的關鍵概念轉變為可回答的子問題

提供了分析人員可以在其資訊收集中解決的要點的簡化列表。

●資訊：

※關鍵資訊：Who? Where? When? How many?

※原因：How? Why?

※效果：近期的短期影響是什麼？

●分析：

※碰撞：會產生什麼影響？ 誰會受到影響？

※這將如何影響客戶：對近期/中期/長期的影響是什麼？

※響應：客戶是否可能需要進一步的 OSINT 來幫助他們進行規劃或決策？

(7)資料來源

思考從何處獲取所需資訊，將有助於解決以下問題：

●我們可能需要哪種類型的資源？

●我們已經知道哪些相關來源？

●我們有哪些可用資源？

有時候我們在面對分析不熟悉的需求主題時，會自然而然的使用搜尋引擎做為首選，但如果從一開始就確定任何潛在且有效的訊息來源會非常有幫助。

(8)確認來源

考慮是否使用以下類型的開源資料：

●離線資料，例如：詢問一個職員。

●政府或官方消息來源

●智囊團、非政府組織、研究機構、慈善機構。

●媒體/新聞來源及專業出版物

●學術文獻。

●數據庫。

●其他。

在進行此步驟時，有必要先考慮所有潛在來源，然後再進行精煉。

(9)研究計畫

結構性的研究計畫應包含下列細節：

●最後期限 Deadline：將最後期限保持在計劃的頂部對於計劃 OSINT 流程的里程碑至關重要。

●顧客 Customer：了解客戶可確保我們牢記 OSINT 的目標。

●需求 Requirement：需要回答的具體問題應該是我們計劃的重點。

●來源 Sources：列出類別和特定來源對於提高收集資料過程的效率至關重要。

●產出 Output：輸出所需的格式決定了所收集資訊的數量和類型

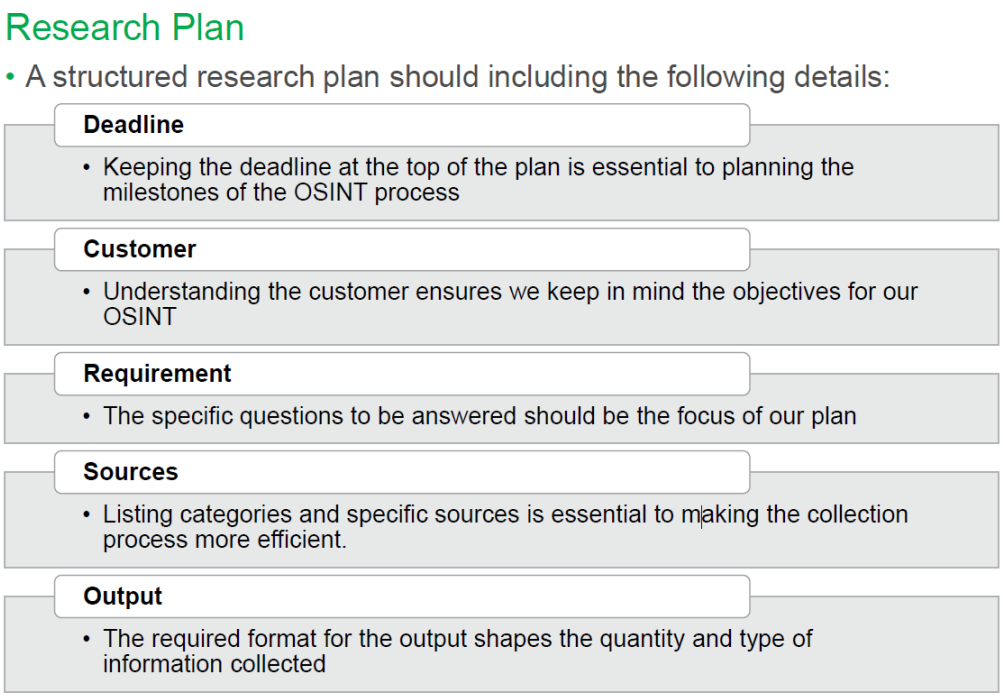

圖 25：結構性的研究計畫

(10)管理並彙整搜索結果

在搜索並收集各類資訊時，分析師應將其記錄到他們的研究計劃中，列出每個項目的基本詳細資訊，例如：

●校對：

※資源

※標題

※日期

※重點摘要

●分類：透過使用此方法，可以針對特定的子問題來追蹤如何找到資訊並統計發現了那些資訊，這有助於校正最終產品的資訊。

●管理：透過使用此方法，分析人員可以快速確定何時獲得了足夠的資訊。

●截止：也許最大的挑戰是知道何時該停止收集資訊，但是設置搜尋限制是必不可少的。

(11) 需求清單

使用需求清單可以幫助分析人員解決需求的具體問題，常用需

求清單範例：

●需要回答的關鍵情報問題是什麼？

●客戶需要哪種格式的產品？

●為什麼這個問題很重要？

●我的分析會做出什麼貢獻？

(12)評估清單

使用評估清單協助分析師計畫收集資料的過程，可以讓整個蒐集情資的過程更有效率，常用評估清單範例：

●我將從哪裡獲得想要的資訊？

●我們可以從哪些基本資訊開始收集？

