

評析智慧警務的前瞻執法應用

高大宇※

目 次

壹、前言	一、執法機關的人工智慧需求
貳、文獻探討	二、整併地域性資料庫，提升資料整合分析能量
一、智慧警務的技術運用	三、聯合查緝專案，納入資訊專業人員
二、執法機關為何要引進人工智慧	
參、智慧警務的人工智慧運用現況	伍、結論
一、前瞻執法的應用現況	參考書目
二、智慧警務的面臨問題	一、中文部分
肆、智慧警務的建議對策	二、英文部分

摘 要

執法機關彙集各種犯罪紀錄資料的電腦系統、分享相關資料、知識、技術、或經驗，廣泛運用於偵查、逮捕等執法應用，為跨機關合作，提供潛在、巨大的可能性。利用搜尋、檢索犯罪模式等新興技術，提供智慧警務的前瞻應用，為各執法機關的努力方向。人工智慧雖可處理大量的數位照片、影片、刑案紀錄等檔案資料，協助達成警務治理任務，卻存在隱私侵犯疑慮、缺乏適當監督、資料錯誤率、或人為偏見等疑慮問題。本文探討人工智慧於警務工作的運用現況，評析後續推行智慧警務的執法任務的可行作法，期強化刑事司法系統的偵查防治能量。

關鍵詞：智慧警務、大數據、人工智慧、科技偵查、隱私侵犯。

※ 中央警察大學資訊管理學系副教授，通訊作者。

■本研究課題得到 109 年度資安旗艦計畫-精進刑事科技能量計畫資助，特此致謝。

Abstract

Law enforcement agencies (LEAs) utilize various computer systems to deal with criminal records or share relevant knowledge for inter-agency cooperation. Using emerging technologies can provide forward-looking applications of smart policing. Although artificial intelligence can process a large number of digital photos, videos, criminal records, and other archival materials to help achieve police governance tasks, there are doubts about privacy violations, improper supervision, data error rate, or human bias. This paper explores the current application of artificial intelligence in police jobs, evaluates the enforcement of smart police, and strengthens the investigation and prevention of the criminal justice system.

Keywords: Smart Policing, Big Data, Artificial Intelligence, Technology Crime Investigation, Privacy Violations e

壹、前言

人工智慧在沒有人為干預運作下，藉由資料分類，感應當下環境、作出適當回應，執行需要人類智慧或決策過程的任務，提高專家或專業處理人員的準確性及生產力[11]。犯罪分子會濫用該技術，執法機關也須善用它，收集大量資料或資訊，透過數位分析和軟體功能預測犯罪行為，追查帳號資金流動，加強清查犯嫌間的互動關係[4]，要求快速獲取、低錯誤率和大數據的準確輸出，以提高執法效率或效能[6]。然而，執法人員常排斥採用新進科技，為降低人工智慧風險並提高執法效益，須了解機關、部門的本身存在問題，透過員工教育訓練、系統實作測試、不斷精進改善，才能讓該資訊科技系統，符合執法人員需求。若真能幫助提升警務工作效能，執法人員自然樂於接受；但須知任何資訊系統的建置開發，不會一步到位，須視待解決的問題之系統重點事項，進行綜合分析，循序漸進找出解決問題的可行方案，不斷改善系統功能，逐步釐清系統目標、分析個案重點，期準確診斷問題，揭露問題本質和原因，輔助使用者在複雜環境中，確認系統目標，比較並找出可行解決方案，滿足執法使用者的需求。

本文相關章節安排如下：第貳節討論智慧警務的人工智慧、機器學習及深度學習等技術運用，並分析執法機關引進人工智慧的必要性。第參節從英國、美國及臺灣地區的前瞻執法應用現況，討論智慧警務面臨的問題。第肆節提出智慧警務的建議對策。第伍節歸納結論。

貳、文獻探討

隨著電腦演算法、數位影像和人工智慧的進步，基礎通訊產業、前端資料儲存及後端運算分析等技術日趨成熟發展，相繼作為公務、商業或執法用途。如人臉辨識技術陸續使用於解鎖智慧手機、辨識過境人員、授權銀行轉帳、監測情緒狀態或偵測可疑犯罪人士。人工智慧技術可提早發現問題，尋求解決策略，並發現罪犯的行為軌跡，能執行搜尋、分類和分析資料等瑣碎任務，改善執法機關的服務內容[9]。

