偵查科技 vs. 科技偵查？以偵查思維為橋接

Comparative Analysis of Investigative Technology vs. Technological Investigation: Exploring Investigative Thinking

施志鴻
中央警察大學刑事警察學系

黃壬聰
內政部警政署刑事警察局

*蘇育緯
基隆市警察局第三分局
ci1114013@mail.cpu.edu.tw

摘要

網路發達亦導致犯罪形態與手法而產生巨大的改變，傳統犯罪偵查標的之「物理世界」與「實體身分」，已逐漸移轉至「網路世界」與「虛擬ID」，許多偵查人員因不熟悉電腦資訊而存在「科技焦慮」，面對網路案件偵查往往因技術障礙而形成瓶頸，無法將犯罪者繩之以法。犯罪偵查目的為系統性尋找、蒐集與分析資訊，以確認犯罪事實與嫌疑人的過程。為達此目的，偵查人員須具備取得、判斷與分析相關資訊，擬訂與驗證偵查假設與方向，直到確認犯罪事實與嫌疑人。在網路犯罪中，犯罪者是運用「網路」實施犯罪行為，與物理世界存在連結而無法切割，倘偵查人員受到網路技術之限制，忽略犯罪偵查蒐集與分析資訊、形成與驗證假設等，將致使偵查效能無法充分發揮。緣此，本文由犯罪偵查本質討論「偵查科技」與「科技偵查」的分野與差異，以「網路兒少性剝削犯罪偵查案例」偵辦過程為個案研究對象，涉案嫌疑人使用俗稱黑莓卡之香港門號sim卡上網、假資料註冊社交軟體帳號後，用黑莓卡（+852開頭之境外門號）於國內漫遊上網，隨機在社群網站及交友平台尋找獵物，誘騙未成年少女自拍裸照、媒介未成年少女性交易及販售彩虹菸、毒咖啡包等新興毒品，本文試圖剖析從案件啟動至案件建構之偵查假設與思維，勾勒出將傳統偵查與科技偵查融合，以因應新型態犯罪之樣版，作為我國在當今網路時代偵查思維訓練與教學研究之參考。

關鍵詞：網路犯罪、偵查思維、偵查科技、科技偵查。

Abstract

The development of the Internet has also led to huge changes in the forms and methods of crime. The "physical world" and "entity identity" that are the traditional targets of criminal investigation have gradually shifted to the "online world" and "virtual ID". Many investigators have People who are not familiar with computer information have "technological anxiety". When faced with the investigation of Internet cases, technical obstacles often form bottlenecks, making it impossible to bring criminals to justice. The purpose of criminal investigation is the

process of systematically searching, collecting and analyzing information to confirm criminal facts and suspects. To achieve this goal, investigators must be able to obtain, judge and analyze relevant information, formulate and verify investigation hypotheses and directions, until the criminal facts and suspects are confirmed. In cybercrimes, criminals use the "network" to commit crimes, which are connected to the physical world and cannot be separated. If investigators are limited by network technology, they neglect collecting and analyzing information, forming and verifying hypotheses, etc. in criminal investigation. , which will result in the inability to give full play to the investigation efficiency. For this reason, this article discusses the distinction and differences between "investigation technology" and "technological investigation" based on the nature of criminal investigation. It takes the investigation process of the "Internet Child Sexual Exploitation Crime Investigation Case" as the case study object. The suspect involved in the case used a card commonly known as a BlackBerry card. After using a SIM card with a Hong Kong phone number to surf the Internet and registering a social software account with fake information, use a BlackBerry card (overseas phone number starting with +852) to roam the Internet in the country, randomly looking for prey on social networking sites and dating platforms, and luring underage girls. Self-portraits of nude photos, sex trade of underage girls through media, and sale of emerging drugs such as rainbow cigarettes and poisonous coffee bags. This article attempts to analyze the investigative assumptions and thinking from case initiation to case construction, and outlines the integration of traditional investigation and technological investigation to cope with new The model of pattern crime serves as a reference for our country’s investigative thinking training and teaching research in today’s Internet era.

Keywords: Internet crime, investigative thinking, investigative technology, technological investigation.

壹、前言

隨著網路資訊與行動上網技術的迅速發展，幾乎人人皆擁有具上網功能手機，並在虛擬網路平台擁有數個不同身分或帳號，從事社交、通訊、購物、搜尋資訊等行為，犯罪者亦利用境外門號、假資料註冊、隱藏真實上網IP等手法，隱匿真實身分以規避警方偵查。傳統犯罪偵查已從「物理世界」與「實體身分」，逐漸移轉至「網路世界」與「虛擬ID」，對偵查人員帶來高度挑戰。犯罪分子正在利用數位科技擴大犯罪範圍並增加其犯罪影響。但科技進步亦為偵查機關提供巨大機會來改變其打擊犯罪方式。為充分受益於科技並跟上科技和網路設備的發展，偵查必須具備有效發揮作用所需的偵查科技，如何有效發揮與運用「偵查科技」，已是當前偵查實務最重要議題。

