

行政院及所屬各機關出國報告

(出國類別：研習) C09200634

研習美國科技犯罪偵查出國報告

服務機關：警政署刑事警察局

出國人職稱：偵九隊隊長

姓名：李相臣

出國地區：美國

出國期間：91年11月18日至91年11月
27日

報告日期：92年01月27日

B3/
C09200634

行政院及所屬各機關出國報告提要

出國報告名稱：研習美國電腦犯罪偵查出國報告

頁數 11

出國計畫主辦機關：內政部警政署刑事警察局

出國人員：李相臣／內政部警政署刑事警察局偵九隊／隊長

出國類別：研習

出國期間：民國 91 年 11 月 18 日～11 月 27 日 出國地區：美國

報告日期：民國 92 年 01 月 27 日

分類號/目：B3、B4

關鍵詞：電腦犯罪、科技犯罪、電腦鑑識

內容提要：

本研習報告分前言、目的、過程、心得與建議等五部分，過程部分為研習者主要之訪查紀錄、美國網路科技犯罪偵查設備、電腦鑑識技術及實地參訪等項；心得部分為研習者研習電腦犯罪偵查技術、情報資訊中心及實地參訪後之感觸；建議部分希能提供國內相關單位在偵辦電腦科技犯罪案件及制定科技偵查政策與資訊運用之參考。

本文電子檔已傳至出國報告資訊網 (<http://report.gsn.gov.tw>)

目次

頁碼

壹、前言	1
貳、目的	1
參、過程	2
肆、心得	5
伍、建議	8

壹、前言

美國執法機關分工極細，如司法部下轄美國聯邦調查局（FBI）可偵辦所有跨州與重大刑案及攸關國家安全之案件，尤其網路科技犯罪多屬跨國、跨州之智慧型犯罪，故劃歸該局執掌；緝毒局（DEA）負責毒品案件之偵辦。財政部下轄海關（Custom Service）專責處理仿冒（盜版）及網路色情案件；秘勤局（Secret Service）負責總統、副總統安全外，另專責偽鈔案件之偵辦；煙酒及槍械管制局（ATF）負責私酒及偽酒之管理與槍械有關案件之偵辦；其他如移民局、衛生稽查及軍方等均有司法行政或警察權可執行取締、查察等公權力。警察機關僅單純負責治安與交通工作，並協辦上述單位相關事項；分工明確，且警察任務單純，可有效專注治安、交通工作。而上述單位依任務均有網路科技犯罪單獨部門負責案件之偵辦與研發工作，可見網路科技犯罪工作受重視之程度。本次訪查學習行程因時間緊湊（出差僅核准十日），且路途遙遠，地點分佈極廣，因而略有走馬看花感覺。然亦盡力蒐集相關資訊，以為國內網路、科技犯罪之參考。

貳、目的

此次共走訪美國海關、秘勤局與緝毒局於華盛頓總部之網路科技犯罪中心，另前往賓夕凡尼州之緝毒局情報資訊交換中心參訪，及前往洛杉磯緝毒局辦事處，實地瞭解第一線幹員所使用之科技設備與犯罪資訊協助案件之偵辦。國內治安機關以往均以美國聯邦調查局為主要合作與參訪單位，然經瞭解，上述單位與聯邦調查局一樣，亦有海外派駐之聯絡官可提供其他國家所需之協助，且其組織架構、編制內亦有情報中心、網路犯罪偵查與科技犯罪研發中心等單位，且任務導向明確，更能凸顯其績效。美國歷經九一一之後，成立國土安全部（HOMELAND SECURITY DEPARTMENT），為僅次於國防部，人數達二萬五千餘人之部門；其將秘勤局、海關全數納入，並將緝毒局與聯邦調查局部分人力、單位併入，主要負責反恐工作之進行及美國執法單位情報整合分享與工作協調等相關工作，以避免重蹈覆轍，肇因情報之疏於整合，致未能防堵九一一之悲劇。