●我還能如何識別有用的資源？

●這個問題有人回答過嗎？

(13)規劃技巧

這些技巧將協助從分析需求轉變到開始信息收集過程：

●在開始資料搜索之前，請嘗試識別並弄清問題中對需求定義的任何不同認知、矛盾或不正確之處。

●搜尋和收集資料的過程中最大的限制就是不清楚問題的內容或錯誤認知，而此狀況將可能導致提供客戶錯誤的答案。

●對於構造不當的問題也會帶來資訊量爆炸的挑戰，導致不知道何時該停止資訊收集。

●始終嘗試提出一個可回答的問題，該問題具有特定的定義的結果，並且足夠清楚地知道何時找到了答案。

2.網路安全 Online Security

(1)標的

●討論基本的網路安全。

●探索在線隱私的挑戰，例如我們的「數位足跡」。

●檢查網路足跡追溯如何影響我們資訊的客觀性。

●學習良好做法以減少資安漏洞。

(2)當我們進行以網路為資料來源的研究時，存在幾個漏洞：

●網路安全。

●電腦安全。

●瀏覽行為。

●個人信息。

(3) OSINT 風險

OSINT 分析師每天大部分時間都在上網，收集和提供資訊。

●數位足跡→我們在線活動的足跡。

●線上影子→有關我們的可用信息。

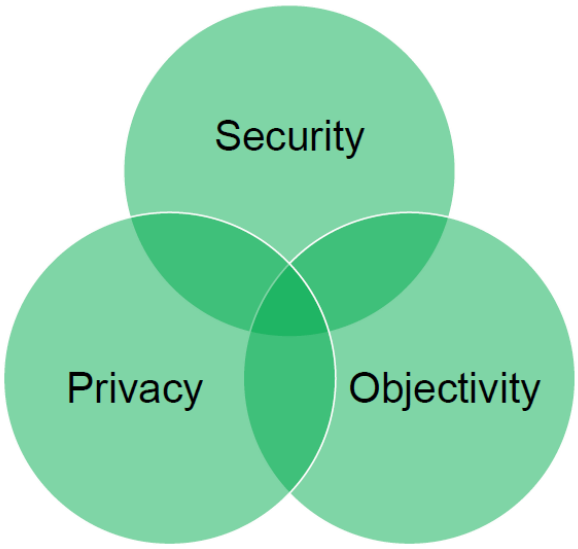

圖 26：三個關鍵問題：安全性，隱私性和客觀性

(4) 隱私權：數位足跡

在網上瀏覽時，會留下「數位足跡」的踪影。

網站會自動收集有關下列訊息：

當訪問網站時，可以輕鬆確定你的 IP 地址、機器類型和螢幕尺寸。還可以通過搜索字詞或您上次訪問的網站來查看你如何到達該網站。你的位置可以通過交叉引用你的 IP 地址和其他數據來找到。Cookies 也用於追溯紀錄你的活動。

(5) 隱私權和安全性：減少來源

下面是兩種可以最大限度地減少讓自己的資訊被人獲知的方式，可以掩蓋瀏覽行動的來源，甚至行動本身：

●代理賜福器和虛擬專用網絡（VPN）有助於最大程度地減少我們在網上瀏覽時向他人顯示的資訊。

●Tor（洋蔥瀏覽器）是透過匿名瀏覽技術，將上網時所傳遞的訊息層層加密保護，從而達成隱藏用戶真實位置、避免網路監控及流量分析目的。

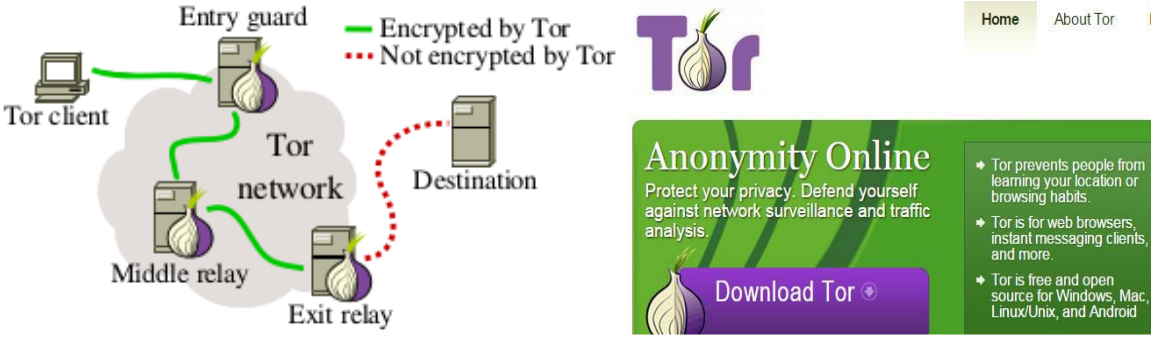

圖 27：洋蔥瀏覽器(Tor)示意圖

(6) 隱私和客觀性：過濾氣泡

線上服務，特別是那些免費為我們提供資料的服務，使用我們的數位足跡和線上影子(online shadows)來對我們進行介紹並提供「相關」廣告和鏈接。

這不僅會影響隱私，還會影響我們資訊的客觀性，因為它可能會導致我們陷入「過濾氣泡」(filter bubble)，在過濾氣泡中我們只能看到某些來源或面向。

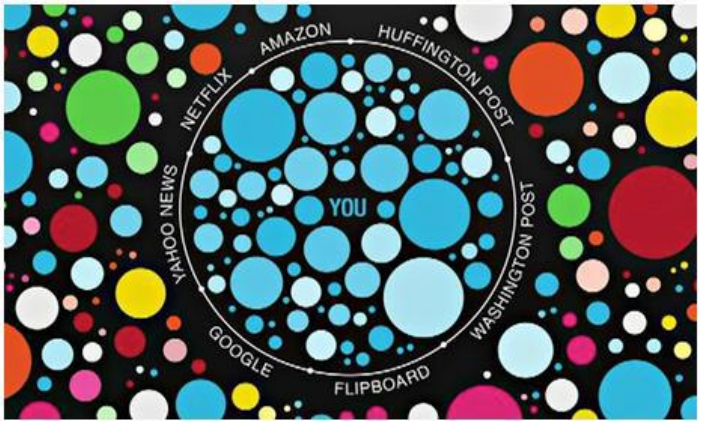

圖 28：過濾氣泡(filter bubble)