一、智慧警務的技術運用

人工智慧、機器學習和深度學習可運用於識別人、事、時、地或物的資料特徵。機器學習的特徵工程（Feature Engineering），乃指經領域專家分析資料，了解資料特性後，才能產生出有用、有效的特徵過程。而深度學習具自動萃取特徵（Feature Extraction）能力，輔助專家快速識別資料特徵[1]。這些技術能滿足執法機關的某些需求[4]，但執行實務任務時，尚須對所獲結果，審慎校對檢查，方能避免疏漏。

（一）人工智慧

人工智慧（Artificial Intelligence）已普遍應用於語音辨識、手機助理或購物網站偏好推薦中，這種電腦軟體處理速度快，也會模擬人類思考方式。這些應用須先有大量、足夠且相關的環境資料與應用資訊，瞭解周遭環境的事件、類別、特性及彼此關係，才能進行相關運算，並獲得妥適、有效的運用；如果沒有適當的人才、資訊及決策演算法，仍是事倍功半[4]。數位生活的科技發展，讓我們身處於資訊爆炸時代，巨大資料量中，存在重複利用的豐富價值，若僅依靠人工方式分類、分析、整理，只能獲得低效率的成果。執法機關有機會採用機器學習、深度學習輔助人工智慧，蒐集和評估刑事案件的大量、相關資料或證據，遂行任務。

（二）機器學習

機器學習（Machine Learning）是人工智慧的一個分支，要讓機器擁有人類認知及解決問題能力，是困難且繁複的工作。機器學習需要程式設計師告訴電腦，該尋找哪些資訊，並進行特徵檢測功能。機器學習讓電腦接觸全新或不斷變動資訊時，透過學習和統計分析資訊內容，找出大量資料的變動模式及隱藏資訊，做出預測[12]。但程式設計的邏輯演算法及人為錯誤因素，亦可能會影響資料判讀的正確性。

（三）深度學習

深度學習（Deep Learning）是機器學習的一個分支，嘗試模擬人腦，透過多層次的線性或

非線性轉換處理，形成知識[12]。取得資料後，系統詢問一連串的是非題或判斷題，再根據獲得答案分類資料，自動萃取足以代表資料的特徵，並透過處理大量資料和演算法，完成如影像識別、語音辨識、機器人、自動駕駛車輛、及醫療病徵定位影像分析等特定工作。

二、執法機關為何要引進人工智慧

隨著大數據的持續增長，擁有大量資料存取權限的執法機關，長期存在專業知識、經驗與能力的學習落差，須掌握快速發展的技術能力，了解最新進展的潛在影響，方能強化人工智慧，協助打擊或預防犯罪[6]。人工智慧技術雖能滿足執法機關的某些需求，也須審慎檢查、評估和調校人工智慧技術的運用方式，作為執法機關判斷模式和分析方法。

（一）串連不同資料：執法機關須與時俱進

資通訊科技日新月異，犯罪手法朝利益合流、專業分工、組織扁平化、跨國境等多面向發展，使執法機關難追查犯罪集團源頭，對社會治安帶來極大威脅與挑戰。執法機關擔負犯罪預防及偵查任務，犯罪者的作案手法涉及各方面知識，執法機關須與時俱進，善用相關資訊及資料庫。若能善用人工智慧、機器學習及深度學習等技術，可從大量資料中，即時識別人員、位置、對象、事件或時間戳記等各種特徵，進行謹慎仔細的篩選作業，能協助執法人員評估刑事案件的相關證據。另外，執法機關可透過增加數位化資料來源，串連不同系統資料，升級數位技術的發展，期運用識別，收集，檢查，分析和呈現等程序，提高打擊犯罪活動的執行效率[9]。

（二）看到、聽到、指揮到：知識整合與智慧分享，快速掌握情資

資料是分析的根本，資訊系統整合須仰賴資訊分析專家，從犯罪偵查人員角度整合資料庫，挖掘大量資料的關鍵價值，快速掌握情資，一步步打破跨機關的資訊藩籬，結合民間資源，提升犯罪偵防能量，進而建構完整的智慧安全防護網。人工智慧能幫助執法機關識別和預測可疑的人員和地點，但警務工作的人工智慧應用還處於初期階段，一些新穎的預測演算法正在與其他傳統的警務方法一起進行試驗，將來以人工智慧為基礎的系統，有機會利用資訊技術為社區服務，打擊犯罪，維護人民權利，確保公共安全，防止暴力，或在執法機關中主動做出決策[7]。