依據「歐洲對抗犯罪威脅跨領域平台」(European Multidisciplinary Platform Against Criminal Threats, EMPACT)策略，歐盟制定2022年至2025年戰略需求(EU-STNA)，共列出「數位技能與新興技術運用」（digital skills and use of new technologies）、「高風險犯罪網絡之打擊」（high-risk criminal networks）、「非法財務資產調查」（financial investigations）、「執法合法與情資交換」（cooperation, information exchange and

interoperability）、「犯罪預防」（crime prevention）、「文書詐欺之辨識」（document fraud）、「刑事鑑識」（forensics）、「基礎權利與資料保護」（fundamental rights and data protection）等八類執法人員核心能力，其中「數位技能與新技術使用」被視為首要需求[1]。

偵查科技運用（如手機鑑識、網路封包分析、遠端監視設備等）已是當前偵查人員基本技能，然受限於知能、訓練、資源、法律等限制，偵查科技能力水平尚且參差不齊。傳統偵查人員可能因不熟悉資訊科技而存在「科技焦慮」（technophobia），在偵辦涉及網路等案件時，限縮其偵查思維運用空間，徒增案件偵辦瓶頸。以網路犯罪偵查為例，偵查起點往往為IP調閱與解讀，若案件涉及境外IP致無法查明嫌疑人身分，可能自認無法突破而予以簽結等。偵查科技能力落差轉型必然現象，隨著訓練普遍與年輕世代入警，全面提昇應是指日可期之事。然而，在推動偵查科技過程中，倘單方面過度偏重偵查科技，忽略傳統偵查思維與能力，恐加深傳統偵查人員的「科技焦慮」，限制其在網路相關案件傳統偵查思維與能力的發揮與運用；而新進偵查人員若僅過度依賴偵查科技等工具，亦易致使忽略偵查思維與能力培養風險。為因應前述問題，本文建議從犯罪偵查本質，釐清與界定「科技偵查」與「偵查科技」之必要，並以實際案例的偵查思維過程呈現兩者內涵與差異，建立以偵查思維為核心作為發展偵查科技，以為我國偵查專業發展與培訓發展的參考。

貳、文獻探討

一、網路犯罪類型

學者Brandl將犯罪偵查定義為「為達成特定目的，進行蒐集犯罪相關資訊的程序」[2]。警察偵查階段是大多數刑事司法系統追訴犯罪起點，擔負發覺與受理犯罪事件、蒐集保全相關事證、調查犯罪事實、連結嫌疑人及提出證據協助起訴等功能，是一個系統性尋找、蒐集與分析資訊，以確認犯罪事實與嫌疑人之過程[3]。為達此目的，偵查人員須具備取得、判斷與分析相關資訊，擬訂與驗證偵查假設與方向，直至確認犯罪事實與嫌疑人。犯罪偵查主要可分為被動式（reactive）以及主動式（proactive）兩種偵查模式，前者通常針對公眾檢舉犯罪而實施，是一種以「犯罪」為核心的偵查模式；後者則以犯罪者為起點，通常是根據警方情報啟動並針對組織犯罪或慣犯等[4]。無論採取何種模式，原則上會包含「啟動偵查」、「初期偵查」、「偵查評估」、「嫌疑人管理」、「證據評估」、「移送起訴」、「案件管理」及「法院審理」等過程，端視個案性質而有不同路徑，某些案件初期即可鎖定嫌疑人，故可直接進入嫌疑人管理階段；而部分案件則需進一步偵查，始往後續階段的可能性[5]。

六〇、七〇年代，多數案件是由警方巡邏查獲或大眾提供線索而偵破，偵訊取得自白亦扮演重要角色。80年代以後，物證逐漸受到重視，鑑識科學（特別是DNA、指紋鑑定等）成為科學辦案代名詞[6]。近數十年，犯罪者利用資通信技術易匿名性，以及現行法律與科技存在落差、難以遭到偵查與起訴等特性，犯罪實施逐漸由實體世界轉移到數位世界（以下統稱網路犯罪）。網路犯罪依網路所扮演角色，可分為「網路依賴犯罪」（cyber-dependent crime）以及「網路借助犯罪」（cyber-enabled crime）兩種類型。「網路依賴犯罪 」係指通過使用資通信技術設備實施犯罪，這些設備既是犯罪工具，又是犯

罪目標（例如，開發和傳播惡意軟體以獲取經濟利益，駭客竊取網路資料或財產等）；而「網路借助犯罪」則為透過使用資通信技術，讓傳統犯罪規模或範圍得以擴大[7,8]。

網路犯罪依照資通信技術依賴及使用程度，可區分為下列三種型態：第一、狹義網路犯罪：例如網路勒贖（ransomware）、駭客攻擊（hacking）、深偽技術（deep fake）等，犯罪者多具網路與資訊專業並隱匿在虛擬世界，偵辦人員所需偵查科技專業技能最高；（二）運用新型科技實施傳統犯罪：例如電信詐欺、網路賭博、加密貨幣洗錢等，犯罪者通常具組織性並一定專業性，利用科技進行犯罪分工與斷點，其行為會同時涉及虛擬世界與實體世界，偵查人員須同時運用傳統偵查技巧與新興偵查科技，所需科技偵查專業次高；（三）在實施犯罪時利用科技便利隱匿身分：例如運用假帳號或人頭帳戶隱匿身分進行非法物品買賣、色情媒介等，此部分所犯罪者主要仍在真實世界實施犯罪行為，僅利用資通訊管理漏洞避免被加以連結，所需科技偵查專業能力則相較前述兩者為低。