(7)安全性：減少漏洞

●社交媒體

※啟用安全/隱私功能以最大程度地減少線上影子。

※禁用記錄地理位置功能。

※警惕陌生人傳送的連結邀請。

●線上活動

※分散風險，例如使用不同的電子郵件來達成不同目的。

※考慮使用代理服務器，如 VPN 或 Tor 瀏覽器來減少來源。

※使用諸如 Privacy Badger 之類的插件來減少數位足跡。

●鏈接意識

※注意可能會要求您點擊的任何連結。

●下載注意事項

※僅接受來自受信任來源的附件，或從經過驗證的網站下載的附件。

3.收集 Collection-資料搜尋

(1)標的

●使用研究計劃來搜索所需的資料。

●了解使用策略性方法進行搜尋資料的好處。

●通過計劃關鍵字和捕獲資料來練習改善搜尋結果。

(2)我們在搜索什麼？

當我們在網路上進行搜尋時，通常會要求搜尋引擎將其關鍵字與索引中的文檔（例如網頁）互相匹配。

搜尋引擎無法為大量線上資料建立索引，例如商業級資料庫，而這些會構成「深層網絡」(Deep Web)。

有些資料則是故意隱藏的，可能是出於犯罪原因藏在「暗網」(Dark Web)中。

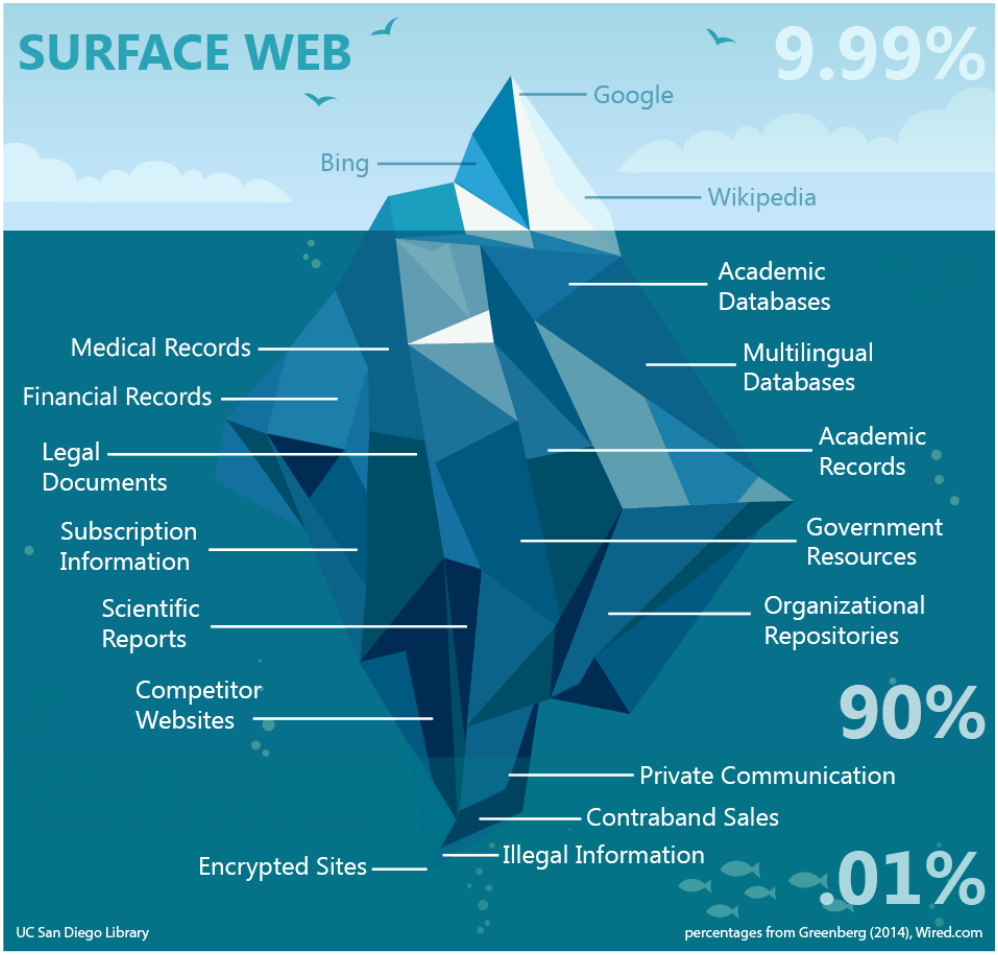

圖 29：一般網路、深網、暗網示意圖

(3)綜合搜尋

●術語

為了獲得有關指定主題的全面資料，我們應該使用大量的潛在關鍵字搜尋。嘗試使用以下類別來擴展關鍵字列表：

※替代條款(Alternative terms)

※相關條款(Related terms)

※縮寫(Abbreviations)

※技術詞彙(Technical terms)

※不同語言(Different languages)