（三）導入人工智慧：執法機關專注優先任務

執法機關預算資源不斷被刪減，執法人員需完成工作需求量卻不斷增加。須引進或善用人工智慧，讓執法機關能夠在人員缺乏情狀下，仍能透過電腦技術輔助人類進行學習、推理和分類，協助打擊犯罪、提高執法效益、降低誤判風險、減少大量證據的收集成本，並將人力資源轉移到優先任務上，有效率地處理複雜、多元且龐大的執法服務工作[9]。例如，社群資訊和媒體等相關的大量資料，可用於識別犯罪分子並預測可能處於危險中的被害者，以視覺化呈現人

脈網路、歷史案件、關聯強度等資料分析。但這樣的預測分析是一個複雜過程，它運用大量的資料，預測可能產生或發生的結果[11]。人們每天都生活在大規模資料資訊中，如何運用人工智慧技術，快速獲取，低錯誤率和準確預測犯罪行為、追蹤資金流動及加強跨機構資料交流[4]，成為執法機關的努力方向。

參、智慧警務的人工智慧運用現況

一、前瞻執法的應用現況

刑事司法工作繁雜、耗時，容易出現偏見和錯誤，犯罪預測可更有效輔助分配警務資源，執行警務工作[6]。但執法機關人員普遍對人工智慧存在專業知識的認知不足問題，須了解最新科技進展的實務可行應用。

(一)英國：國家警察資料庫之整合平台

英國的國家警察資料庫（The Police National Computer，PNC）由 PNC 資訊存取小組（PNC Information Access Panel，PIAP）管理，主要小組成員為國家警察局首長委員會（National Police Chiefs' Council，NPCC），警察當局協會（The Association of Police Authorities）和內政部（Home Office）。並提供英國、北愛爾蘭的警察部門、稅務海關總署、安全局（軍情五處）、秘密情報局（軍情六處）、國防情報人員、工作和養老金部、國家警察局長理事會等使用者存取資料。運作架構如圖 1，可區分警務治理及技術程序兩部分探討[3, 9]。

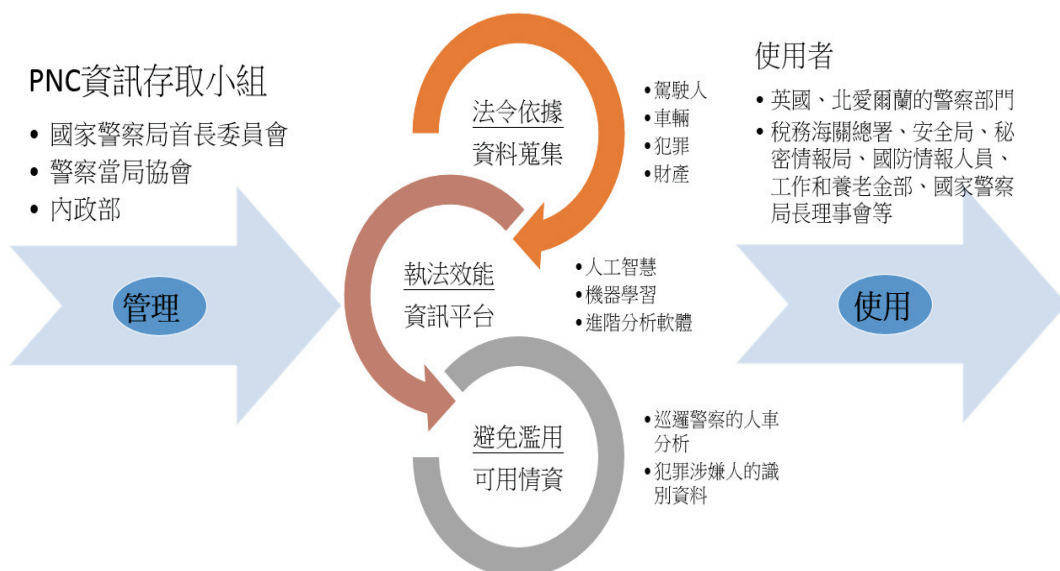


圖 1：英國國家警察資料庫運作架構

1. 警務治理

(1) 法令根據

根據法令，在不違反個人資料保護法、隱私權等法律問題下，蒐尋大量人為跡證或數位證據，使用人工智慧技術。並建立一個監督小組，由警察、法律及技術專家組成，專門監督人工智慧的使用成效及結果，以符合法規，避免偏見。