二、偵查人員科技焦慮

面對科技發展帶來社會型態改變過程，研究發現某些人存在抗拒新技術態度與焦慮，「科技焦慮」（technophobia）概念因而被提出討論[9]。在電腦科技發展階段，Jay將「科技焦慮」定義為（1）拒絕討論甚至思考電腦，（2）對電腦具恐懼或焦慮感，（3）對電腦產生敵意或詆毀等 [10]；Rosen 和 Weil則將「科技焦慮」定義為（1） 對目前或未來與電腦或電腦相關技術存在焦慮，（2）電腦或電腦相關技術對社會影響抱持負面態度，（3）實際運用或考量未來運用電腦相關科技時，存在負面認知與批評等[11]。研究發現，具較資深經歷者存在較高的科技焦慮[12]；而執法人員與學生同樣皆有高度科技焦慮[13]。

另有研究者從警察組織文化討論導致科技焦慮的因素，Khan[14]認為警察組織本身特徵，包含使命感、渴望行動、憤世嫉俗和悲觀主義、懷疑、孤立與團結、保守主義、男性主義、 實用主義等組織文化，會形成缺乏諮詢與溝通管道、長時間工作、提出績效的壓力、計畫常被打斷、時效壓力、輪班工作、工作時間無法預期、下班後被召回、無法掌握足夠的主動性等特性。前述警察文化特性對在職學習形成阻礙，致使抗拒從課堂及書本學習知識或解決問題方法，並而執著在傳統偵查方法與手段，亦是助長偵查人員科技焦慮的重要因素。網路犯罪的特性亦是阻礙偵查人員偵辦動機因素，Goodman[15]指出警察不關心網路犯罪偵查有如下原因：第一、從警動機：許多警察選擇此份工作是因希望幫助民眾或抓捕壞人，而非處理複雜的科技犯罪；第二、偵查困難度：網路分散性致使蒐證困難，而網路跨域的法律管轄問題亦增加執法挑戰；第三、資源不足：缺乏專門訓練和設備，調查網路犯罪花費成本高昂；第四、法律和政策支持不足：法律體系和政策未能有效支持對網路犯罪的追查和起訴。

綜合前述文獻，強化偵查人員的偵查科技能力，提昇網路犯罪偵查量能過程，存在諸多障礙。其中，資通訊技術對偵查人員（尤其資深人員）產生「科技焦慮」，以及偵查科技未與偵查思維結合，致使被歸類為技術問題與門檻，是阻礙偵查人員願意學習與運用偵查科技，而偏重於依賴傳統偵查手段原因之一。基於此，本文提出區分「科技偵

查」與「偵查科技」差異，從偵查思維角度重新理解偵查科技的定位，或可讓資深偵查人員採納偵查科技的學習與運用，同時亦可引導新進偵查人員重視偵查思維養成。

三、科技偵查與偵查科技的嘗試分野

偵查是透過偵查作為蒐集資料形成假設，引導後續偵查作為進一步蒐集資料，並檢驗假設過程。除前述狹義網路犯罪型態，多數犯罪是運用資通信技術擴大犯罪規模或隱匿其身分，但其犯罪仍與現實世界存在連結尚無法切割，偵查思維仍有其運用的重要性。倘偵查人員侷限於科技門檻的限制，在偵查初期即停止偵查，而忽略偵查本質為持續蒐集與分析其他資訊、形成假設、實施偵查作為驗證假設等本質，將致使偵查效能無法充分發揮，致使錯失案件偵破之契機。綜上所述，傳統偵查與偵查科技在偵查客體、證據性質、偵查方法、證據分析等具有差異，兩者比較如下表。

表一：傳統偵查與科技偵查思維比較

	傳統偵查	科技偵查
偵查本質	蒐集資料形成假設，引導後續偵查作為蒐集資料，並進一步檢驗假設過程	
偵查客體	侷限在物理世界及實體身分	除物理世界及實體身分，並涉及網路世界、虛擬身分
證據性質	存在物理空間，具時空限制性與不易竄改，在符合程序要件即可蒐集保全	存在虛擬空間，數位證據具容易竄改、不受時空限制性，並受限於密碼等難以蒐集保全
偵查方法	現場採證、監視器分析、跟監、詢問等偵查技術	除傳統偵查技術外，尚須透過資通訊等科技協助證據蒐集分析
證據分析	多可透感官或者鑑識分析證據內容與特徵	難以直接判斷證據內容與特徵，需透過資料分析或鑑識解析始得瞭解證據內容
思維瓶頸	對科技不熟悉或排斥，致偵查停滯	過度依賴科技，忽略傳統偵查方式

