出國報告（出國類別：進修）

有關打擊網路犯罪（Cybercrime）法制及國際合作之研究
-以暗網及虛擬貨幣為中心

服務機關：臺灣臺北地方檢察署
姓名職稱：羅韋淵檢察官
派赴國家/地區：美國/ 哈佛大學
出國期間：111年8月25日至112年8月19日
報告日期：112年11月18日

誌謝

本篇公務出國報告係筆者於 2022 年 8 月至 2023 年 8 月間，在美國哈佛大學擔任訪問學者的研究心得，於 2020 年蒙時任蔡部長擇定由筆者前往哈佛大學擔任訪問學者，出國計畫，歷經一波三折（可參報告附錄：哈佛見聞），2022 年出國前夕承蒙最高檢察署邢泰釗檢察總長、時任臺灣臺北地方檢察署林邦樑檢察長及各位長官、學長姐的期許及祝福，讓我更有信心地毅然決然赴美研究。

語文方面，因筆者對於語言學習小有興趣，曾擔任數次司法官學院國際研討會的接待檢察官，負責接待外賓，在國際研討會的場合中，認識時任法務部國兩司蔡秋明司長、林明誼學長、粟威穆學長、時任司法官學院教務組盧筱筠組長、調學院辦事的林彥均學姐及共同擔任接待檢察官的學長姐伙伴們，深受蔡司長、組長及學長姐們的啟迪與鼓舞，其後也陸續受國兩司汪南均代理司長、孟玉梅司長及國兩司的學長姐指導與照顧，讓筆者有持續接觸英文及國際事務的動力，雖然筆者英文稱不上好，但透過長期的累積，也讓筆者在美國生活可以溝通無礙。

在美期間除了學校內之學術研究外，筆者對於虛擬貨幣偵查技巧、網路犯罪偵辦議題，也向美國司法部檢察官 Catherine Pelker、Ryan Dickey、時任加州聖塔克拉拉郡副檢察長（Deputy District Attorney）Erin West 請益，都獲得很正面友善的回應。另自費參加全美網路犯罪會議，在會議中與美國檢察官、執法機關對於網路犯罪、虛擬資產追查等議題的交流，亦令筆者獲益良多，在此向他們表示由衷感謝。在這個透過網路犯罪的時代，唯有持續不斷與國際交流，臺灣的檢察官及執法機關才能累積日後國際合作的能量。

回國後，仍然回到熟悉的北檢忠組，受時任北檢鄭銘謙檢察長（現為部長）、王俊力檢察長及蔡偉逸襄閱、高一書主任、北檢學長姐的照顧及指導，除了黑金專組的案件外，讓筆者有機會可以處理跟網路犯罪、虛擬貨幣相關的案件。後調至士檢服務，也深受時任顏迺偉檢察長、張云綺檢察長、張志明襄閱及士檢學長姐的指導與照顧。此外，筆者赴英國倫敦參與國際檢察官協會第 28 屆年會擔任報告人、二度前往位於泰國曼谷的美國國際執法學院（ILEA-Bangkok）受訓、至韓國釜山參加 APG 關於虛擬資產調查的訓練、赴新加坡考察虛擬貨幣金流查緝與詐欺犯罪調查實務，都讓筆者對於同行的長官、學長姐、同仁及執法單位的伙伴們對我的照顧銘感在心，並對於大家一同代表臺灣參與國際事務的熱情，深受感動。礙於篇幅有限，筆者在此感謝一路上支持、照顧我的長官、學長姐、學弟妹及執法機關的伙伴們。

最後，謝謝本件報告的內部及外部審查委員，提供筆者諸多寶貴建議。又本報告完成後，虛擬資產相關法規已有變動，諸如：洗錢防制法第 6 條（登記制）業已施行、金管會亦提出虛擬資產服務法草案，本報告建議的若干法制調整內容似得到某程度的落實，期待未來各界能透過公私協力，共同完善打擊網路犯罪、虛擬資產相關犯罪、返還資產予被害人的目標。

摘要

本文為筆者受法務部選派，至美國哈佛大學擔任訪問學者之研究。從筆者在國內偵辦網路犯罪之經驗談起，赴哈佛大學博克曼中心、法學院、甘迺迪學院修習網路犯罪與虛擬貨幣相關最新知識，並參加全美網路犯罪會議，學習美方關於偵辦暗網、虛擬貨幣之偵辦技巧及相關法律程序。再者，筆者參與美國檢察官及執法機關之虛擬貨幣偵查聯盟（Crypto Coalition），定期線上討論。故本文對於網路犯罪之研究，將綜合筆者對於網路犯罪的偵辦經驗、粗淺認識及學習所得，聚焦在暗網、僵屍網路及虛擬貨幣之犯罪案例，並介紹網路犯罪之國際公約、國際合作模式及打擊網路犯罪之國際組織。

關鍵字：網路犯罪、電腦犯罪、暗網、區塊鏈、虛擬貨幣、虛擬通貨、虛擬資產、國際合作

目錄

壹、 前言

網路（Internet）是由全球各地連接在一起的數十億個電腦和其他數位裝置所構成的龐大網狀結構。這些裝置透過一系列的通信協議（例如 TCP/IP 協議）來彼此連接，形成了一個全球性的資訊交流和資源分享的系統。網路允許使用者透過電纜、光纖、衛星等媒介傳送數據，使得資訊能夠快速而有效地在全球範圍內流通。網際網路的發展促進了許多應用的興起，包括電子郵件、網際網路瀏覽器、社群媒體、視訊等。網路的基礎結構包括網際網路服務提供商（ISP）、伺服器、路由器、交換機等設備。人們可以透過各種設備，如個人電腦、智慧手機、平板電腦等，連接到網路，以存取各種資訊和服務。而基於網路世界的匿名性及跨國界的特性，透過網路技術所進行的犯罪亦應運而生。而近年全球性的 COVID-19 疫情影響了大眾生活及工作模式，俄烏戰爭 也引發全球資安韌性議題，加上新興科技的多元應用伴隨各式的資安威脅及挑戰，都使得因應資安風險為必須面對之重要課題。微軟在 111 年 12 月發表第 3 期網路威脅情報研究報告 Cyber Signals 指出，在其客戶的 OT 網路中發現，有超過 75%最常見之工業 控制器存在高嚴重性之漏洞且未修補。就漏洞揭露趨勢來看，從 109 年到 111 年間，於主要供應商生產之工業控制設備中，被揭露為高嚴重性漏洞之數量成長至少 78%。雖然有高嚴重性漏洞之威脅風險，但發現即使是資源充分與管理良好之組織，面臨需要將關鍵資訊基礎設 施停機以修補漏洞之情形時，管理人員仍常選擇讓高風險之漏洞繼續 存在，以維持其系統運作之可用性。如此一來，當這些漏洞被揭露於外或利用時，就容易成為有心人士入侵之破口[1]。

[1] 數位發展部，111 年度國家資通安全情勢報告，112 年 6 月。https://www-api.moda.gov.tw/File/Get/acs/zh-tw/dsAqeYCbJqwvgBt (Last viewed: Nov, 15, 2023)

筆者於 2019 年 5 月間前往法務部調查局參加「執法人員網路偵查技術研習班」，由亞太網路資訊中心（Asia-Pacific Network Information Centre, APNIC）之資深網路安全專家 Jamie Gillespie 以英語授課，課程中除介紹 IP 調查方法、洋蔥網路與暗網、網路犯罪與數位鑑識外，更實際操作各項方法，包括透過安裝虛擬機（Virtual machine, VM）操作進入暗網等，令個人深感科技日新月異，必須持續學習。後於 2019 年 6 月間，經法務部選派至美國華盛頓哥倫比亞特區（Washington, D.C.）參與由美國財政部國家稅務局刑事調查處處（IRS-Crime Investigation）與世界銀行（World Bank）合辦之 2019 年電腦網絡研討會（Cyber NETwork 2019），該次研討會之主題為「全球協力追查金流並打擊網路犯罪（Connecting Globally to Follow the Money and Fight Cybercrime）」，探討涵括虛擬貨幣、暗網、公開來源情報及社群網路（Virtual Currency, the Dark Web, Open Source Intelligence and Social Media）等新興網路及金融犯罪議題，並透過案例分享、以區塊鏈追蹤洗錢流向（Blockchain Tracing）之演練，增進筆者對此類犯罪之認識並提升偵查技巧。

上開經驗及知識，對於筆者實際偵辦網路犯罪相關案件之助益甚大，筆者在承辦國內某成人平台涉嫌散布猥褻物品之案件中，亦與刑事警察局電偵大隊合作，首次嘗試以聲請扣押「網域名稱」之方式，向法院聲請扣押裁定獲准，事後亦與「iWIN 網路內容防護機構」合作，嘗試建立業者自律改善之準則，以期保護兒少的網路使用安全。

另於 2021 年 11 月間，國內數家證券商遭受「密碼撞庫攻擊」（Credential Stuffing，係指駭客自暗網或其他不法來源處，取得民眾不慎外流的帳號和密碼，利用民眾使用共通密碼的習性，嘗試登入各大網站及手機應用程式），駭客以「撞庫攻擊」之手法，非法登入投資人之證券暨期貨帳戶，透過複委託功能下單購買香港交易所之股票，致使投資人帳戶遭扣

款而令投資人及券商蒙受重大損失，甚至影響資本市場之安定。在該案件中，駭客使用之攻擊來源 IP 位址涵蓋國內及境外，且攻擊證券商之來源 IP 具有共通性，在追查過程中也因為 IP 位址位於境外，而遭遇偵辦之瓶頸，令筆者體悟到偵辦網路犯罪案件，除了專業知識以外，更需要透過國際間的合作，始能有效追查。該案也促使金融監督管理委員會責成臺灣證券交易所及臺灣期貨交易所督導證券商及期貨商，採用多因子認證方式，並強化針對密碼撞庫攻擊之用戶端防禦強化相關機制。

於 2022 年間，筆者承辦以比特幣等虛擬貨幣詐欺、洗錢之案件，自行透過區塊鏈瀏覽器之操作，查詢公開帳本資訊，追蹤數層幣流後至境外交易所，復透過向境外交易所之資料調閱，而查得幣流之流向。然而，除了有追查、分析幣流之專業以外，如果不具備向境外交易所調取資料之能力，在案件偵辦上亦將功虧一簣。而如何向境外交易所調取資料，亦成為一大問題，蓋境外交易所遍布世界各地，位處不同司法轄區，有時連如何取得該境外交易所之聯絡資訊也難以得知，遑論瞭解其等對於資料調閱之法律要求、程序及所需檢附之文件，而向境外交易所調取資料如皆須循司法互助途徑，則將造成偵辦案件的巨大困難，經筆者向某國外執法機關請教，瞭解到目前國際上執法機關向境外交易所調取資料的趨勢，都是盡可能以非正式國際合作、由境外交易所在執法機關提供一定之公文信函之情形下，自願配合提供為優先，而目前境外交易所達數百家，筆者亦蒐集國外之執法機關、歐洲刑警組織整理的境外交易所相關資訊，並提供予國內之執法單位使用。

又筆者偵辦某線上購物平台客戶資料外洩之案件中，查知來源 IP 後，雖循線查得該 IP 之申登人，然經搜索、扣押被告之電腦並送鑑定後，查知被告係提供其伺服器作為暗網使用者之出口節點（Exit Node），亦造成該案溯源追查之斷點。而暗網之追查在國外之執法機關偵辦暗網市集已有相當

之經驗，然對於我國執法機關而言，仍屬較為不熟悉之領域，就此部分，宜多與國外執法機關交流，學習、精進相關知識與經驗。

筆者於 2022 年 8 月間經法務部選派至美國哈佛大學博克曼網際網路與社會研究中心（Berkman Klein Center For Internet & Society，下稱博克曼中心）擔任訪問學者一年，該中心自 1996 年哈佛大學法學院教授 Charles Nesson 與教授 Jonathan Zittrain 創立「法律與科技研究中心（Center on Law and Technology）」後，並於 1998 年更名博克曼中心，該中心致力於電腦網際網路尖端議題研究。筆者除了積極參與該中心訪問學者每週之討論會外，亦旁聽法學院「刑事程序法：偵查」（Criminal Procedure: Investigations）、「國際刑事法」（International Criminal Law）、「網路安全及網路衝突之法律問題」（Legal Problems in Cybersecurity and Cyber Conflict）等課程，除了法學院以外，筆者較常參與的課程係哈佛大學甘迺迪學院（John F. Kennedy School of Government, Harvard Kennedy School, HKS）所開設之課程及講座，其中 Belfer Center for Science and International Affairs 於該學年邀請諸多 AI 人工智慧之研究者舉辦系列研討會，因筆者此行研究主題為網路犯罪相關，故參加該中心於秋季學期關於 AI 議題之系列研討會「人工智慧與網路午餐系列：探索人工智慧與演算法之規範與實踐」（AI Cyber Lunch Series：Explores AI and Algorithm Regulations and Practices）；另筆者亦參與 Mossavar-Rahmani Center for Business and Government 舉辦之針對虛擬貨幣及 WEB3.0、區塊鏈等議題舉辦系列講座（關於筆者赴美期間之詳細學習歷程，可參見附錄：我的哈佛見聞）。

除了積極參與學校課程、講座以外，自 2022 年 11 月起，筆者加入由美國加州聖塔克拉拉檢察官 Erin West 創立之「虛擬貨幣偵查團體」（Law Enforcement Crypto Group），固定期間參與該團體之線上視訊會議，與美國

各執法機關、歐洲刑警組織、其他國家之執法機關討論交流關於虛擬貨幣之犯罪手法、趨勢、偵查技巧、扣押等議題，返國後仍持續至今。

在美期間，筆者亦參與全美最盛大的網路犯罪討論盛事，即由麻州檢察長辦公室舉辦之「全美網路犯罪會議」（National Cyber Crime Conference 2023），會議內容包含網路犯罪偵查、數位鑑識、執法技巧、如何在法庭呈現數位證據、IoT-反思數位威脅（Internet of Things - Rethinking Digital Threats）、社群媒體偵查技巧、暗網（Darkweb）介紹、偵查實際案例、手機追蹤、撰寫數位證據之聲搜書教學、虛擬貨幣追查、區塊鏈證據之證據能力及法庭應用等近百場課程。教授課程之講師有美國檢察官、FBI 探員、國土安全部犯罪調查部門（HSI）之探員、美國緝毒局（DEA）、鑑識人員等眾多專業講師，為筆者收穫最豐富的一場會議。又因該會議探討內容多涉及美方執法機關之偵查手法，故原則上僅有美國檢察官、執法機關能夠參加，而筆者身為該場會議中唯一的外國人，能夠聽到美國執法機關分享第一手的網路偵查技巧，實屬難能可貴之經驗。

基此，本文對於網路犯罪之研究，將綜合筆者對於網路犯罪的粗淺認識及學習，聚焦在暗網、僵屍網路及虛擬貨幣之犯罪案例，並介紹國際上之執法行動、網路犯罪國際公約、國際合作組織。

貳、 網路犯罪概論

現今世界透過網路的運作，透過網路搜尋引擎、電子郵件、社群媒體、即時通訊、多媒體的分享、遠端工作、網路購物等方式，讓人們可以更便利、跨越國界地檢索、獲取資訊，數位化程度比以往任何時候都更加緊密。然而，犯罪分子利也用這種網路的型態，以網路系統、網路和基礎設施之弱點作為目標。這對世界各地的政府、企業和個人產生了巨大的經濟和社會影響。網路釣魚、勒索軟體和資料外洩只是當前網路威脅的幾個例子，而新型網路犯罪一直在出現。網路犯罪分子的反應變得越來越快速和有組織，利用新技術、客製化攻擊並以新方式進行合作。而網路犯罪不分國界，犯罪分子、受害者和技術基礎設施跨越多個司法管轄區，為各國之檢察官及執法單位調查和起訴帶來許多挑戰。因此，公共和私營合作夥伴之間的密切合作至關重要[2]。

而網路安全整體威脅態勢比以往任何時候都更加複雜，造成的損失也急遽飆升。根據美國聯邦調查局（Federal Bureau of Investigation, FBI）2022年網路犯罪投訴中心（Internet Crime Complaint Center）報告，網路犯罪產生的潛在總損失總計超過 102 億美元[3]。

近年來，與暗網（Dark web or Dark net）有關之犯罪亦與日遽增。所謂暗網，係透過分層加密系統使得暗網使用者的身分和位置保持匿名，無法被追蹤。暗網的加密技術透過大量中間伺服器傳送使用者資料，保護了使用者身分並保障匿名。也正因為匿名、無法追蹤之特性，許多犯罪者透過暗網傳遞犯罪訊息、從事犯罪交易，甚至成立暗網市集。與暗網有關之犯罪包含：兒童色情、毒品、槍枝交易、駭客服務、洗錢服務、販賣個資、恐怖主義之聯絡管道等，而為了打擊暗網相關犯罪，美國司法部與歐

[2] https://www.interpol.int/Crimes/Cybercrime (Last viewed: Nov,11,2023)
[3] Federal Bureau of Investigation Internet Crime Report at 3, Internet Crime Complaint Center, 2022.

洲國家、歐洲刑警組織等盟友，陸續成立調查團隊，共同合作打擊暗網犯罪，陸續破獲了絲路（Silk road[4]）、Wall Street Market[5]、Helix[6]、Hydra[7]、Monopoly Market[8]（Operation SpecTor）、Hive[9]（勒索軟體集團）、Genesis Market[10]（買賣被駭帳戶）等暗網市集或服務，而在暗網市集交易所使用交易媒介多為比特幣等虛擬貨幣。基於區塊鏈為底層技術之虛擬貨幣的架構下，使用者無須仰賴任何第三方公正機構來維護交易之公正透明，只須透過數位化的個人簽章執行轉移，交易紀錄連同電子簽名將被記載在公開帳本裡。換言之，任何交易將不受政府監管，在雙方互信、社群內互信且可驗證的基礎下即可完成。而各式之犯罪者，為了隱藏不法金流，亦多使用虛擬貨幣作為洗錢之媒介。又根據區塊鏈情報公司 TRM Labs 的報告顯示，2023 年年初迄今，與北韓相關的駭客組織已竊取超過 2 億美元的虛擬貨幣，過去 5 年間更已盜走逾 20 億美元的虛擬貨幣[11]。綜上可知，現今之網路犯罪與虛擬貨幣之關係緊密，甚至可以說是如影隨形。在我國之情形，虛擬貨幣則多遭詐欺集團作為詐欺之手法（例如：個人幣商或假幣商之案件），並以之為洗錢之工具。

一、 網路犯罪之定義

網路犯罪（Cybercrime）可以廣義和狹義來理解：

[4] https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road (Last viewed: Nov,15,2023)
[5] https://www.justice.gov/opa/pr/three-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us (Last viewed: Nov,15,2023)
[6] https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million (Last viewed: Nov,15,2023)
[7] https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace (Last viewed: Nov,15,2023)
[8] https://www.justice.gov/archives/atr/competition-and-monopoly-single-firm-conduct-under-section-2-sherman-act-chapter-2 (Last viewed: Nov,15,2023)
[9] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant (Last viewed: Nov,15,2023)
[10] https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation (Last viewed: Nov,15,2023)
[11] https://www.trmlabs.com/post/inside-north-koreas-crypto-heists (Last viewed: Nov,15,2023)

（一） 廣義網路犯罪

廣義上（Broad Definition of Cybercrime），網路犯罪是指使用電腦和網際網路技術作為犯罪工具或目標的任何犯罪行為。這包括了網路詐欺、身分盜取、網路攻擊、數位恐怖主義、侵犯智慧財產權、電腦病毒和蠕蟲等。廣義的網路犯罪範疇非常廣泛，牽涉到許多不同類型的犯罪活動，涵蓋了幾乎所有可以透過電腦網路進行的非法行為。舉例而言，網路詐騙、駭客攻擊、惡意軟體、網路間諜活動、網路霸凌、網路販毒等都可以被歸類為廣義網路犯罪的範疇。

（二） 狹義網路犯罪

狹義上（Narrow Definition of Cybercrime），網路犯罪特指直接涉及到電腦系統和網路的犯罪行為。這包括非法侵入、系統破壞、資料竊取等與電腦和網路安全直接相關的活動。狹義的網路犯罪著眼於網路和電腦系統的破壞和侵害，通常與資訊安全和數位系統保護相關。舉例而言，駭客攻擊、惡意軟體、非法入侵電腦、數據洩漏等都是狹義網路犯罪的典型例子。

總的來說，廣義網路犯罪包含了所有在網路環境中使用電腦技術進行的犯罪行為，而狹義網路犯罪則專注於直接威脅和損害電腦系統和網路安全的犯罪活動。而本文以下討論網路犯罪的範圍，不侷限在狹義之網路犯罪，舉凡是透過網路技術作為犯罪工具、以網路作為犯罪目標之犯罪行為，均在本文討論之範圍。

二、 美國關於網路犯罪之法制

美國的關於打擊網路犯罪的聯邦法律包括多項法令，且為了應對不斷演變的網路犯罪威脅，同時強調公私協作，以提高打擊犯罪的效果。隨著科技的不斷發展，相應的法律和執法手段亦持續演進。以下僅就與網路犯罪有關之主要聯邦法令介紹之。

（一） 電腦詐欺和濫用法

電腦詐欺與濫用法（Computer Fraud and Abuse Act, CFAA） 編入《美國法典》第 18 章第 1030 條[12]（18 US Code § 1030），是美國檢察官處理網路犯罪的重要法律。該法規範禁止未經授權、超出授權範圍訪問電腦系統、取得電腦資料，或故意使用程式、資訊、程式碼或命令的傳輸，並由於此類行為而在未經授權的情況下故意對受保護的電腦造成損害。

18 US Code § 1030 以下規定包含：竊取國家安全資訊[13]（Obtaining National Security Information）、入侵電腦獲取資訊[14]（Accessing a Computer and Obtaining Information）、入侵公務電腦[15]（Trespassing in a Government Computer）、入侵詐欺[16]（Accessing to Defraud and Obtain Value）、毀損電腦或資訊[17]（Damaging a Computer or Information）、傳輸密碼[18]（Trafcking in Passwords）、威脅毀損電腦[19]（Treatening to Damage a Computer）、意圖與共謀[20]（Attempt and Conspiracy）、沒收[21]（Forfeiture）等細部規定。

（二） 電子通訊隱私法

美國檢察官通常援引電子通訊隱私法（Electronic Communications Privacy Act of 1986, ECPA）在偵查程序中實施通訊監察，因為此乃規範通訊監察之法律。而該法第三章（Title III）又稱為監聽法案（Wiretap Act），不僅是程序法，也是實體法，不只規範執法機關，也規範一般人不得實施非法截取、揭露違法截取之內容[22]。

---

12 https://www.law.cornell.edu/uscode/text/18/1030 (Last viewed: Nov,17,2023)
13 18 US Code § 1030(a)(1).
14 18 US Code § 1030(a)(2).
15 18 US Code § 1030(a)(3).
16 18 US Code § 1030(a)(4).
17 18 US Code § 1030(a)(5).
18 18 US Code § 1030(a)(6).
19 18 US Code § 1030(a)(7).
20 18 US Code § 1030(b).
21 18 US Code § 1030(i)&(j).
22 U.S. Department of Justice, Prosecuting Computer Crimes Manual (2010). Availabe at: https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ccmanual_0.pdf (Last viewed: Nov,17,2023)

18 US Code § 2511 以下規範包含：截取通訊內容（Intercepting a Communication）、揭露所截取之通訊內容（Disclosing an Intercepted Communication）、使用所截取之通訊內容（Using an Intercepted Communication）等規定。

（三） 其他網路犯罪相關法律

包含：非法取得儲存之通訊內容[23]（Unlawful Access to Stored Communications）、身分竊盜[24]（Identity Teft）、加重身分竊盜[25]（Aggravated Identity Teft）、接取設備詐欺[26]（Access Device Fraud）、反垃圾郵件法[27]（the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, CAN-SPAM Act）、電信詐欺[28]（Wire Fraud）、干擾通訊[29]（Communication Interference）。

[23] 18 US Code § 2701.
[24] 18 US Code §1028(a)(7).
[25] 18 US Code § 1028(A).
[26] 18 US Code § 1029.
[27] 18 US Code § 1037. Also see: https://www.law.cornell.edu/wex/inbox/what_is_can-spam (Last viewed: Nov, 17, 2023)
[28] 18 US Code § 1343.
[29] 18 US Code § 1362.