●初始來源

關鍵字的良好初始資源包括：字典、百科全書、詞庫和數據源（書籍、期刊等）。

(4)術語-比照網頁的思考模式

為確保不會遺漏相關資料，必須了解想要搜尋的資料極易讓人產生反感。

資料來源將使用不同的單詞和術語來指向相同的主題或事件。

通過使用替代術語進行搜尋，可能會擴大資料搜尋結果的範圍。

(5)信息管理系統搜尋

在檢查來源時，盡量去注意有效的細節，例如：

●權威作家

●研究機構的名稱

●出版商名稱

●出版物名稱

●片語或句子，以及關鍵字的不同說法，例如拼寫方式、通用名或暱稱、翻譯、同音異義詞和同義詞等。

(6)搜尋技巧

在現有搜尋工具(如 Google)使用包含 AND、OR、NOT 等基礎語法將關鍵字、詞配合搜尋工具中的時間區段、語言、來源類型來更精確地找到想要的資訊。

4.資訊監控 Information Monitoring

(1)標的

●考慮監視技術的前後關係。

●探索幾種資訊監控方法。

●權衡公開資訊監控方法的實用性。

(2)Google 自定義搜尋引擎

透過登入 Google 帳號，並經過一系列的設定後，完成自定義搜尋，可以將搜尋的範圍大幅度的降低。

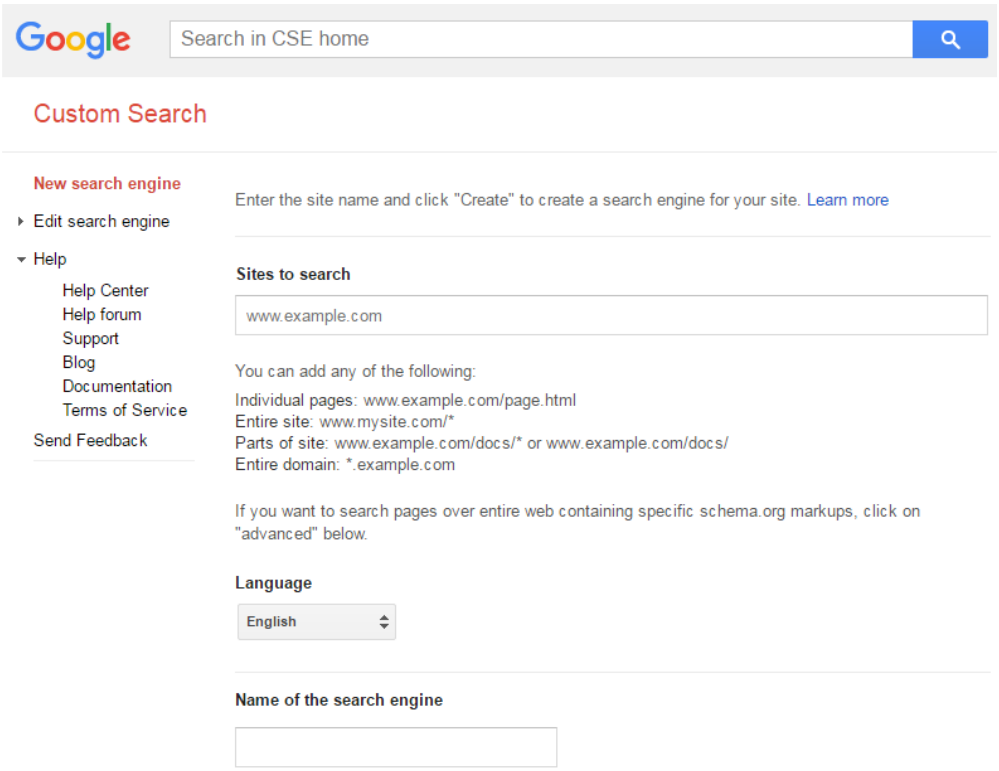

圖 30：Google 自定義搜尋引擎

(3)資訊監控基本方法

●新聞電子郵件警報：Google 新聞可以提供各種新聞來源的定期更新的有效資訊。

●新聞匯總：新聞聚合器將一個地方的各種新聞提要匯集到一起

●RSS 訂閱：仍在使用中，並由許多新聞來源和部落格發布

●商業工具：有一些潛在有用的商業工具具有免費版本，可以啟用新聞監視和篩選功能。

5.社群媒體 Social Media

(1)標的

●了解社群媒體的關鍵特徵如何影響我們的收集和分析過程。

●考慮將社群媒體用於情報目的的好處、潛在的陷阱和安全問題。

(2) 社群媒體的使用和挑戰

●社群媒體資訊將如何滿足您的需求？

●您想要的資訊是否可用？

●將分攤多少時間在搜尋社交媒體上的資料？

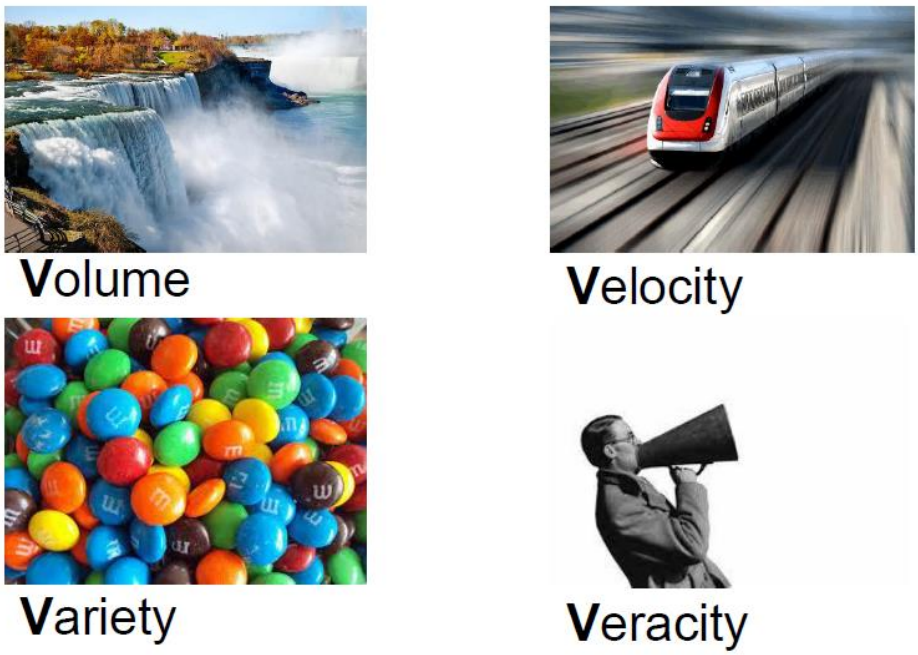

圖 31：4V(準確性、速率、總量、多變)

