中華警政研究學會
警政與警察法相關圓桌論壇(第 50 場)
【智慧警政論壇 2】論壇紀錄
日期：2022 年 9 月 30 日 14:30

主持人：中央警察大學刑事警察學系 廖有祿教授

本次論壇是延續上次智慧警政的議題，探討如何運用智慧在警政工作。今天很榮幸邀請刑事警察局林主秘故廷引言，說明以科技的角度來說服大眾修改不合時宜的法令（以警械使用條例修法為例），並思考以智慧科技來精進執法效能，分別探討網路匿蹤工具追查、運用 AI 防制詐欺、整合刑案證物管理系統。與談人則分別邀請產官學界就此議題有深入研究的專家，其中二位業界專家曾參與多項警察的專案，二位實務界專家均具備科技偵查豐富經驗，而二位學者則是在本領域已耕耘研究多年，最後請副理事長總結與談內容。透過此種跨領域溝通方式，期盼能擦出不同火花，引發更深層的思考，共同探索這個重要議題，以因應科技犯罪日新月異的趨勢，讓警察能快速適應環境變遷，提昇維護治安的工作效能。

引言人：內政部警政署刑事警察局 林故廷主任秘書

智慧警政不僅可以強化有效的治安策略，更可以節省不必要的警力浪費，以創新科技提升犯罪偵查與防制是當前警政治理的趨勢與重點。例如今年 7 月高雄市政府警局與遠傳發布合作開發的「高雄 3D 治安巡檢預警系統」，結合 AI 影像及聲音感測辨識技術，透過 AI 分析異常治安事件，第一時間由系統向轄區分局勤務指揮中心自動發送告警（？）通知，值勤員警可立即透過管理平台確認現場即時影像，遠端判斷採取即時廣播警告或通報線上警網迅速抵達現場處理。這套系統若真有效，對於諸如 KTV、酒店、檳榔攤或幫派易聚集場所等常發生滋事的治安熱點就可以減少守望勤務的警力編排。

而當前刑事警察工作所面臨的挑戰，一方面應以科技的角度來說服大眾修改不合時宜的法令，讓警察更能有效的執勤；另一方面則以智慧科技來精進執法效能。以下就從法律面及科技面提出一些智慧警政的想法：

一、 警械使用條例的修法：

只要當過外勤警察幹部都知道，一旦員警開槍傷及人身百分之九十以上會是賠錢和解息訟。從文件上可能看不太出來，因為大部分的和解金不是同仁募集、就是警友人士贊助，這代表著警械使用條例用槍時機的規定有很大的問題。由於今年七月再度發生讓人悲痛的台南殺警案，引發外界討論已經在立法院初審完成近 2 年的警械使用條例修正草案，內容包括放寬員警使用輔助工具作為警械、成立警械使用調查小組，刪除補償定額制，回歸國家賠償，並擴大補償對象。日前朝野協商已經決定，拚 9 月底完成三讀。

其實警察執法擔心的不是執法時機條件的嚴苛，而是執法條件模稜兩可。警察機關會要求嚴正、強勢執法，但有時被送到司法審查卻被認定違法，這是員警最容易習得無助感的時

候。若用槍傷及當事人(先不討論傷及第三人) 百分之九十以上會是賠錢和解息訟，就代表面臨司法審查的時候，檢察官或法官在以當前警械使用條例審查用槍時機的規定，大部分結果不是同仁故意就是有過失。私下請教過幾個檢察官或法官，他們也很無奈的表示：以當前的規定，要用我們的經驗法則來審查警械使用條例第六條的「急迫需要、合理使用、必要程度」、第九條的「非情況急迫，應注意勿傷及其人之致命部位」，大部分的案件實在有困難。我們知道所謂不得逾越必要程度，白話一點就是比例原則，針對有效性、必要性（侵害最小)、法益衡平原則的審查。第九條只是將必要性原則做具體規定，再說一遍。而司法在審查必要程度時，經常會將自己定格在以靜止的狀態來審查員警用槍比例原則的三要件，最後看到不少套用行政程序法的比例原則的標準來審核，因此要安全全然通過審查的可謂廖廖無幾，這也是司法官好心要同仁和解的原因所在，也是警察人員畏於開槍的關鍵。最近我在想我們應該以更科學的角度來讓社會大眾及立法委員理解用槍情境，進而合理的修改警械使用條例的相關規定。警大畢業生射擊要 60 分及格才能畢業，刑事警察人員身射擊規定要 70 分。我們應該可以隨機找 30 位行政警察及 30 位刑事警察，以持刀定靶及動靶，各打 30 發子彈，要求員警只能打手上的刀，並統計射擊結果其打到四肢外的身體比例有多高，並以統計標準差的概念(68-95-99.7法則)，來描述若警械使用條例第六條、第九條不限縮，警械使用條例執行的可能性有多高，以此向社會大眾說明可行的方向，並教育好我們自己的員警，認清執法環境及現實。

二、建構網路匿蹤工具的追查與管理

近來犯罪人經常利用網路匿蹤工具進行犯罪，以逃避身分追蹤，造成偵查機關追緝的困境。國內常見網路匿蹤工具的類型有：(一)VPN(virtual private network)，有商業或私人的節點，使用方便，只要在連線裝備設定即可使用。(二)IDC 機房(VPS)，只有付費的的選項，利用雲端伺服器架設虛擬主機，可從虛擬主機連線至目標主機，使用難度較高。(三)Tor，使用方便，僅需使用洋蔥瀏覽器即可進入 tor 協定，達到匿蹤的目的。

而常見使用匿蹤工具之犯罪類型有：(一)網路恐嚇：犯罪集團利用匿蹤工具刊登恐嚇文章或寄送恐嚇信，因犯罪者多在國內，所使用的匿蹤工具呈現的 IP 多為國外 IP。(二)網路詐騙：犯罪集團利用匿蹤工具在網拍平臺或臉書上刊登賣東西的資訊進行網購詐騙，或者利用匿蹤工具隱匿自身 IP 至網銀進行轉帳洗錢。(三)網路攻擊：犯罪集團利用匿蹤工具，進行網站駭侵或使用 DDOS 攻擊癱瘓網站連線。