(2) 執法效能

在有限經費、人力及時間下，節省開銷，建立績效評量標準與促進執法效能。

(3) 避免濫用

制定技術道德規範，律定執法人員的使用時機、範圍與程序，避免資料濫用。

2. 技術程序

(1) 資料蒐集

2007 年，該國家警察資料庫原本僅為查察贓車（Stolen Vehicles）的資料庫；之後，不斷地精進改善，擴及檢查駕駛人（Drivers File）、車輛（Vehicle File）、犯罪（Names File）和財產（Property File）等資料庫，並納入檢查犯罪紀錄、特定人員、遭竊財產及申根資訊等更多調查功能。2019 年，儲存 35 億筆記錄，供 51 個英國執法機關，查詢 220 個資料庫[5]，並思索納入人工智慧於警務工作。

(2) 資訊平台

發展人工智慧、機器學習和進階分析軟體平台，整合執法機關相關資料，發掘犯罪模式、幫助處理犯罪和加強執法能量。

(3) 可用情資

即時產出可用情資。例如，巡邏警察的人車分析、犯罪涉嫌人的識別資料等。

(二) 英國：人工智慧為基礎之危害風險評估工具

2017 年，英國杜倫警察（Durham Constabulary）透過人工智慧為基礎的危害風險評估工具（AI-based Harm Assessment Risk Tool，HART），用統計方法結合再犯風險的預測，為監護人員提供參考意見，緩解刑事司法系統的壓力。本危害風險評估工具，具備四項程序特色，如圖 2[4]：

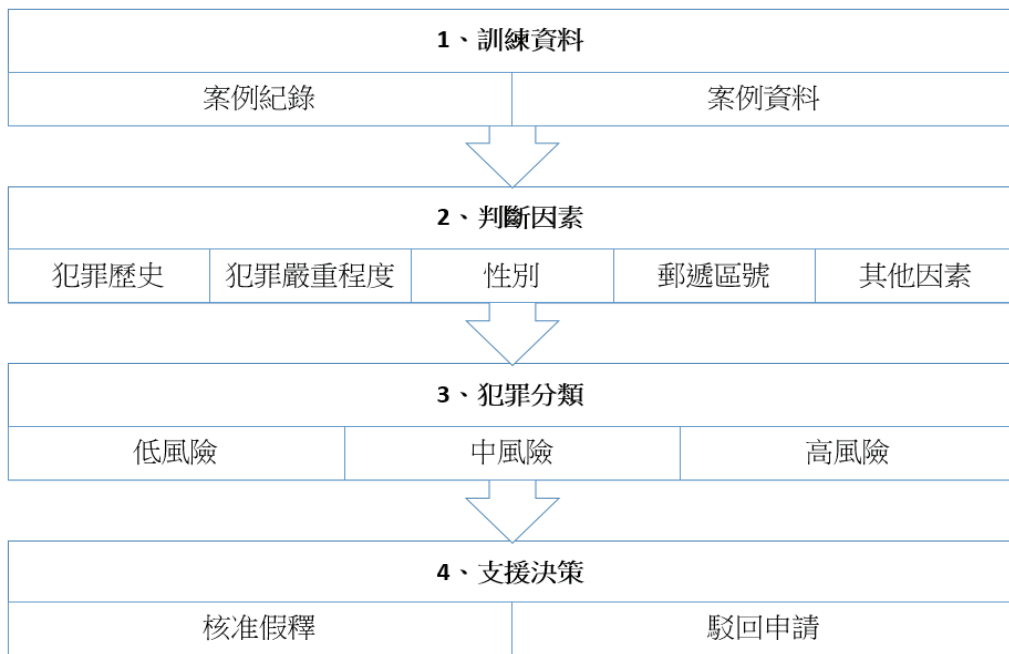


圖 2：英國人工智慧為基礎之危害風險評估工具程序

1. 訓練資料

接受 104,000 個英國案例紀錄與資料的訓練。

2. 判斷因素

該人工智慧分析，以犯罪歷史、犯罪嚴重程度、性別、郵遞區號和其他預測等因素來判斷，了解刑事司法監督下的犯罪者再次犯罪的可能性。

3. 犯罪分類

以嫌疑人是否會在未來兩年重新犯罪為分類標準，將嫌疑人分為三個風險級別：低風險、中風險或高風險。然而，這種演算法工具也同樣有可能將人類偏見帶入系統中，未必完全客觀精準。