參、過程

以下就參訪相關單位內容略述如下：

一、參訪美國海關華盛頓網路犯罪防治中心：

經簡報與深入訪談瞭解海關於偵辦網路盜版與網路色情所使用之工具，偵查程序與數位證據（電腦鑑識）操作之程序與方法等。

二、參訪美緝毒局情報（資訊）支援交換中心：

該中心成員多為久任之約聘僱人員，待遇平平，然其熟悉電腦操作、犯罪資料內容與資訊軟硬體之技術，且對犯罪資料分析有多年之經驗，尤其專注於通聯分析與電話、電腦使用者資料之管理。緝毒局總部全國性情報（資訊）支援交換中心，除處理全國緝毒資料整合支援外，亦處理其他國家等國際性毒品情報；而緝毒局於全美各地近六十個辦事處亦各有地區情報（資訊）支援交換中心，可見該中心之重要性。當外勤幹員處理重大或特殊案件時，可要求指派一資訊員（諮詢員、情資員）負責本案件所有資訊之提供，外勤幹員專注於案件之偵辦與歹徒行踪之掌握，所需之犯罪資訊，均由熟悉電腦操作與資料分析之資訊員提供。以通聯分析為例，當外勤幹員將目標電話號碼提供與資訊員，資訊員隨

即依程序自電話公司調閱通聯資料，全國所有案件之所有通聯均依單一窗口由情報（資訊）支援交換中心人員調閱，以資整合與存檔。資訊員取得電話公司傳回之通聯後，再以電腦通聯分析軟體，分析通話對象、頻率次數、基地台位置及電話序號等相關訊息，並以樹狀網路圖分析，鎖定目標之交往關係。如通聯對象僅有電話，則資訊員會自動發文查詢電話公司用戶資料庫，並予建檔，再將前科背景等犯罪資料一併查出，提供給外勤幹員。外勤幹員可直接聯繫資訊員提出各類需求，由資訊員負責以電腦分析提供。由於資訊員熟悉電腦操作與資料特性，又負責聯繫電話公司等私人企業取得通聯與用戶資料，並建立資料庫；由於歷經長時間之投入與專業，資訊員提供整合分析之情資可謂駕輕就熟，事半功倍，外勤幹員全力投入案件之查察又有專責之內勤資訊員支援，節省許多時間，使案件偵辦更有效率。反觀國內外勤偵查員花費相當多時間，製作公文查詢電話等資料，又不熟悉犯罪資料內容特性與電腦操作，耗費相當多無謂之人力時間。

三、科技偵查設備支援中心：

美國執法單位多有設立專責機構，提供或研究運用外勤幹員偵查犯罪所需之科技設備，以符合保障人權依法蒐證之精神與有效遂行偵查及搜索任務；如運用衛星定位器（GPS）依不同案件需求協助外勤人員安裝於汽車、機車、贖款皮箱或電腦內；針孔攝影機或竊聽器依現場環境偽裝成適合之外形，以能有效蒐證；此類蒐證所需之科技設備極為普遍，然必須有一科技單位協助裝設方能產生功能；面對日益進步之智慧型犯罪與運用科技設備犯罪，科技偵查設備支援中心不斷運用研究、改裝科技偵查設備以符合科技辦案所需。觀諸目前國內犯罪大都脫離不了行動電話與金融人頭帳戶之問題，行動電話做為聯絡通訊工具，金融人頭帳戶做為取錢之用，如能解決行動電話定位，即時找出發話者位置，與有效監控提款機提領人頭帳戶，即時逮捕提款者，當可解決目前國內七成以上犯罪，又可嚇阻歹徒，預防犯罪。

肆、心得

一、智慧型科技犯罪手法的不斷浮現

隨著社會經濟的不景氣，資訊科技犯罪日趨嚴重，高科技知識份子紛紛以本身所知的科技方式，運用在傳統犯罪案件上，如設置假提款機及假銀行網站等不法事件中，再三顯現出智慧型罪犯伺機盜領存款的創新巧思與花費心機。在真實案例中，有的高科技人士更會在私人利益作祟下，鋌而走險，竊取原任職公司的重要商業機密資料，以從中獲取高價回饋或謀取新任職公司更優渥的薪資，這樣類似的案件正日漸增加中，而各警政機關所面臨的挑戰壓力亦日益沈重。

二、高科技設備的犯案運用

資訊科技多變化應用產品的不斷相繼出產，亦衍生多種不同類型犯罪手法，不僅加深偵辦資訊犯罪案件的困難度，更迫切需要先期人力投入逆向反查的追蹤技巧研析，以面對爾後即將發生的不法科技犯罪事件。舉凡盜拷行動電話、USB 隨身碟、電話交換機、衛星通訊、網路電話通訊、PDA 個人數位助理(包含 Palm 掌上電腦)、PHS 手機及無線寬頻上網等高科技產品

的日漸興盛，相對增加資訊科技犯罪的複雜性。對於高科技設備之犯罪運用問題，我警政機關實有必要在未趨嚴重之前，洞燭先機，規劃籌備，以應付日益繁瑣艱深的高科技犯罪問題，尋求縮短成功緝獲嫌犯的有效方法。