資料來源：自行研究之成果

由上述比較可知，無論傳統偵查與科技偵查本質皆屬於犯罪偵查一環，然而因網路犯罪特性，犯罪行為與結果多存在於虛擬世界，故科技偵查須結合偵查科技技術，以蒐集並分析犯罪事證。本文對偵查科技作出以下界定：「運用各種資通訊等科技，協助蒐集數位等相關事證」；而科技偵查則為：「以行為人之視野為出發點，分析、理解行為人如何使用科技進行犯罪，再藉由各種偵查技術（包含偵查科技）協助蒐集事證，進行偵查假設與驗證，以遂行偵查目的之過程」。

犯罪偵查過程中，偵查人員依據案件中相關事證，包含被害人或證人供述、現場跡證、監視器畫面、通訊軟體對話紀錄等各項證據，分析研判，運用偵查思維做出決策，研判是否需持續追查線索、蒐集事證、調查犯罪事實、查明犯嫌身分，聲請拘票、搜索票等強制處分，拘捕犯罪嫌疑人到案，製作詢問筆錄、移送檢察署偵查，逐步確認犯罪事實，偵查人員做出正確偵查決策之能力，與案件偵辦結果正確與否高度相關。偵查決策是偵查人員經由案情分析、證據蒐集和查緝犯罪嫌疑人的偵查過程中之專業性思維[16]。本文試圖以實施犯罪時利用科技便利隱匿身分的犯罪類型「網路兒少性剝削犯罪偵查案件」為案例，呈現偵查人員面對犯嫌使用境外門號以假資料申請帳號等偵查困境

時，如何由傳統行為特徵分析，搭配多重網路身分及境外門號漫遊上網歷程等各項資料交叉比對，再透過文字訊息分析嫌疑人之人格特質，並搭配社交工程之科技偵查技巧，取得線索進而掌握嫌疑人及共犯真實身分，並經由搜索與詢問以確認犯罪事實之目的，以偵查思維為橋接，呈現「偵查科技」與「科技偵查」兩者分野與差異。

參、案例分析

一、 案件受理

被害少女母親因知悉少女所使用之Instagram帳號密碼，某日登入少女所使用之Instagram帳號後，發現與帳號xi〇〇〇〇11〇〇之人有許多異常訊息，且被害少女在嫌疑人誘導下自拍多張裸露照片、影片傳送給對方，因此帶同被害少女向警報案，派出所受理員警依規定通報社工到場陪同製作筆錄。

受理員警根據雙方Instagram帳號對話紀錄詢問被害少女，是否認識對方？是否有與對方見過面？對方年齡、特徵？ 被害少女回答「不認識。」、「沒有。」、「忘記了。」、「不記得。」，供稱「聊天內容都是開玩笑的」等，消極配合警方調查。偵查初期，警方僅能取得被害少女母親提供的對話紀錄截圖畫面。警方進一步調查發現，嫌疑人於社群網站Instagram以暱稱「㊗」之帳號(xi〇〇〇〇11〇〇)，向未成年之十五歲少女以介紹工作賺錢為由，誘騙被害少女自拍傳送裸露私密處身體部位等影片及照片。承辦刑警調閱Instagram帳號xi〇〇〇〇11〇〇申請資料，發現註冊帳號未使用真實姓名、帳號驗證門號為+8526564〇〇〇〇(香港門號)、登入IP 203.160.71.168為境外電信商UNICOM-HK香港中國聯通，因相關資料皆於境外，故將案件簽結歸檔。

本案通訊作者（下稱筆者）在審核此簽結案件，從雙方對話紀錄內容研判，犯罪人在境內犯案可能性甚高，存在將其查緝到案的機會；且由犯罪手法判斷，嫌疑人再犯其他案件可能性高，恐有更多少女受到傷害，故決定重啟偵辦此已簽結之案件。

二、 過濾可能嫌疑人

因本案涉案Instagram帳號登入IP與驗證門號均非屬本國業者，無法查詢實際使用者，故由被害人母親提供被害少女與嫌疑人之間完整對話紀錄，進行深入分析。

1.文字內容分析人格特質

涉案帳號xi〇〇〇〇11〇〇所發送之文字訊息內容簡短、發送速度快、頻率高、用語皆為繁體字，未出現簡體字或大陸用語，內容提到「你目前裝扮是怎樣」、「要賺錢就快回覆」、「全空一樣全身」、「我就當你經紀人」、「我過濾保護你」、「但我要的話 我要免費」、「我世足他媽輸270你最好乖乖的」等內容，推測犯罪人應為國內年輕人，具有經濟基礎，年齡為25歲至35歲之間（對話紀錄如圖一）。