參、 暗網

一、 暗網運作原理

（一） 暗網的定義

一般使用者每天連上的網站是所謂的表層網路或開放網路（surface web or open web），該網站是一般使用者無需使用 Tor 或任何其他特殊瀏覽器或軟體即可看到的網站。表層網路上的網站也可索引，可以使用搜尋引擎輕鬆找到。儘管表層網路由許多最受歡迎的 .com、.net 和 .org 網站組成，但據估計，它僅佔網際網路上可用內容總量的 5%左右，其餘內容都在深層網路（深網）或暗網（deep web or dark web）。在一個經典的例子中，表層網絡可以被想像成一座大冰山的一角，其隱藏在表面之下的大部分冰山則為深網及暗網[30]（如圖 1）。

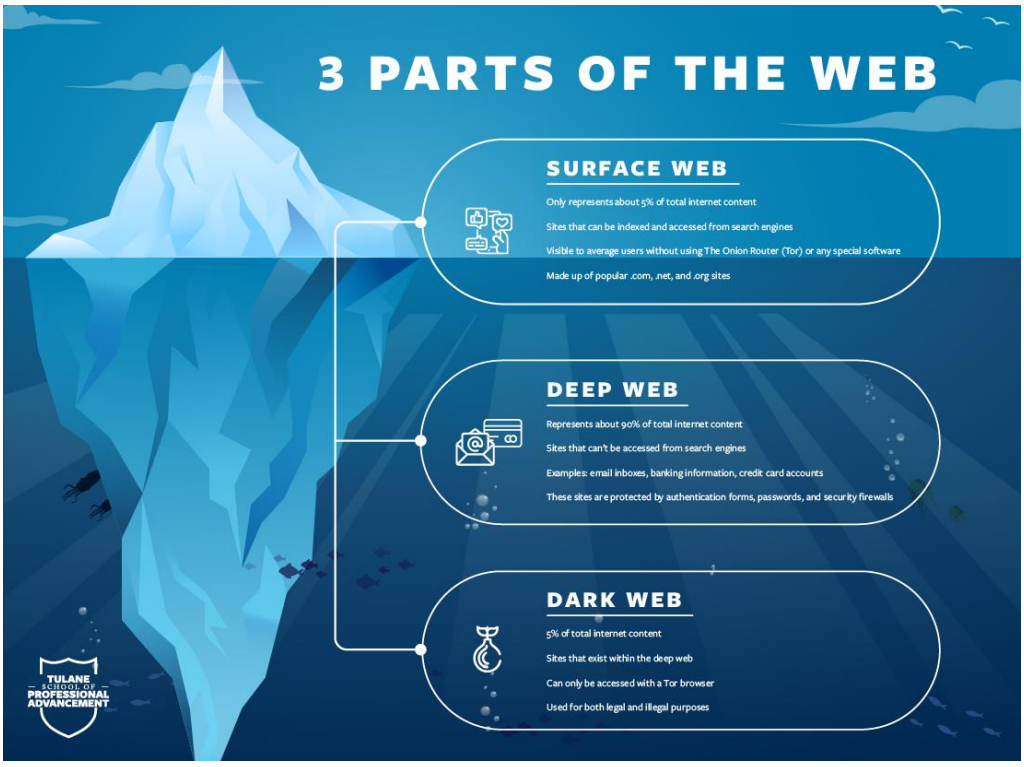


圖 1

[30] https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web (Last viewed: Nov,16 , 2023)

深網則指數以百萬的普通網路使用者每天都會存取私人資料庫，例如電子郵件收件匣和網路銀行帳戶。這些頁面不會被搜尋引擎索引，並受到深網安全牆、身份驗證表單和密碼的保護。大約 90% 的網站位於深層網路上，其中許多網站由公司、政府機構和非營利組織等實體使用。

所謂的暗網存在於深層網路中。它是網路的一個區域，只有安裝了 Tor（The Onion Router, 洋蔥路由器）瀏覽器或其他特殊瀏覽器的使用者才能存取。最受歡迎的三種暗網是 I2P（Invisible Internet Project，即「隱形網際網路計劃」）、Freenet[31] 和 Tor，以下介紹最廣為人知的 Tor。

雖然現今暗網被犯罪集團拿來作為交易毒品、炸彈零件、槍枝、兒童色情、偽造之身分證明文件、駭客服務等不法用途，然 Tor 本身最初係由美國海軍研究實驗室 20 世紀 90 年代開發，並於 2002 年向公眾發布[32]。Tor 的最初目的是「隱藏試圖在壓迫政權內進行交流的美國特工或持不同政見者的身分」。除了犯罪用途外，有些媒體為了突破集權國家的網路封鎖，抗衡集權政府的言論管制，讓使用者可以看見真實的訊息，也建立暗網的網站，例如臉書（Facebook）[33]、紐約時報（NYTimes）[34]、英國廣播公司（BBC）[35]。水能載舟，亦能覆舟，基於技術中立原則（Technological neutrality），一項新的科學技術的發明，可能應用在各種方面，有好的也有壞的，故暗網並非全然拿來作為犯罪之用，特此說明。

（二） 暗網的運作

使用者可透過 Tor 接達由全球志願者免費提供，包含 6000 多個中繼的覆蓋網路，從而達至隱藏使用者真實位址、避免網路監控及流量分析的目

[31] 自由網（Freenet）是對等網路的一個應用軟體。用 Java 編寫的跨平台軟體，有 5 個以上節點的使用者群，就可以用寬頻分享種子檔案，組成獨立的網路系統。主要應用在匿名網際網路領域，如海盜灣、維基解密、絲綢之路等，具有抗審查（censorship-resistant）之特性，。可參見：https://en.wikipedia.org/wiki/Freenet (Last viewed: Nov,17,2023)

[32] www.torproject.org (Last viewed: Nov,17,2023)

[33] 其 Tor 位址為：facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion.

[34] https://www.nytimes3xbfgragh.onion/

[35] https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion/.

的。Tor 使用者的網際網路活動（包括瀏覽線上網站、貼文以及即時訊息等通訊形式）相對較難追蹤。Tor 的設計原意在於保障使用者的個人隱私，以及不受監控地進行秘密通訊的自由和能力。

Tor 通過一種叫做路徑選擇演算法的方式自動在網路中選擇 3 個 Tor 節點，這三個節點分別叫做入口節點（Guard relay）、中間節點（Middle relay）和出口節點（Exit relay）。在網路連接的應用層，資料以一種叫做洋蔥路由的方式進行傳輸。資料首先在使用者端連續加密三層，而三個中繼各自解密一層，這樣它們就能知道接下來把資料傳送給誰。在這種情況下，資料就像剝洋蔥一樣被一層一層地解密，所以被稱為「洋蔥路由」。最後的出口節點會解密最內層的加密數據並得到真實的資料內容，並把它傳送給目標位址。出口節點雖然知道真正的資料內容，但是它只知道上一個中繼節點的位址，並不知道資料最初的傳送者是誰，從而保證了資料傳送者的安全。相對應地，入口節點僅知曉使用者的 IP 位址而無法得知其訪問的網站，而中間節點既無法得知 IP 位址也無法得知使用者所訪問的內容[36]（如圖 2）。

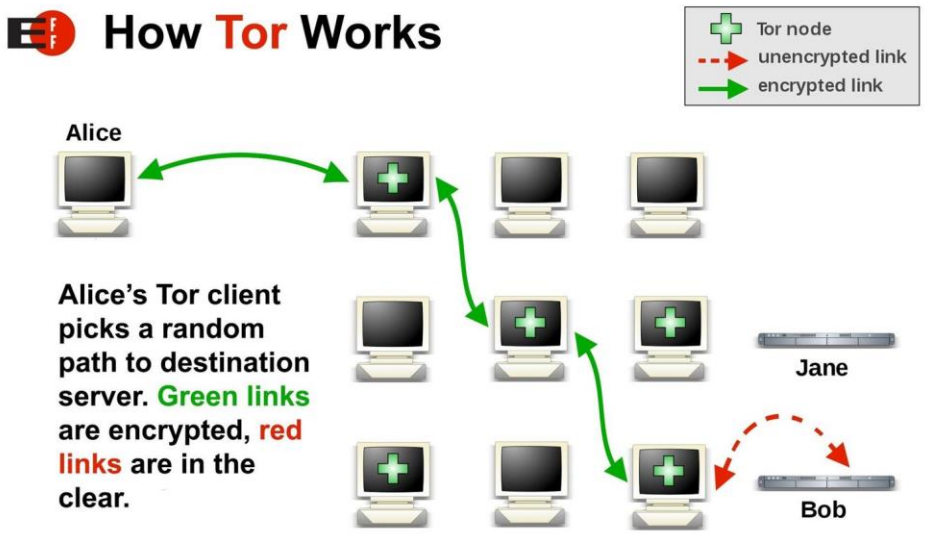


圖 2（來源：Electronic Frontier Foundation）

[36] https://zh.wikipedia.org/zh-tw/Tor (Last viewed: Nov, 16, 2023)

二、 最大的暗網市集 Hydra 案

（一） Hydra 暗網市集[37]

在 2022 年被美國司法部及德國聯邦刑事警察局(Bundeskcriminalamt)合作查封之前，Hydra Market（Hydra）是世界上最大、運行時間最長的暗網市集，這網站註冊了 1,700 萬客戶和 19,000 多個賣家帳戶。2021 年，Hydra 估計佔所有暗網市場相關加密貨幣交易的 80%，自 2015 年以來，該市場已收到約 52 億美元的加密貨幣。Hydra 上的供應商可以在網站上建立帳戶來宣傳他們的非法產品，買家可以建立帳戶來查看和購買供應商的產品。Hydra 供應商提供各種非法藥物出售，包括古柯鹼、甲基安非他命、LSD、海洛因和其他鴉片類藥物。供應商在 Hydra 上公開宣傳他們的藥物，通常包括照片和受管制物質的描述。買家還可以根據五星級評級系統對賣家及其產品進行評分，供應商的評分和評論會在 Hydra 網站的顯著位置顯示（如圖 3[38]）。

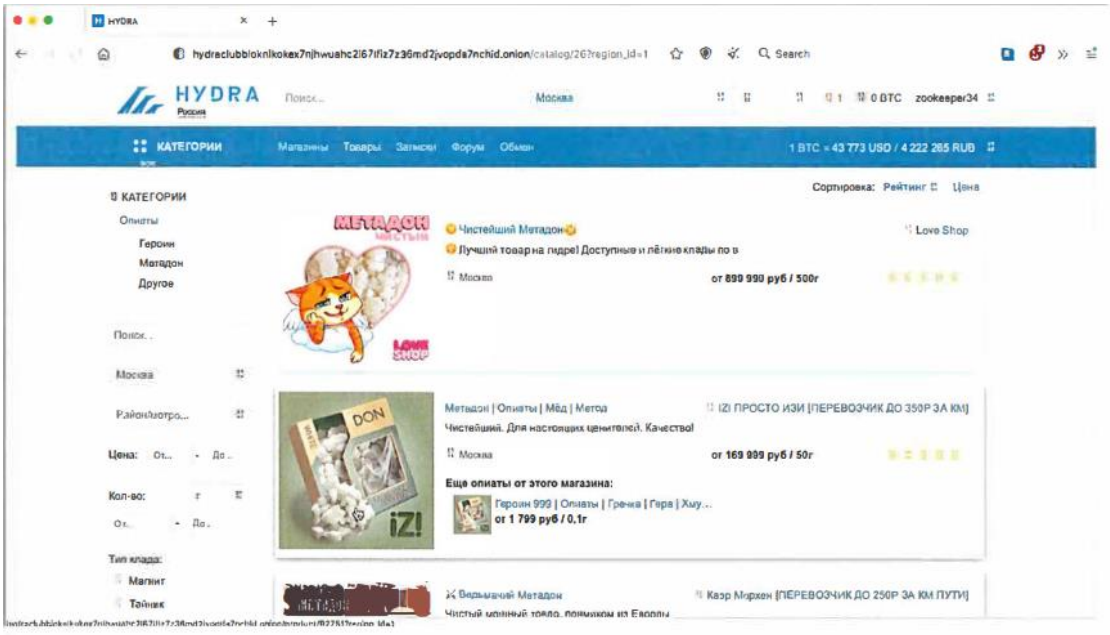


Exhibit 1: Screenshot of Hydra Market Drug Listings

[37] https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace (Last viewed: Nov,17,2023)

[38] Indictment, United States v. pavlov Dmitry, Cr-22-143 (APR, 5, 2022), at 2, available at https://www.justice.gov/opa/press-release/file/1490906/download (Last viewed: Nov, 16, 2023)

圖 3

Hydra 也被發現許多供應商出售虛假身分證明文件。使用者可以搜尋銷售所需類型身分證明文件（例如美國護照或駕駛執照）的供應商，並按商品價格進行過濾或排序。許多虛假身分證明文件的供應商可以根據買家提供的照片或其他資訊定製文件（如圖 4[39]）。

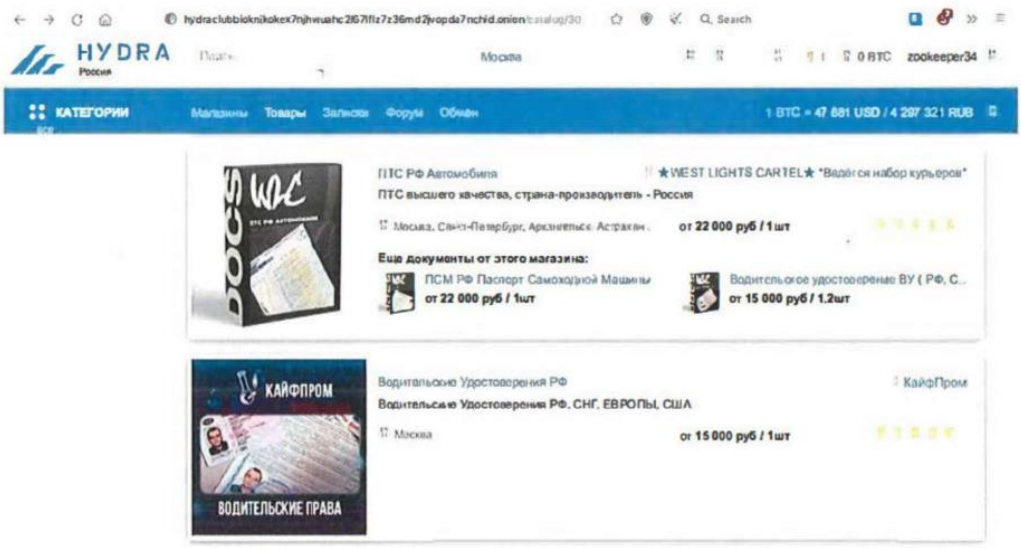


Exhibit 2: Vendor listings for false identification documents. The bottom vendor offered driver's licenses for the U.S., Europe, and Russia.

圖 4

許多供應商也透過 Hydra 出售駭客工具和駭客服務。駭客供應商通常會非法存取買家選擇要入侵的的線上帳戶。透過這種方式，買家可以選擇受害者並聘請專業駭客來存取受害者的通訊並接管受害者的帳戶（如圖 5[40]）。

[39] Id. at 3.
[40] Id. at 5.

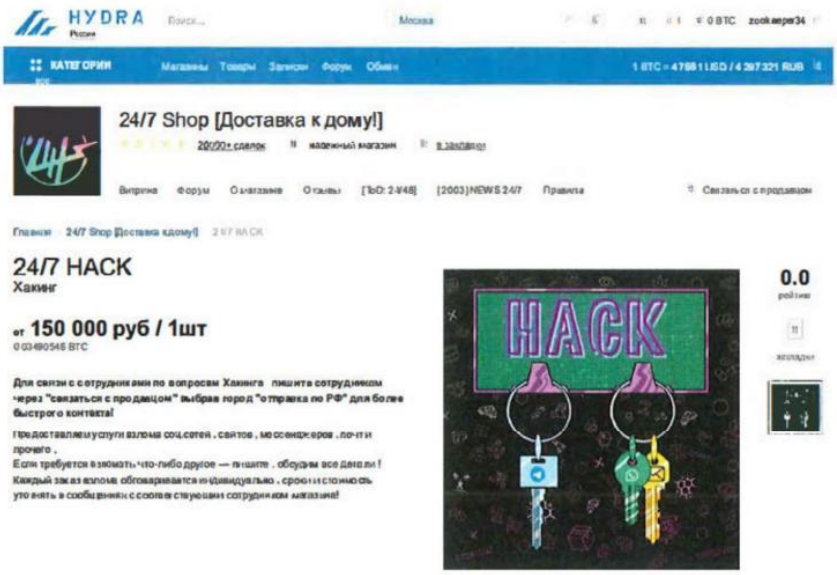


Exhibit 5: Vendor offering hacking services. The vendor claimed expertise in hacking social media accounts, websites, messengers, and emails.

圖 5

Hydra 供應商還提供一系列的洗錢和所謂的「兌現」服務，允許 Hydra 用戶將其比特幣（BTC）轉換為 Hydra 眾多供應商支援的各種形式的貨幣。此外，Hydra 還提供內部混合服務（又稱為混幣器，Mixer）來清洗並處理供應商的提款。混合服務允許客戶在付費的情況下以隱藏比特幣來源或所有者的方式將比特幣發送給指定的接收者。Hydra 的洗錢功能非常受歡迎，以至於一些用戶會設立空殼供應商帳戶，真實的目的是透過 Hydra 的比特幣錢包作為洗錢技術來運作資金（如圖 6[41]）。

從 2015 年 11 月左右開始，pavlov dmitry 經營了一家名為 Promservice Ltd. 的公司，以 Hosting Company Full Drive、All Wheel Drive 和 4x4host.ru 之名義負責管理 Hydra 的伺服器（Promservice）。在此期間，Pavlov 透過他的公司 Promservice 管理 Hydra 的伺服器，該伺服器允許該市場作為數千名毒販和其他非法供應商使用的平台進行運作，向數千名毒

[41] Id. at 6.