然而，目前匿蹤工具的偵查遭遇以下困境：(一)國內 VPN 服務業和 IDC(VPS)服務業均屬資服業者，非特許行業國內無相關規範，業者對於客戶 KYC 和網路連線資料保留均不足。(二)大部分 VPN 和 IDC(VPS)業者均在國外，無法調閱資料，部分個人 VPN 也無法管理。(三)Tor 為一種網路工具，所使用的出口節點均是隨機，且節點多在國外，無法逆向追蹤。

首先，國內情治機構是否可考慮廣設 tor 出口節點。Tor 網路係由數千個出口節點組成，洋蔥瀏覽器會隨機擷取 3 個以上的節點進行連線，若能以國家的力量，廣設出口節點，是有機會取得相關資料的，唯 Tor 網路出口節點眾多，所架設出口節點數量如果不夠，即無法有效取得資料；另外應加強國內 VPN 和 IDC(VPS)機房業者管理：雖然國內 VPN 和 IDC(VPS)業者均為資服業者，非特許行業，但前述業者需要向電信業者租用網路方能執行業務，因此電信業者在提供電路出租服務時，除落實用戶雙證件查核外，並應提醒經營 VPN 業者，於提供 VPN 服務時，須落實使用者身分(KYC)查核及實名制。並建立國內連線紀錄，針對國外的

VPN 和 IDC(VPS)業者，應保留電信業者對國外連線紀錄，以利進行反求追查，這部分目前通保法修正案，也已將保留對外連線紀錄列入修正條文中。

三、運用 AI 技術防制詐欺

行政院於今年七月成立打詐國家隊，希望結各部會的力量遏止國內猖獗的詐欺犯罪。本局 165 負責全國詐騙案件諮詢、受理、分派及犯罪手法分析，為了強化詐欺案件之預防，在金融防制面：165 目前和許多銀行合作，有的是銀行資安單位運用 AI 偵測偽冒該銀行之網址，提供可疑資訊供警方偵處；有的是雙方交流網銀、數位帳戶犯罪態樣，以利偵測客戶異常交易進行即時關懷，並同步提供本局情資偵處；有的是由 165 專線分析車手提款熱點，透過銀行 ATM 提領情形將異常帳戶提供銀行進行提款監測，減少民眾被害款項遭提走。另外，為有效提前預防民眾遭詐之風險，進一步與銀行合作以 AI 智慧分析方式，期能建立更有效預警指標模組，以及早阻擋可疑交易及關懷所屬客戶，未來若能提高模組的預測能力，或可供各銀行做預警參考，並採取必要防範措施。

另外，在電訊面與whoscall、趨勢科技等公司合作，以防堵電信詐欺及防堵網路詐騙；並為加速偵測偽冒網站效率，由電信公司推出「AI 反詐守門員-偽冒網站及 APP 偵測」服務，將偵測結果循線通報 165 反詐騙專線做後續處置。

未來更期待能建立偵測假投資網站 App，以強化詐騙攔阻能力與宣導效果，可參考政府防疫大作戰模式，將防詐概念深植人心，透過協助民眾施打「詐騙預防針」理念，委請國內具打擊詐騙經驗業者及知名廠商開發 165 反詐守門員 APP，針對行動裝置進行即時攔阻及警示，供民眾免費安裝使用。該 APP 預期可攔阻及彈跳警示詐騙網站、可疑來電及詐騙簡訊：透過 AI 分析網站特徵、蒐集大數據等方式，在用戶瀏覽網站時主動偵測詐騙網址自動阻擋已知詐騙或高風險網站，並顯示警語提醒、攔阻及彈跳警示。由政府來建立偵測假投資網站 APP，供全民免費安裝或許是未來可行的思考方向。

四、整合刑案證物管理數位化系統

建置全國刑案證物管理數位化系統，不僅可以強化證物監管鍊的要求，更可以進一步做情資分析，提升證物管理及送驗品質。目前國內部分警察局建置自己所屬刑案證物管理數位化系統，但多屬鑑識單位。刑事局則於近年建立毒品證物、尿液採驗等數位化管理系統。由於目前刑案證物管理系統僅部分警察局建立，且缺乏統整，為利整體刑案情資分析，警政署計畫未來建置刑案證物管理數位化系統，並開發手機 App 以結合 QR code 來連結證物的監管鍊，建構中央與地方間縱向及橫向的連結，在第一階段，在刑案發生從取得證物開始至移交地檢署贓證物庫、留存證物室保管、發還當事人、逾刑事追訴時效、無留存必要依規定銷毀等情形，證物交接相關流程以電子化方式記錄、管理，包括員警搜索扣押及現場勘察所採獲之現場證物。利用刑案證物管理數位化系統進行證物送鑑及交接流程，並與已建立的「毒品扣押物數位管理系統」中毒品查扣、尿液採驗等資訊進行資料交換，完備扣押物與現場勘察證物監管，提供即時監控、查詢證物交接情形及鑑定結果。讓刑事人員有完整的案件資訊，在處理案件可以更快速、流暢、便捷，並可避免相關文件散落、佚失，落實行政院刑案證物監管之要求。

未來該系統建置完成後，可以提升刑案案件管理、證物管理、情資管理、鑑識報告、檔案管理及系統管理等功能，提供各項證物鑑識工作資訊，供使用者進行分析運用，提升整體

鑑識與偵查的工作效益。在第二階段，並將數位採證與鑑識一併納入，建立一完整刑案證物管理數位化系統。

有了上述的完整資訊，該系統將可進一步發揮資料探勘及分析的功能，提供案件關聯分析(如：透過指紋、DNA、鞋印、數位採證等證物鑑定結果串聯案件)，作為偵查有利線索，藉由作業平臺輔助，結合偵查及鑑識加速緝捕犯嫌，以保障社會安全。屆時亦可將縣市警察局送鑑檢體品質分析統計，回饋使用者進行分析運用，提升整體鑑識與偵查工作效益。