圖一: 本案Instagram對話記錄研判犯罪人年齡等特徵

2.地理位置研判

犯罪嫌疑人與被害少女對話訊息中，提到要求被害少女坐計程車「到新莊化成路」、「下來殘障廁所鎖門」、「我要進去先解決一次」（如圖二），研判其居住應在新北市新莊區。

圖二: 從對話訊息研判犯罪人位於境內，與新北市新莊區有地緣關係

3. 網路帳號分析

網路帳號的英數組合與使用者可能具有一定程度之關聯，就中文使用者而言，網路帳號之英文字母組合部分，可能是使用者之英文名或中文英譯，數字部分可能為生日。

若嫌疑人刻意隱匿真實身份，可能會使用隨機的英文字母或數字組合。同一組帳號可能存在於其他網路社群平台中，其他網路社群之相同帳號，可能因而透露出嫌疑人之個人資訊等重要線索，但經查涉案帳號xi〇〇〇〇11〇〇在其他網路平台查無相關線索。

4.通聯分析

嫌疑人使用社交軟體Instagram註冊帳號，雖然未使用真實姓名且使用境外門號漫遊上網，但上網仍需要使用電腦或手機等硬體裝置。雖然涉案帳號之驗證門號+8526564〇〇〇〇是境外電信商，無法查知門號基資，但該門號如果是在國內漫遊上網，便會使用國內電信業者之4G基地台，因此本案亦可從涉案境外門號在國內漫遊上網之基地台歷程及雙向通信紀錄找尋線索。經報請檢察官指揮偵辦，調閱境外門號於國內漫遊之雙向通聯及上網歷程通信紀錄（如圖三）顯示+8526564〇〇〇〇境外門號曾經搭配使用之手機IMEI碼有3556〇〇〇〇〇〇〇〇050、3555〇〇〇〇〇〇〇〇530及3577〇〇〇〇〇〇〇〇450等三支手機。

圖三: 境外門號於國內漫遊之通信紀錄

經再報請檢察官調閱IMEI碼之雙向通聯及上網歷程，發現IMEI碼3555〇〇〇〇〇〇〇〇530之手機曾經搭配台灣大哥大門號090926〇〇〇〇受話及收簡訊，基地台位置位於新北市新莊區（如圖四）；門號090926〇〇〇〇申請人為設籍新北市新莊區之29歲男性陳〇〇，符合前述對犯罪人年齡與區域之假設。

圖四: IMEI碼之雙向通聯雙向通聯及上網歷程

（三）釐清嫌疑人涉案程度

人性具有好奇心且有時缺乏警覺性，而社交工程便是利用此種人性進行互動進而取得資訊的技術。本案從犯罪者「要賺錢就快回覆」、「但我要的話 我要免費」等文字訊息分析其喜好，研判嫌疑人對「想找工作」、「有賺錢需求」之「年輕女性」有強烈關注，便以此人物設定進行社交工程，試圖進一步取得更多有關犯罪人之線索。

1.運用社交工程取得嫌疑人微信帳號

經偵查人員以無關緊要的問題透過Instagram與嫌疑人攀談，嘗試取得其他線索，得知嫌疑人微信帳號暱稱「ㄉㄡ拉a孟」及嫌疑人可能居住於某捷運站附近之個人資訊（如圖五）。

圖五: 分析犯罪者喜好，以年輕女性帳號進行社交工程

2.取得嫌疑人門號

以社交工程技巧與嫌疑人攀談多日，逐漸建立熟悉感後，嫌疑人主動撥打電話給偵查人員，因而取得嫌疑人來電顯示之門號「095353〇〇〇〇」，以及嫌疑人後續以文字表示「在地下室」等資訊（如圖六）。

圖六: 嫌疑人撥打偵查人員電話，留下來電號碼及「在地下室」等資訊

3.經查該門號「095353〇〇〇〇」登記為NFJ-9〇〇〇車主鄭〇〇之聯繫電話，研判門號使用人為鄭〇〇、男性、23歲、住新北市新莊區建中街（如圖七）。

圖七: 以嫌疑人電話查出嫌疑人身分及使用車輛，與新北市新莊區具地緣關係

（四）建立共犯關係

1.從嫌疑人與被害人對話中文字內容分析，研判嫌疑人是經濟闊綽之台灣年輕男性，推測年齡為25~35間，而以社交工程技巧查知嫌疑人為鄭〇〇僅23歲、與當初之偵查假設並不相符。因此懷疑可能有其他嫌疑人涉案，再次從其他面向追查涉案帳號xi〇〇〇〇11〇〇之其他使用者。

2.上網IP分析

案件再次回到關鍵的涉案Instagram帳號xi〇〇〇〇11〇〇從登入IP歷程進行分析，2022年10月至2023年1月間，總共有221次登入紀錄，每次登入皆紀錄登入時間及IP位

址，其中發現曾經有4次登入之IP為國內電信之業者101.8.0.0至101.15.255.255配發之網段。

3.鎖定嫌疑人B

向國內電信業者查詢IP對應行動上網之門號，得知用戶為門號090926〇〇〇〇申請人為陳〇〇、男性、29歲、帳單地址在新北市新莊區化成路（如圖八），與前述對話內容所得之假設相符。