販和其他非法商品和服務發送大量非法毒品、其他非法商品和服務。並為從這些非法交易中獲得的數十億美元不法所得進行洗錢。

作為 Hydra 伺服器託管的管理員，被告 pavlov 與 Hydra 的其他運營商合謀，透過提供關鍵基礎設施使 Hydra 在競爭激烈的暗網市場環境中運營，並蓬勃發展，從而進一步推動該網站的成功。被告這樣做為 Hydra 的活動提供了便利，並允許 Hydra 從透過該網站進行的非法銷售中獲取價值數百萬美元的佣金。

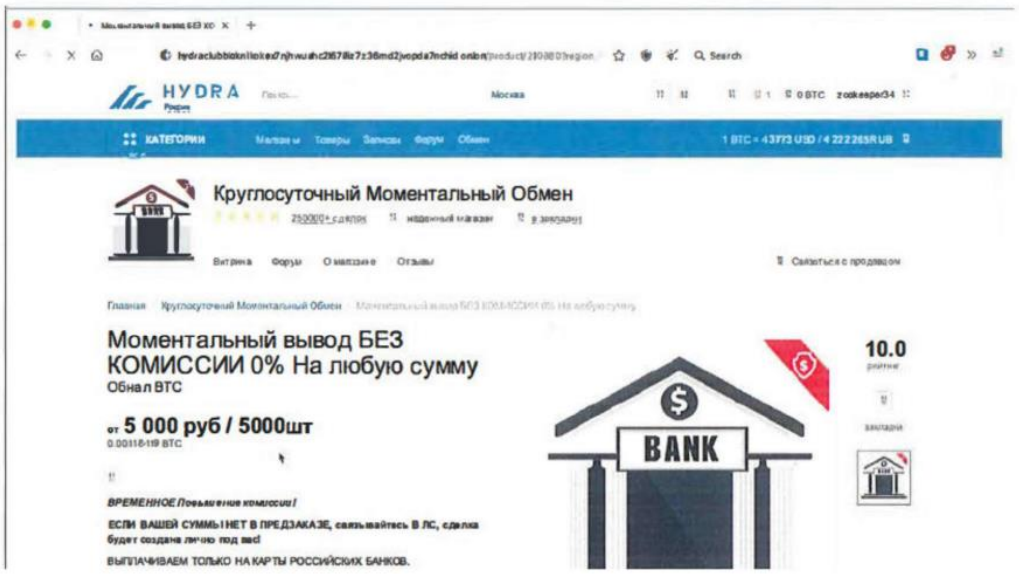


Exhibit 6: Vendor offering 24/7 instant exchange of bitcoin to rubles via a Russian bank card.

圖 6

（二） 調查團隊成員[42]

美國的調查是在司法部多機構特別行動司（Department of Justice's multi-agency Special Operations Division）和刑事鴉片類藥物和暗網聯合執法小組 （the Joint Criminal Opioid and Darknet Enforcement, JCODE） 的支持和協調下進行的，美國執法機關參與的有緝毒局邁阿密分部（DEA's Miami Field Division）、聯邦調查局（FBI）、國稅局犯罪調查科（IRS-CI）、美國郵政調查局（U.S. Postal Inspection Service）、美國國土安全調查處（DHS/ICE

[42] Supra, note 37.

Homeland Security Investigations, HSI）。上開調查團隊並跨國與德國聯邦刑事警察局合作。於查獲被告並查扣上開網域後，該案由加州北區美國檢察官辦公室的助理檢察官 Claudia A. Quiroz 和 Robert S. Leach 以及刑事部門電腦犯罪和智慧財產權科的檢察官 C. Alden Pelker 和 Christen M. Gallagher 起訴此案。

這次起訴是有組織犯罪緝毒工作小組（Organized Crime Drug Enforcement Task Forces, OCDETF）調查的一部分。OCDETF 透過利用檢察官主導、情報驅動、多機構偕同辦案的方法，利用聯邦、州和地方政府的優勢，以識別和瓦解威脅美國的最高級別毒販、洗錢者、幫派和跨國犯罪組織。透過州和地方的執法機構共同打擊犯罪網絡。此外，司法部國際事務辦公室（Justice Department's Office of International Affairs, OIA）和美國哥倫比亞特區檢察官辦公室也提供了大量援助。司法部國家加密貨幣執法小組（National Cryptocurrency Enforcement Team, NCET）也提供了協助。

需特別說明者，筆者於 2023 年至位於泰國曼谷的美國國際執法學院[43]（International Law Enforcement Academy Bangkok, Thailand, ILEA Bangkok）受訓，學習到美國不同辦案單位間，有因應案件需求而進行境內跨單位聯合辦案之機制，分析是否與其他單位進行境內跨單位聯合辦案時，會先從預防、偵查、起訴到不法所得追討等部分，評估金融調查項目，也評估各該執法機構在聯合辦案中可提供之辦案工具，並評估是否適合聯合辦案的項目包含該單位的風險評估、偵查能力、轉介能力、聯合辦案及分享意願、機構誠信及機構政策發展等項目，以及聯合辦案會遇到的挑戰。

境內跨單位聯合辦案主要分成聯合調查（Joint Investigation）及專案執行（Task Forces），聯合調查是個別案件中臨時組成的辦案團隊 ；專案執行

[43] 係美國國務院所屬國際毒品及執法事務局 (BUREAU OF INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT AFFAIRS, US Department of State) 與泰國皇家警察於 1998 年 9 月 30 日成立於泰國曼谷樂喜區的國際執法人員訓練學院。目的在訓練及提升亞太國家執法人員的打擊犯罪能力，且促進學員間情誼。

則是短期或長期的團隊合作，用以同時辦理多件案件，協調偵查及其他議題之團隊 。藉由聯合辦案及專案執行，可以達到增加執行能力、強化偵查能量與工具及犯罪追查能力、資源分享、避免執行行動中的衝突、同步進行專案、增加情資分享及提高遏制犯罪等優勢。

成功建立境內跨單位聯合辦案的程序：1.評估是否有適切的法律基礎；2.確認單位間合法情資交換的嫁接；3.研析執行疑義；4.考量將合作內容以書面形式化之方式進行[44]。

（三） 防彈主機

網路犯罪集團要能長期維持順暢隱密的運作，一項基本要素就是穩定可靠且不怕遭人檢舉、也不畏懼執法機關警告的網站代管服務。這類所謂的「防彈主機代管服務」（Bulletproof hosting）基本上就是出租給網路犯罪集團躲藏的地方。

經過調查團隊使用種種偵查技巧追查後，終於查知 Hydra 網站的伺服器存在德國境內，而該伺服器係由被告之俄羅斯網路託管公司 Promservice, Ltd 所營運，透過德國警方查獲上開網路託管公司，並查扣 Hydra 網站的伺服器，並沒收了價值 2,300 萬歐元的比特幣。在德國警方查扣該網站伺服器後，網站顯示之遭查扣之頁面（如圖 7[45]）。

[44] 可參見：公務出國報告「泰國曼谷國際執法學院 2023 年『跨機關（緝毒局及國稅局）合作金融偵查課程』出國報告」（2023），第 6 頁至第 8 頁。

[45] https://www.bbc.com/zhongwen/trad/world-60911545 (Last viewed: Nov,17,2023)

圖 7

（四） 制裁[46]

美國財政部長 Janet L. Yellen 就上開打擊暗網之行動表示：源自俄羅斯的網路犯罪和勒索軟體的全球威脅，以及犯罪首腦在俄羅斯開展活動而不受懲罰的能力，令美國深感擔憂。我們今天的行動向犯罪分子傳達了這樣一個訊息：你無法隱藏在暗網或其論壇上，你也無法隱藏在俄羅斯或世界其他任何地方。我們將與德國和愛沙尼亞等盟友和夥伴協調，繼續破壞這些網絡等語。

並表示：俄羅斯是網路犯罪分子的天堂。今天針對 Hydra 和 Garantex 的行動是基於最近對虛擬貨幣交易所 SUEX 和 CHATEX 的制裁，這兩家交易所與 Garantex 一樣，都是在俄羅斯莫斯科聯邦大廈運作。財政部致力於對 Hydra 和 Garantex 等故意無視反洗錢和打擊資助恐怖主義 (AML/CFT) 義務並允許其係統被非法行為者濫用的行為者採取行動。虛擬貨幣交易所經營者肆意無視監管和合規的行為將受到嚴格調查，並在適當情況下追究肇事者的責任。此外，美國敦促國際社會在虛擬貨幣領域有效實施反洗錢/打擊資助恐怖主義的國際標準，特別是在虛擬貨幣交易方面。虛擬貨幣產業在實施適當的反洗錢/打擊資助恐怖主義和制裁控制方面可以

[46] https://home.treasury.gov/news/press-releases/jy0701 (Last viewed: Nov,17,2023)

發揮關鍵作用，以防止受制裁人員和其他非法行為者利用虛擬貨幣破壞美國及其合作夥伴的國家安全。

除了制裁 Hydra 之外，OFAC 還確定了 100 多個與該實體營運相關的虛擬貨幣位址，這些位址已被用於進行非法交易。財政部致力於在其他非法虛擬貨幣地址可用時予以共享。

（五） 起訴法條

共謀散布毒品[47]（conspiracy to distribute narcotics）、共謀透過營運 Hydra 伺服器而洗錢[48]（conspiracy to commit money laundering in connection with his operation and administration of the servers used to run Hydra）、共謀身分竊盜[49]（conspiracy to commit identity thef）、共謀侵入設備詐欺[50]（conspiracy to commit access device fraud）、共謀電腦詐欺[51]（conspiracy to commit computer fraud）等罪嫌。

[47] 21 U.S.C. §§ 846, 84 1 (a)(l) and (b)(l)(A).
[48] 18 U.S.C. § 1956(h).
[49] 18 U.S.C.1028(f).
[50] 18 U.S.C. 1029(b)(2).
[51] 18 U.S.C. 1030(b).

肆、 僵屍網路

一、 僵屍網路之意義

殭屍網路（Botnet）是指眾多連接網路的設備，受到駭客、電腦病毒或是木馬程式入侵，使惡意人士可以以 C&C（Command & Control）的方式遠端控制大量受到入侵的設備，進而構成「殭屍網路」（Botnet），發動惡意攻擊。由於殭屍網路影響的設備並不只侷限於可以連接網路的電腦，甚至包含了智慧型手機、家庭路由器、網路監視攝影機等。並且隨著物聯（IOT, Internet of Thing）日益興盛，大量可以連接網路的設備也隨之增加，除降低了殭屍網路建構的難度外，也提高了一般使用者的設備被殭屍網路感染的風險[52]。殭屍網路可專門用來完成非法或惡意工作，包括傳送垃圾郵件、竊取資料、勒索軟體、以欺騙性手段點擊廣告或分散式阻斷服務 (DDoS) 攻擊[53]。

二、 僵屍網路 IPStorm 案

（一） IPStorm 的運作

崛起於 2019 年 6 月的 IPStorm 是以 Golang[54]所撰寫，原本鎖定 Windows 裝置進行感染，隨後並將版圖擴大到 Linux、macOS 與 Android，其惡意程式目的是令這些裝置為 Makinin 所控制，Makinin 對外宣稱總共握有全球 2.3 萬個裝置的控制權，遍及亞洲、美洲與歐洲。根據羅馬尼亞資

[52] https://www.apeiro8.com/why-cdn-log-is-important-to-prevent-from-botnet-attack/ (Last viewed: Nov,17,2023)

[53] https://www.cloudflare.com/zh-tw/learning/ddos/what-is-a-ddos-botnet/ (Last viewed: Nov,17,2023)

[54] Go（Golang）語言是由一個 Google 團隊開發的，該團隊在打造傑出程式語言和作業系統方面都已有悠久歷史。他們創造出一種能讓程式設計師喜愛的語言 ,讓人感覺神似 JavaScript 或 PHP 的動態特性，卻又具備 C++ 和 Java 這些強型別語言的性能和效率。可參見：https://www.flag.com.tw/activity/edm/F1741/ (Last viewed: Nov,17,2023)

安業者 Bitdefender 在 2020 年針對 IPStorm 所發表的分析白皮書，被植入 IPStorm 惡意程式的受害者主要位於亞洲，前三名是香港、南韓與臺灣[55]。

（二） IPStorm 案的調查[56]

從 2019 年 6 月到 2022 年 12 月，摩爾多瓦國民 Sergei Makinin（被告）開發並部署了惡意軟體（malicious software），以攻擊包括波多黎各在內的世界各地數千台連網裝置。Makinin 將這些受感染的設備作為廣泛的殭屍網路的一部分進行控制，成為受感染設備的網路。這個殭屍網路的主要目的是將受感染的設備轉變為代理伺服器(proxy server)，作為營利計劃的一部分，該計劃允許透過 Makinin 的網站 proxx.io 和 proxx.net 訪問這些代理伺服器。透過這些網站，Makinin 向尋求隱藏其網路活動的客戶出售對受感染、受控設備的非法存取權限。單一客戶每月可以支付數百美元來透過數千台受感染的電腦路由傳輸流量。Makinin 的公開網站宣稱他擁有來自世界各地的 23,000 多個「高度匿名」代理商。Makinin 承認，他從該計劃中獲得了至少 55 萬美元。根據認罪協議，Makinin 將被沒收與犯罪相關的加密貨幣錢包。

美國檢察官 Stephen Muldrow 表示：這項調查表明，我們將使用一切可用的合法工具來打擊網路犯罪分子，無論他們身在何處。此案是一個警告，表明法律的影響範圍很大，任何地方使用電腦犯罪的犯罪分子最終都可能在他們沒有預料到的地方面臨其行為的後果等語。另執法破獲的範圍僅限於禁用被告的基礎設施，並未延伸至電腦所有者和使用者的資訊，對此，FBI 強調讓電腦保持最新安全性修補程式和作業系統更新的重要性。

---

55 https://www.ithome.com.tw/news/159835 (Last viewed: Nov,17,2023)

56 https://www.justice.gov/usao-pr/pr/russian-and-moldovan-national-pleads-guilty-operating-illegal-botnet-proxy-service (Last viewed: Nov,17,2023)

（三） 調查團隊

該案由美國聯邦調查局 FBI San Juan 網路小組、駐 Madrid 的法律聯絡官辦公室（legal attaché office），與西班牙國家警察網路打擊小組（Spanish National Police-Cyber Attack Group）的合作下進行調查；聯邦調查局駐 Santo Domingo 法律聯絡官辦公室，與多明尼加國家警察國際刑警組織（Dominican National Police-Interpol）、多明尼加國家警察國際有組織犯罪司（Dominican National Police-International Organized Crime Division）以及內政部和警察移民局（Ministry of the Interior and Police-Immigration Directorate）協調。此外，此團對亦納入私部門的協助，由國家網路鑑識和培訓聯盟[57] (The National Cyber-Forensics and Training Alliance, NCFTA.net) 提供幫助，其中包括 Bitdefender DRACO 團隊、Anomali 威脅研究和 Intezer。

該案由美國波多黎各地區檢察官辦公室的 AUSA Jonathan Gottfried 以及司法部電腦犯罪和智慧財產權科的資深顧問 Jane Lee 和 Jeff Pearlman 在國際事務辦公室（Office of International Affairs）的協助下起訴。

（四） 起訴法條

在未經授權下，故意傳輸程式、資訊、程式碼或指令，因而造成應受保護之電腦受有損害罪嫌[58]（共三罪）。每一罪最重可判處 10 年有期徒刑，目前被告業經認罪（plead guilty），尚待聯邦地方法院法官（federal district court judge）於考慮美國量刑指南和其他法定因素後做出判決。

[57] NCFTA 是一個由企業和執法部門組成的聯盟，共同致力於打擊網路犯罪。請參見：https://www.ncfta.net/ (Last viewed: Nov,17,2023)

[58] 18 U.S.C. § 1030(a)(5)(A)：”knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer”.

伍、 虛擬貨幣[59]

一、 前言

今日的逮捕，及美國司法部史上最高金額之查扣，表示虛擬貨幣對於犯罪者來說，並非安全的天堂，我們會追著錢，不管錢轉換成什麼形式-美國司法部副部長 Lisa O. Monaco 2022.02.08

近年來與虛擬貨幣[60]有關之犯罪日益增加，據統計，於西元 2022 年間，全球關於兒童色情、勒索軟體、竊盜、制裁、恐怖份子、詐欺、電腦犯罪、暗網等與虛擬貨幣有關之犯罪，其虛擬貨幣交易總金額達到歷史新高的 206 億美元[61]。於 2021 年間，美國東部最大燃油公司 Colonial Pipeline 遭駭客攻擊勒索比特幣，導致關鍵基礎設施停止運營，造成美國東部多州進入緊急狀態[62]。於 2022 年間，南韓更首次查獲現役軍官收受比特幣而向北韓特工洩露軍事機密的案件[63]。再再顯示虛擬貨幣相關犯罪不只限於詐欺，更已有實際案例顯示已影響國家基礎關鍵設施，甚至是國家安全。

而虛擬貨幣相關犯罪在臺灣也屢見不鮮，根據我國 2021 年國家洗錢資恐及資武擴風險評估報告首次將虛擬資產業被列為非常高風險弱點[64]。在偵查實務上，近來跟虛擬貨幣有關之感情詐欺、投資詐欺案件日益增長，

---

[59] 羅韋淵，偵辦虛擬貨幣相關犯罪之戰略思考－美國司法部史上最大查扣案之借鏡，檢察新論第 32 期，第 23-43 頁。此文為筆者在美期間研究撰寫而成，撰寫過程中某日傍晚，筆者抬頭一看，發覺窗外竟開始飄雪，此為筆者赴美後，在波士頓經歷的第一場雪，迄今難忘。

[60] 各國對於虛擬貨幣之用語不一，有稱之為加密貨幣、數位貨幣、數位資產、虛擬通貨、虛擬資產等，而我國洗錢防制法之用語為「虛擬資產」，本文為避免與國外用語不一而產生困擾，故以下以通俗之虛擬貨幣稱之。

[61] Chainalysis, The 2023 Crypto Crime Report, at 5 (Feb. 2023).

[62] 該公司於支付比特幣贖金後，大部分比特幣業經美國司法部追回並扣押，可參見美國司法部新聞稿：https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

[63] 參見：https://www.bbc.com/news/world-asia-61255779

[64] 2021 年國家洗錢資恐及資武擴風險評估報告，行政院洗錢防制辦公室，47 頁。

更不乏向透過中間幣商購幣後轉至詐欺集團所控制之錢包，造成偵查斷點。對於偵查機關而言，如何運用公開情報來源（Open-source intelligence，OSINT）、區塊鏈之公開帳本特性及區塊鏈瀏覽器等工具追查幣流，進一步凍結、扣押不法虛擬貨幣，即為當務之急。

於 2022 年 2 月 8 日，美國司法部宣布逮捕一對比特幣洗錢夫妻，其查扣 9.4 萬顆之比特幣，依當時之比特幣價格[65]，折合美金約 36 億美元，創下美國司法部史上查扣金額最高之虛擬貨幣紀錄，同時亦為查扣金額最高之金融犯罪案件。根據美國司法部公布之起訴書及相關文件，內容詳述該案被告關於虛擬貨幣之洗錢手法及美國執法機關[66]之追查經過，筆者認為實值參考，茲介紹如下，並提出個人對於國內偵辦虛擬貨幣犯罪之戰略思考之淺見。

二、 事實概要[67]

（一） Bitfinex 駭客案

於 2016 年 8 月間，虛擬貨幣交易所 Bitfinex 遭駭客入侵，並遭執行了逾 2000 次之比特幣交易，該交易所錢包內之 119754 枚比特幣遭駭客轉出至外部錢包（Wallet 1CGA4s），當時上開比特幣價值約為 7100 萬美元。隨著比特幣價格上漲，該批遭竊之比特幣的價值於 2022 年 7 月間已高達 45 億美元。

---

[65] 當時一枚比特幣價格約 4 萬 4,000 美元，可參：https://coinmarketcap.com/currencies/bitcoin/historical-data/

[66] 本案係由多個執法機關共同合作，包含美國國稅局電腦犯罪部門 DC 辦公室電腦犯罪小組（IRS-CI Washington, D.C. Field Office's Cyber Crimes Unit）、聯邦調查局芝加哥辦公室（the FBI's Chicago Field Office）、移民及海關執法局國土安全調查部門紐約分部（HSI-New York）。及由德國 Ansbach 警察局（Ansbach Police Department in Germany）提供協助。See Press Release, "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency", U.S. Dept. of Justice (Feb. 2, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[67] Id.

（二） 夫妻比特幣洗錢案

美國執法機關持續在比特幣區塊鏈上追查上開遭竊之比特幣的下落，於 2017 年 1 月間，一部分遭竊的比特幣透過為數甚多的帳號及交易平台，以一系列小額、複雜的交易從錢包地址 Wallet 1CGA4s 轉出。這些為數甚多的混亂交易係欲造成隱匿遭竊比特幣之金流，讓執法機關難以追蹤。但執法機關仍然透過區塊鏈分析等方式，追蹤到這批比特幣的流向，流入了由具有美國及俄羅斯雙重國籍之被告 ILYA “DUTCH” LICHTENSTEIN（下稱李斯坦），及其妻子 HEATHER MORGAN（下稱摩根）所掌控之帳戶。

儘管於 2017 年被告二人進行了上開複雜的洗錢交易，但從 2016 年 8 月至 2022 年 1 月 31 日間，大部分的比特幣還是存放在 Wallet 1CGA4s。於 2022 年 1 月 31 日，執法機關破解了被告李斯坦存放於雲端硬碟中的加密檔案，該檔案中臚列了 2000 各虛擬貨幣錢包地址，以及所對應之「私鑰」。根據區塊鏈分析，可以確認這些錢包地址幾乎可以全部回溯至駭客的錢包地址。於 2022 年 1 月 31 日至 2 月 1 日間，執法機關在緊急情況下認為具有相當理由（Probable cause），而使用李斯坦存放於雲端硬碟中之私鑰，從 Wallet 1CGA4s 中扣押了約 94,636 枚比特幣，當時價值大約 36.29 億美元。於 2022 年 2 月 4 日法院核發了扣押命令（Seizure warrant）核准扣押上開比特幣。而這一批比特幣目前仍由美國政府保管中。

三、 案件分析

（一） 名詞說明

1. 虛擬貨幣

虛擬貨幣（Virtual Currency[68]）或加密貨幣（Cryptocurrency[69]）一詞在我國法制上並非法定用語，其用語在各國亦非一致，有「數位資產」（Digital Assets[70]）、虛擬資產（Virtual Assets[71]）等不一而足。

因虛擬貨幣依我國之法制並非「貨幣」，而係「通貨」，洗錢防制法第 5 條第 2 項之規範用語為「虛擬通貨」，另虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法第 2 條第 1 項第 2 款則定義：「虛擬通貨：指運用密碼學及分散式帳本技術或其他類似技術，表彰得以數位方式儲存、交換或移轉之價值，且用於支付或投資目的者。但不包括數位型式之新臺幣、外國貨幣及大陸地區、香港或澳門發行之貨幣、有價證券及其他依法令發行之金融資產。」「密碼學」、「分散式帳本」技術二者即為區塊鏈之核心特色，可認我國所指虛擬通貨雖未言名係基於區塊鏈技術而發展，但所指即為包含目前國內偵查實務上遇到最多的比特幣、以太幣等基於區塊鏈技術而發展之虛擬貨幣。

---

[68] 美國財政部所屬金融犯罪執法局（Financial Crimes Enforcement Network, FinCEN)多以 Virtual Currency 稱之。see https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering (Last visited Mar. 19, 2023)

[69] U.S. Department of Justice, Report of the Attorney General's Cyber-Digital Task Force: Cryptocurrency Enforcement Framework (2020) [hereinafter 2020 Cryptocurrency Enforcement Framework], https://www.justice.gov/archives/ag/page/file/1326061/download .