與談人1：捷睿智能股份有限公司 羅健誠副總經理

捷睿智能是大猩猩科技集團，主要專注在大數據分析與資訊安全等領域。不論是捷睿智能或大猩猩科技，20年來我們非常榮幸有機會參與刑事警察局、各縣市刑大、科偵隊、以及高檢署等單位各種犯罪偵查系統的建置。

一、網路匿蹤追查

在網路匿蹤追查部分，國內外比較常見的解決方案，是透過 IP 資料保存 (IP Data Retention) 的方式，將電信用戶的 DNS 查詢紀錄、連線紀錄保存下來，並關聯用戶資訊、IP 地理資訊等，進一步個化出嫌疑人的身分。

電信(或 ISP 業者)端的連線紀錄保存系統包含幾個重要的原件：

1. 分光器：布署在固網或行動網路業者對外的線路上，所有進出業者的網路封包都會被複製一份出來。
2. 封包過濾器：主要負責分析並過濾特定封包或連線(如：DNS 封包或 HTTPS 加密連線的憑證)，同時輸出連線紀錄。
3. 連線紀錄資料庫：負責保存連線紀錄以及 DNS 查詢紀錄。
4. 中介系統：提供執法單位調取連線紀錄，並保存相關稽核紀錄。

這樣的系統雖然看起來簡單，但是由於網路流量龐大，要長時間完整保存所有 IP 連線紀錄會需要非常高的建置經費。此外，即使國內電信業者以及 ISP 業者都保留了連線紀錄並提供調取功能，還是有可能無法追查到境外的 IP 目標。為了克服這個問題，我們認為有幾個可能的解決方案：

1. 整合國外網路連線紀錄查詢服務，有些資安公司有提供這類的情資，但價格昂貴，也未必能包含所有連線紀錄。在偵查遇到境外 IP 的斷點時，也許可以用這類服務碰碰運氣。
2. 在受害目標明確的情況下，如駭侵事件，可採用“誘餌”方式誘捕，讓網路攻擊方取回“誘餌”後，由誘餌回報攻擊方的 IP 位址。但這種作法爭議性較大，需要有適當的法源依據；且同時要避免“誘餌”被偵測到，技術難度較高。

除了上述做法之外，與各種電商/拍賣平台、社群網路服務、外賣服務、虛擬貨幣交易所等業者建立調閱機制，也是可以解決部分網路匿蹤問題的手段；刑事局過去已經建構了上

述這些系統並實際介接國內外重要的各類網路服務業者，也的確在實際案件偵查中應用相關系統。未來可繼續擴大整合的更多服務，提供更多資訊協助辦案。

二、AI 技術防制詐欺

近年由於硬體效能提升以及大數據數技術成熟，Deep Learning AI 技術已經成為目前最熱門的技術，應用在許多影像、語音、文字、語意等分析識別等應用，最近 AI 甚至被用來進行藝術以及文學創作。

這兩年因為 COVID-19 的關係，宅經濟大行其道，相對而言，卻也衍生出許多網路詐騙手法，例如：投資詐騙網站、假網拍詐騙等。

AI 技術其實也能夠應用在防制詐欺。我們曾經跟刑事局合作，進行概念驗證(PoC, Proof of Concept)，針對 165 統整回報的投資詐騙網站進行分析，我們找出更多類似但卻不在 165 統整清單上的詐騙網站。我們推論這些網站應該是同一集團所建置但卻尚未投入“營運”的網站。換句話說，如果我們可以利用已知的詐騙網站清單，去擴大尋找出更多尚未投入“營運”的詐騙網站，就可以事先加以阻擋，降低民眾被詐騙的可能性。以下是可用來進行識別詐騙網站的一些因子：

1.網域、IP、網址、憑證
2.網頁內容的關鍵詞彙，包含圖片中的文字（可用 OCR 進行辨識）
3.網頁外觀、圖片、以及原始碼的相似度比對
4.整合國內外資安威脅情資加強研判

此外，很多詐騙案件的發生，追根究柢，跟電商個資外洩密不可分。政府部門有行政院技服中心提供威脅情資，但民間企業，尤其是擁有民眾個資的電商卻沒有類似的機構可以提供這些網路威脅情資。目前電商被駭後，大多會向刑事局報案。建議未來刑事局可以主動出擊，協助民間企業，尤其擁有民眾個資的電商、旅行社、電子購票等，建立網路威脅情資的共享機制，減低民眾個資被竊的機會，從根本剷除或降低詐騙發生的機會。

三、刑案證物數位管理

就像引言人林主秘所說的，有些時候，一個案件破案，等於很多案件也都跟著破案，關鍵因素在於擁有一個完善的刑案證物數位管理系統，且系統中的資料，例如：DNS、槍彈鑑識資料等可以跨案件進行關聯比對。對於實體證物是如此，對於原本就是數位化的數位證據更是如此。目前各檢警調單位已經著手進行“司法聯盟鏈”的開發建置，但這個鏈的主要目的在於確保資料的完整性與不可否認性，避免數位證據遭到竄改。但是針對數位證物的內容卻無法加以應用。

目前各縣市刑大、科偵隊很多都具備數位證物採證以及分析的能力。未來若能以縣市警局為單位，在法規許可並有完整的管理與稽核機制的前提下，對其他執法單位提供“數位證物調取”機制，形成一個虛擬的分散式數位證物管理系統，相信對於科技刑偵會有非常大的幫助。