4. 支援決策

利用人工智慧，協助矯治機關，使用資料進行決策參考。

(三) 美國：地域認知系統之即時警告系統

2008 年，紐約市警察局（New York Police Department，NYPD）和微軟公司共同開發的地域認知系統（Domain Awareness System，DAS），將大量不同來源、低價值、數量繁雜、關聯性不明確的分散資料，以視覺化方式轉化為少量、易於理解、高關聯性、高價值的可用情資，可透過各機關間的資訊共享，交叉比對檢查，參考各種地圖資料，分析熱點的所在位置，在特定

區域內將犯罪紀錄圖像化，輔助全球定位系統，分析犯罪資料，發掘關鍵線索，探索關聯事實，進行犯罪分析和問題偵測，找出事件脈絡。本即時警告系統，具備五項架構特色，如圖 3[7, 8]：

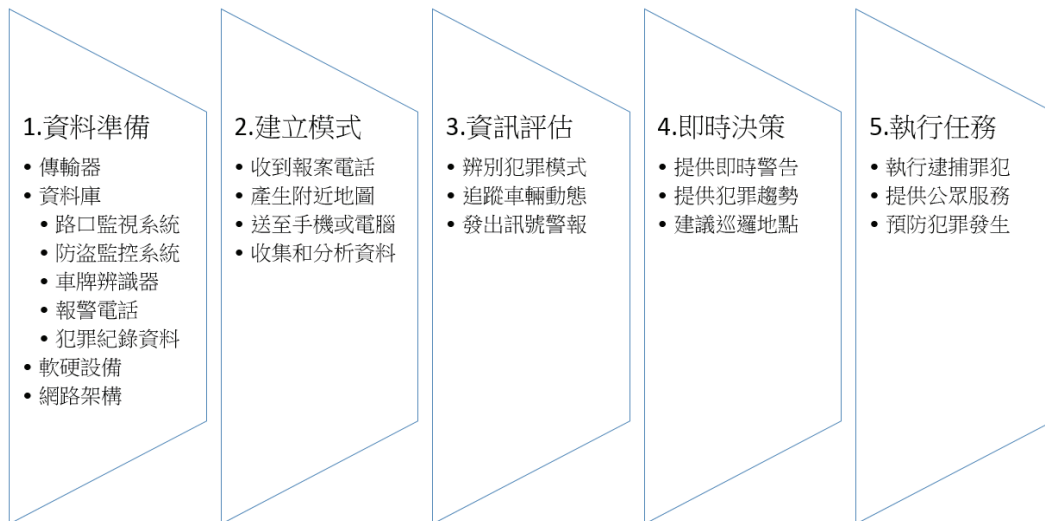


圖 3：美國地域認知系統之即時警告系統架構特色

1. 資料準備

該系統包含傳輸器、資料庫、軟硬設備和基礎網路架構的即時分析工具。該資料庫，包括路口監視系統（Closed Circuit Television，CCTV）、防盜監控系統、車牌辨識器、報警電話、過去犯罪紀錄及其他公開資料庫等。

2. 建立模式

當紐約市警察局收到 911 報案電話時，該系統可產生附近地區的互動式地圖和影像，並傳送到紐約市警察局的智慧型手機，移動設備或桌上型電腦，讓執法人員收集、掌握和分析犯罪相關資料。