[70] U.S. Department of Justice, The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Oder 14067: The Role of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets(2022) [hereinafter The Role of Law Enforcement Report], https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf

[71] 近年來國際防制洗錢金融行動工作組織（Financial Action Task Force, FATF）所制訂之指引多使用虛擬資產（Virtual Assets）一詞，可參見：https://www.fatf-gafi.org/en/publications/Virtualassets/Virtual-assets.html (Last visited Mar. 19, 2023)

比特幣即為在比特幣區塊鏈上運作的一種虛擬貨幣[72]，在區塊鏈的基礎上，礦工（Miner）靠著解決密碼學上的難題將交易記錄上區塊內，一般稱之為挖礦[73]，一旦礦工解決了難題，就可以獲得獎勵，而獎勵即為系統生之比特幣或交易手續費（Transaction fee），因比特幣之產生非由中心化之機構發行，故有「去中心化」之特性。區塊鏈上的交易記錄會同步到各個挖礦節點（Nodes）上，而由成千上萬非由同一人控制之節點紀錄著相同的交易內容，稱為分散式帳本，如欲修改帳本內的某筆交易記錄，除了需要更動關連之哈希值（Hash value）以外，更須經由多數節點認同，始能修改，而節點成千上萬、散布世界各地[74]，縱使有心人欲竄改其中某交易記錄，其亦難以串通說服多數節點竄改資料，故比特幣區塊鏈之交易記錄有其「難以竄改」之特性。

一般獲取比特幣或其他虛擬貨幣之管道除了挖礦以外，有虛擬貨幣交易所、比特幣 ATM、或者直接從其他持有虛擬貨幣之人獲得。而另一種實務上較常遇到的是「泰達幣」（USDT），其與比特幣之原理不同，詳下述。

2. **私鑰、公鑰與錢包地址**

虛擬貨幣交易過程中需要錢包地址（address）、公鑰（Public Key）及私鑰（Private Key），關於其間之生成關係及作用原理，礙於篇幅故不多做著墨，僅就偵查實務上所需之概念簡單說明。錢包地址可以理解為銀行帳號，而私鑰可以理解為密碼，如欲交易虛擬貨幣則必須有交易對象之錢包地址，始能移轉虛擬貨幣，而私鑰則儲存在錢包內，擁用有私鑰即代表擁

---

[72] Damien Cosset, Blockchain: What is Mining?, DEV (Jan. 5, 2018), https://dev.to/damcosset/blockchain-what-is-mining-2eod

[73] 以比特幣區塊鏈而言，大約 10 分鐘會生成一個區塊，區塊內紀錄著這 10 分鐘內的交易記錄。筆者在哈佛大學擔任訪問學者時，適逢哈佛大學甘迺迪學院邀請麻省理工學院 Steve Derezinski 教授開設「介紹 web3-從零到發行代幣」（Intro to Web3--From Zero to Token Launch）課程，筆者全程參與課程獲益良多，課堂中 Steve Derezinski 教授亦介紹一以卡通動態顯示各區塊鏈生成之狀況之網站（https://txstreet.com/v/eth-btc），十分有趣。

[74] 據統計，目前比特幣區塊鏈節點計有 1 萬 6,652 個，遍佈美洲、歐洲、亞洲等地，可參：https://bitnodes.io/。

有動用該對應錢包地址內之虛擬貨幣之權限，在幣圈的諺語道「擁有私鑰，才擁有虛擬貨幣」（Not your key, not your coin）即為此道理。於執法機關欲扣押被告之虛擬貨幣時，取得被告之私鑰即為關鍵。

比特幣錢包地址以數字「1」或「3」、「bc1」開頭[75]，地址中的英文區分大小寫，但不包括英文字母大寫 I、小寫 l、大寫 O、數字 0 等容易誤認的字母，而「1」開頭的地址長度為 26~34 位，「3」開頭的地址長度為 34 位，「bc1」開頭的地址長度為 42 位。

不同區塊鏈上之錢包地址之特徵或有不同，例如以太幣（ETH）和以太坊（含以太坊 ERC20 代幣）錢包地址則是「0x」開頭的 42 位大小寫英文字母加上數字[76]。另波場鏈（TRON）之錢包地址（含 TRC20 代幣）之特徵為大寫字母「T」開頭的地址長度為 34 位。但相同地址亦可能存在於不同之區塊鏈上。而透過錢包地址可初步識別該錢包地址是屬於哪一個區塊鏈[77]，以利後續選擇正確的區塊鏈查詢相關幣流，故此節在幣流追蹤上亦屬重要。

助記詞（Recovery seed or Mnemonic phrase）：因為比特幣之私鑰係透過隨機生成而符合密碼學原理之 64 位元十六進位字串字串[78]，包括大小寫字母和數位。由於私鑰呈現的形式難以記憶，故也有錢包是透過助記詞來生成私鑰，助記詞一般係由 12 個、24 個或其他數字的英文單字組成，其功能相當於私鑰，故執法機關在執行搜索現場時，需特別留意有無記載英

[75] 例如美國政府用以查扣暗網絲路駭客之比特幣地址為：bc1qmxjefnuy06v345v6vhwpwt05dztztmx4g3y7wp。

[76] 例如美國財政部海外資產控制辦公室（Office of Foreign Assets Control, OFAC）對於北韓駭客組織所持有之以太幣地址發布制裁，該駭客組織之以太幣地址為：0x098B716B8Aaf21512996dC57EB0615e2383E2f96。可參見：https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220422

[77] 如欲確認某一錢包地址存在於何等區塊鏈上，可將錢包地址輸入網站：https://blockscan.com/ 查詢。

[78] 例如筆者透過比特幣地址產生網站（https://www.bitaddress.org/ ）隨機生成之比特幣私鑰為：KzoEJt2yv3RYZGY7K5qsmacmsT15utWCKptiABkG3tmzQwyVwozx。

文單字之紙張或其他載體[79]，於取得後始有可能以移轉虛擬貨幣至執法機關錢包之方式扣押之。

3. **錢包**

冷錢包（Cold wallet）與熱錢包（Hot wallet）：其係以是否隨時連上網路為區別，一般安裝在手機或電腦端之錢包程式，因為隨著手機、電腦連上網而錢包程式也會隨時連接網路，稱為熱錢包。冷錢包則係將私鑰儲存於離線儲存裝置，外型有的像隨身碟，有的像一張金融卡大小的卡片，又稱為離線錢包或硬體錢包，因為平常不連接網路，只有要交易時才透過藍芽或插入 USB 等方式連接上網，理論上比較不易有私鑰外洩的風險。故執法機關在搜索現場，除了需注意被告手機、電腦內有無錢包程式外，冷錢包之識別亦為重點。此外，近來也有冷錢包內建指紋辨識，美國執法機關在搜索票聲請書上亦會註明請法院授權執行強制按壓（depress）受搜索人之指紋以解鎖裝置[80]。

託管錢包（Custodial/ Hosted wallets）與非託管錢包（Non-custodial/ Unhosted wallets）：一般而言，託管錢包係指使用者下載至手機或電腦端使用之錢包程式是由交易所提供，使用者端所做之操作均會連接至交易所端，私鑰係由交易所保管，使用者不擁有私鑰。非託管錢包則不透過交易所，私鑰由使用者自行保管，例如常見之 Metamask（一般暱稱為小狐狸錢包）。二者在偵查實務上之差別為託管錢包既係由交易所提供，由使用者在該交易所開設帳戶，則交易所依我國洗錢防制法第 5 條第 2 項、虛擬通貨

[79] 據筆者瞭解，美國聯邦調查局（FBI）曾於 2022 年 12 月間發出警示，指出發現有被告係以特殊墨水書寫助記詞，如僅以肉眼看是看不出任何書寫痕跡，需以紫外線光（UV）筆照射才能顯現，此節亦提供偵查機關參考。

[80] 依我國刑事訴訟法第 128 條第 2 項第 3 款之規定，身體得為受搜索之對象，復依同法第 132 條：「抗拒搜索者，得用強制力搜索之。但不得逾必要之程度。」或可為聲請搜索時，將命受搜索人按壓指紋作為註記，並附加說明之依據。另如犯罪嫌疑人或被告係經拘提、逮捕到案者，司法警察亦得依該條規定，採取犯罪嫌疑人或被告之指紋。以上可供偵查機關思考於聲請搜索票時，是否將生物辨識（指紋或手機照相鏡頭自拍）解鎖裝置，一併登載於搜索票聲請書上。

平台及交易業務事業防制洗錢及打擊資恐辦法之相關規定，即負有確認客戶身分[81]（第 3 條、第 4 條）、持續審查（第 5 條以下）、保存交易記錄（第 10 條）、大額申報（第 11 條）、交易持續監控（第 12 條）等義務。

目前國內交易所確認客戶身分之方式，除了綁定電話門號及匯款銀行帳號外，在申請交易所帳號時，多會要求使用者上傳身分證正反面，並持證件自拍，並註明係欲開設帳戶使用，經交易所審核後始會開通帳戶。故交易所留存之客戶相關資訊亦可供偵辦機關調取查詢。而非託管錢包因為不是向交易所申請帳號，而係用戶自行下載使用之錢包程式，故沒有經過上開所述之 KYC/AML 等程序，偵辦機關自難以調取相關資訊。

另需強調者為，錢包本身並不存放虛擬貨幣，蓋虛擬貨幣之交易記錄、錢包地址餘額均存在於區塊鏈之帳本上之記錄，而錢包儲存者為「私鑰」，私鑰才是表彰擁有錢包地址上之虛擬貨幣，也才有動用之權限。

4. **公開帳本**

不同區塊鏈有不同帳本：基於區塊鏈公開帳本之特性，虛擬貨幣之交易記錄會公開在帳本上，而不同的區塊鏈有不同之帳本，例如比特幣之交易記錄只能在比特幣區塊鏈上查詢得到，如果至狗狗幣區塊鏈上欲查詢比特幣之交易記錄，則屬緣木求魚。舉例而言，如同臺鐵火車與高鐵各有其時刻表，在臺鐵官網上可查詢臺鐵時刻表，但如果欲查詢高鐵時刻表，則應至高鐵網站查詢。應特別說明者，以太坊區塊鏈上除了以太幣以外，尚有諸多以部署智能合約方式而發行之虛擬貨幣，例如：泰達幣、BNB、USDC 等（ERC-20 標準協議），另也有以 ERC-721、ERC-1155 標準協議[82]而發行之 NFT，均可在以太坊區塊鏈上查詢。

---

[81] 一般稱之為 Know your customer, 簡稱為 KYC。

[82] ERC-20 等標準協議係指在以太坊區塊鏈上提供給代幣（Token）開發者遵循之標準協議，確保依該等標準協議發行之代幣可以相容於以太坊區塊鏈。可參見：https://ethereum.org/en/developers/docs/standards/tokens/

常見之區塊鏈瀏覽器（Blockchain explorer）：基於區塊鏈公開透明之特性，虛擬貨幣交易之錢包地址、幣種、數量、交易序號、日期時間等均會記錄在公開帳本上，在追查虛擬貨幣幣流過程中，會使用區塊鏈瀏覽器查詢，其多係以網站方式呈現，點進入網址後，輸入欲查詢之交易序號[83]、錢包地址等檢索條件即可查詢，常見者如比特幣區塊鏈瀏覽器[84]、以太坊區塊鏈瀏覽器[85]、波場區塊鏈瀏覽器[86]等，另也有結合多區塊鏈查詢之瀏覽器、可呈現幣流視覺化之網站工具等。

交易所之內帳：需特別說明者，雖然虛擬貨幣交易記錄均會呈現在區塊鏈之公開帳本上，然如果是透過交易所購買或在交易所內部交易，因此時交易係發生在交易所內，如交易所將每一筆交易均上鏈，而上鏈會產生礦工費（Gas fee），故多數交易所均會將在其交易所內部交易之記錄以內部記帳程式記錄，而不會將交易記錄上鏈，以節省礦工費，惟如用戶欲將交易所內之虛擬貨幣移轉至外部錢包時，交易所方會將該筆記錄上鏈。

5. 比特幣 ATM

比特幣 ATM 係外觀上與 ATM 相似之機器，其功能為交易虛擬貨幣，通常係由使用者將欲購買之比特幣等虛擬貨幣換算之新臺幣紙鈔放入機器，機器將虛擬貨幣發送至使用者出示之錢包地址（通常係以 QR Code 形式掃描讀取），有少部分機型亦提供使用者販賣虛擬貨幣予機器，而由機器吐鈔，且透過該等機台購買比特幣之手續費均比透過交易所更高，一般約高達 12%至 20%。由於比特幣 ATM 各機型是否有提供 KYC 功能不一而足，有些會提供手機簡訊驗證功能，部分甚至有鏡頭拍攝功能，而可供辨

[83] 交易序號（Transaction hash or Transaction ID, TXID）係指足資特定該筆交易之序號，其係將該筆交易經過雜湊（Hash）運算而來，可用在節點或區塊鏈瀏覽器上查詢該筆交易。
[84] See https://www.blockchain.com/explorer
[85] See https://etherscan.io/
[86] See https://tronscan.org/#/

識、留存用戶資訊，惟並非所有機台經營者均會開啟上開功能，甚至會刻意關閉簡訊驗證或拍照功能，故常為犯罪者使用作為詐欺、販毒之用[87]。

6. **泰達幣**

泰達幣係由泰達（Tether）公司所發行，其發行方式係過智能合約部署在區塊鏈上而發行，故與比特幣區塊鏈之完全去中心化不同，因該公司宣稱提撥儲備金[88]，故泰達幣之價格可錨定（Peg）美金，亦即 1 枚泰達幣之價格相當於 1 美金，其價格相對於其他種虛擬貨幣的價格波動較小，故在我國實務案件中，亦常見詐欺集團對被害人施以感情詐欺或投資詐欺之詐術後，指示被害人向詐欺集團介紹之「幣商」購買泰達幣，由被害人轉帳、匯款至「幣商」（或其人頭）之銀行帳號，並由被害人將詐欺集團指定之錢包地址傳送予「幣商」，由「幣商」將泰達幣移轉至上開錢包地址。而被害人因為對於虛擬貨幣不熟悉，誤信自己擁有該錢包，實則該錢包地址係由詐欺集團掌控。而當警方追查到「幣商」時，「幣商」多會提出泰達幣交易記錄截圖，證明確實有移轉泰達幣，並抗辯自己只是單純賣幣，故實務上對於「幣商」多為不起訴處分[89]。

泰達公司透過部屬（Deploy）智能合約之方式在諸多區塊鏈上均有發行泰達幣[90]，故在透過區塊鏈瀏覽器查詢時，務必先行確認該泰達幣係在何區塊鏈上發行，始能正確查詢。另近來在波場鏈（Tron）上發行之泰達

---

[87] See FinCEN Advisory, FIN-2019-A003, at 7 (May 9, 2019) ,https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

[88] 關於泰達公司提撥之儲備金是否足額、狀況如何，一直備受爭議，之前曾遭紐約州檢察長辦公室調查，該案嗣於 2021 年 2 月 18 日達成和解，由泰達公司繳交 1,850 萬元美金和解。可參見：https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf

[89] 實務上多因無法證明「幣商」與詐欺集團有所關連，而為不起訴處分。而此種案件因被害人散在各地，且「幣商」多被當成一般人頭帳戶案件處理，而致無法看見案件全貌。關於部分不法幣商與詐欺集團合作之洗錢手法，可參見臺灣屏東地方法院 111 年度金訴字第 32 號判決引用之臺灣屏東地方檢察署檢察官 109 年度偵字第 11904 號等起訴書。

[90] 諸如：Bitcoin (Omni & Liquid protocol), Ethereum, TRON, EOS, Algorand, Solana, and Bitcoin Cash (SLP).，可參見泰達公司官網：https://tether.to/en/transparency/ (Last visited Mar. 19, 2023)

幣也有越來越受犯罪集團青睞的趨勢，原因可能在於波場鏈上之交易手續費（Gas fee）大幅低於以太坊之故[91]。又泰達幣有一特別之處，即泰達公司在以太坊及波場鏈上部署的 USDT 智能合約內設有黑名單（Blacklist）功能，當使用者發生大額泰達幣轉帳地址錯誤，或是地址涉及洗錢、駭客盜取等犯罪時，泰達公司可以將涉及上開情況的錢包地址納入黑名單，使列入黑名單內地址內之泰達幣無法動用，而達成凍結之效果，目前泰達公司已有協助美國執法機關凍結之案例[92]。

（二） 洗錢手法

1. 洗錢軌跡

回到本案，經美國執法機關之調查結果，被告夫妻的虛擬貨幣洗錢手法包含：使用虛構之身分設立帳戶、使用電腦程式自動執行交易、透過不同交易所及暗網多層化交易、Peel chain、轉換虛擬貨幣種類（Chain-hopping、Cross chain）、使用銀行商業帳戶、使用比特幣 ATM、購買 NFT 等諸多方式[93]，以下僅就 Peel chain、轉換虛擬貨幣種類，包括強化匿名性之虛擬貨幣（Anonymity Enhanced Cryptocurrencies, AECs）、混幣器（Mixer or tumbler）、比特幣 ATM 等洗錢手法說明（被告二人部分洗錢軌跡如圖 8[94]）。

---

[91] 於美東時間 2023 年 4 月 6 日上午 0 時 7 分許，以太坊上之泰達幣（ERC-20）交易手續費折合美金約為 1.899 元，而波場鏈上之泰達幣交易手續費折合美金約為 0.315 元，惟交易手續費會是交易情形而呈現浮動狀態，可參：https://gasfeesnow.com/ (Last viewed APR. 6, 2023)

[92] See https://tether.to/en/tether-law-enforcement-and-financial-freedom/ (Last viewed APR. 6, 2023)

[93] Complaint, United States v. Ilya Lichtenstein, and Heather Rhiannon Morgan, No. 1:22-mj-00022-RMM (Feb. 7, 2022), at 3, 10, https://www.justice.gov/opa/press-release/file/1470211/download

[94] Id at 9. 另本案主筆逮捕令宣示書（affidavit）的 IRS 特別探員 Christopher Janczewski，事後轉至民間區塊鏈分析公司任職，並於 2025 年來台，筆者有幸與之見面，並當面請教本案的細節。

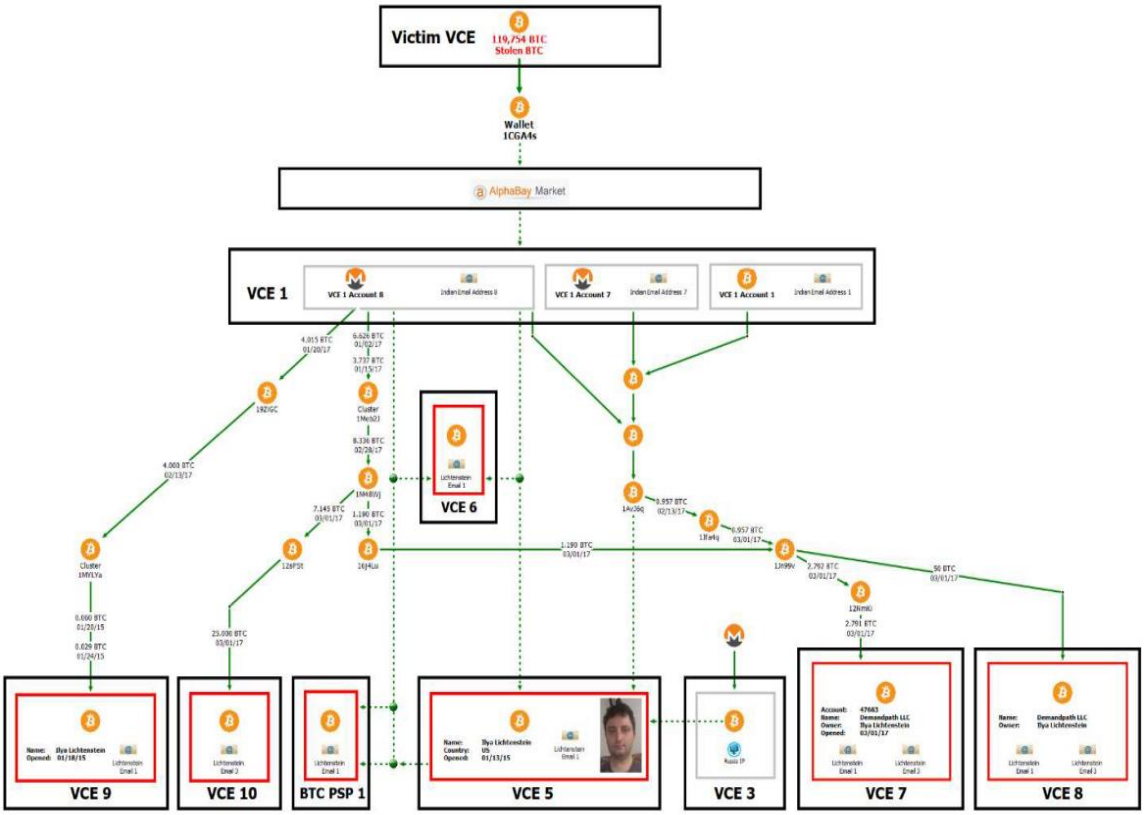


圖 8

2. Peel chain

Peel chain 是一種隱匿虛擬貨幣之方法，其係將原本置於一個地址內之大額虛擬貨幣，透過一系列的交易，每次都將小額之虛擬貨幣發送至新的地址，如下圖 9 所示[95]。此圖係用以描述行為人將地址原存有 100 枚之比特幣，透過一系列約 20 次之分化陸續將 100 枚比特幣以不等小額之方次存入交易所，每存入一次即將餘額轉入新的地址，反覆進行，而達成難以追蹤之目的。實務上，精心策劃的電腦犯罪者時常以超過百次的交易來混淆幣流追查[96]。

[95] 2020 Cryptocurrency Enforcement Framework, supra note 69, at 28.