與談人2：碩文拓智慧科技股份有限公司 陳銘宏首席執行顧問

刑事偵查人員的生活日常，不是正在辦案，就是正在去往辦案的路上。刑事偵查人員所肩負的勤務繁多且極耗心力，舉凡佈線埋伏、蹲點勘查、圍捕攻堅、現場搜扣、支援勤務、刑事蒐證、製作筆錄、請票聲監、偵查報告、情資調閱、案情研判、影像清查、期中報告、各式書類、長官提報、本轄統計、送勘送驗、證物保管等工作，因此，誠如林主秘所引言，智慧警政的第一步，應是構思如何藉由科技力量的引進，盡量節省不必要的警力浪費。尤其對第一線查緝同仁而言，若能透過資訊科技簡化或降低其處理各項衍生業務的時間，就將能有更多的時間投入到本業職能專業上，舉例來說，數年前的刑警在調閱取得通聯紀錄後，需要自己費心將不同電信業者的格式統一、自己動手將不同門號的紀錄貼在一起，才能開始研判，但現今已經有現成的轉檔工具、有視覺化關聯工具等可以協助刑警降低前置準備時間，而可以更快的開始進入案情分析；同理，在過去有所謂的神目小組要負責過濾監視器影像，而現今已有許多便捷的影像分析工具可以輔助，包括影像的人臉/車牌辨識、特定物件搜尋、影像濃縮等，都代表在警政科技上的進展。

智慧警政本質上是一個警政領域數位轉型的過程，一般在談數位轉型會涉及三個階段：數位化(Digitization)、數位優化(Digital Optimization)、數位轉型(Digital Transformation)，對照我們過往10年警政情資整合平臺發展經驗，說明如下：

一、數位化：在電腦普及後，公務機關其實就已經持續進行將既有的紙本作業改以電子化作業，警政機關自然也是，例如報案三聯單就是很典型的代表。而在刑案偵查面向上，包括刑事案件登輸管理系統、筆錄系統、三四級毒品資料庫以及林主秘引言提到的刑案證物管理數位化系統，均可視為從源頭端將資訊數位化的一種進程。

二、數位優化：當來源資料本身是數位化存在，即可對其進行利用，例如警政署的智慧決策分析平臺、刑事局的刑案知識庫、各地警局的在地情資分析平臺等應用功能均屬之。在這個階段，主官(管)與使用者開始可以收穫數位治理的果實，例如可以分析M-Police的臨檢盤查紀錄，來推敲可能哪些人在事發時是在同一個包廂內、可以透過路口監視器交叉比對來找出目標車輛可能的同行車對象。

三、數位轉型：當資料隱含的價值可以有效的被洞察以後，決策者自然就會開始反思相關的規劃是否有調整的必要性。例如從特定案類熱區、熱時的分布與趨勢，作為巡邏或臨檢勤務動線的規劃參考。而異質資料間所迸發出的火花，也會促使決策者開始思考是否建立新的資料互惠模式，例如行車糾紛衍生的街頭聚眾事件，可以從交大形成一個通報機制，讓刑大可以較快獲知有淺在的預警進而防範。

因此，一個相對較全面的智慧警政生態可以從一條河川來比喻：

一、上游：為源頭之始，重點是要做好資料治理，在這個區域將涵蓋所有智慧警政所需的資料數據，大致上可以分為三大類：

1、交換資料：由警政署、刑事局、縣市政府或網路上取得之開放資料，通常是以整批資料交換形式納入，且會定時更新。

2、前線資料：在第一線執行勤務所得之資訊，例如路口監視器影像、蒐證/跟監、臨檢盤查、現場鑑識採證、毒品初篩等，通常這類資料因為是第一線取得，所以資料正

確性與更新性較佳。

3、在地資料：具有轄區或屬人特性的資訊，例如筆錄、偵查報告、交通違規/事故、停車拖吊、刑案投單、組織幫派等，這類資料通常具有特定業務目的，且掌握在特定機關或人員身上。

二、中游：為智慧警政的核心，目的是將源頭資料進行充分的解讀與分析，並依據業務需求發展不同的應用功能。例如在我們過往的經驗中，與 Google Search 類似的關鍵字全文檢索功能，因為學習門檻低，且使用者透過隻字片語即可很快查得所需資訊，因此使用黏著度很高，據統計，某刑大單位在半年的使用次數逾百萬次，可見一斑。另外，具有直覺、易理解的設計，在近年來愈受重視，因此除了視覺化關聯工具、電子地圖導入外，更需留意使用者操作體驗(UX)的考量。近來隨科技的進展，有關機器學習(ML)、人工智慧(AI)、深度學習(DL)等技術的引進，期盼整合原有警政應用功能發揮更大成效或減省更多人力，亦是一大發展趨勢，惟這些新技術的訓練仍須仰賴有經驗的人來介入，日前在全球範圍內仍相當缺乏現成可用的警政模組。

三、下游：此段訴求為終端的戰術應用，亦可視為一種感知器(Sensor)部署的概念，例如員警身上的密錄器或刑事人員架設的遠端監控設備等，就是一種走動式的偵查之眼。當然，除了期望可以透過第一線的反饋而得到更多更即時的資訊外，亦必須同時思考可以提供什麼樣的戰術應用讓第一線同仁更加便利，例如數位搜扣的 APP、可以直接拍照即時比對人臉庫的機制、甚至是提供讓同仁間可以逗相報協同合作的協查平臺等，均是以資訊科技改善或提升同仁執行日常業務品質的手段。

綜觀整體智慧警政生態系，除了上述上、中、下游的劃分外，不可輕忽的是從最開始就應該要有很好且合適的攔砂壩(資訊安全)規劃，方能在整個數位演化的過程中，確保各項業務數據、機敏數據不會跑到不該去的地方或是外洩。同時，在整個智慧警政生態系的發展過程中，亦應該提供配套的 API 機制，以利與他轄或他單位進行潛在合作，攜手為共同的目標努力。