(3)種類：社群媒體平臺

社群媒體平臺類型的範圍很複雜，並且在不斷發展。

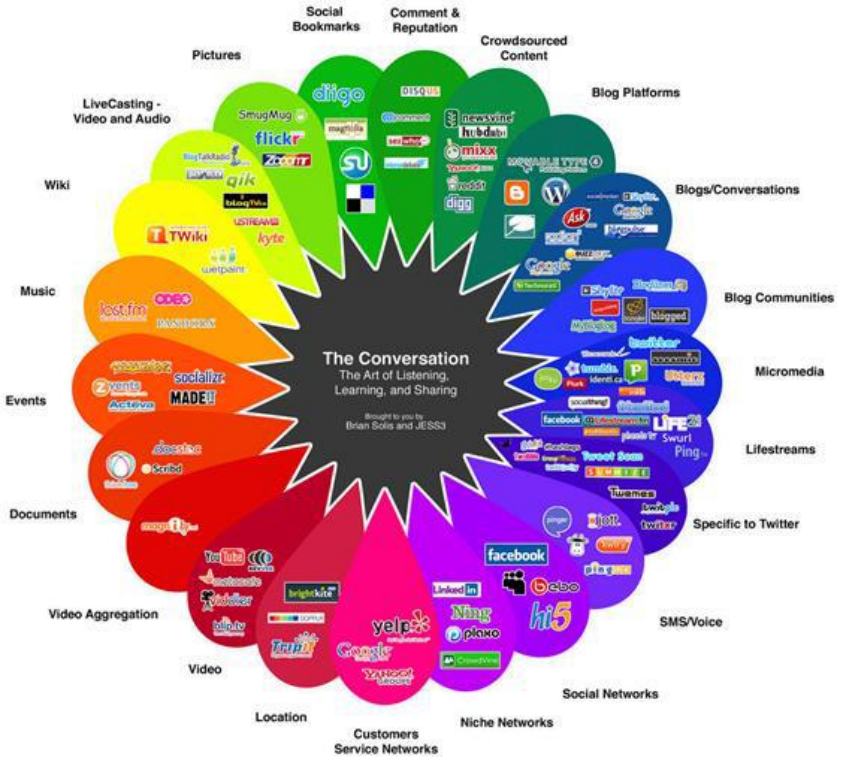

圖 32：現有的社群媒體

(4) 在社群媒體上收集資訊

●通過網站抓取收集大量數據：通常會獲取大量可公開獲得的社群媒體資訊（即不位於訪問控制後面的資料）的演算法。

●通過 API 進行批量數據收集：允許直接從平臺的開發人員獲取數據和元數據。

●人肉搜尋：透過公開搜尋、監控和手動調查技術。

(5) SOCMINT 信息環境

為了蒐集社群媒體情報，首先需要了解社群媒體的資料環境：

●在我們的地區/國家/地區有什麼可用的？

●那個地方的人們如何使用社群媒體？

●我們感興趣的對象使用哪些社群媒體平臺？

●我們需要開發什麼級別的訪問權限？

●潛在的風險是什麼？

(6) 法律和道德考慮

確保有能依循的法律依據。對於某些類型的社群媒體調查，政府部門和執法機構可能有必要申請適當的授權以進行社群媒體研究。

●仔細考慮您需要進行的研究類型。

●考慮一下您可能收集到的資訊類型。

●規劃過程中要解決的問題：

●可能會在多大程度上侵犯某人的隱私？

●是否需要所有這些資訊？

●資料要保存在哪裡？(考慮資料搜尋的風險）

●資料可以保留多長時間？

●是否需要在社群媒體平臺上建立假帳戶(角色)，以及是否違反服務條款。

●是否有違反其他法律的可能?

UK police levels of online investigation		
Level	**Descriptor**	**Required training**
1	Overt Open Source Investigation/ Research	Open Source Research – level 1
2	Covert Core Open Source Investigation/Research	Open Source Research – level 2
3	Covert Advanced Open Source Investigation/Research	Advanced Open Source Research – level 3
4	Network Investigations (Advanced Specialist Training)	Advanced Specialist Training
5	Undercover officer online/Covert Internet Investigator	Advanced Specialist Training

Source: IHS Markit/National Police Chiefs' Council (UK) © 2018 IHS Markit: 1740607