3. 資訊評估

分析人員可利用圖形介面，聯繫不同的活動資訊、地理位置等資料，整理相關線索、辨別犯罪模式、調配資源追蹤可疑車輛動態，應用於日常警務，發出訊號警報。

4. 即時決策

提供潛在安全威脅的即時警告、犯罪趨勢和模式給執法人員，提供巡邏或搜尋地點建議，協助做出決策。

5. 執行任務

執行逮捕罪犯、控制犯罪、提供公眾服務等任務，預防恐怖攻擊與街頭犯罪的發生。

(四) 臺灣地區：智慧分析資料，掌握問題關鍵

為監控治安狀況，政府或民間機關常廣設路口監視器，以數位化的攝影機對城市進行安全監控，資料龐大複雜，是犯罪偵查的核心數位資料；這雖被批評侵犯隱私權，卻也不斷協助執法機關查獲案件。2013 年，警政署為達治安改善成效，擴大整合各縣市的路口監視系統，建置雲端影像調閱系統，克服影像格式、資料傳輸技術、調閱系統迥異的任務，讓執法人員能跨轄區調閱，提高辦案即時性。2018 年，完成 19 個縣市、約 7 萬 5 千餘支路口監視器的整合作業，提供遠端影像調閱功能，達到全國影像無縫介接的目標[2]。如何結合人工智慧，朝向自動化處理判別，應用視訊濃縮、車牌辨識、物件偵測等智慧化監控，仍須不斷強化各類型案件手法的分析及工具的使用，方能有效節省員警人力，掌握辦案契機的關鍵。

未來，可導入數位化車牌辨識功能，納入人工智慧分析、過濾大量影片，再輔以人工確認，提取出有用的資訊，提升執法成效，期藉由機器的自我學習判斷，進一步引導並協助新進偵查人員進行情資的篩選、整理及分析。許多執法機關亦陸續提出下列規畫作為[2, 4]：

1. 群眾畫面的偵測、識別與警示

群眾活動畫面的自動偵測與警示，可快速篩選尋找失蹤人口、涉案人物或可疑車輛，如自動偵測人群的聚眾鬥毆、人潮移動軌跡、與特定人物或車輛。人臉資料庫，亦可協助人員識別協尋失智老人與涉案嫌犯；但人臉辨識需要平衡公共利益與自由隱私的本質，宜加強謹慎行事，避免人別身份的識別錯誤。

2. 透過智慧監控科技協助犯罪偵查

智慧影像分析的軟體技術，乃根據大量範本資料，從中學習人、事、物之特徵後，進行辨識作業，結構化處理影像資訊，將畫面從無意義的數位訊號轉為有意義的行為描述，例如，跨越警戒線、人潮移動軌跡、人臉辨識、車牌辨識等等。傳統監視器最大的問題在於長時間的人工監看下，會因疲勞造成疏失。連續監看螢幕會讓分析人員忽略部分細節，時間越長忽略越多的細節。如何透過先進的智慧影像分析科技，視訊濃縮、縮短辦案時間，協助解決這些問題，是目前執法機關犯罪偵查與預防的主流之一。

3. 警用無人機的警務輔助勤務

警用無人機可輔助執法機關執行治安及交通勤務，扮演空中巡邏角色，應用於偏鄉巡邏或大型集會維安，增加巡邏範圍與頻率。它結合熱顯像、警示燈及蜂鳴器等設備，具備自動排程巡邏、多機輪勤指派、影像即時回傳等功能。

4. 網路客服或聊天機器人的即時諮詢服務

為精進執法機關服務品質，可使用網路客服或聊天機器人技術，提供民眾一個即時諮詢的管道，不僅可減輕處理員警的人力負擔，也能夠提升服務品質。惟須經常更新問答內容的實用性與充實性。

二、智慧警務的面臨問題

人工智慧處理大量的數位照片、影片、刑案紀錄等檔案資料之警務治理任務，雖可協助達成執法任務，卻存在隱私侵犯疑慮、缺乏適當監督、資料錯誤率、或人為偏見等疑慮問題。

(一) 隱私侵犯疑慮

1. 隱私侵犯疑慮

人工智慧允許利用更好資源，改善執法結果。但是，須考慮道德因素，特別是隱私和資料處理的法律方面[9]。執法機關處理公眾資料，須避免侵犯隱私，或濫用資料，才能讓執法機關有足夠的技術、資源與能力，處理犯罪問題。

2. 適當監督管制

連結分析（Linkage Analysis）可根據作案手法、嫌犯描述或給定區域，串連嫌疑人與一系列事件的關係[13]。這樣的資料分析，須登入帳號管理、使用權限管制及事後稽核機制等適當監控，避免執法人員的濫權使用。

(二) 犯罪熱點佈署

透過大數據分析技術，可快速理解犯罪模式，提前掌握徵兆，有效達到預防犯罪效果，卻也存在放大執法成效差距的問題。例如：警方會在特定時段將主要警力佈署在市區犯罪熱點，降低犯罪率，相對降低其他偏鄉警力。對於臨時起意作案的犯罪行為，仍難事先預防監控。