與談人 3：刑事警察局科技研發科 莊明雄代理科長

一、近年來資通訊科技日益發達，員警所面臨不僅只是傳統犯罪上必須調閱大量監視器畫面來找出嫌犯身分與犯罪活動軌跡。從本次林主秘提出利用洋蔥(TOR)、VPN 等跳板進行對於國內重大交通設施(高鐵、台鐵)、總統府、六都等從事網路恐嚇犯罪，已經讓很多執法單位疲於奔命，這些沒有犯罪實體現場的攻擊手法，且透過境外 IP 來進行，已經讓執法單位摸不著頭緒，形成非常大的困境。近期選舉期間，所面臨的大量境外挹注的假訊息案件也是相同的問題，更況且許多事件是發生在境外的社群媒體，雖不諾殺人放火的重刑，但造成的紛擾已經嚴重影響政治生態，也讓執法單位不得不重視網路犯罪的問題威脅。

二、刑事警察局曾經處理一件連續恐嚇案，歹徒假冒日本律師唐澤貴洋名義，從事網路恐嚇案件，透過電信偵查大隊與中華電信等業者，在中間伺服器進行資料 IP 反求，確實可以利用一些技術找出跳板犯罪的人，但是如果要大量蒐集電信業者端資料，必須耗費大量系統建

置及完備的法令規範，這些都必須防範未然，並且要提前準備，如果真能蒐集大量的 IP 資訊，未來更可透過這樣的機制來強化偵查能量。此外，國內更應對黑暗網路之類加密網路型態進行槍枝、毒品、人口販運、個資外洩等交易關注，並提早因應類似犯罪發生，避免未來無法掌握。

三、刑事局近期所關注的三大人工智慧 AI 做法，首先錄影監視系統，不在環繞在影像辨識，而是如何智慧的透過通聯軌跡，結合各地錄影監視器，能快速掌握嫌犯的活動脈絡，既使對象變裝也能找出來，縮短時間。其次，近期我們也關注到高嘉瑜立委等女性遭犯嫌小玉使用 deepfake 的影片來進行數位性剝削，當然這樣的技術也能發生在假訊息或其他犯罪之上，本局也引進外國鑑識 deepfake 軟體或技術，近期已經制定相關數位鑑識流程與辨識標準，對方用 AI 來假造影片，我們則用 AI 來辨識影片，而這條預料將持續走下去，日後將視 AI 來對抗 AI。第三，疫情期間，國內民眾遭防投資詐騙威脅，動輒畢生積蓄或上千萬財產遭詐騙，主要原因在於假冒的釣魚網站太多，而當民眾受騙後通報 165 專線，然後執法單位再向電信業者通報停止解析，已經緩不濟急，因此未來透過主動分析網域名稱註冊、釣魚網站型態比對官方網址相似度(例如官方 www.cib.npa.gov.tw 與釣魚網站 www.cib.npagov.com 相仿)或者其他加權的作法等，透握 AI 的研發能預先發動，避免更多民眾受害。

四、臺灣的優良治安是建構在許多警察日以繼夜血汗調閱錄影帶或埋伏布建而來，許多案件的發生小則 3 天，多則數月或超過一年以上的刑事偵查人員不眠不休追查，但這些不應該是標榜科技大國的臺灣所應出現血汗警察，未來如何透過科技運用，有效資料庫分析，專業人才的研發，讓真正的偵查工作走入科技偵查，導入專業的經驗，提升工作效能，讓 90%的工作在辦公室裏面資料分析，僅花 10%工作進行實體偵查，落實 smart work，讓警察工作不必血汗，真正事半功倍。

與談人 4：桃園市警察局刑警大隊科偵隊 林應龍副隊長

誠如林主秘所言，智慧警政是當前與未來警政治理的重要課題，如何有效運用科技節省警力並精進執法效能，仰賴大家的共同努力與智慧。以下就個人在實務上的經驗，針對智慧警政提出 3 項淺見。

一、網路匿蹤追查與資安強化

現今網路犯罪常透過網路匿蹤工具隱藏蹤跡，包含隱藏個人 IP 的 VPN、TOR 及隱藏網站 IP 的 CDN 等，核心概念皆為透過代理伺服器(Proxy Server)轉送，在資訊流偵查上基本是以來源 IP、目的 IP 及時間逐層調閱帳號基資或伺服器紀錄(Server Logs)，但 VPN 及 CDN 服務多為境外業者，不會進行使用者身分查核(KYC)，因此除調閱困難外，罪犯只要結合假帳號即可製造資訊流偵查的斷點。

由於境外 VPN 或 CDN 業者會租用本國 IDC(VPS)機房服務，作為在地轉送節點，因此如同林主秘之高見，雖因網路無國界，罪犯會有多種規避網路偵察的方法，但本國或許可透過法規要求

境外 VPN 或 CDN 業者擔負起責任，保存在本國設置或租用之轉送伺服器紀錄並落實使用者身分查核(KYC)，使罪犯在本國之網路非法行為可被追蹤，不再以 No Logs 等商業政策為由，在本國形成網路犯罪斷點；而在本國商業網站部分，亦應強化宣導資安觀念，妥善設定防火牆白名單及黑名單，減少被駭客攻擊成為跳板之可能性。在阻擋境外攻擊及落實境內紀錄之雙重政策下，持續提升本國資安及網路犯罪偵查能量。

另在網路偵察技巧上，應強化科技偵查人才之培育，使其熟悉網路運作模式，嘗試透過罪犯可能疏忽的部分加強偵查，例如網路賭博網站或詐欺網站，只透過 IP 或網域(Domain)查詢，就會因 CDN 形成斷點，但若透過網站偵查(Web Reconnaissance)及公開來源情報(OSINT)等技巧，就可能橫向拓展找到罪犯疏忽未隱藏的線索，增加破案之可能性。

二、智慧警政資訊系統研發

本國智慧警政相關資訊系統依其應用面向大致上可分為業務管理及犯罪偵查等 2 類，近年來由於數位化(Digitization)、大數據(Big Data)、人工智慧(Artificial Intelligence)、物聯網(Internet of Things)等技術迅速發展，各警政單位都積極進行引進新技術進行概念驗證(Proof of Concept)，透過數位轉型提升警察工作效率。