圖 33：英國警方在網路蒐集資料擁有的權限

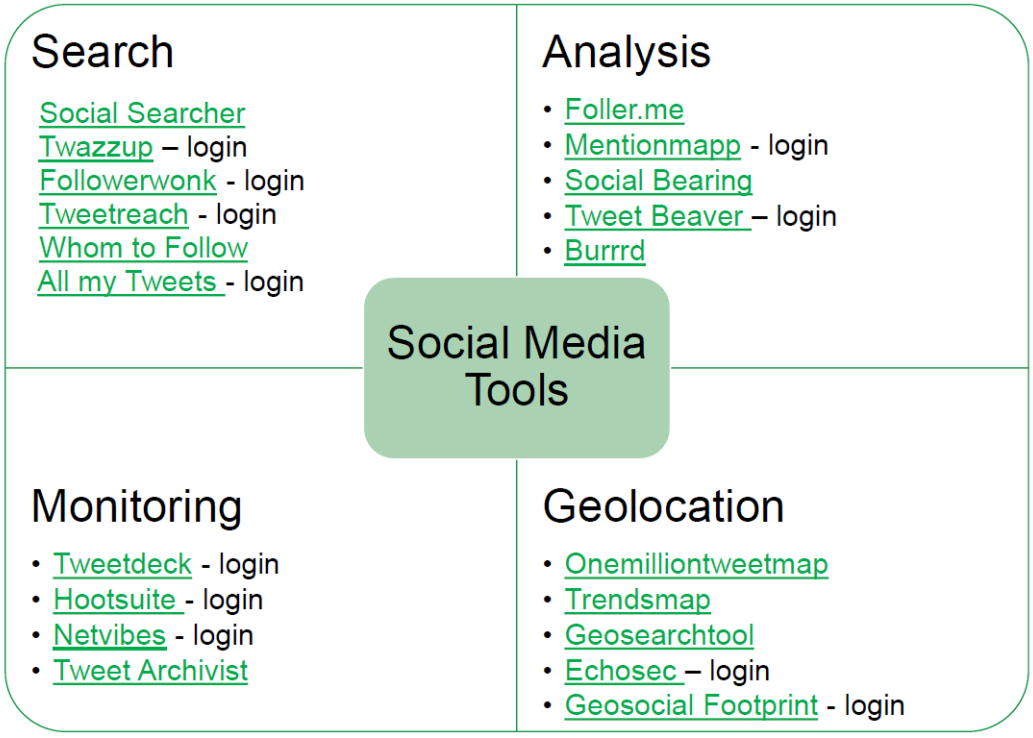

圖 34：社群媒體搜尋工具

6.驗證與確認 Verification and Validation

(1)標的

●了解以有條理的方式分析資料源的重要性。

●找出可以說明我們的資訊是否可靠的關鍵問題。

●嘗試使用一個簡單的清單來幫助分析人員查看其來源並對該資訊的可靠性進行更嚴格的評估。

(2) 驗證原則

●三角：在其他來源可用時使用多個來源，並且可能提供不同的觀點。

●交叉檢查：確認其他權威來源的關鍵訊息點。

●使用原始資料：如果可用，請使用原始資料，不要過度依賴輔助資源。

●資料來源限制：確定消息來源的背後是誰，以及他們的報告是否受到任何限制。

●確定故事和目標：了解消息來源呈現的故事，以及它是試圖說服還是影響閱讀者。

●字裡行間：嘗試在資料來源中辨別出其是否含有造假或誤導成分，無論明不明顯。

(3)假新聞議題

(4)以圖搜圖應用

圖 35：常用以圖搜圖工具

7.分析和結構化技術 Analysis and Structured Techniques

(1)標的

●檢查進行分析的過程。

●在分析過程中考慮潛在的陷阱。

●探索有助於我們分析的整理方法和分析框架。

●測試結構化技術以改善分析結果。

(2)分析

●分析的關鍵要素

資料分析需要應用人類判斷才能進行分類：

※從不重要的資料找出重要的資訊。

※從過時的資料找出適用的資訊。

※從不相關的資料找出有關聯的資訊

※從不信任的資料找出可以信任的資訊。

●信息與答案

※分析可以讓我們收集的資訊成為對客戶有用的關鍵。

※生產分析需要三個要素：前後文、聯繫、結論。

(3)兩種思維模式

●系統 1

※這是我們對日常情況進行思考和響應的快速或本能方式。

※通過觀察和學習熟悉的模式，我們建立起系統 1 的思考方式。

●系統 2

※深入思考，我們將其用於更困難的問題和挑戰。其過程較慢，也更加深入。

※我們的大腦自然是「懶惰的」，並且經常抵抗向系統 2 的轉變。

(4) 批判性思考

●批判性思考模式是系統 2 的核心，其定義為：

清晰而理性地思考的能力。包括參與反思和獨立思考的能力。具有批判性思考能力的人可以做到了解推測之間的邏輯關聯。

●我們會自然的在收集的資料之間建立關聯。

●這些關聯的本質成為了解釋因果關係的假設。這是我們在進行分析時自動尋找的東西。

●批判性思考涉及運用一種更有條理的方法來做出正確、有力的邏輯判斷。

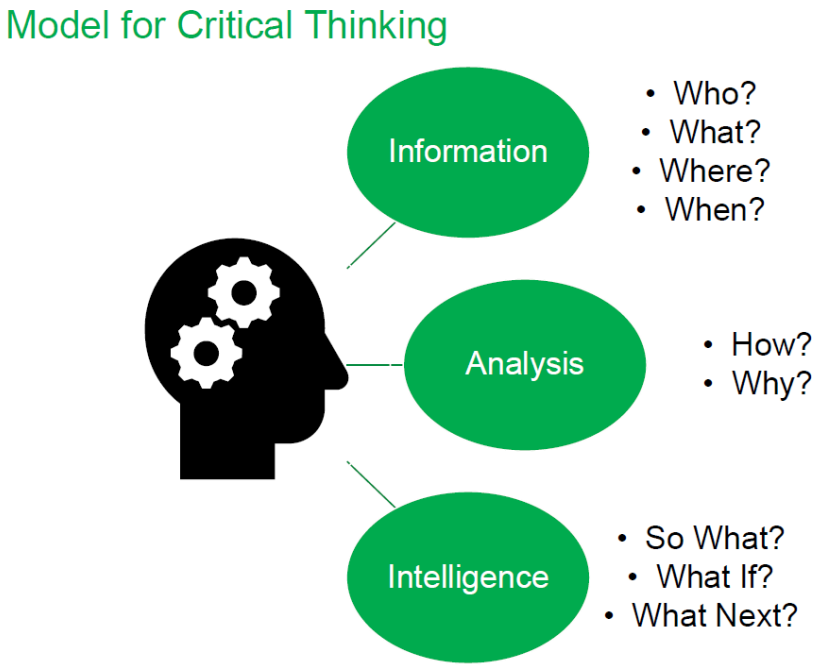

圖 36：批判性思考模式

(5)常見的認知偏見

●計劃謬誤 Planning fallacy

●確認偏差 Confirmation bias

●可用性偏差 Availability bias

●投影偏差 Projection bias

●錨定效果 Anchoring effect

●過度自信效應 Overconfidence effect

●偏見失明 Bias blindness

(6)線上資訊加劇了認知偏見

●認知偏見會影響：

※處理資料的能理

※理解力

※思考模式

※判斷錯誤

●線上搜尋的個性化設置可能會加劇我們的自然偏見的影響。

●線上搜尋會導致我們陷入「過濾氣泡」，在其中很難發現新的資

源。

(7)集體思維困境

●當團體壓力導致心理效率、現實考量和道德判斷惡化時，就會發生集體思維困境。

●受集體思維影響的群體會忽略替代方案，並傾向於採取非理性的行動。

●在以下情況下，群體特別容易受到集體思維的影響：

※其成員背景相似。

※當小組與外界意見隔離時。

※沒有明確的決策規則。

(8)如何有效的避免集體思維困境-有條理的腦力激盪

●給小組一個關鍵問題

●每個人都有時間考慮潛在的假設

●將它們寫到白板上

●分組並分類以縮小範圍