[96] Verified Complaint, United States v. 113 Virtual Currency Accounts, Civ. No. 20-606, at 4 (Mar. 2, 2020), https://www.justice.gov/opa/press-release/file/1253491/download

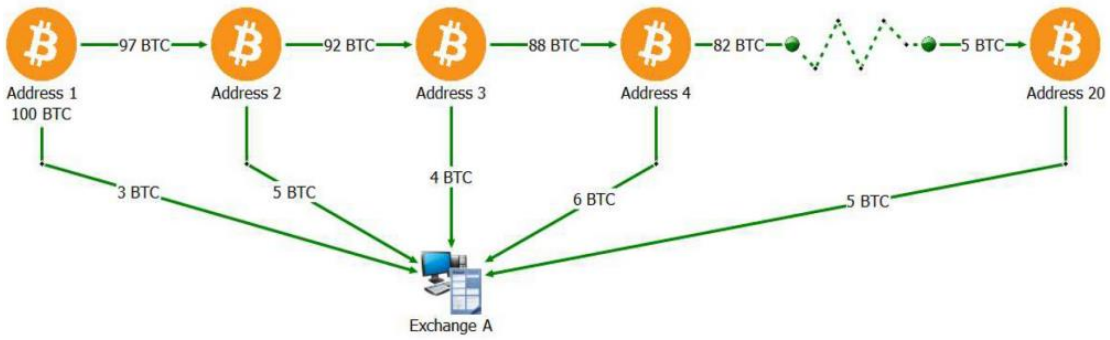


圖 9

3. 轉換虛擬貨幣種類

犯罪者使用「跳鏈」，意即將一種虛擬貨幣換成另一種，通常會連續快速轉換（運作模式例如圖 10）[97]。依據美國司法部的觀察，「跳鏈」通常頻繁地發生於嫌疑人欲對於竊得之虛擬貨幣進行洗錢。「跳鏈」通常被視為是以將一種區塊鏈上之虛擬貨幣，透過交易轉換成另一個區塊鏈上之虛擬貨幣，用以逃避、混淆虛擬貨幣之流向[98]。

除了透過中心化交易所進行「跳鏈」以外，犯罪者為求留下更少犯罪足跡，更透過沒有 KYC 程序之去中心化交易所（Decentralized exchange services, DEXs）、跨鏈橋（Cross-chain bridges）、代幣交換服務（Coin swap services）等，進行虛擬貨幣之轉換，除了犯罪者外，亦有為數甚多的合法虛擬貨幣交換者、玩家、投資人使用上開服務平台，自 2020 年起，上開服務金額大量成長，約有價值高達 6150 億美元之比特幣及以太幣透過上開服務平台交易[99]。上開服務平台欠缺 KYC/AML 程序，對於幣流追查而言，造成十分大的阻力。

---

[97] U.S. Department of Justice, The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Oder 14067: How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets (2022) [hereinafter International Law Enforcement Cooperation Report], at 5, 42, https://www.justice.gov/ag/page/file/1510931/download

[98] 2020 Cryptocurrency Enforcement Framework, supra note 69, at 44.

[99] ELIPTIC CROSS-CHAIN REPORT, The State of Cross-Chain Crime (2022), at 4.

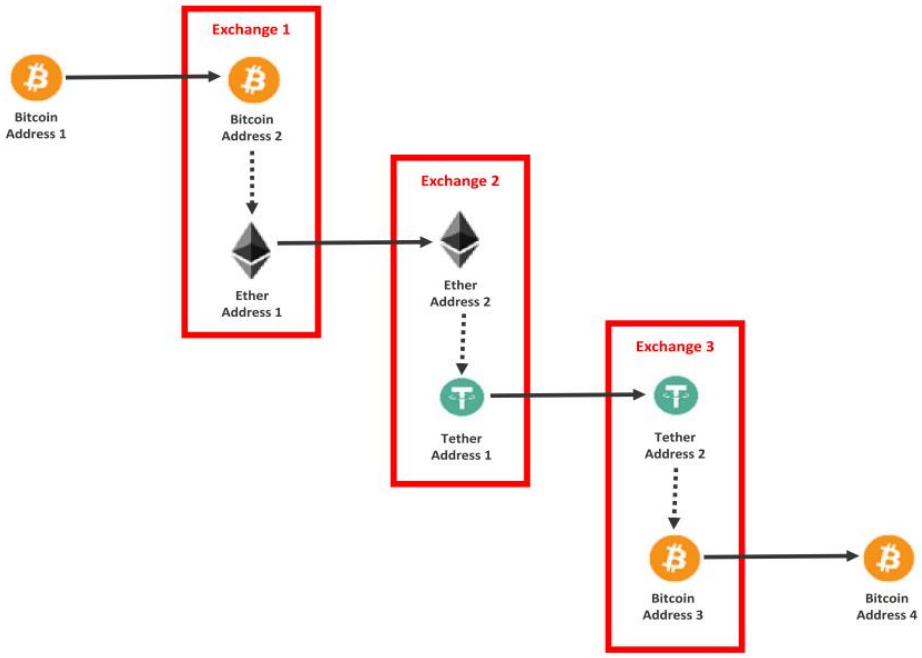


圖 10

4. **強化匿名性之虛擬貨幣（又稱隱私幣）：**

有些虛擬貨幣交易就是設計來保持匿名性，例如「強化匿名性之虛擬貨幣」就是用以隱藏錢包與錢包之間的連結，使區塊鏈分析無法輕易地對於複雜的交易找出關連性。使用此類虛擬貨幣，加上透過未遵守 AML/CFT (Countering The Financing Of Terrorism)之虛擬貨幣服務業者，大大地協助犯罪者隱藏資金來源、流向，及逃避偵查。於本案中，被告二人洗錢過程中，即將比特幣換成此種隱私幣 Monero (XMR)後，再層層轉換。

5. **混幣器：**

其係提供軟體服務，可將原本可被追蹤之虛擬貨幣與他人之虛擬貨幣混合，並頻繁地加入其他客戶之虛擬貨幣，最終再移轉至客戶指定之其他地址。美國司法部於 2021 年間曾破獲專為暗網 Helix 服務之混幣商，該名被告以混幣之方式洗錢金額高達 300 萬美元[100]。另美國財政部外國資產控

[100] Press Release, Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million, U.S. Dep't of Justice (Aug. 18, 2021),

制辦公室對於混幣商的處理方式為施加制裁（混幣器運作模式如圖 11）[101]，封鎖相關之錢包地址[102]，透過此方式讓虛擬貨幣交易業者及個人避免與相關遭制裁之錢包地址交易。

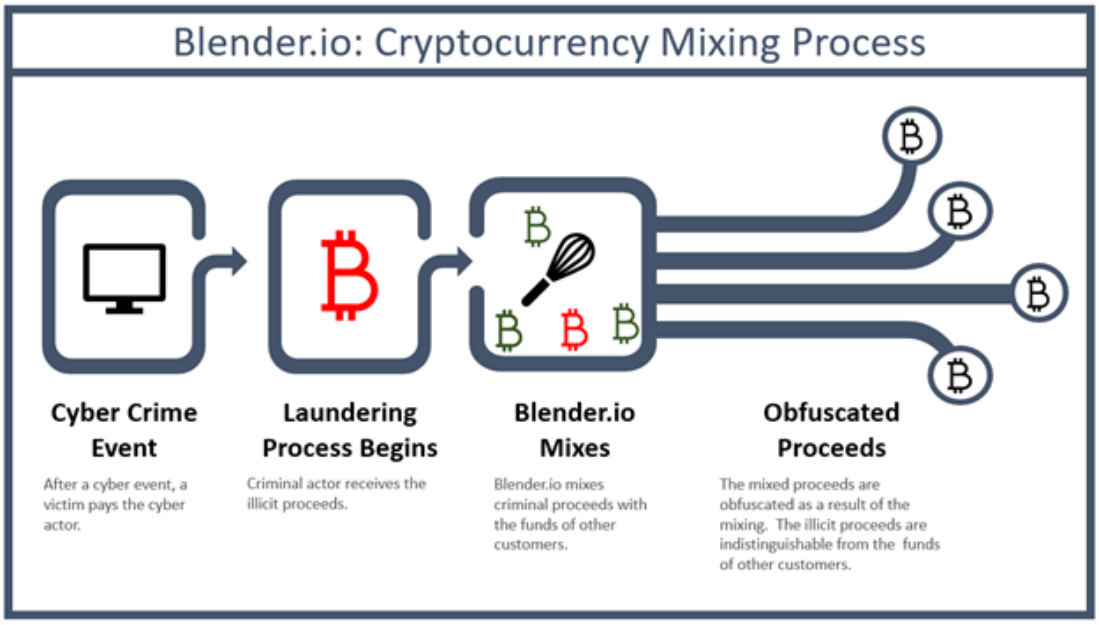


圖 11

6. 比特幣 ATM：

雖然本案起訴書內對於被告夫妻如何使用比特幣 ATM 洗錢較少著墨，然以本案情形而言，因為被告夫妻業已取得比特幣，其目的應係將比特幣變現，故可藉由具有吐鈔功能之比特幣 ATM，將虛擬貨幣錢包內之比特幣轉入該比特幣 ATM 顯示之錢包地址後，由比特幣 ATM 吐鈔（相當於賣比特幣給機台業者），而達成將比特幣轉換成現金之洗錢目的。

又依據美國銀行保密法（Bank Secrecy Act）之規定，涉及金錢服務提供之業者（Money service Business，MSB）必須向金融犯罪執法局註冊，且需符合反洗錢、資恐之相關規定，而比特幣 ATM 之營運涉及虛擬貨幣與現

https://www.justice.gov/opa/pr/ohio-resident-pleads-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million.

[101] Press Release, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (August 8, 2022), https://home.treasury.gov/news/press-releases/jy0916

[102] See https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220506

金之轉換，而被認為屬於 MSB，故須符合上開相關規定[103]。美國 S&P Solutions 公司涉嫌無照營運比特幣 ATM，且放任諸多詐欺被害人透過其經營之比特幣 ATM 將款項轉為比特幣轉至詐欺集團之錢包地址，俄亥俄州凱霍加縣 (Cuyahoga County)檢察官辦公室於 2023 年 3 月間起訴該公司負責人及高階主管，並扣押了 51 台比特幣 ATM，起訴罪名為共謀洗錢、收受贓款、無照營運金錢傳輸服務等[104]。另在我國詐欺集團以感情詐欺或投資詐欺等手法，亦多有指示被害人至比特幣 ATM 操作將現金轉為比特幣而發送至詐欺集團控制之錢包之情形，實值注意[105]。

（三） 美國執法機關追查重點

1. 鏈上追查

透過區塊鏈公開透明之特性，故查詢區塊鏈公開帳本以追查幣流[106]。雖然依照本案起訴書所載，並未提到執法機關有請民間區塊鏈分析公司協助，但通常在涉及金額龐大且幣流複雜之情形下，美國司法部、執法機關多會請數家民間區塊鏈分析公司協助[107]。另據筆者所知，Chainalysis、TRM Lab、CipherTrace、Elliptic 等公司均為國際知名區塊鏈分析公司，且有協助執法機關分析區塊鏈資訊。

---

[103] See FinCEN Guidance FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", May 9, 2019. See also FinCEN Advisory FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency", May 9, 2019, https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

[104] See https://www.secretservice.gov/newsroom/releases/2023/03/three-individuals-and-one-business-indicted-engaging-pattern-corrupt.

[105] 目前臺灣約有 36 處設置比特幣 ATM，可參：https://coinatmradar.com/country/208/bitcoin-atm-taiwan/(Last viewed APR. 5, 2023)。另依據筆者先前在臺北市至少三處操作比特幣 ATM 之經驗，該等機台均無身份驗證或其他反洗錢措施，甚至關閉機台原本內建提供使用者輸入電話門號之簡訊驗證功能。又筆者赴美後在波士頓附近之超市內見到由 COINME 公司設置之比特幣 ATM，而操作購買少量比特幣，在操作之初即要求使用者輸入手機門號，並會以簡訊傳送驗證碼至筆者手機，並要求在筆者手機端下載該公司之錢包程式，上傳相關個人證件資料，始能完成購買程序，其嚴謹之 KYC 之程序可見一斑。

[106] Complaint, United States v. Ilya Lichtenstein, and Heather Rhiannon Morgan, No. 1:22-mj-00022-RMM (Feb. 7, 2022), at 2.

[107] Verified Complaint For Forfeiture In Rem, United States v. 280 Virtual Currency Accounts, Civ. No. 20-2396, at 4 (Aug. 27, 2020), https://www.justice.gov/usao-dc/press-release/file/1310411/download

透過鏈上追查雖然可能追蹤虛擬貨幣之幣流，然至多僅能追蹤到錢包地址，至於在錢包地址背後實際掌控者之身分，則無從單純藉由鏈上追查得知，仍須透過其他偵查方法續予追查。誠如美國司法部副部長 Lisa O. Monaco 於本案記者會上所言：除了依靠高科技的偵查方法及檢察官、各執法機關持續不斷的努力追查，也要感謝非常棒的傳統警察工作（Good old-fasioned police work），才能順利從交易所追回本案虛擬貨幣。可見幣流分析固為虛擬貨幣犯罪偵查不可或缺的一環，但仍須搭配傳統偵查方法，始能克竟其功。

2. 交易所資料調閱

遭竊之比特幣首先從錢包地址 Wallet 1CGA4s 轉入暗網 AlphaBay[108]，接續以複雜之洗錢手法轉入非託管錢包及美國境內、境外為數甚多之交易所。追查過程中向交易所調閱資料，並逐層追查至被告二人以真實身分申辦之交易所帳戶。

人頭帳戶間關連性突破：從某一交易所查知有數帳戶係使用同一由印度某電子郵件服務供應商所提供之電子郵件，且地址風格相近；復經調閱其等之 IP 位址發現係使用相同 IP 位址；又該等電子郵件創建之日期係在 Bitfinex 交易所之比特幣遭盜取後不久；且數帳戶間有相同交易對象，並續行「跳鏈」轉換至隱私幣；對於交易所進一步詢問帳戶持有人關於客戶身分，均未有回應，完全忽視交易所之 KYC 要求，甚至帳戶因此遭交易所以未完成 KYC 為由而凍結（Freeze）時，亦放任虛擬貨幣凍結在帳戶中而未積極向交易所爭取。對於部分交易所之 KYC 要求說明資金來源，被告則以

[108] AlphaBay 為暗網市集，作為一線上平台，賣家在其上販賣非法物品與服務，例如毒品、外洩之金融個資、駭客工具等。一般而言暗網市集允許用戶創設虛擬貨幣帳戶儲值、儲存及提領虛擬貨幣，用以交易該暗網市集之物品。AlphaBay 係最大之暗網市集之一，自 2014 年 12 月間營運至 2017 年 7 月間。

與客觀事實、區塊鏈交易記錄不符之理由搪塞。執法機關依上開由交易所提供之客戶資訊研判各該人頭帳戶應係由同一人所控制[109]。

其餘由交易所提供之資料顯示被告曾將虛擬貨幣轉出至某美國境內之虛擬貨幣支付服務商，以購買金條，執法機關循線查獲該購買金條之收件地址，發覺即為被告李斯坦之地址。

透過交易所提供之資訊，查知該等帳戶有轉出折合美金 500 元之虛擬貨幣購買美國超市 Walmart 之禮物卡，另有轉出至 Uber、Hotels.com、Playstation 等消費，其中 Walmart 之禮物卡係透過 3 次交易儲值至某 iPhone 下載之 Walmart 應用程式，而 3 次交易綁定之使用者、電子郵件申登人均為被告摩根，且物品收件地址則為被告二人之住處。

又雖然被告李斯坦在數家交易所使用假資料申請帳戶，但其使用之 IP 均為 Cloud Provider 所提供，進而追查該租用用戶即為被告李斯坦。

綜上所述，可推論本案各該交易所人頭帳戶應係由被告二人實際掌控（相關幣流可參圖 12[110]）。

[109] Complaint, United States v. Ilya Lichtenstein, and Heather Rhiannon Morgan, No. 1:22-mj-00022-RMM (Feb. 7, 2022), at 6,7.
[110] Id at 17.

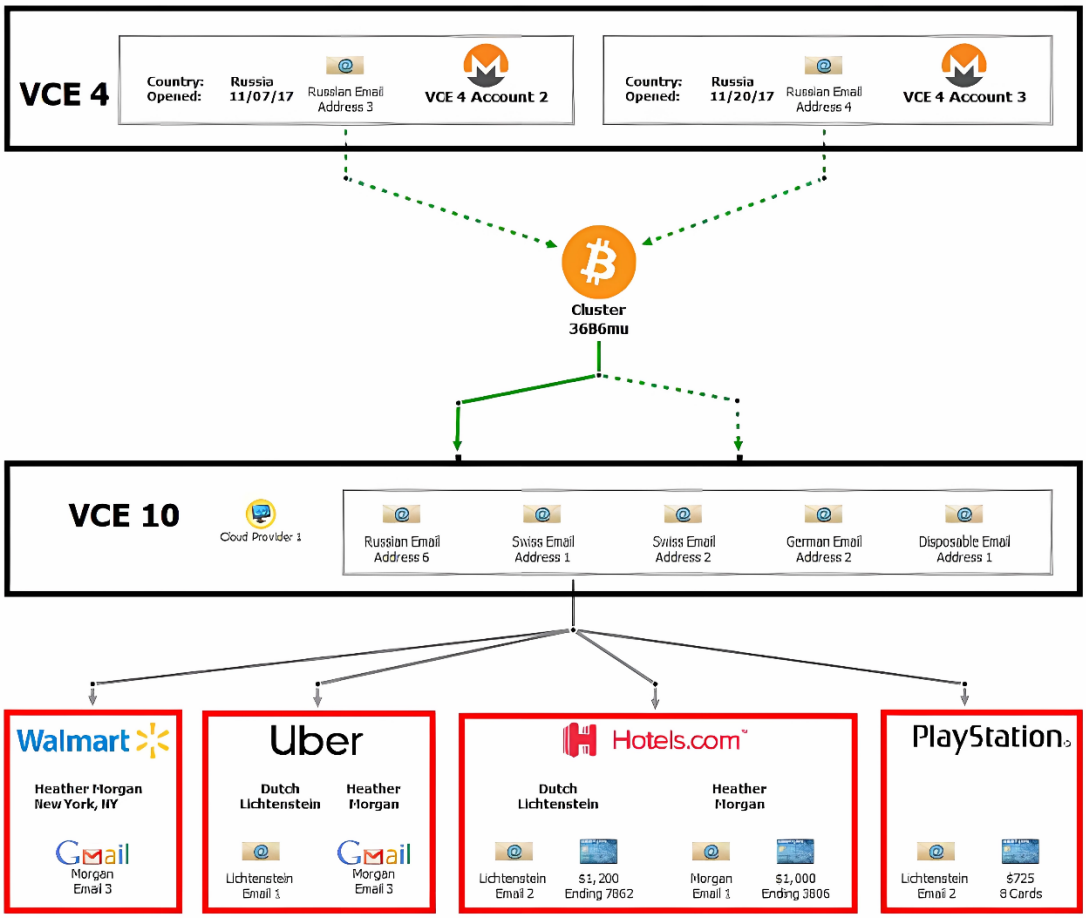


圖 12

3. **雲端硬碟搜索**

執法機關追查得知被告李斯坦使用之某電子郵件服務提供商係美國境內公司，且同時有提供雲端硬碟服務，執法機關依據搜索票向該公司取得該雲端硬碟之內容，雖然經研判該雲端硬碟帳戶係由被告李斯頓所使用，然其中部分檔案係經加密而無法直接閱覽。

約於 2022 年 1 月 31 日，執法機關解密了部分關鍵加密檔案，發現其中記錄了駭客最初轉出之外部錢包 Wallet 1CGA4s 及本案相關之大約 2,000 個錢包地址及對應之私鑰、各該帳戶登入記錄等，甚至有標註哪些帳戶被凍結或已清空。此外，雲端硬碟中存有人頭帳戶之個資、數個販賣假護照、假個資之暗網賣家之網頁連結。

4. **虛擬貨幣及現場查扣物品**

執法機關依據雲端硬碟搜索所得上開相關錢包地址及對應之私鑰，因而扣押了 94,636 枚比特幣[111]。雖司法部並未透露執行扣押之方式為何，然筆者推論應係以取得被告錢包私鑰，進而控制被告錢包，而以移轉其內之虛擬貨幣至執法機關控制之錢包之方式執行扣押。

執法機關尚在被告二人住處扣得為數甚多之手機、SIM 卡、手寫「Burner Phone」（意指便宜的拋棄式手機，多用以躲避追查）之塑膠袋 1 個、多個冷錢包、銀行硬體金鑰，更特別的是，搜到 2 本中間挖空的書籍（如圖 13[112]）