個人認為在業務管理上須全國統一標準的系統，宜由中央蒐集地方意見後，統一規劃並律定執行方式與流程，避免標準不一或系統整合不易等後續問題。而在犯罪偵查上的創新系統，則較適合採用快速且成本低的雛型在實際場域測試，取得實驗結果並驗證概念是否正確，因為研發非百分之百都會成功，創新程度越高、規模越大，未知風險與失敗的機率就越高，在技術尚未成熟時直接導入新科技，將有可能變成人在服務科技，而非科技在服務人。

如近期高雄市政府警察局的「3D 治安巡檢預警系統」、新北市政府警察局的「警蜂動態影像蒐集及辨識系統 1.0」及桃園市政府警察局的「AI 巡防系統」，皆屬人工智慧及物聯網技術應用在警察工作的實際場域概念驗證，當累積的經驗足夠成熟後，中央即可參考替全國警察規劃及研發更完善且先進的應用系統，這樣的協作模式，或許可以加速警察在智慧警政上的發展。

三、科技人才培育

智慧警政的長期發展重點，個人認為在仍於警界科技人才的量跟質，無論是要研發科技偵查方法或開發智慧警政系統，都需要有具備相對應能力的科技人才，因此如何吸引、培育與留才會是智慧警政長遠且重要的課題。

在吸引部分，如何提供足夠的誘因，吸引警專、警大畢業生願意持續學習並適應各種科技的迅速發展；在培育部分，如何針對警察所需的不同科技能力切分專業並提供完整的訓練學程；在留才部份，如何避免訓練完成後的科技人才離開警察工作崗位，都將影響科技建警政策的推動。

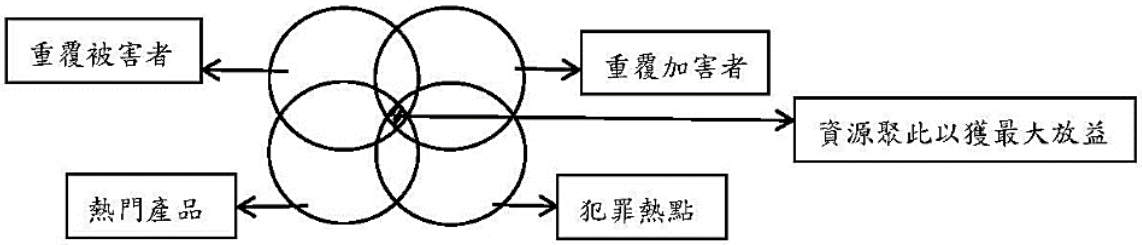
前揭議題中央都已十分重視，並持續辦理「精進科技偵查人才教育訓練」及「犯罪情資分析」等課程培訓種子教官，今年亦協調陽明交通大學的資訊學院開設科技犯罪偵查資通訊的碩士在職專班，增加每年的容訓總量，在吸引與培育部分已規劃的十分完善，相信警界很快就會有更多的中、高階科技人才，感謝中央的努力。在地方上亦有部分機關訂定科技偵查人員的訓用計畫，期望能透過中央與地方的交流與訓練，持續提升科技人才的能力。

與談人5：中央警察大學行政警察學系 許福生教授

近年來隨著人工智慧（AI）與大數據（big data）的發展，警察活動逐漸走向數據導向與預測性，逐漸形成預測性警政（predictive policing）。依據Bennett Moses & Chan列出預測性警警政週期分成下列四個階段與十個假設：

1. 第一階段：數據收集（data collection），此階段中，第一個假設在於使用的數據精準地反映了現實。
2. 第二階段：數據分析（data analysis）在分析上，第二個假設是未來就和過去一樣，也就是有關在某些區域系列或事件群。第三個假設則是排除不相關的變數，分析工具都會注重在有限的變數群，即使它們很大，都會進行排除。第四個假設在於演算法是中性的。第五個假設則是數據分析不會不當地歧視。第六個假設是指地區的首要性（Primacy of place）。
3. 第三階段：警察行動（police operations），在警察行動中，第七個假設即是警察目標性部署應該是首要的干預措施。第八個假設是完善執行。
4. 第四階段：對犯罪的反應（criminal response），此階段，第九個假設是改變警方部署能夠預防犯罪。第十個假設在於對犯罪的關注總是適當的。基於上述的幾個假設，最早出現的預測性警警政，就是以地點為基礎的預測，後來的發展，不僅於此，也對於人物，乃至於時間進行預測(王正嘉，預測性警察活動在犯罪偵防運用與問題，刑事政策與犯罪防治研究第25期，2020年8月，頁17-23)。

至於預測是預防犯罪很重要的組成部分，有效的犯罪預防重心，將因資源投入至重覆被害、熱門產品、犯罪熱點及重覆加害者的重疊處，以達成犯罪預防最大的放益，如圖所示(Steven P. Lab, Crime Prevention: Approaches, Practices and Evaluations. Eighth Edition,Routledge.,2015.p213)。



一、預測可能犯罪地點

關於犯罪可能地點預測，是因為區域或處所本身的不完善或是缺陷所致，例如光線昏暗、沒有執法人員的巡邏或監控，或是有容易逃逸的路線，而無論何理論，都承認環境因素與犯罪發生是有關聯的。如同地震會導致餘震，而犯罪行為也有同樣的特點。在發生入室盜竊或汽車失竊案之後，短時間內同一地點發生類似犯罪行為的可能性會增至之前的4~12倍，這種傳染作用叫作「鄰近重複」(near repeat）效應。又犯罪是社會、物理空間及行為等各個不同因素交互作用下的產物，其考慮的不僅是過去犯罪而已，同時看到社會、物理與行為因素等有助犯罪發生的因素，故將不同犯罪因素標誌在地圖上，成為犯罪風險地形圖，