●確定每組假設背後的關鍵力量和因素

(9) 整理和分析框架

●意識到認知偏差和集體思維的影響是克服它們的第一步。

●用有條理的方法整理和組織我們的資訊有助於更客觀地識別邏輯關聯，例如因果關係。

●適合多數需求和主題的簡單分析方法：

※時間軸

※概念圖

※主題大綱

●分析報告也可以應用於不同的分析上，例如：

※環境掃描可用於定期報告或戰場情報準備

※SWOT 分析可用於威脅及風險評估

※情景分析有助於估計情報

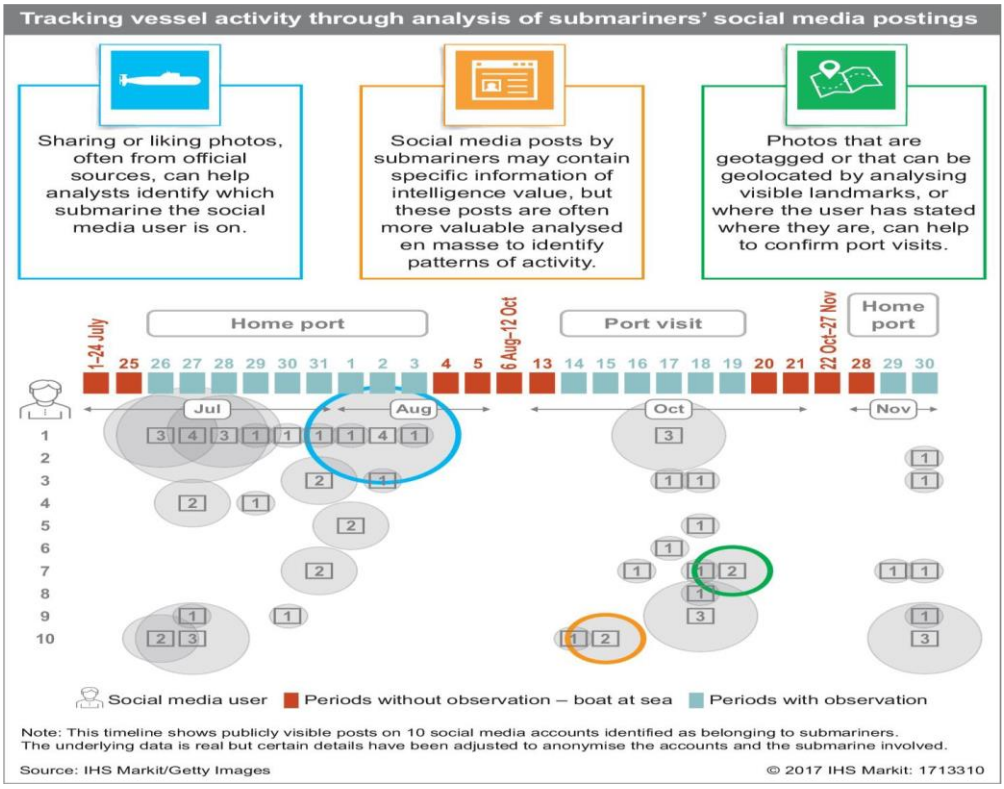

圖 37：以時間軸分析之模式

8.產出成果 Production

(1)透過閱讀並參考優秀的分析報告，並學習其撰寫方式。

(2)疑似(Likely)是情資分析報告中最常使用的單字。

(3)估計概率與分析評估的可信度不同

●高可信度通常表示基於高質量資訊的判斷，使用 AND 跟 OR 找出的結果可以做為可靠的判斷。但是「高可信度」不一定是完全正確的，仍然存在錯誤的風險。

●適度的信心通常意味著來源可靠且可信的資訊，但其質量或確鑿性不足以保證更高的可信度。

●低可信度通常意味著使用了可疑或令人難以置信的資訊，資訊過於分散或證實不足，無法做出可靠的分析推斷，或者對資料來源存在重大擔憂或其他問題。

(4)分析的注意事項：佐證的重要

引用單個來源或可靠性未知的來源是可以被接受的，只要明確指出了

不確定性即可。

(5) 常見分析報告錯誤程度：如何處理情資報告

●使用很長的句子，且包含許多贅句和兩個以上的評估方向

●對句子主題或代詞相關性的困惑

●使用冗長的描述，但其實用一個字說明就足夠了

●使用方言、俚語、成語或不知所云的用字（假想的知識）

●過度使用形容詞和副詞

●使用被動時態

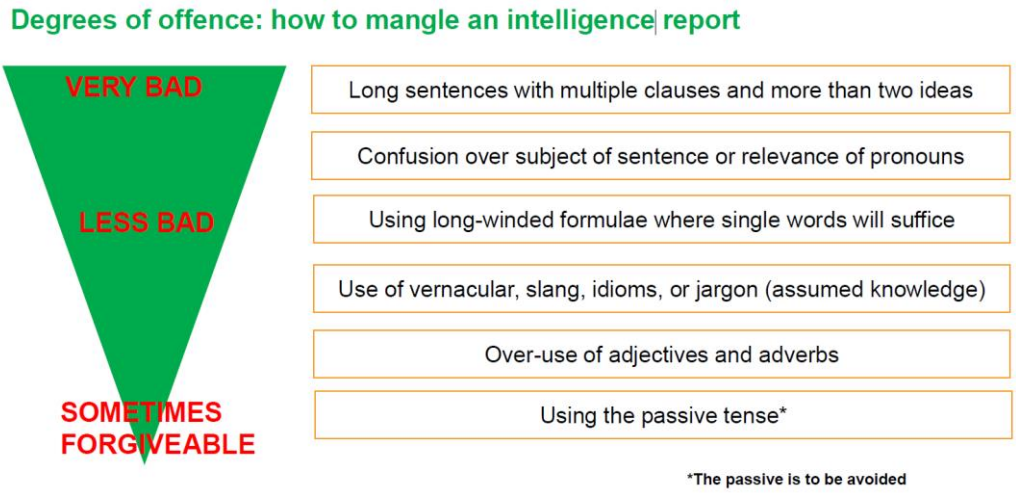

圖 38：常見分析報告錯誤

(6)如何有效撰寫報告的準則

●使用簡短精要的描述，最多包函兩個想法或三個補充的句子

●盡量不使用代詞(你、我、他)

●不要寫贅句

●保持用語的合宜跟正式性

●刪除（幾乎所有）形容詞和副詞

●優先使用主動動詞形式（在描述開頭明確表達主題）

肆、心得及建議

一、 強化培訓資料分析專家，開設進階資料分析專家課程

本署為打破犯罪斷點、落實署長「刑案協作平臺」理念，自 107 年開辦首屆「資料分析課程」，在署長「建立平臺、分享情資、協作偵查、共享成果」之理念與指導下，培養各警察單位執行刑案協作平臺所需之資料分析人才。本課程共計 5 日，由各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，學員結業後擔任各縣市警局資料分析團隊種子教官，並負責刑案協作平臺資料分析員。本次參訪學習 OSINT 公開情資技術，可加入本署未來資料分析課程內容，並參考英國 Peel House 各種教學方式，提升員警學習效果。

二、 強化既有影像辨識系統，導入 AI 影像辨識技術

英國的影像辨識系統資料來源龐雜，且不受限於一套辨識引擎，同時用三家不同公司的引擎進行影像辨識，本署既有影像辨識系統資料來源僅戶政司及本署刑事局，未來於法令許可下可增加比對資料源，使比對資料庫更加豐富而完整。另英國系統採用的三種引擎中，操作人員公認最強的為 NEC 最新研發的 AI 引擎，本署未來可將現行的 NEC 傳統 Neoface S14 引擎強化為 AI 辨識引擎，並爭取系統能採購多種不同公司引擎，因各家引擎所擅長的情境不同，如低光源、高曝光度、高傾斜角度、遮蔽影像，各有不同公司鑽研相關突破技術，若本署系統能排除受限於單一辨識引擎，期能提升員警辦案效率，加速找出身分不明人士。

三、 結合大數據資料，強化偵辦案件工具