圖 13

[111] 據筆者查詢公開資料及區塊鏈瀏覽器等相關免費資源，發現於 2022 年 2 月 1 日有 26 個比特幣錢包地址移轉共約 94,643.29856151 枚比特幣至錢包地址「bc1qazcm763858nkj2dj986etajv6wquslv8uxwczt」，基於時間及比特幣數量之比對，推測該地址可能係美國執法機關之執行本案比特幣扣押之錢包地址。

[112] Government's Reply in Support of Review of Detention Order, United States v. Ilya Lichtenstein, and Heather Rhiannon Morgan, No. 1:22-mj-00022-RMM (Feb. 10, 2022), at 17-20, https://fingfx.thomsonreuters.com/gfx/legaldocs/xmvjojyexpr/Microsoft%20Word%20-%20Lichtenstein%20Detention%20Rply_20220210_v3.pdf?utm_source=Sailthru&utm_medium=email&utm_campaign=The%20Daily%20Docket%20--%20Feb.%2014%2C%202022&utm_term=DailyDocket-MailingList%20v2

（四） **起訴法條**

共謀洗錢（18 U.S.C. § 1956(h)）及詐欺美國政府罪（18 U.S.C. § 371）。

（五） **案件後續**

依據美國司法部新聞稿指出[113]，被告二人於 2023 年 8 月 13 日在法庭上坦承涉犯洗錢罪嫌。李斯坦使用了多種先進的駭客工具和技術來存取 Bitfinex 的網路。一旦進入他們的系統，Lichtenstein 就以欺詐方式授權了 2,000 多筆交易，其中 119,754 比特幣從 Bitfinex 轉移到李斯坦控制的加密貨幣錢包中。隨後，李斯坦採取措施掩蓋自己的蹤跡，他返回 Bitfinex 網路並刪除可能將他暴露給執法部門的存取憑證和其他日誌檔案。

李斯坦在摩根的協助下，採用了許多複雜的洗錢技術，包括使用虛構身份建立線上帳戶；利用電腦程式實現交易自動化；將被盜資金存入各種暗網市場和加密貨幣交易所的帳戶，然後提取資金，透過打亂資金流向來混淆交易歷史的蹤跡；以「跳鏈」的方式，將比特幣轉換為其他形式的加密貨幣，包括隱私幣；將部分犯罪所得存入加密貨幣混合服務，例如 Bitcoin Fog、Helix 和 ChipMixer；使用美國的企業帳戶使其銀行活動合法化；摩根將部竊取的資金兌換成金幣，並藏匿之。

李斯坦承認共謀洗錢罪，最高可判處 20 年監禁。摩根承認一項共謀洗錢罪名和一項共謀詐欺美國罪名，每項罪名最高可判處五年監禁。該案前經美國聯邦檢察官起訴[114]，現由聯邦地區法院（United States District Court for the District of Columbia, D.D.C.）法官將在考慮美國量刑指南和其他法定因素後做出判決。

---

113 https://www.justice.gov/opa/pr/bitfinex-hacker-and-wife-plead-guilty-money-laundering-conspiracy-involving-billions (Last viewed: Nov,17,2023)

114 C. Alden Pelker 檢察官是負責本案的聯邦檢察官之一，其具有科技、區塊鏈分析調查之專長，原隸屬於 NCET，現 NCET 業納入刑事司電腦犯罪和智慧財產權科，成為常設部門。筆者在美期間，透過聯邦檢察官的引介，得以與 C. Alden Pelker 檢察官進行視訊會議，並向其請教關於美國司法部對於虛擬貨幣追查、扣押、拍賣、交易所調資、商用分析工具之使用、區塊鏈分析報告法庭之採用度等節，C. Alden Pelker 檢察官並與筆者分享其對於偵辦虛擬貨幣案件的熱情，實令筆者獲益良多。

四、 偵辦虛擬貨幣犯罪之戰略思考

依上開案件所示，可見虛擬貨幣相關犯罪具有涉及價值甚鉅、新興科技之使用、複雜之洗錢手法、移轉迅速、跨境犯罪、追蹤所需時間甚長、現有法規仍在發展中等特色，在在對於檢察官偵辦案件造成挑戰，筆者拋磚引玉，提出如下偵辦是類案件之戰略思考。

（一） 法制及監管面

1. 反洗錢相關規定

Travel rule 之落實：依洗錢防制法第 5 條第 4 項之規定，我國行政院 110 年 4 月 7 日發布院臺法字第 1100167722 號命令，該命令依 FATF 的指導方針劃定虛擬通貨平台及交易業務範圍，明確規範 VASP（虛擬資產服務提供商）需遵守的洗錢防制義務，該命令於同年 7 月 1 日起生效，VASP 須落實 KYC（了解你的客戶）及 AML（反洗錢），以及交易監控、可疑交易通報等措施。金融監督管理委員會（下稱金管會）復於同年 6 月 30 日公布〈虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法〉，並於同年 7 月 1 日施行（第 7 條除外）。再於同年 7 月 27 日以金管銀法字第 11001396511 號令發布〈虛擬通貨平台及交易業務事業疑似洗錢、資恐或武擴交易監控態樣例示〉，因此金融機構以及虛擬通貨平台均有法令遵循之義務，如能落實以及完善，對於調取資料加以比對部分大有助益。然虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法第 7 條規範業者應取得轉出人及接收人之正確必要資訊（第 1 項）、應採取適當措施以辨識缺少必要資訊之虛擬通貨移轉、具備以風險為基礎之政策及程序以判斷何時執行、拒絕或暫停缺少必要資訊之虛擬通貨移轉，及適當之後續追蹤行動（第 2 項）、應確認交易對手之事業受監理規範與防制洗錢金融行動工作組織（FATF）所定防制洗錢及打擊資恐標準一致（第 3 項），本條固然立意良善，如落實執行則可大大減少犯罪行為人透過虛擬貨幣為洗錢等犯罪行

為，然本條迄今尚未定施行日期，諒係因平台業者恐有實際執行之困難，舉例言之，虛擬貨幣之移轉僅需對方之錢包地址即可轉出，業者要如何辨識出對方之錢包係託管或非託管錢包？果若係交易所之託管錢包，又要如何得知對方所受之監理規範是否與 FATF 所定標準一致？又如係擔任接收方時，當轉入方移轉虛擬貨幣時，係由持有私鑰之轉入方操作，經過區塊鏈之驗證程序即會記錄在區塊鏈帳本上，接收方又有何能力可以阻止或拒絕？以上良善之立法意旨與實際執行之困難，宜由主管機關儘速與 VASP 相關協會等組織商討可供實際執行之因應方法。

金管會為虛擬資產平台業者之主管機關：金管會於 2023 年 3 月 30 日公布奉行政院指定擔任具金融投資或支付性質之虛擬資產平台的主管機關，該會將參考國際監理趨勢，以循序漸進方式強化國內虛擬資產平台對客戶之權益保護。並提及近期由於境外虛擬資產交易所破產等事件，各國及相關國際組織已著手研議或採行對虛擬資產業者之監理規範，監理重點包括：客戶資產保管、交易公正透明、市場誠信、利益衝突管理及資訊揭露等。各國監理法制規範仍在持續發展中。其將透過訂定指導原則、推動 VASP 相關協會等組織訂定自律規範、與其他部會共同協力等方式，循序漸進強化國內虛擬資產平台對客戶之權益保護[115]。後續金管會業於 2023 年 9 月發布「管理虛擬資產平台及交易業務事業（VASP）指導原則[116]」。

P2P 幣商問題：依據 FATF 對於 P2P 之定義為：虛擬資產之移轉係透過二個非託管錢包之使用者自行為之，而不透過虛擬資產服務提供者作為中介，依據 FATF 之標準，並非必然適用 AML/CFT 等規範，此係因負有相關義

[115] 請參見金管會新聞稿：https://www.fsc.gov.tw/ch/home.jsp?id=2&parentpath=0&mcustomize=news_view.jsp&dataserno=202303300001&dtable=News。

[116] https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202309260005&dtable=News (Last viewed: Nov, 17, 2023)

務者係中介者，而非個人之間[117]。又 FATF 雖有意識到如將 P2P 排除在 FATF 相關建議之外，將造成潛在之風險，例如有人專門以非託管錢包進行交易，然 FATF 仍認為尚無立即納入其建議之必要[118]。又觀諸我國虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法第 2 條第 2 項明定：「前項第一款所稱本事業，係以在國內設立登記者為限」則個人幣商因未有登記，似不在上開辦法之規範範圍內[119]。然依筆者實際偵辦虛擬貨幣相關案件之經驗，近來個人幣商涉及詐欺或幫助詐欺案件與日遽增，姑不論是否能進一步以幣流分析、搜索、扣押，或透過熟悉虛擬貨幣之運作而以訊問技巧等方式找出其等間之關連，如能將其納入行政管制範圍內，應可有效降地相關爭議（惟如納入行政管制範圍內，主管機關是否能有足夠人力、資源實質執行相關規定，又係另一需面對之問題）。

2. **建構凍結錢包之法律依據**

關於詐欺案件之偵辦，找出詐欺集團背後之行為人固然重要，惟儘速阻止金流遭被告或犯罪行為人提領，以減少被害人之損失之重要性，亦有過之而無不及。關於金融帳戶之凍結部分，依銀行法第 45 條之 2 第 3 項授權，由金管會訂定「存款帳戶及其疑似不法或顯屬異常交易管理辦法」，銀行依上開辦法如接獲法院、檢察署或司法警察機關通報為警示帳戶者，應暫停該帳戶全部交易功能，匯入款項逕以退匯方式退回匯款行（俗稱凍結帳戶），以求時效。然關於虛擬貨幣交易所帳戶並未有準用或適用之規定，

---

[117] FATF, UPDATED GUIDANCE FOR A RISK-BASED APPROACH, VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, at 18 (Oct. 2021), file:///C:/Users/user/Desktop/Updated-Guidance-VA-VASP%20(2).pdf

[118] FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, at 21 (JUN. 2022), file:///C:/Users/user/Desktop/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf

[119] 金管會雖以新聞稿表示：「從事虛擬通貨活動為業之自然人，自應依商業登記法及稅籍登記規則相關規定辦理商業登記及稅籍登記，並遵循洗錢防制法及本辦法相關規定。尚未完成洗錢防制法令遵循聲明而以虛擬通貨活動為業者，自屬違法。」然其法律依據為何？似值進一步探究。請參見：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202306240001&dtable=News (Last viewed: Nov, 17, 2023)

如遇詐欺被害人報警欲透過警方先行通知虛擬貨幣交易所以凍結詐欺帳戶者，此時因為尚無搜索票或扣押裁定等依據，虛擬貨幣交易所並無法律依據可凍結客戶之帳戶（當然，或可由虛擬貨幣交易所與用戶訂定契約條款之方式作為依據，然實際執行上可能也會產生疑義），其不論凍結或不凍結，均易生爭議。筆者以為，或可參照存款帳戶及其疑似不法或顯屬異常交易管理辦法之規定，訂定虛擬貨幣交易所凍結客戶帳戶之法律依據，供其遵循，以免爭議[120]。

3. 加強監管及跨部會合作：

目前我國虛擬貨幣平台業者所受之規範似僅有洗錢防制法相關規定，然虛擬貨幣所涉及之面向廣泛，不限於反洗錢，包含其業務監管、消費者/投資人保護、是否適用銀行法、證券交易法等諸多面向，目前在國際上之討論方興未艾，以美國為例，該國總統拜登於 2022 年 3 月 9 日簽署一份確保負責任地發展數位資產之行政命令（Executive Order on Ensuring Responsible Development of Digital Assets[121]）。本行政命令要求美國政府機關必須跨部會共同協商並研究數位資產對於金融市場以及交易安全之影響，重點略為：保護美國消費者、投資者和企業，包括資料隱私與安全、保障美國及全球之金融穩定與降低系統性風險、降低非法金融及相關犯罪，尤其是防止數位資產作為洗錢與逃避制裁之工具、降低國家安全風險、穩固美國在數位資產技術及全球金融之競爭力和領導地位、促進普惠

[120] 目前依洗錢防制法第 13 條第 1 項：「檢察官於偵查中，有事實足認被告利用帳戶、匯款、通貨或其他支付工具犯第十四條及第十五條之罪者，得聲請該管法院指定六個月以內之期間，對該筆交易之財產為禁止提款、轉帳、付款、交付、轉讓或其他必要處分之命令。其情況急迫，有相當理由足認非立即為上開命令，不能保全得沒收之財產或證據者，檢察官得逕命執行之。但應於執行後三日內，聲請法院補發命令。法院如不於三日內補發或檢察官未於執行後三日內聲請法院補發命令者，應即停止執行。」惟適用此條之前提為涉犯洗錢、特殊洗錢罪，並不及於其他犯罪類型（例如：詐欺），打擊面較為有限，且程序上需經由檢察官聲請由法院核發命令，或是檢察官逕行執行後聲請法院補發命令，在效率上亦不若對金融帳戶通報警示帳戶那樣快速。

[121] See https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/

金融、支持數位資產的技術進步並確保發展負責任的數位資產金融體系、鼓勵發展中央銀行數位貨幣（CBDC）等，並要求司法部、財政部、美國聯邦儲備系統委員會主席、科學技術政策辦公室主席等人須於一定期間內提出報告；足認美國係以全方面思考虛擬貨幣對於彼國之影響，此節足供我國參考。

（二） 偵辦能量之建構

1. 人才專業訓練

檢察官科技專業訓練：科技日新月異，犯罪集團使用最新的科技、網路、資訊、通訊技術犯罪，偵查機關亦須與時俱進，使用科技偵查技術偵辦犯罪。基於區塊鏈技術而產生的虛擬貨幣相關犯罪日增，宜多舉辦相關課程訓練，諸如：查詢公開帳本、使用分析軟體追查幣流，並特定錢包地址等技術[122]。惟錢包地址背後之犯罪者為何人，則有待在層層追查中，向國內、外虛擬貨幣交易所調取資料，始有機會突破。除了區塊鏈技術以外，網路基礎知識、通訊技術、社群媒體相關資訊調取等科技相關知識，亦屬重要，畢竟科技可以作為犯罪工具，而通常犯罪集團都使用得比司法警察或檢察官更早、更純熟，且涉及各種類之犯罪，雖然只能跟在犯罪集團後追趕，但也只能持續追趕、持續進步。又檢察官如在法庭上面對辯方對於幣流分析報告提出質疑時，是否能夠以淺白的方式說明區塊鏈及分析、追蹤原理，讓法院或是國民法官瞭解，以鞏固相關分析報告之證據能力及可信度，亦屬重要。

持續關注國外法制、案例：在美國方面，除了本文介紹之案例以外，近期仍有發生諸多與虛擬貨幣有關之犯罪，且涉及金額龐大，而現今犯罪

[122] 關於幣流追蹤技巧及可使用的免費工具操作，涉及基礎知識之建構及較為複雜之追蹤技術，本文礙於篇幅等因素，在此略過。

無國界，宜持續關注國外法制、案例，吸收他國案例之經驗，供作借鏡及未來因應各式犯罪之準備。

建構專業團隊：美國司法部為因應虛擬貨幣犯罪日增，且影響層面廣大，特於 2021 年 10 月宣佈成立國家級的虛擬貨幣執法團隊（National Cryptocurrency Enforcement Team, NCET），成員由司法部電腦及智慧財產小組（CCIPS）之檢察官、反洗錢及資產追討小組（MLARS）和資安專家組成，並 2022 年 2 月 17 日指派檢察官 Eun Young Choi 為該團隊主管。NCET 領導來自全美各地檢察官辦公室相關團隊，以識別、調查、針對虛擬貨幣交易所、基礎設施提供商、以及其他濫用虛擬貨幣和相關產品實施或促進犯罪活動的實體，並對全美各地之檢察官提供虛擬貨幣相關之訓練及協助。又因應全球化之虛擬貨幣犯罪趨勢，建立全球合作、夥伴關係亦為 NCET 之任務之一[123]。美國司法部於 2023 年 7 月 20 日宣布，NCET 將合併到 CCIPS，創建一個單一辦公室，整合刑事部門在打擊網路犯罪各個方面的專業知識。在 CCIPS 內，NCET 將繼續履行其使命。NCET 將調查並在適當情況下起訴涉及濫用加密貨幣的刑事犯罪。這包括與刑事司洗錢和資產追回科（MLARS）合作，調查和起訴促進洗錢的加密貨幣交易所。NCET 繼續與 MLARS 在這些領域合作，利用 MLARS 在洗錢、銀行保密法、金融機構案件以及數位資產扣押和沒收方面的專業知識。NCET 也繼續履行其其他核心職責：建立和加強與專注於加密貨幣的聯邦檢察官辦公室和其他部門之訴訟檢察官的關係；透過培訓讓這些檢察官及執法機關熟悉這些複雜案件的調查和起訴策略的最佳做法，發揮其在能力建構方面的關鍵作用[124]。

[123] International Law Enforcement Cooperation Report , Supra note 97, at 39.
[124] https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-center (Last viewed: Nov, 17, 2023)

此外，日本檢察界為因應新興科技、網路犯罪及跨境犯罪之偵辦，日本最高檢察廳於 2021 年 4 月間設立「新興犯罪檢察官小組[125]」（先端犯罪検察ユニット、Japan Prosecutors unit on Emerging crimes、JPEC)，其主要任務為與私部門及學術部門合作蒐集、分析情資，提供檢察官法律與實務建議、訓練與協助，以及國際合作（同時為電腦犯罪檢察官之非正式合作管道），其成員係從各級檢察廳具備科技、電腦專長，且需具備海外留學相關經驗之檢察官中挑選，目前成員共約 80 人。JPEC 於 2021 年 12 月與美國聯邦調查局（FBI）合作偵辦「索尼生命保險公司」員工透過虛假交易，將正在辦理清算手續的海外子公司向美國銀行帳戶非法匯款約 170 億日元換成「比特幣」之案件，透過雙方合作，由東京地檢署取得該比特幣的相關密碼，以違反「有組織犯罪處罰法」等罪名起訴該員工[126]。他山之石，可以攻錯，我國在面對新興科技犯罪的挑戰時，可參酌上開國外之經驗，厚植檢察官科技辦案能力，並培養國際合作之經驗，以建立專業檢察官團隊。

2. 公私協力

交易所資料調取：從本文介紹之案例來看，虛擬貨幣案件追查之目標在於建立錢包與人之關連性，而區塊鏈分析至多僅能看出錢包之關連性及幣流，如欲找出錢包背後之人，則勢必要透過交易所資料調閱，目前國內數家交易所業與司法警察單位業建立電子化資料傳輸，檢察機關亦著手建立線上調閱 KYC 資料之管道，俾利檢察官快速取得虛擬貨幣帳號或地址之申設人資訊。而國外交易所部分，因境外交易所數量達數百家，各家交易所之聯絡方式、調閱程序、所需檢附之法律文件、是否需經司法互助程序等各有不同，故縱使查知案關錢包係屬國外交易所之託管錢包，國內之執

[125] See https://www.kensatsu.go.jp/kenjisouchou/kenjisouchou_english_00001.htm
[126] See https://www.justice.gov/usao-sdca/pr/japanese-language-version-united-states-files-civil-action-return-150-million-embezzled (Last viewed Mar. 19, 2023)

法機關亦會在這個步驟遭遇困境。筆者前與某國外執法機關開視訊會議，請教該國執法機關如何因應此，經該國執法機關回覆：該機關業經蒐集 200 餘家國際上之交易所資訊，包含各交易所之名稱、所在國家、聯絡方式、調取程序等，並提供歐洲刑警組織（Europol）對於國際上交易所之資料調閱相關資訊供參考。建議國內執法機關可相互交流關於國外交易所之資料調閱資訊，甚或與國外執法機關相互交流，應能減少自行摸索之勞費時間。

區塊鏈分析：除了可以公開資源查詢區塊鏈上之資料外，亦有諸多民間公司提供區塊鏈分析服務，且經國內外機關採用，得以精進幣流追查之程度。惟需注意者，若操作該等軟體工具所輸入之錢包地址、交易序號、註記等資訊會傳輸至該等公司後台者，則是否會有偵查中資訊外傳之疑慮，宜多加留意。

3. **區塊鏈偵查資料庫**

美國關於網路詐欺、駭客、違反智慧財產權等案件，於聯邦調查局下設有「電腦犯罪申訴中心」（Internet Crime Complaint Center, IC3），除了提供被害人通報管道之外，亦藉由該平台蒐集、彙整、分析相關資訊，包括虛擬貨幣錢包地址、移轉時間、數量等資訊，提供予各執法機關。曾有美方執法機關偵辦詐欺案件，查得被告在某虛擬貨幣交易所帳戶有大量虛擬貨幣，但其受理之被害人之受害虛擬貨幣金額不高，其即利用 IC3 平台查詢被告案關之錢包地址，查得另有多位被害人，故可整合被害人及加總被害金額，以利向法院聲請扣押加總被害金額之虛擬貨幣。

我國目前似未有全國執法機關及檢察官共同可使用之區塊鏈偵查資料庫，如能建立蒐集全國被害人相關受害之錢包地址、虛擬貨幣數額、交易序號等資訊，較能以宏觀之角度看出犯罪集團之犯案規模。又或者能將警

方之 165 反詐騙資料庫增加登記錢包地址或交易序號、虛擬貨幣種類等資訊，亦可達與美國聯邦調查局 IC3 平台之相同效果。

又錢包地址、交易序號等字串甚長，登打過程中難免發生錯誤，如能於一開始登記時及確實登打並存檔傳送，或者以 QR Code 方式呈現，並設定防錯機制，以讓後續接手案件之執法機關人員、檢察官可以直接以電子檔複製錢包地址等資訊之方式，用作後續區塊鏈分析[127]，亦可減省重複登打或登打錯誤之時間耗費。