1. 擔憂錯誤，減低誤報

執法機關開發預測分析系統，雖可輔助理解、研判、預測支持（或反駁）犯罪相關事件，但實際個案的犯罪分析中，尚難完整考量所有的犯罪特徵。例如：人臉識別或車牌辨識仍存在一定程度的誤差，偵測技術的準確性仍待持續改善[10]。更何況，沒有一種運算法是完美的，即使高達百分之九十，仍須人為介入輔助運用，注意誤差的影響後果，避免執法疏誤。

2. 放大人為偏見問題

人的偏見是根深蒂固的，很難剷除，人工智慧也會因而沿襲偏見。當人們參與人工智慧分析，在某種程度上會有意識或無意識地形成偏見，再導致主觀的結論。以人工智慧為基礎的系統還是有偏見的存在，偏見來自資料產生過程，演算法原理和系統設計邏輯等程序。由於這些來源都會有人為參與，使得偏見很難避免。對於弱勢群體如少數民族和窮人的偏見，可能會在以人工智慧為基礎的系統不斷複製，進而擴大其影響力。系統發出的警報中，可能存在偏見或甚至依據這些偏見，把這些街區發現的某些行為認定為犯罪可疑行為，形成惡性循環的可能性，影響警察、檢察官和法官做出決定[7]。當執法機關運用先進科技，期達到犯罪偵預目的時，需注意此一問題。

肆、智慧警務的建議對策

本節探討人工智慧於警務工作的運用現況，評析後續推行智慧警務的執法任務的可行作法，期強化刑事司法系統的偵查防治能量。

一、執法機關的人工智慧需求

(一) 資料縮減過濾分析

人工智慧可幫助查看大量資料，經過資料縮減後，執法人員只需查看系統過濾、分析過的標記內容，不需讀取所有資料，這樣執法人員就不會花費大量時間查看無意義資料[9]。執法機關可開發、運用人工智慧演算法，識別犯罪、協助調查、檢測調查對象活動、或描述一系列資料和資訊中特定對象的上下脈絡關係[11]。例如，在不良畫質的圖像或影像中，識別車牌或嫌疑人；以圖像分析法進行人臉辨識，可識別眼睛形狀，眼睛顏色和眼睛之間的距離等特徵；自動測速照相，能夠識別違規行為。

(二) 閱讀、知道和理解人工智慧

人工智慧的知識、技術、或經驗為跨機關的協調合作，提供潛在、巨大的可能性。執法人員需適當的訓練來閱讀、知道和理解人工智慧，以充分利用其優勢。它雖能輔助決策判斷，尚不足以獨立完成執法人員的決策形成，仍要人承擔決策結果，即使執法人員透過人工智慧演算法，輔助判斷或預測事件的發生，面臨著重要決定，仍須根據執法專業續行判斷。這判斷過程須經過充分培訓，以具備發現資料或系統，可能的判斷錯誤或疏漏。

(三) 產官學的互助合作

警力有限、民力無窮，產官學的互助分工、協力合作，為推動科技建警或智慧警務的不二法門。號召產官學共同合作建構社會安全防治網，善用智慧化、行動化、雲端化之警政資訊系統，融入警務服務流程，提高勤務機動性，以強化科技辦案能力，提升治安管理能量，跟上時代潮流，也是執法機關戮力合作的致力方向。

二、整併地域性資料庫，提升資料整合分析能量

(一) 情資共享整合數位資料

人們每天都生活在儲存大量數位資料的環境中，執法機關可善加優化處理這些資訊，期進一步識別、收集、檢查、分析和呈現這些資訊，達成科技執法目的。執法機關雖收集大量的歷史犯罪資料，仍需不斷充實、整合相關執法機關、公務機關或第三方資料，提升資料分析能量。例如，2001年，911恐怖攻擊事件後，美國開始致力整併不同執法機關的資料庫資料，再建立