三、資訊鑑識數位證據的迫切需要

資訊科技所提供的偵查技巧及佐證資料已變得日益重要，偵查人員如未保持相關電腦科技知識的領先優勢，則很難提供具體有效的證據，因為電腦操作程式中可能會破壞電腦中的儲存資料，所以，面對未知(或不同)儲存媒體(或格式)的電腦資料，均需小心、妥善因應，以免在電腦證據採集過程中，不慎錯過隱藏檔案或執行破壞程式。然而有關數位證據部分，在國內尚無專責處理機構或研究單位，本局既已在電腦犯罪偵查實務上累積六年多經驗，實有必要針對電腦偵查技術及數位證據採證部分再行深入研究，以持續充實本局電腦犯罪偵查能力之後勤支援，無懼於資訊科技犯罪層出不窮犯罪手法的翻新變化，迎接未來新的偵查挑戰。

四、科技法律的研究充實

科技相關法律的形​​成往往落後在科技發展之後，為了研議適用、合宜的科技法律，我警政機關亦需針對現行發現的科技犯罪行為，協助政府新增或修改現行法律規範，以符現況。如正在研議中的國家科技保護法及刑法電腦犯罪專章等相關科技法令，本局偵九隊先前均提供相當多的實務訊息，作為研議法令過程的主要參考依據。

五、定期舉辦科技犯罪教育訓練

科技犯罪的出現已然成為高科技現代社會中急遽成長的新興犯罪類型，隨著高科技設備的大眾化，亦使高科技犯罪者的範圍逐漸擴大，幾乎任何心中存有不滿情緒的人，都有可能在一時激動下而誤觸法網，相對增加防制此類犯罪的困難度。故有必要由專責人力針對科技犯罪做一深入研究，並對全國治安機關相關同仁施行教育訓練，以宣導處理科技犯罪過程中的應有認知及相關注意事項，期許在科技犯罪發生之初能予以防範，進而提升治安機關的整體偵緝戰力。

伍、建議

一、人頭戶資料庫之建立通報

近來國內犯罪不論是刮刮樂詐欺、簡訊詐財或一般刑案，大都使用人頭戶以取得金錢規避警方追查；手機、金融帳戶及設立公司行號等均由人頭頂替，而這些人頭戶多為游民或不知情之第三者。將身分證等個人資料有意無意流出，倘政府單位能互享資料，建立人頭戶電子資料庫，並有互相通報機制，審核用戶申請時能嚴加篩選過濾將職業人頭戶找出，當能減少案件發生與追出元兇。

二、行動電話定位功能之開發

行動電話得透過基地台傳輸訊號，而為能於高速移動時不斷訊，行動電話只要開機必定同時可與二至三個以上之基地台聯繫，而後選擇訊號最強之基地台為收、發基地台（訊號強度 DB 比），而每一基地台可鎖定一二〇度之方向角，如此以三點定位方式加上基地台方向角與收訊信號強度比，技術上應可鎖定使用者位置，如再輔以獵狐槍（偵測行動電話、無線電等微波位置用），則可將發話者位置範圍鎖定至最小；上述功能應已內含於行動電話業者之交換機功能內，然

尚須運用少許人力與電腦分析功能方能有效運用，此點須協調業者大力支持。

三、有效監控提款機（ATM）提領人頭帳戶金額

協調財政部及各銀行將全國自動提款機建檔，並配合電子地圖成立提款機電子資料庫，各提款機由轄區分局或派出所之最近警力點為責任區；另將歹徒使用之洗錢人頭帳戶列為警示目標。當歹徒提款時，一則設計程式延遲付款時間，一則自動立即通報最近之責任派出所或分局，迅速趕往現場。由於跨行提領自動提款機，每次僅能提領二萬元，當日最高提領為十萬元，歹徒須提領五次，需時約三分鐘以上方可完成，警力應可適時抵達逮捕。

四、成立科技情報中心的迫切需要

傳統刑事偵查人員，對於電腦軟體之使用與科技設備之運用，在先天上普遍存有疑慮，為使全國治安機關偵辦科技犯罪相關案件時，均能獲致良好的處理品質，實有必要因應個案配合熟悉警政資訊系統、電話通聯分析及犯罪知識庫相關操作的專業人力，協助個案承辦人，針對不同需求，進行研究、分析與解讀，

提供專業有效的資訊技術支援管道，以快速鎖定嫌犯範圍，提升整體破案率。上述人力宜由警政署、刑事局、入出境管理局資訊室約聘僱人員轉任最適宜。