圖八: 從涉案帳號IP發現可能之涉嫌人

4.嫌疑人A、B之關聯

從境外門號使用手機IMEI序號、帳號IP歷程分析、社交工程等各種科技偵查技巧，研判涉案帳號xi〇〇〇〇11〇〇可能有2名使用者，分別為29歲之陳〇〇及23歲鄭〇〇。為檢驗兩者具共犯關係之假設，進一步從刑案資料分析發現陳〇〇與鄭〇〇等人曾於112年1月在新北市新莊區某汽車旅館施用K他命毒品，研判二人為朋友關係，在本案中可能為共犯。

（五）嫌疑人到案與案件建構

案件的成敗關鍵在於，能否查扣犯罪物證「犯案用手機」、「被害少女影像」及「帳號xi〇〇〇〇11〇〇登入畫面」。若無相關物證且嫌疑人否認犯行，將難以認定其犯罪事實。偵辦人員檢具相關證據，向法院及檢察官聲請核發搜索票及拘票後，編排警力分二組同步執行搜索、拘提二名嫌疑人。筆者率隊持搜索票及拘票至嫌疑人B（陳〇〇）新北市新莊區位於電梯大樓四樓之住處執行搜索，現場有嫌疑人B及其配偶與剛滿月之嬰兒，筆者出示搜索票及證件後，開始執行搜索，客廳、房間、儲藏室各處逐一搜索，現場有5支iPhone手機，經嫌疑人B解鎖後檢視內存相片、影片及登入帳號，均未發現涉案帳號及相關事證。

1. 透過詢問突破心防

搜索執行過程中，嫌疑人B主動配合出示手機及解鎖，初步查看手機內各社群軟體APP均未發現涉案之Instagram帳號xi〇〇〇〇11〇〇及微信帳號「ㄉㄡ拉a孟」，詢問嫌疑人B是否還有其他手機或「工作用手機」之時，同步觀察嫌疑人B表情及反應，明顯出現了停頓、思考、猶豫及移開視線等行為特徵，藉此研判嫌疑人B在說謊或是在隱匿

某重大事情。在遍尋不著重要證據「涉案手機」時，取得嫌疑人的配合主動交付，是最有效率的偵查作為，搜索進行中的溝通、談判是實務上最重要且難有既定標準作業流程之技巧，需視現場狀況而臨機應變。因此在發現嫌疑人B在說謊、隱匿時，筆者暫停搜索，將嫌疑人B單獨帶至一旁，明確告知：

(1)：「法院核發搜索票，表示警方掌握相當證據。」

(2)：「多名警察在你家搜索，會造成你家人的困擾，自己做的事要自己承擔。」

(3)：「主動交付涉案手機，就結束搜索。」

(4)：「偵查內容會保密，維護你的尊嚴，讓你在家人前留有面子。」

(5)：「家中搜索結束後，會到地下室搜索，搜索會持續到查獲涉案手機為止。」

嫌疑人B聽到筆者提及「會到地下室搜索」時，出現「驚恐和焦慮」面部表情，對應先前以社交工程技巧與嫌疑人攀談，取得嫌疑人以文字表示「在地下室」(如圖九)等資訊，至此已大致確認涉案手機藏放處所，就是在「地下室」。

圖九: 嫌疑人以文字表示「在地下室」

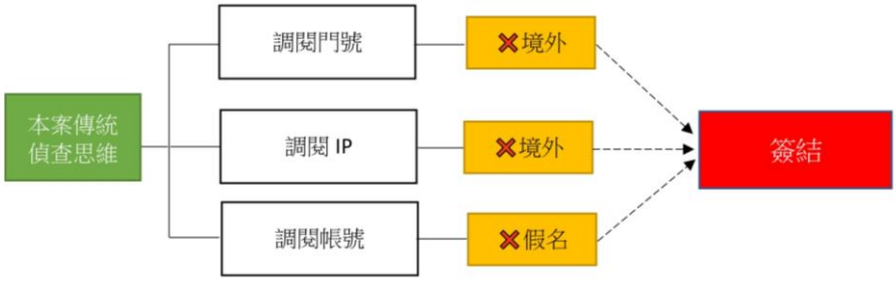
筆者隨即率隊至地下室執行搜索，此時嫌疑人B提出要求，希望與筆者單獨前往地下室，表示會交付涉案手機；為取得嫌疑人B之配合，評估雙方體型差距（筆者身高181公分、80公斤、嫌疑人B身高170公分、70公斤），體型上佔有優勢，便與嫌疑人單獨從四樓搭乘電梯前往地下室搜索。停放在地下室停車場的白色HONDA FIT為嫌疑人B所使用之車輛，旁邊放有一白色塑膠箱，塑膠箱旁擺放一張露營椅，嫌疑人B在地下室時再次出現焦慮及猶疑不定之情狀，眼神張望著落在地下室車道出口及車旁的白色塑膠箱，筆者仔細一看發現有一把刀械插放在塑膠箱與牆壁之縫隙中，僅留木柄手把在外，察覺嫌疑人B似乎在研判與警方搏鬥後逃亡之成功機率。隨即不動聲色，在手機專案群組傳送「來」。在四樓待命之同仁，見「來」之訊息後，抵達地下室會同以優勢警力執行搜索，使嫌疑人B在心理上放棄脫逃之意圖。