聚集著越多犯罪因素的區域，便是越有可能發生犯罪，此理論又稱為風險區域理論（the Risk Terrain Theory)。

二、預測可能犯罪人及被害人

在新科技運用下，從事犯罪偵防的警察，會熱衷於預測接下來可能會發生的犯罪，除了在何處發生外，誰是可能的犯罪人或被害人，也是重要預測點。如同芝加哥警方採用由伊利諾理工大學的 Miles Wernick 設計出的熱門名單（heat list）作法，辨認出 1,400 名青少年，為熱門名單中的目標，該名單使用 11 個變數來創建 1 到 500 的風險評分，分數越高意味著成為槍枝暴力犯罪人或被害人風險越大。而在辨識出可能犯罪人後，警察採取查訪、警告方式，向其說明犯罪活動將導致的法律後果，或者告知也有可能成為未來被害人，透過這種聚焦嚇阻，並利用針對性和顯示訊息傳達給警察、檢察官和社區，通知他們知道誰正捲入暴力行為中，以便及早結束殺人犯罪的發生。

三、即時預測

如桃園市啟用的 AI 巡防系統，讓警方巡邏車在行駛過程中，透過鏡頭及 AI 自動辨識比對路邊車輛的車牌，過濾警政署通報協尋的失竊或侵佔的汽車或機車，大幅提高警方巡邏的效率。這支 iPhone 扮演 AI 巡防的前線大腦，自動辨識汽車、機車的車牌號碼，比對警政署通報協尋的車輛資料，一旦發現失竊、侵佔、遺失，或是重大刑案所通報的可疑行駛車輛，立即向巡邏車上的員警發送提醒，員警確認車牌辨識影像無誤後，下車找到通報車輛，還可將比對結果，透過手機的 4G 網路傳至勤務指揮中心，勤務人員經由 AI 巡防系統的後臺，根據視覺化地圖位置、車牌辨識結果，協調指派其他巡邏車前往支援(2022.03.24 https://www.ithome.com.tw/news/150091)。

四、省思

只是我們真的能用 AI 或大數據來預測犯罪發生的地點和時間？以及能否預測誰成為被害人或犯罪人的風險最大？縱使美國洛杉磯警局曾用大數據分析，富特希爾區的犯罪率下降了 36 個百分點，但以美國芝加哥警察局的「熱門名單」(治安顧慮人口名冊)為例，其使用演算法篩選出芝加哥治安顧慮的年輕人，且該列表使用 11 個變量建立一個「風險評分」從 1 到 500，數字越高，成為被害人或犯罪人的風險就越大，況且篩選出轄區治安顧慮人口之同時進行「警察家庭通知」查訪。然而，自使用「熱門名單」以來，芝加哥的暴力事件一直保持不變，最主要是「熱門名單」解決不了社會和經濟風險，因為縱使確定了犯罪「高風險」對象後，然後又如何呢？如此也提醒我們雖然大數據可能適用於棒球或商業模式，但在處理個人自由時仍須小心謹慎，亦即我們不要只根據計算機輸出數據，進行犯罪人剖繪，因為過去的逮捕紀錄可能成為數據的主要來源，而所有系統都會出現數據問題（參照 Richard G. Greenleaf，2019 年 4 月 1 日於警大之演講)。

縱使如此，近年來隨著 AI 或大數據的發展，警政逐漸走向數據導向的「智慧警政模式」，已逐漸形成現代警政的趨勢，故運用上應思考如何在使用過程發揮效益，降低缺失。

與談人 6：中央警察大學刑事警察學系 蔡馥瑔助理教授

智慧警政(Intelligent Policing)最主要的關鍵在於「智慧」兩個字，智慧的工作方式(Work Smart)就是可以用更少的資源，發揮更大的功效。以往我們總認為智慧僅存在於人腦中，隨著科技的發展，人工智慧與人腦對抗已成為熱烈討論的話題。雖然大多數的學者認為人腦有不可取代的重要性，但人工智慧的軟硬體技術蓬勃發展，在某些領域已有人工智慧勝過人腦的例子。其中 1997 年超級電腦深藍戰勝了國際象棋冠軍起，開啟了人腦與電腦一系列的對抗。包含 Google 開發的 AlphoGo 也在 2016 年打敗了來自韓國的世界圍棋冠軍，自 AlphaGo 在圍棋比賽中取得絕對優勢的成績後，學者們普遍認為在圍棋比賽中，人腦已無法與人工智慧比敵，從 1997 年至 2016 年雖然都是使用人工智慧來開發下棋程式，但人工智慧的設計邏輯截然不同，因為象棋的複雜度比圍棋小很多，所以深藍可以使用窮舉法，也就是把可能的棋路都估算出來，然後從中尋找最佳解。然而圍棋的高度複雜性，讓人工智慧無法將所有的可能性算出來，因此 AlphaGo 使用強化學習，讓人工智慧自我對抗，從大量的自我對弈中，進行大量的訓練，等於人類世界中幾千年的棋局智慧，如此才成就了自我學習的成果。

人工智慧其實早於 1950 年代就開始相關研究，至目前為止已超過 70 年。在這長時間的發展歷程中，總共經歷了三次的繁榮，但在繁榮的期間，也渡過了二次的低潮。第一次的興盛期在 1950-1960 間，這個期間主要是以感知器(Perceptrons)模擬人腦的運作，但這個期間人工智慧模型僅能解決簡單的問題，與人類期待機器能通過「圖靈測試」的差距太大，許多應用都僅止於雛型階段，無法進入真正的商業應用，因此人工智慧進入了第一次低谷。第二次的興盛期在 1980-1990 間，「專家系統」是這個時期最重要的應用。專家系統可在特定的領域內，提供成熟及專業的建議，簡單的來說就是把人類專家的知識淬取出來，以法則(Rules)的型態存在電腦之中，所以知識發現(Knowledge Discovery)也成為這個時期的重點發展，然而這個時期的專家系統，因運算能力不足，故應用仍多局限特定領域，況且將知識從人類專家淬取出來的過程，大部分需人為介入，缺少自動化的機制，故知識淬取機制無法大量擴展至各領域。第三個興盛期自 2010 年至今仍蓬勃發展中，這段期間的發展是以深度學習為主，深度學習是以多層次感知器所組成，多層次感知器可更真實的模擬人類大腦，學習更細微、廣泛的知識。專業領域比較容易界定範圍，但廣泛的知識則需要考慮更多面向，例如：瞭解人類講話內容、分辨任一張圖片中的物件等。這些廣泛且通用的知識，無法用上個世代的專家系統來解決，所以第三個興盛期的人工智慧，必須改變上一次興盛期的專家系統，不把知識從專家的大腦中取出來，而是訓練一個電腦專家來取代人類專家。