4. **國際合作**

國外交易所資料調閱、凍結：除了循正式國際刑事司法互助管道以外，如能與他國執法機關採取警務合作、情資交換等模式交換資訊，或協助調閱他國之交易所資料，甚至協助凍結交易所帳戶，則實屬理想。惟此節目前並無國際共識，此過程宜靠實際個案累積經驗。又國際間關於反洗錢有艾格蒙組織，其由各地的金融情報單位（Financial Intelligence Units，FIU）所組成，可協助各國交換金融情報，衡量目前虛擬貨幣之交易價值及特性，及可能造成之洗錢風險，如能將虛擬貨幣相關情報亦納入該組織，協助各國交換關於虛擬貨幣洗錢情資，則可較為完整防堵國際洗錢，以免造成國際洗錢防制之漏洞[128]。

五、 小結（未來的挑戰）

隨著虛擬貨幣市場的發展，去中心化金融（Decentralized Finance, DeFi）所產生之詐欺、洗錢等議題益發成長，如何特定出實際運行該 DeFi 平台之人亦屬困難重重，甚至是駭客利用 DeFi 平台智能合約漏洞而盜取虛擬貨幣亦時有所聞。面對混幣器、跨鏈對於幣流追查產生之困境，均屬對

[127] 近來 ChatGPT 之熱潮席捲而來，國外亦有區塊鏈分析公司研發以自然語言結合虛擬貨幣分析之軟體，可以口語文字輸入之方式查詢比特幣區塊鏈上之相關資訊，可參考：https://decrypt.co/124928/blocktrace-introduces-ai-chatbot-for-easy-blockchain-transaction-tracking (Last viewed APR. 6, 2023)

[128] 洗錢防制法第 21 條參照。

於檢察官及執法機關不斷的挑戰。又美國關於虛擬貨幣之扣押、保管、沒收、變價等已累積諸多討論及經驗，而我國目前似仍未有統一之虛擬貨幣扣押、保管、沒收、變價之標準作業流程，亦需費心思量。最後，犯罪者應用最新科技犯罪，檢察官是否也要像希臘神話中的薛西弗斯一樣，就算知道推上山的巨石仍會滾落，還是持續推著巨石上山，持續學習以面對挑戰。

陸、 國際合作

一、 網路犯罪之國際公約

（一） 布達佩斯公約

《布達佩斯公約》（Budapest Convention）或《網路犯罪公約》（convention on cybercrime）之正式名稱為《歐洲委員會網路犯罪公約》（Council of Europe Convention on Cybercrime, ETS No. 185），是世界上第一個旨在關注日益增加的網路犯罪的國際條約。該公約於 2001 年開始實施，並於 2004 年 7 月 1 日生效。其有三個主要目標，包括改善調查技術、建立快速有效的國際合作機制、統一各國法律標準。除此之外，參與國還需要立法禁止特定的網路相關犯罪以及一些明確的證據蒐集規則。歐洲委員會在法國史特拉斯堡和 64 個簽署《布達佩斯公約》的國家簽署了該公約[129]。這些國家包括加拿大、日本、菲律賓、南非、美國等，而目前簽署公約的國家已達 68 國（如圖 14），另有 23 個觀察員國家（如圖 15）。這是第一個具有法律約束力的多邊規範網路犯罪的法律文件。惟自公約生效以來，中國、印度等國家均以未參與起草為由拒絕通過公約[130]。俄羅斯反對該公約，認為透過該公約將侵犯俄羅斯主權，通常拒絕配合與網路犯罪有關的執法調查。

[129] https://www.coe.int/en/web/cybercrime/the-budapest-convention (Last viewed: Nov,17,2023)

[130] 未加入該公約亦可能發生無法參與國際上關於網路、通訊工程的競標，例如：哥斯大黎加頒布了規範 5G 行動網路開發的法令，禁止不屬於 68 個國家支持的《布達佩斯公約》(Budapest Convention) 的國家參與投標，該禁令適用於中國、韓國、俄羅斯和巴西等國。顯示拉丁美洲各國政府和美國正努力製定 5G 網路安全標準和合法替代方案，以全面維護關鍵部門和基礎設施的主權。可參見：https://www.voacantonese.com/a/with-no-precedent-in-central-america-costa-rica-excluded-china-from-participating-in-5g-auction/7344872.html (Last viewed: Nov,17,2023)

Parties to the Budapest Convention

圖 14

Observer countries to the Budapest Convention

Signatories and invited to accede

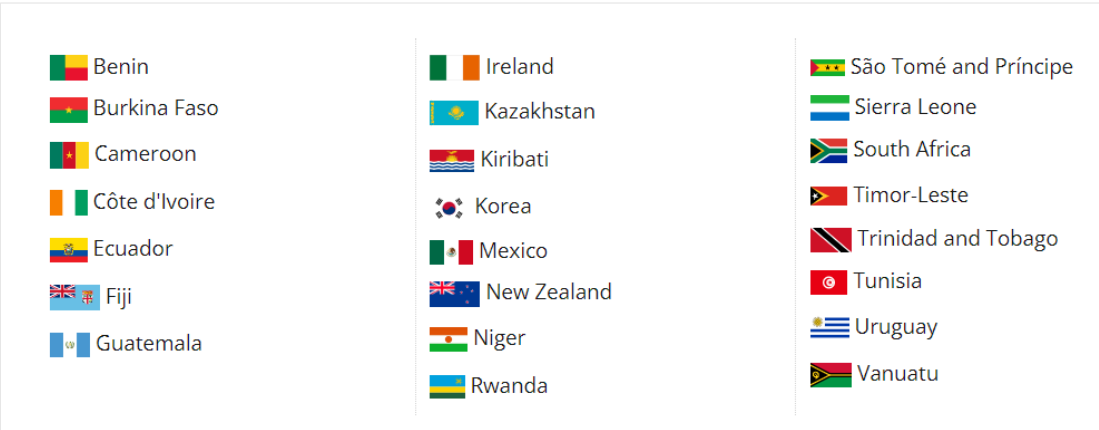


圖 15

布達佩斯公約規範了重大網路犯罪包括非法存取（illegal access）、數據干擾（data interference）、非法截取（illegal interception）、濫用設備（misuse of devices）、系統干擾（system interference）、網路詐欺

（computer-related fraud）、網路偽造（computer-related forgery）、兒童色情犯罪（offenses related to child pornography）以及涉及著作權及鄰接權[131]（copyright and neighboring rights）的犯罪。

（二） 布達佩斯公約第二附加議定書

自 2001 年簽署《布達佩斯公約》以來，資訊與通訊科技的發展帶來了新的機會和挑戰，特別是在刑事訴訟中獲取電子證據。一直以來，《公約》締約方一直在試圖突破與司法和警察機關獲取電子證據有關的障礙。《布達佩斯網路犯罪公約第二附加議定書（Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence, CETS No. 224），下稱「第二附加議定書」》的目的，即是透過確保加強國際合作來面對這些挑戰。該議定書的談判於 2017 年 6 月開始，嗣於 2022 年 5 月 12 日，包括義大利在內的歐洲理事會 22 個成員國在斯特拉斯堡批准了關於加強電子證據合作和披露的「第二附加議定書」[132]。截至目前為止，已有 40 個國家簽署[133]。

該協議應對這一挑戰，並提供加強電子證據合作和披露的工具，例如與服務提供者和註冊商的直接合作、獲取訂戶資訊和流量數據的有效手段、緊急情況下的立即合作或聯合調查。而上開的資料調取也需受到人權和法治體系的約束，包括資料保護保障措施。

第二附加議定書提供與簽約國的法律工具包括[134]：直接請求其他司法管轄區的註冊服務機構獲取域名（Domain）註冊資訊（第 6 條）、與其他司法管轄區的服務提供者直接合作獲取訂戶（Subscriber）資訊（第 7

---

131 關於公約全文可參見歐洲委員會官方網站：https://rm.coe.int/1680081561 (Last viewed: Nov,17,2023)

132 該議定書由網路犯罪公約委員會 (T-CY) 於 2017 年 9 月至 2021 年 5 月，期間舉行了 T-CY 議定書起草全體會議、起草小組和分組會議 90 餘次會議以及六輪利益相關方磋商。該議定書於 2022 年 5 月開放簽署。關於磋商過程及歷次會議內容，請參見：https://www.coe.int/en/web/cybercrime/t-cy-drafting-group (Last viewed: Nov,17,2023)

133 https://www.coe.int/en/web/cybercrime/second-additional-protocol (Last viewed: Nov,17,2023)

134 全文可參：https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (Last viewed: Nov,17,2023)

條）、透過政府間合作更有效的手段取得使用者資訊和流量數據（Traffic Information）（第 8 條）、緊急情況下的迅速合作，強化 24/7 機制之功能（第 9 條及第 10 條）、向位於被請求國之證人或專家進行視訊訊（詢）問（第 11 條）、設立聯合調查團隊（第 12 條）。

（三） 聯合國網路犯罪公約草案

於 2017 年由俄羅斯向聯合國大會提交了一封信，內含《聯合國打擊網路犯罪合作草案》，擬向成員國分發。後於 2019 年 11 月間，由俄羅斯、白俄羅斯、柬埔寨、中國、伊朗、羅馬尼亞、尼加拉瓜、敘利亞和敘利亞共同發起的一項旨在建立打擊網路犯罪的國際決議在聯合國大會上獲得通過。於 2022 年 2 月，聯合國特設委員會[135]（Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, AHC）首輪為期 10 天的會議在紐約舉行，這是談判《打擊將資通訊技術用於犯罪目的公約》（Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes）的開始。會議採納了路線圖[136]和工作模式。重要的是，在 AHC 會議談判期間提出的批准閉會期間，以徵求包括人權和數位權利組織在內的各利益相關方對草稿制定者提出的意見。

上開公約草案經過數輪陸續協商，第六輪協商會議已於 2023 年 9 月落幕，此輪談判後，各國對新公約的主要分歧猶在、進展有限。主要爭議點在於條約範圍與定義，美國與歐盟主張，新約應僅處理核心網路犯罪行為；但中國及俄羅斯認為，新約適用於所有將資通訊技術用於犯罪目的之情況。有人權組織批評，新約缺乏對人權的保障，這恐導致政府監控權力

[135] 關於各次協商會議內容、進程，可參見：https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (Last viewed: Nov,17,2023)
[136] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/CRPs/V2201024.pdf (Last viewed: Nov,17,2023)

擴大，且使羅織入罪和政府跨境存取個資情況增加，且草案並未處理越權或司法監督等重要議題[137]。上開草案討論的閉幕會議，預計於 2024 年 1 月 29 日至 2 月 9 日在紐約舉辦，將涉及對公約草案的討論、最終確定和是否批准，並將該草案將作為附件提交給 2024 年聯合國大會進行討論[138]。

二、 國際合作

一般而言，國際合作有分成正式與非正式的國際合作。正式的國際合作通常指司法互助，須遵循較為嚴格的法律程序。而非正式的國際合作，則包含透過情資交換、聯絡官合作、國際組織平台合作等。

（一） 正式國際合作

我國之「國際刑事司法互助法」於 2008 年 4 月 10 日經立法院三讀通過，此為我國與他國進行刑事司法互助之基礎。其制訂之緣起，乃為處理日益嚴峻之跨境犯罪案件。在訂定此法之前，僅得依國際法上「互惠原則」提出請求，全然繫諸實務運作與他國意願，不但欠缺可預測性，而且缺乏穩定性。難以符合請求態樣複雜之司法互助實務所需。本法適用範圍包含審判以外之偵查、執行層面；得予協助之事項，亦不限於既有之送達及調查證據，而增列了搜索、扣押、執行沒收裁判，甚至包含其他未違我國法律規定之協助類型，以因應新興之犯罪型態，讓打擊跨境犯罪之手段更加豐富多元。此外，本法增訂沒收犯罪所得裁判之執行程序，可有效解決目前僅得協助他國扣押、而無法交還之困境[139]。

又隨著全球化的趨勢，人員、貨物及金流移動頻繁，跨境犯罪亦隨之增加，面對跨國（境）犯罪的威脅，必須透過國際刑事司法互助、引渡等

137 https://igwatch.tw/2023/09/13/%E8%81%AF%E5%90%88%E5%9C%8B%E7%B6%B2%E8%B7%AF%E7%8A%AF%E7%BD%AA%E5%85%AC%E7%B4%84%E7%AC%AC%E5%85%AD%E8%BC%AA%E5%8D%94%E5%95%86%E6%9C%83%E8%AD%B0%E8%90%BD%E5%B9%95/ (Last viewed: Nov,17,2023)

138 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_concluding_session/main (Last viewed: Nov,17,2023)

139 請參法務部新聞稿：https://www.moj.gov.tw/2204/2795/2796/58341/ (Last viewed: Nov,17,2023)

機制，以進行調查取證、追查資金流向、查扣犯罪資產及追緝外逃人犯。另基於人權考量，跨國移交受刑人亦屬近年來各國之熱門議題。我國身為國際社會之一員，為善盡共同維護國際秩序及人道主義之精神，持續由法務部國際及兩岸法律司（下稱國兩司），積極推動此類條約、協定及協議之簽署。雖然我國在國際情勢艱困之情形下，國兩司仍努力不懈，積極與各國洽簽司法互助協議（定）及引渡條約，其情形詳見下表[140]：

***民刑事司法互助條約、協定、協議**

簽訂國	條約、協定、協議 名稱
美國	駐美國台北經濟文化代表處與美國在台協會間之刑事司法互助協定
中國大陸	海峽兩岸共同打擊犯罪及司法互助協議
越南	駐越南臺北經濟文化辦事處與駐臺北越南經濟文化辦事處關於民事司法互助協定
菲律賓	駐菲律賓臺北經濟文化辦事處與馬尼拉經濟文化辦事處間刑事司法互助協定
南非	駐南非共和國臺北聯絡代表處與南非聯絡辦事處刑事司法互助協議
波蘭	駐波蘭代表處與波蘭臺北辦事處刑事司法合作協定
諾魯	中華民國（臺灣）政府與諾魯共和國刑事司法互助條約
貝里斯	中華民國（臺灣）政府與貝里斯政府刑事司法互助條約

140 https://www.moj.gov.tw/2204/2205/2263/%E5%9C%8B%E9%9A%9B%E5%8F%8A%E5%85%A9%E5%B2%B8%E5%8F%B8%E6%B3%95%E4%BA%92%E5%8A%A9/%E5%8F%B8%E6%B3%95%E4%BA%92%E5%8A%A9%E7%8F%BE%E6%B3%81/109341/109716/post (Last viewed: Nov,17,2023)

斯洛伐克	1.斯洛伐克台北代表處與斯洛伐克經濟文化辦事處刑事司法合作協議 2.駐斯洛伐克台北代表處與斯洛伐克經濟文化辦事處民事暨商事司法合作協議
聖文森及格瑞那丁	中華民國(臺灣)政府與聖文森及格瑞那丁政府刑事司法互助條約

***引渡條約**

簽訂國	條約名稱
哥斯大黎加共和國	中華民國政府與哥斯大黎加共和國政府間引渡條約
巴拉圭共和國	中華民國與巴拉圭共和國間引渡條約
南非共和國	中華民國政府與南非共和國政府間引渡條約
史瓦濟蘭王國	中華民國政府與史瓦濟蘭王國政府間引渡條約
多明尼加共和國	中華民國與多明尼加共和國間引渡條約
多米尼克	中華民國與多米尼克引渡條約
馬紹爾群島共和國	中華民國政府與馬紹爾群島共和國政府間引渡條約
帛琉共和國	中華民國政府與帛琉共和國政府間引渡條約
聖克里斯多福及尼維斯	中華民國與聖克里斯多福及尼維斯間引渡條約

除了與簽有司法互助協議之國家可以依據各該協議進行司法互助以外，縱使雙方沒有簽訂司法互助協議者，依據國際慣例，基於互惠原則，也可能進行司法互助。這也體現在我國刑事司法互助法第 1 條「在相互尊重與平等之基礎上，為促進國際間之刑事司法互助，共同抑制及預防犯罪，並兼顧人民權益之保障，特制定本法。」及第 5 條「依本法提供之刑事司法互助，本於互惠原則為之。」

依據筆者承辦國人跨境運輸毒品至澳洲案的經驗，雖然我國與澳洲之間沒有刑事司法互助協議，然筆者透過國兩司，經由外交部循外交管道，向澳洲檢察總長辦公室國際犯罪合作中心（International Crime Cooperation Central Authority, Attorney-General's Department）提出司法互助請求，請求澳方提供相關證據，在歷經 10 個月之後，終獲澳方回覆，且提供該案所需之完整證據，包括通訊監察譯文、對話聲音電子檔光碟、手機鑑識資料等，讓該跨境運輸毒品案件能順利起訴並判決有罪確定。在此需要特別說明者，在兩國簽有刑事司法互助協議之情形下，原則上司法互助之進行可直接由我國法務部與受請求方或請求方之中央司法互助權責機關進行，無須經由外交部，然若雙方沒有簽訂司法互助協議者，則須經外交部提出[141]。

又為遏阻犯罪集團持續運用不法所得經營非法事業，資產沒收為案件偵查中重要的項目，美國執法單位運用國內刑事沒收及民事沒收等制度，刑事凍結對象是犯罪行為人，目的是追訴處罰犯罪者，民事凍結標的是不法資產，目的是尋求犯罪所得之追討與賠償，刑事沒收需有對被告刑事審判之結果，民事沒收則可以以法院在對被告尚未判決定讞前，以非定罪沒收之方式進行。如前所述，現今犯罪所得之金流均以跨國洗錢之方式操作，美國執法單位在進行資產查扣及資產沒收時，除善用警務間金融情資交換管道外，亦會善用運用司法互助管道取得證據或進行資產查扣及沒收，美國透過條約協定或互惠原則，執法單位提供犯罪事實暨相當理由（Probable Cause）之證據，正式向被請求國提出司法互助請求。美方亦可提出相同之資產查扣、沒收之司法互助協助。又美國司法互助之程序訂有分享制度，部分案件在符合美國法規規定，經美國檢察總長批准，以及議

[141] 可參國際刑事司法互助法第 7 條、第 30 條。

會決議後，亦可將沒收之不法所得分享與受請求國，分享之成數則依據協助內容佔成案比例多寡來決定[142]。

（二） 非正式國際合作

與正式的國際合作不同，非正式的國際合作往往較具彈性，也較有效率，惟取得之情資除了在例外情形（例如：取得提供國或國際組織之同意），原則上不得提出於法庭做為證據使用。非正式的國際合作例如：國際刑警組織（國際間警方之間之溝通管道）、透過駐外聯絡官與當地警方交換情資、執法機關間的公務會談、自願性提供資料、行政協查等方式。也可透過國際間打擊犯罪之情資交換平台，例如：艾格蒙特集團財富情報聯盟[143]（The Egmont Group，中文簡稱：艾格蒙聯盟），提供各國金融情報中心（Financial Intelligence Unit, FIU）交換關於洗錢、資恐的情資。

又「亞太區追討犯罪所得機構網絡（Asset Recovery Interagency Network - Asia Pacific, ARIN-AP）」係韓國大檢察廳乃於 2011 年 12 月，在 FATF/APG 當年度之大會上提出建立專屬亞太區之追討犯罪不法所得機構網絡之構想，並於 2012 年 12 月在歐洲追討犯罪所得機構網絡（CARIN）年度大會中提出計畫方案。此一構想與計畫提出後，隨即獲得亞太地區許多國家之響應。我國檢察官協會首先獲得該網絡設立之訊息通知，嗣由法務部、外交部及駐韓國代表處積極向韓國主辦單位表達我國參與之意願並說明我國在區域司法互助網絡有不可欠缺之地位，幾經協商，我國終能順利於 2014 年 1 月 28 日加入 ARIN-AP[144]。

歐洲追討犯罪所得機構網絡[145]（Camden Asset Recovery Inter-agency Network, CARIN）是資產追蹤、凍結、扣押和沒收領域執法和司法從業人員的非正式網絡，每個成員國均由一名執法官員和一名司法人員代表。此

142 同註 44，第 19 頁。
143 https://egmontgroup.org/ (Last viewed: Nov,17,2023)
144 https://www.moj.gov.tw/2204/2795/2796/56840/post (Last viewed: Nov,17,2023)
145 https://www.carin.network/ (Last viewed: Nov,17,2023)

外，英國打擊犯罪機構（the National Crime Agency，NCA）下的跨國反貪腐合作中心[146]（International Anti-Corruption Coordination Centre）。以上國際組織各依其所著重之領域，成為國際上情資交換之平台。

在非正式國際合作中取得之情資，務必謹慎使用並注意保密，於 2009 年間曾發生前調查局長葉盛茂被控貪污等犯嫌，經高等法院向艾格蒙反洗錢組織詢問，提供給調查局有關扁家涉嫌洗錢情資的開曼群島、澤西島及列支敦士登三地的情報中心，都不同意將提供我國洗錢情資列入此案訴訟使用，將無法做為證據。該案中引起檢、辯交鋒，該案公訴檢察官認為：有些「洗錢天堂」不可能同意讓我國做為訴訟依據，「那我們要洗錢情資做什麼？」辯護人則同意不列為證據，並認為若我國違反世界各國、地區簽訂的協約，有可能因個案，被排除反洗錢聯絡網，將得不償失[147]。此案例值得我國司法人員及執法機關深思。

（三） 24/7 Network

八大工業國家高峰會（Group of Eight,下稱 G8），G8 於 1995 年注意到網路安全之議題，其所轄「高科技犯罪分項工作組」（Subgroup on High-Tech Crime）旋即在美國司法部刑事司「電腦犯罪暨智慧財產組」（CCIPS）主導下，號召各國加入這個全名「高科技犯罪執法情資聯絡窗口全天候聯防組織」（24/7 Network of High-Tech Crime Points of Contact）。我國於 2003 年 10 月透過美國司法部推薦，以臺灣名義正式加入，成為第 35 個會員國（如圖 16）。