2.搜索取得證據

專案小組警力於嫌疑人B住處地下室執行搜索，在白色置物箱內查扣犯案用「工作機」，開啟Instagram檢視使用者，確認即是涉案帳號xi〇〇〇〇11〇〇，搜索發現手機相簿內存有被害少女裸照。嫌疑人B自知已無法隱匿犯行，主動交付藏放於自小客車上之毒咖啡包、毒梅片及彩虹菸等新興毒品，並坦承與另嫌疑人A共同使用犯案用「工作機」及涉案帳號xi〇〇〇〇11〇〇仲介被害少女與他人性交易。

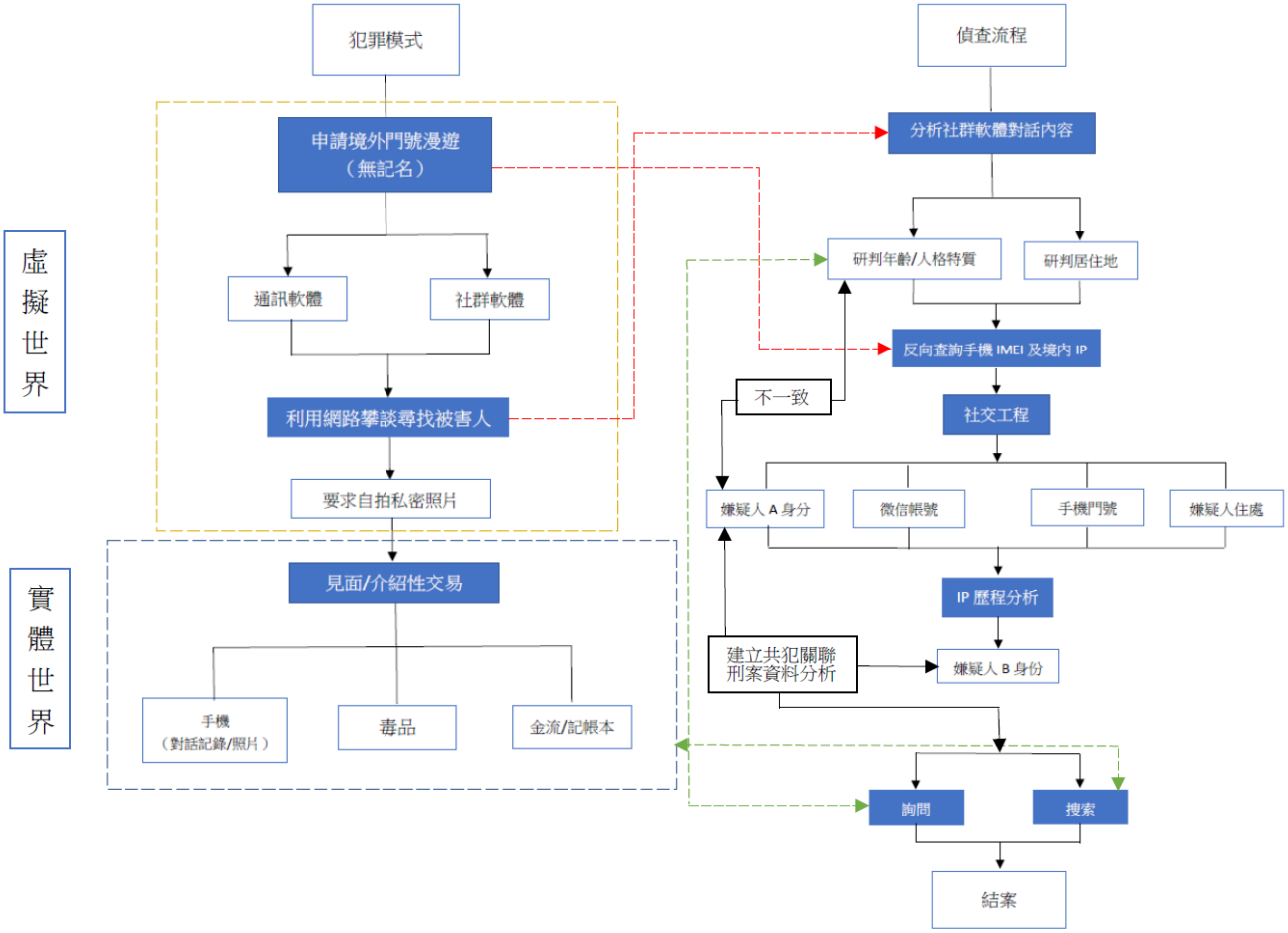
肆、結論

本文以「網路兒少性剝削犯罪偵查案例」為例，屬本文所述「在實施犯罪時利用科技便利隱匿身分」之類型，雖所需偵查科技專業技能無須過高，但就本文所提出案例窺知，該案原承辦偵查人員依循傳統偵查的步驟：（一）線上投單調閱或公文發函查詢涉案帳號註冊(registration)資料；(二)取得涉案帳號申登資料中的使用者姓名、註冊時間(Registration Date)、註冊IP(Registration Ip)、註冊信箱、驗證門號(verified phone numbers)及登入IP歷程等資訊；(三)調閱涉案嫌疑人門號及IP使用者資料，查明嫌疑人身分；因涉案嫌疑人使用境外門號、登入IP位於境外，案件簽結（如圖十），即是偵查科技門檻為障礙之事例。