資料共享方式，分送給各個機關。

(二) 關聯分析巡邏犯罪熱點

評估、分類、預測未來犯罪的地點、位置，須納入案件情資關聯分析，進行未來犯罪的熱點分析[3]，並事先對最需要的地方，投入有限的巡邏資源。

三、聯合查緝專案，納入資訊專業人員

(一) 數位跡證無所不在

幾乎所有的執法機關調查任務，均須處理電子人為跡證或數位證據，故任何連續或長期的聯合查緝專案小組，均要納入資訊專業人員，處理潛在高價值資料之數位跡證。

(二) 大範圍歷史犯罪資料

預測分析過去的歷史犯罪資料，應納入大範圍資料，宜避免限定單一區域性資料[3]，期有效識別犯罪風險、強化分析效能、提升執法人員的判斷力。

(三) 異常偵測驗證假設

犯罪團體或人員往往會隱藏非法行動，減少警方的注意力。嫌疑人被逮捕時也會意圖運用偽造資料，謊報身份。將人工智慧技術應用於預測性執法任務中，可幫助調查人員的即時反應能力，協助快速處理犯罪事件。但相關整合的警務應用仍然有限，尚處於持續發展中。人工智慧提供的許多可行機會，卻又存在誤判風險，執法機關必須同時使用人臉辨識或多個資料庫，加以驗證被害人、證人或嫌犯所稱事項是否為真。

伍、結論

警務工作的需求資料，往往散置於各資訊系統，情資整合、合併是一項大工程，需有經常性地資料交換與維護，方能歷久彌新。執法機關彙集、分享各種豐富的犯罪紀錄資料，已廣泛運用於偵查、逮捕等執法應用。執法機關正逐漸將人工智慧運用在治安實務中，以解決執法及調查的需求，例如，影像中識別個人的違規行為，或從執法機關資源中開發犯罪預測。如何利用人工智慧等新興技術是警務工作的可行方向，也能替執法部門提供許多前瞻應用的可能性；然而，尚無法全部取代人工處理，相關創新作為的背後，亦會相對出現誤判、錯誤率等其他缺失問題，宜審慎面對、因應。

參考書目

一、中文部分

1. 周秉誼，〈淺談Deep Learning原理及應用〉，《國立台灣大學計算機及資訊網路中心電子報第38期》，2016年9月20日（存取日期2019年6月2日），<
http://www.cc.ntu.edu.tw/chinese/epaper/0038/20160920_3805.html>。
2. 蘇清偉，黃家揚，〈內政部警政署「前瞻警政、科技警察」智慧聯網專案〉，政府機關資訊通報，第352期，107年4月，頁1-9。

二、英文部分

1. Babuta, A. "Big Data and Policing : An Assessment of Law Enforcement Requirements, Expectations and Priorities," (Access Jul. 26, 2019), <
https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf>.
2. Campbell, T., "Opportunities and Challenges from Artificial Intelligence for Law Enforcement," Future Grasp, Jul. 2018, pp. 1-10.
3. Datalynx, "Police National Database: Connecting Law Enforcement throughout the UK," (Access Jul. 26, 2019), <http://www.datalynx.net/case-studies/police-national-database/>
4. Hazenberg, A. and Beridze, I., "Artificial Intelligence and Robotics for Law Enforcement," United Nations Interregional Crime and Justice Research Institute (UNICRI), 2019, pp.1 -44.
4. Joh, E.E., "Artificial Intelligence and Policing: First Questions," Seattle University Law Review, Vol. 41, No. 4, 2018, pp.1139-1144.
5. Levine, E. S., Tisch, J., Tasso, A., and Joy, M., "The New York City Police Department's Domain Awareness System," INFORMS Journal on Applied Analytics, Vol. 47, No. 1, Jan. 2017, pp. 70-84.
6. O'Connell AM, S., "Artificial Intelligence: A New Era in Policing, " (Access Jul. 26, 2019), <
https://www.glaconservatives.co.uk/uploads/1/1/7/8/117899427/artificial_intelligence_in_policing_report.pdf>.
7. Perrot, P., "What about AI in Criminal Intelligence? From Predictive Policing to AI Perspectives," European Police Science and Research Bulletin, Vol. 16, Summer 2017, pp.65-76.
8. Rigano, C. "Using Artificial Intelligence to Address Criminal Justice Needs," National Institute of Justice Journal, Vol. 280, Nov. 2018, pp. 1-10.
9. Ryżko, D., Gawrysiak, P., Kryszkiewicz, M., and Rybiński, H., Machine Intelligence and Big Data

in Industry, (Switzerland: Springer International Publishing, 2016), pp. 11-170.

10. Wulf, J., “Artificial Intelligence and Law Enforcement,” Information Security Reading Room, SANS Institute, 2017.

轉載自『2019年第十四屆海峽兩岸暨香港、澳門警學研討會交流論文集』頁299-312。