本次參訪英國 HOLMES、ACRO 及 Action Fraud 等系統，發現英國警方系統與本署系統有根本設計原則的差異，英國的系統注重深度，著重打造專家系統，如 HOLMES 系統專門收集重大謀殺案件資料，不夠重大的、跟謀殺無關的案件皆不納入，所登打的資訊則包羅萬象，所有與案情相關的文件及資訊（不含照片）皆需輸登進這個資料庫，且只提供專責資訊人員使用，全國有使用權的人不過幾十人；本署系統則著重完整度，著重打造協助員警完成業務的系統，如刑案管理系

統及智慧分析決策支援系統，提供所有刑事人員使用，納入資訊則為案件移送等司法文書，以及警察紀錄、相片等資訊，內容結構化。未來能參考英國專家系統模式，於案件管理系統增加員警自行上傳非結構化文字資料，並結合大數據資料，強化員警偵辦案件工具之深度，使案件情資更加完整。

四、導入即時情資推播訂閱工具

本次參訪發現英國並沒有如本署行動警察載具「M-Police」的即時查詢各種資訊的警用行動裝備，在英國人權相關法律的規範下，英國警察使用資訊相當受限，以這方面來說，本署於服務民眾及偵辦刑案的技術方面相對進步，員警可於 M-Police 即時查詢如民眾是否為通緝犯、是否為失蹤人口、是否為失車等重要訊息，減少將民眾帶回辦公處所的時間，及過程中產生的風險。在參訪波蘭大使館時，筆者亦與來自國際刑警組織的荷蘭高階警官進行交流，荷蘭警方所用資訊設備則與本署使用專用機狀況不同，其可於個人手機上存取各類刑案相關資訊，並可接收包含五眼情報聯盟(Five Eyes)及歐盟等國家的即時情資通報，不僅打破時間及地域的限制，也突破資訊安全技術的限制，在確保資料安全的同時，提供荷蘭所有員警即時有效的工具。未來本署能比照荷蘭警方作法，導入即時情資推播訂閱工具，打破時間及空間的限制，使員警能即時得知重要情報，全面提升員警辦案效能。

伍、參考資料

一、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

二、反恐辦公室

https://www.counterterrorism.police.uk/our-network/

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

三、HOLMES 系統

https://en.wikipedia.org/wiki/HOLMES_2

https://www.opkenova.co.uk/history-of-holmes

四、國家詐騙情資局

https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/Pages/default.aspx

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

五、國家詐欺通報服務中心

https://www.actionfraud.police.uk/

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

六、刑事紀錄局

https://www.acro.police.uk/

https://policecautions.uk/tag/acro-criminal-records-office/

七、皮爾中心

https://www.bennettsassociates.com/projects/met-police-peel-centre/

https://en.wikipedia.org/wiki/The_Peel_Centre,_Stockport

八、Hydra Foundation

http://hydrafoundation.org/

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

九、Google Deep Mind

https://deepmind.com/

十、IHS Markit 公司及講師

https://ihsmarkit.com/index.html

https://ihsmarkit.com/experts/pattar-terry.html