圖十: 本案傳統偵查思維流程示意圖

而筆者面對前述障礙時，仍以偵查思維為中心，佐以其他傳統偵查作為而達到偵查目的：(一)分析犯罪者的文字訊息特徵，研判犯罪者性別、國籍及年齡；(二)從犯罪者與被害少女對話中之關鍵字，找出線索； (三)分析涉案帳號登入IP歷程，找出異常IP位址；(四)犯罪者以境外門號卡於國內漫遊，以手機IMEI追查嫌疑人身份；(五)掌握犯罪者的喜好，與嫌疑人攀談，進而取得其他線索；(六)達到嫌疑程度進行搜扣程序，並透過被搜索人現場反應，研判關鍵證物所在位置、提出有利方案，促使當事人自行配合交付證物，即為以偵查思維為中心，同時運用其他傳統偵查技術與偵查科技，進行各種偵查假設驗證，而達到偵查目的之案例（如圖十一）。



圖十一:本案科技偵查思維示意圖

本文由偵查本質，重新界定「偵查科技」是運用各種資通信科技，協助蒐集數位等相關事證；而「科技偵查」是藉由各種偵查技術（包含偵查科技）協助蒐證，進行偵查假設與驗證，以遂行偵查目的之過程。科技偵查並非僅僅仰賴偵查科技，尚需其他傳統偵查技術與作為蒐集其他相關事證，並以偵查思維為中心，進行各種偵查假設驗證。兩者之界定與區分，將有利於讓傳統偵查人員奠基在既有偵查專業能力，隨著犯罪型態的需要，學習並吸收相關的知識與技能，或許將能降低其面對技術門檻之科技焦慮，從案件偵查過程學習並接受偵查科技為偵查專業必要條件之一；而新進偵查人員亦能夠在犯罪偵查的脈絡下，強化其偵查科技對於案件偵查之效果，避免過度偏重偵查科技工具而忽略其他偵查專業與思維之培養。換言之，「偵查科技」是「科技偵查」的體用關係，就當前偵查專業發展而言，兩者應相互利用並提昇、缺一不可。

參考文獻

[1] Coman, Iulian, and Noemi Alexa. "EU Law Enforcement Training Needs on Digital Skills and the Use of New Technologies." European Law Enforcement Research Bulletin 22 , 2022..

[2] Brandl,Steven G. Criminal Investigation，4th ed, SAGE Publications, 2017.

[3] 施志鴻，2013，『偵查專業之概論-以英國偵查專業發展計畫為中心』，執法新知論衡，第八卷，第二期: 181-208頁。

[4] Jansson, Krista, Volume crime investigations: a review of the research literature , Vol. 44, No. 05. Home Office, 2005.

[5] National Policing Improvement Agency, Practice advance on core investigative doctrine, Association of Chief Police Officer, 2012.

[6] Bradbury, Sarah-Anne, and Andy Feist. "The use of forensic science in volume crime investigations: a review of the research literature." 2005: 05-91.

[7] HM Government, National cyber strategy 2016-2021, HM Government , 2020.

[8] Kävrestad, Joakim, Marcus Birath, and Nathan Clarke. "Cyber-Dependent Crime, Cyber-Enabled Crime, and Digital Evidence," in Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications. Cham: Springer International Publishing, 2024: 57-60.

[9] Brosnan, Mark J. Technophobia, The psychological impact of information technology, Routledge, 2002.

[10] Jay, Timothy B, "Computerphobia: What to do about it," Educational Technology 21.1 , 1981: 47-48.

[11] Rosen, Larry D. and Michelle M. Weil, "Computer availability, computer experience and technophobia among public school teachers," Computers in human behavior 11.1 (1995): 9-31.

[12] Marquié, Jean-Claude, Bernard Thon, and Bruno Baracat, "Age influence on attitudes of office workers faced with new computerized technologies: A questionnaire analysis," Applied ergonomics 25.3 , 1994: 130-142.

[13] Marcoulides, George A., Bronston T. Mayes, and Richard L. Wiseman, "Measuring computer anxiety in the work environment," Educational and Psychological Measurement 55.5 , 1995: 804-810.

[14] Khan, Muhammad Quraish, Police Technophobia, Lambert Academic Publishing, 2015.

[15] Goodman, Marc D. "Why the police don’t care about computer crime," in Cyberspace Crime, Routledge, 2017: 447-476.

[16] 施志鴻、Ivar Fahsing、楊智晴，2022，『刑事警察偵查決策之研究』，中華心理學刊，第六十四卷，第一期:111~136頁。