在人類自幼小訓練過程中，以辨別貓狗的問題為例，我們只要看到小動物具有兩個尖耳朵、四條腿、一條尾巴、身有毛皮等特徵，就會判定這個動物是狗還是貓，雖然偶爾會判斷錯誤，父母這時就會糾正我們，讓我們從反覆的錯誤中學習更精準的知識，慢慢的錯誤會愈來愈少，最後長大成人後，我們在辨別貓狗的問題上，便幾乎不會發生錯誤了。人工智慧的訓練方式就如同人類一般，只是把訓練的對象改變成電腦，而人腦中的神經元以多層次的感知器取代。從人類長達幾十年的訓練歷程人得知，如果我們想要在短時間內(例如：訓練 3 年的人工智慧取代 50 年訓練的人類智慧)訓練一個電腦專家來代替人類，就必須要有「夠多的學習素材」及「夠快速的學習效率」這兩個要素，而這兩項需求在 2010 年剛好達到可用於訓練人工智慧的程度，搜尋引擎的發達，讓收集大數據學習素材變的更簡單，而各 GPU 算

力的發展快速增加，讓人工智慧可進行比人類更快速且不眠不休的學習，這兩項要素的滿足，讓人工智慧在各領域的應用突飛猛進，符合人類對人工智慧的期待。

有了成熟的人工智慧之後，該怎麼應用在警察工作呢？在回答這個問題之前，也許我們應該思考怎警察需要何種類型的人工智慧，鑑於人工智慧的強項就是藉由大量的資料，以最快的速度進行學習，使其效能強過人類，而警察機關擁有最大最複雜的資料是什麼呢？我認為是全國超過 10 萬台的監視系統影像，這些大量的影像資料，如果讓人類去學習，時間大概只能濃縮 2 倍(影片以 2 倍播放)，但讓機器去學，可用超過 10 倍的濃縮時間，且讓上千臺機器同時去學，等於以很短的時間，廣泛的訓練並結合上千位專家的知識來代替人類解決問題。

人工智慧在智慧警政的應用，若以影像資料為學習標的，筆者認為可分為以下幾個面向:

1、交通管理

為了讓民眾用路順暢，路口交通號誌的時間規劃非常重要，但以往為了要計算車流，必須耗費大量人力去統計即時資料，而這些即時資料又隨時都會變動，所以為了交通運用，必須有一套機制能夠模擬人類，準確快速的判斷車流狀態。而目前人工智慧技術即可經由物件識別技術，可從路口監識器的影像中，識別車輛種類、速度、方向、軌跡，轉向等，蒐集多種交通特性資料，包含各車種轉向交通量、延滯、佔有率、密度等等，可提供交通管理單位進行交通監測及號誌控制應用。

2、人臉識別

人臉影像對於警察執勤亦非常重要，在警察利用穿戴裝置(例如：智慧眼鏡、秘錄器、智慧手錶、M-police 等)所收集的影片中，存在非常多樣的場景，而如何在不同情境的影像資料中，快速的識別出人臉，以人類來說都是非常困難的，但鑑於網路中無版權且出現人臉的影像學習素材非常多，藉由人工智慧廣泛的學習內容及快速的學習效率，在警方執法過程中協助即時辨識人臉，並進行後續加值運用(例如：通緝犯偵測)，預期將可大幅提升執法效率。

3、行為模式

人類肢體行為內含許多隱性的資訊，目前在醫學領域中已有許多應用，例如以人工智慧分析人體姿態，預防年長者的危險動作，或分析運動人活動姿態預防與治療運動傷害，而這些細微動作的差異，是需要專業的防護員才能做到的，但近期的研究成果指出，人工智慧軟體已能協助專業人員提出建議方案。如運用到執法領域，可經由人工智慧機制，偵測犯罪在街頭可能即將進行犯罪的肢體行為模式，或在製作警詢筆錄時偵測其肢體動作是否說謊等，等同於訓練一位資深警察全天候協助警方執法，強化執法品質。

與談總結：銘傳大學犯罪防治學系 章光明主任

一、引言人林主秘之內容

引言人從四個方面討論智慧警政: 警械使用方面，建議進行用槍情境下合理必要性的實證研究，頗具理論與實務雙重意義；網路暱蹤追查方面，VPN 實名制服務的建議，可以提高犯罪成本，達到預防目的；AI 防詐部分，開發實用的警政 APP，十分必要；刑案證物數位化

管理系統，尤具劃時代意義，果能落實，功效無限。

二、與談者的內容精要

1、所謂「智慧」指降低資源，增加功效，人工智慧即具如此特質，可達「大量資料，快速學習」目標；(蔡馥瑔助理教授)

2、智慧警政有別傳統勞力密集重視體能的警察工作取向，科技使九成偵查工作能在辦公室內透過資料處理完成，另一成則是在法律面與院檢溝通；(莊明雄科長)

3、大數據的蒐集、分析和運用(big data collection, analysis, and utilization)是智慧警政核心，須「建構搜尋引擎資料庫的大數據平台，做大數據分析，偵查，預防詐欺犯罪。」(陳銘宏首席顧問）；也就是「發展智慧警政基礎建設，結合資料治理（資訊安全)，與外勤的戰術運用」(羅健誠副總)

4、「科技人才培育」是智慧警政的軟性建設，譬如，在陽明交大為警政署開設科偵資通專班，培養人才，即為顯例，然一般行政警察如何使用大數據資料，也須教育；(林應龍副隊長)

5、運用智慧警政分析所得資料可發展 predictive policing（預測警政），發揮預防犯罪功效；(許福生副理事長)