[146] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/bribery-corruption-and-sanctions-evasion/international-anti-corruption-centre (Last viewed: Nov,17,2023)
[147] https://news.ltn.com.tw/news/politics/paper/301401 (Last viewed: Nov,17,2023)

Members of the G8 24/7 Network (as of December 2007)

AUSTRIA	GERMANY	MALTA	RUSSIA
BELGIUM	HONG KONG, CHINA	MAURITIUS	SINGAPORE
BRAZIL	HUNGARY	MEXICO	SOUTH AFRICA
BULGARIA	INDIA	MOROCCO	SPAIN
CANADA	INDONESIA	NAMIBIA	SWEDEN
CHILE	ISRAEL	THE NETHERLANDS	TAIWAN
CROATIA	ITALY	NEW ZEALAND	THAILAND
CZECH REPUBLIC	JAMAICA	NIGERIA	TUNISIA
DENMARK	JAPAN	NORWAY	UNITED KINGDOM
DOMINICAN REPUBLIC	REPUBLIC OF KOREA	PAKISTAN	UNITED STATES
ESTONIA	LITHUANIA	PERU	
FINLAND	LUXEMBOURG	THE PHILIPPINES	
FRANCE	MALAYSIA	ROMANIA	

圖 16

2004 年 2 月 G8 高峰會所轄「高科技犯罪分項工作組」主席 Christopher M.E. Painter 邀請我國出席同年 3 月於義大利羅馬舉行之第一屆網路犯罪聯盟會議，討論國際網路犯罪調查結果、發佈網路偵防訓練教材及線上調查工具、更新網路測試結果等相關議題，並與其他會員建立網路犯罪偵防的合作模式。會中我國代表並分別就「國家資通安全會報組織及任務」、「我國網路犯罪執行情形」以及「駭客入侵經驗分享」議題提出報告，獲得會員中各國代表的熱列討論及嘉許。

基於第一屆會議的成功，G8 高峰會所轄高科技犯罪分項工作組復於 2006 年 10 月 17~19 日假義大利羅馬，針對已加入「G8 Network of 24-Hour Points of Contact for High-Tech Crime」之會員舉辦第二屆網路犯罪聯盟會議（Second G8 Training Conference for 24/7 Points of Contact）。時任美國司法部刑事司電腦犯罪及智慧財產組助理副司長 Richard W. Downing 及法務專員 Aubrey Rupinta（同時擔任聯盟會議之行政聯絡人）以電子郵件將前開研習會議訊息（含分項工作組主席 Christopher M.E. Painter 之邀請函）通知法務部，該次即指派時任調法務部檢察司辦事朱應翔檢察官（現已轉任律師）、調法務部資訊處辦事孫治遠檢察官代表出席[148]。

《布達佩斯公約》於 2004 年生效後，其中第 35 條規定應建立有效運

[148] 以上過程可參：公務出國報告「參加第二屆網路犯罪聯盟會議」（2007）。

作的聯絡窗口。於 2007 年歐洲理事會（Council of Europe）在法國史特拉斯堡（Strasbourg）召開「Octopus Interface Conference - Cooperation against Cybercrime，以下簡稱 OIC 國際研討會」，時任歐洲理事會人權暨法律事務總署技術合作處科長 Alexander Seger 先生邀請我國派員參加，經法務部指派時任臺灣臺北地方法院檢察署張紹斌主任檢察官（現已轉任律師）率時調檢察司辦事吳炳標檢察事務官（現回任臺灣臺北地方檢察署）共同參加。於該次會議中，確立了 G8 24/7 聯防組織的聯繫網絡未來會與依《布達佩斯公約》規定建立的聯繫網絡兩者合而為一的作法，由兩個組織共同合作進行彙集、維護、更新「聯絡窗口名錄」的工作。此項在歐洲理事會場域的提案業於 2007 年 11 月間獲得 G8 高科技犯罪分項工作組認可[149]。

惟需注意者，經由 G8 24/7 Network 可向其他會員國請求者，係為求時效，避免數據資料因時間而消滅，故請求先行「保存」（Data Preservation）該國境內之網路服務提供者（ISP）之數據資料，至於要取得該資料，仍須經由司法互助管道為之[150]。我國目前 G8 24/7 Network 之聯絡窗口係設於刑事局科技研發科，惟據筆者瞭解，目前我國檢察官使用該項機制請求他國協助保存資料的案件數並不多。

三、 打擊網路犯罪之組織

（一） 國際刑警組織

在教育訓練方面，國際刑警組織（INTERPOL）為了幫助其會員國成員打擊網路犯罪，在新加坡成立 INTERPOL Global Complexfor Innovation

[149] 以上過程可參：公務出國報告「出席歐洲理事會網路犯罪公約委員會合作打擊網路犯罪國際研討會出國報告」（2007）。

[150] 關於向美國、歐洲請求數位證據之保存、調取之相關程序、限制等，可參閱：粟威穆、蔡百凌，公務出國報告「參加歐洲司法網絡第 47 屆會議報告」（2007），第 12 頁至第 16 頁。

(IGCI)，對其會員提供網路犯罪偵查之指引、數位鑑識協助、暗網追查、惡意軟體分析等。

另成網路整合中心（Cyber Fusion Centre, CFC），齊聚從執法機關及業界網羅之網路專家，分析網路犯罪資訊，提供有效情資給會員，從預防犯罪及識別犯罪者二方面，以轉化為具體行動。此外，成立數位鑑識實驗室（Digital Forensics Laboratory），協助會員在日常工作中偵測、取出並使用數位證據。為了面對日新月異的網路犯罪手法，INTERPOL 亦與網路業界合作，嘗試最新的科技，以期未來實際應用在真實案件上[151]。

（二） 歐洲網路犯罪中心[152]

歐洲網路犯罪中心（European Cybercrime Centre, EC3）由歐洲刑警組織設立，旨在加強歐盟對網路犯罪的執法回應，從而幫助保護歐洲公民、企業和政府免受網路犯罪的侵害。自 2013 年成立以來，EC3 為打擊網路犯罪做出了重大貢獻，並參與了許多備受矚目的行動和數百次行動支援部署。其重點打擊以下類型的網路犯罪：網路相關犯罪、兒童性剝削、付款詐欺，並提供打擊暗網上的犯罪活動的支援。

EC3 作為犯罪資訊和情報的中心樞紐，透過提供案件分析、協調和專業知識來支持會員國的行動和調查，並為調查和行動提供高度專業化的技術和數位鑑識支援能力。在歐洲刑警組織的職責範圍內，為歐盟危機管理結構提供支持，並促進執法機構(LEA)和其他相關網路社群與歐盟機構、實體與機關（例如 Eurojust、EEAS、ENISA、CERT-EU、歐盟委員會、歐盟理事會等）。透過待命值班和歐盟執法緊急應變協議(EU LE ERP)向執法機關提供「24/7」運作和技術支持，以便對緊急網路事件、網路危機立即做出反應。此外，EC3 主辦並促進聯合網路犯罪行動特別工作小組（J-CAT）打擊

[151] Cybercrime, Future-oriented policing projects, INTERPOL.
[152] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Last viewed: Nov, 17, 2023)

網路犯罪，並針對成員國相關執法機關的培訓和能力建設，提供各種策略分析工具，有助於就打擊和預防網路犯罪做出明智的決策；在整合資源方面，EC3 將打擊網路犯罪的執法機構與私部門、學術界和其他非執法夥伴連結起來，有助於在網路犯罪授權領域準備和開展標準化預防和宣傳運動及活動。

值得一提的，針對勒索軟體，EC3、荷蘭警方國家高科技犯罪部門和 McAfee 發起一項名為「No More Ransom (NMR) 」（終結勒索軟體）的行動，旨在幫助勒索軟體受害者解密加密數據，而無需向犯罪分子支付贖金。NMR 展示了公私合作在打擊利用勒索軟體犯罪的價值。受害者不應再被迫支付贖金或遺失文件。透過免費恢復對受感染系統的訪問，EC3 為受害人提供了第三種選擇。這些免費資源於 2016 年 7 月推出，已幫助了超過 600 萬人，目前已擁有來自執法部門、私營部門和學術界的 170 多個支持合作夥伴。這些資源有 37 種不同語言版本，並包含 120 多種工具，能夠解密 150 多種不同類型的勒索軟體。

「No More Ransom (NMR) 」的運作方式如下：受害人先連上「No More Ransom (NMR) 」的網站[153]，點選「加密警長」（Crypto Sheriff）功能，上傳二份遭到勒索軟體加密之檔案，並填入與勒索軟體有關的電子郵件、網址、比特幣錢包地址或勒索軟體留下之文字檔等，讓網站檢索是否已有解密的方法，如果經檢索業有解密方法者，則會提供給被害人。

（三） 歐盟網路安全局

歐盟網路安全局[154]（The European Union Agency for Cybersecurity, ENISA）是致力於在整個歐洲實現高水準網路安全的聯盟機構。歐盟網路安全局成立於 2004 年，並根據《歐盟網路安全法》（EU Cybersecurity

[153] https://www.nomoreransom.org/crypto-sheriff.php?lang=en (Last viewed: Nov, 17, 2023)
[154] https://www.enisa.europa.eu/about-enisa (Last viewed: Nov,17,2023)

Act[155]）得到強化，為歐盟網路政策做出貢獻，透過網路安全認證計畫增強 ICT 產品、服務和流程的可信度，與成員國和歐盟機構合作，並幫助歐洲做好準備應對未來的網路挑戰。透過知識共享、能力建構和提高意識，該機構與其主要利益相關者合作，加強對網路經濟的信任，增強歐盟基礎設施的韌性，並最終確保歐洲社會和公民的數位安全。

在一個高度互相連動的世界中，網路犯罪分子對歐盟的內部安全及其公民的網路安全構成了重大威脅。COVID-19 大流行凸顯了數位世界提高安全的必要性，因為人們增加在網路上的使用以維持個人和專業關係，而網路犯罪分子則利用這種情況，特別將目標放在電子商務和電子支付企業以及醫療保健系統。

當網路侵駭事件發生時，會涉及多個單位的啟動及處理，包含：電腦資安事件應變小組（Computer Security Incident Response Team，CSIRT）負責緩解事件，執法機構負責進行調查，而司法機關（法官、檢察官）則負責司法程序之進行。儘管每個機關都有其特定的角色，但經常處理相同的案件，其中一個機關的處理有時會重疊，也可能干擾其他機關的目標和活動。此外，其他因素也可能對合作產生影響，其中包括技術、法律、組織挑戰，有時甚至是機關之間的行為差異。ENISA 闡述了電腦資訊安全事件應變小組（Computer Security Incident Response Team, CSIRT）、執法機關和司法機關的法律和組織框架、角色和職責。並分析了其等所需的能力，以及各自活動中的協同作用和潛在干擾。透過促進彼此之間的合作以及互動，並提供各機關培訓，最終目標是為更好地應對網路犯罪做出貢獻[156]，對於各機關的合作，ENISA 也提出了年度報告供參[157]。

---

[155] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (Last viewed: Nov, 17, 2023)

[156] https://www.enisa.europa.eu/news/enisa-news/incidents-handling-and-cybercrime-investigations (Last viewed: Nov,17,2023)

[157] 2021 Report on CSIRT-Law Enforcement Cooperation, availabe at: https://www.enisa.europa.eu/publications/2021-report-on-csirt-law-enforcement-cooperation (Last viewed: Nov,17,2023); Aspects of Cooperation between CSIRTs and LE - Toolset 2021, availabe at:

（四） 網路犯罪計畫辦公室

位於羅馬尼亞布加勒斯特（Bucharest, Romania）的歐洲委員會網路犯罪計畫辦公室（Cybercrime Programme Office, C-PROC） 負責協助世界各國加強其法律系統能力，以根據《布達佩斯公約》的標準應對網路犯罪和電子證據帶來的挑戰。包括：根據法治和人權（包括資料保護）標準加強網路犯罪和電子證據立法；訓練法官、檢察官和執法人員；建立專門的網路犯罪和鑑識單位並改善機構間合作；促進公私合作；保護兒童免受網路性暴力；提升國際合作成效等工作內容。C-PROC 以其能力協助補充網路犯罪公約委員會[158]（Cybercrime Convention Committee, T-CY）的工作，締約國透過該委員會追蹤《布達佩斯公約》的實施情況[159]。

（五） 歐洲司法組織

歐洲司法組織（Eurojust）的成立倡議於 1999 年 10 月 15 日、16 日在芬蘭舉行的歐盟理事會會議，與會領袖希望能創立一個司法合作單位，藉由增強、鞏固各國的合作來打擊跨境犯罪，以確保歐盟地區的自由、安全與司法正義。隨後歐盟理事會作成決議，由歐盟各國的檢察官、預審法官、警官或其他相類職務之官員組成前述的歐盟司法單位，並由各國指派司法官員派駐其中。歐盟理事會嗣以 2002/187/JHA 決定成立歐洲司法組織。歐洲司法組織也致力於與第三國及其他歐盟機構簽訂合作協議，使雙邊得以交換司法資訊與個人資料。而挪威與美國更派駐檢察官在歐洲司法組織擔任聯絡官。歐洲司法組織除與前述國家、機構簽訂協定者外，另在全球多個國家有聯繫窗口之合作而構成完整的網絡。是以，從 2002 年開

https://www.enisa.europa.eu/publications/aspects-of-cooperation-between-csirts-and-le-toolset-2021 (Last viewed: Nov,17,2023)

158 https://www.coe.int/en/web/cybercrime/tcy (Last viewed: Nov,17,2023)

159 https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc- (Last viewed: Nov,17,2023)

始，歐洲司法網路就在歐洲的司法合作中扮演著重要角色，並參與很多實際運作的任務[160]。我國目前亦擔任該組織之聯絡窗口[161]。

近年來在歐洲惡名昭彰的 EncroChat 加密通訊軟體，即由 Eurojust 與 Europol、法國、荷蘭警方等等共同合作而破獲。簡介如下：2016 年成立的 EncroChat 為一通訊網路與服務供應商，該公司改造 Android 手機與黑莓手機，在裝置上內建各種加密應用程式，從文字傳訊、語音通話到筆記程式等，且裝置上的 GPS、攝影機及麥克風都被禁用，還設有緊急按鍵以刪除所有資料。每支 EncroChat 手機的售價為 1,000 歐元，6 個月的服務合約為 1,500 歐元。法國憲兵隊在 2017 年發現犯罪集團經常利用 EncroChat 手機作為加密通訊工具，於是通知了 Eurojust 與荷蘭，並與荷蘭建立了共同調查小組，再由 Europol 擔任協商各國調查與逮捕行動的角色。法國在 2020 年取得了法官的同意，於設於境內的 EncroChat 伺服器上安裝了惡意程式，可攔截藉由伺服器送出的訊息並記錄用戶密碼，4 月即開始監控 EncroChat 用戶的通訊。而法國與荷蘭在 Europol 與 Eurojust 的協助下，於 2020 年摧毀及破解了受到犯罪集團青睞的加密網路 EncroChat，在進一步分析該加密網路中的 1.15 億則通訊之後，數年來已於全球逮捕了 6,658 名嫌犯，扣押或凍結近 9 億歐元的不法所得[162]。

（六） 歐洲司法網路犯罪網絡

歐洲司法網路犯罪網絡（European Judicial Cybercrime Network, EJCN）成立於 2016 年，旨在促進專門應對網路犯罪、網路犯罪和網路空間調查人員之間的聯繫，並提高調查和起訴的效率。EJCN 透過交流有關調查和起訴

---

160 我國前國兩司司長蔡秋明及前調部辦事林明誼檢察官曾於 2017 年拜會總部設在荷蘭海牙之歐洲司法組織，可參見：拜會海牙國際組織與參加歐洲司法網路第 48 屆全體會議公務出國報告。於 2023 年 7 月，我國法務部長蔡清祥率團訪歐，拜會 EUROJUST，由西班牙籍對外關係部主席阿瑪雅（José de la Mata Amaya）親自接見，此行為我國史上進入該組織的最高層級，立下里程碑，可參見：https://news.ltn.com.tw/news/politics/breakingnews/4358085 (Last viewed: Nov,17,2023)

161 https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-cooperation-with-third-countries.pdf (Last viewed: Nov,17,2023)

162 https://www.ithome.com.tw/news/157533 (Last viewed: Nov,17,2023)

網路犯罪的專業知識、最佳實踐和其他相關知識，促進和加強主管司法當局之間的合作。

EJCN 在歐洲司法組織的支持下每年舉行兩次全體會議。這些會議提供了一個機會，讓 EJCN 成員與其他利益相關者就司法當局在網路犯罪案件中面臨的共同挑戰和最佳實踐進行交流。除了 EJCN 成員和歐洲司法組織代表外，參與者還包括歐洲刑警組織、歐洲司法網絡、歐洲委員會和歐盟委員會[163]。

最近一次的全體會議係於 2023 年 6 月 15 至 16 日舉辦[164]，參與者包含來自歐盟成員國、挪威、塞爾維亞、瑞士、美國、日本檢察院的代表、Europol、Eurojust 等。本次討論的主題聚焦於封閉性及開放性之「元宇宙」（Metaverse）、去中心化等新新概念及科技所產生的網路犯罪問題。此外，對於虛擬資產相關犯罪之偵辦，因為虛擬貨幣交易所成為投資者進入投資的門戶，引領去中心化金融的生態，同時也是犯罪者將其犯罪所得轉化至鏈下生態系統的門戶，故如何與虛擬資產服務提供者合作，即成為取得證據並接續進行調查之關鍵。在該次會議中特別介紹 SIRIUS 計畫[165]，一個由歐盟資助的項目，可協助執法和司法機關在刑事調查和訴訟中取得跨境電子證據。該計畫係由歐洲刑警組織、歐洲司法組織與歐洲司法網絡密切合作共同實施，是歐盟跨國取得電子證據知識共享的中心點。

如今，超過一半的刑事調查都包括跨境請求存取電子證據（例如來自訊息或電子郵件服務或社交媒體的數據）。該計畫提供了主管機關和特定服務提供者（Service provider, SP）之間合作流程的標準化，包括調查工具和 SP 的聯絡方式，該計畫是從其他司法管轄區的 SP 取得電子資料的首選，

163 https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network (Last viewed: Nov,17,2023)
164 關於最近一次會議之內容，可參見：https://www.eurojust.europa.eu/document/european-judicial-cybercrime-network-14th-plenary-meeting-outcome-report (Last viewed: Nov,17,2023)
165 https://www.europol.europa.eu/operations-services-innovation/sirius-project (Last viewed: Nov,17,2023)

其內有超過 1,000 家公司的最新聯絡資訊庫，讓執法機關能夠在一次交易中檢索多個地址，以更有效地處理複雜和大量的資訊。該服務可透過歐洲刑警組織專家平台[166]（Europol Platform for Experts, EPE）存取，其資源可供所有歐盟成員國的執法和司法機關以及與歐洲刑警組織或歐洲司法組織簽訂業務協議的非歐盟國家使用[167]。

（七） 全球檢察官打擊電腦犯罪網路

全球檢察官數位犯罪網路[168]（Global Prosecutors E-Crime Network, GPEN）於 2008 年啟動，旨在透過確保檢察官擁有有效應對網路犯罪的工具，協助所有國家為使用者建立安全可靠的線上環境。其目標包含：加強打擊數位犯罪領域的國際合作；改善資訊交流，減少重複並提高跨國界分析和起訴能力；使所有司法管轄區能夠制定協調一致的方法來處理數位犯罪，以支持有效的起訴並強化《網路犯罪公約》。此網路不會與 24/7 協議或正式的司法互助衝突或競爭。被指定為國家聯絡窗口的數位犯罪專家將負責任何必要的國內聯絡；提供一個擁有來自世界各地的資源和專業知識的全球培訓論壇。培訓檢察官起訴網路犯罪案件是國際打擊網路犯罪努力的優先事項。該網絡將制定適當的培訓課程來培訓檢察官，檢察官可將學習得到之知識分享予其同事；使全球檢察官能夠快速有效地交換關鍵資訊和數據。

GPEN 是一個由專業數位犯罪檢察官組成的網絡，每個 IAP 組織成員都會提名至少一名檢察官註冊為 GPEN 國家聯絡窗口。GPEN 提供：來自世界各地的提名數位犯罪檢察官資料庫；交流專業知識、疑問和建議的論

166 https://epe.europol.europa.eu/ (Last viewed: Nov,17,2023)

167 值得一提的是，筆者於 2023 年至英國倫敦參加國際檢察官協會第 28 屆年會，代表我國檢察官擔任報告人，期間與二位瑞典檢察官聊到境外虛擬貨幣交易所資料調取的議題，該二位瑞典檢察官向筆者表示境外交易所的聯絡方式對其等造成很大困擾，筆者即向其等介紹歐洲刑警組織之 EPE 平台，並提供相關資料供參，而瑞典檢察官亦致贈筆者印有「瑞典檢察機關（Swedish Prosecution Authority）」字樣的筆供筆者留念。

168 https://www.iap-association.org/GPEN/About-GPEN (Last viewed: Nov,17,2023)

壇，例如，數位犯罪起訴資源資料的集合；國家立法和法律指導；虛擬的全球數位犯罪檢察官學院，數位犯罪培訓課程和演示的資料庫；分享專業知識和經驗的全球數位犯罪檢察官社群。

（八） 美國打擊網路犯罪之部門

美國打擊網路犯罪的執法機關包含：聯邦調查局、國稅局犯罪調查組（IRS-CI）、國土安全調查署網路犯罪中心（HSI Cyber Crimes Center）等。筆者以下擬介紹關於美國司法部刑事司下的電腦犯罪暨智慧財產權組[169]（Computer Crime and Intellectual Property Section, CCIPS）（組織架構如圖17）。

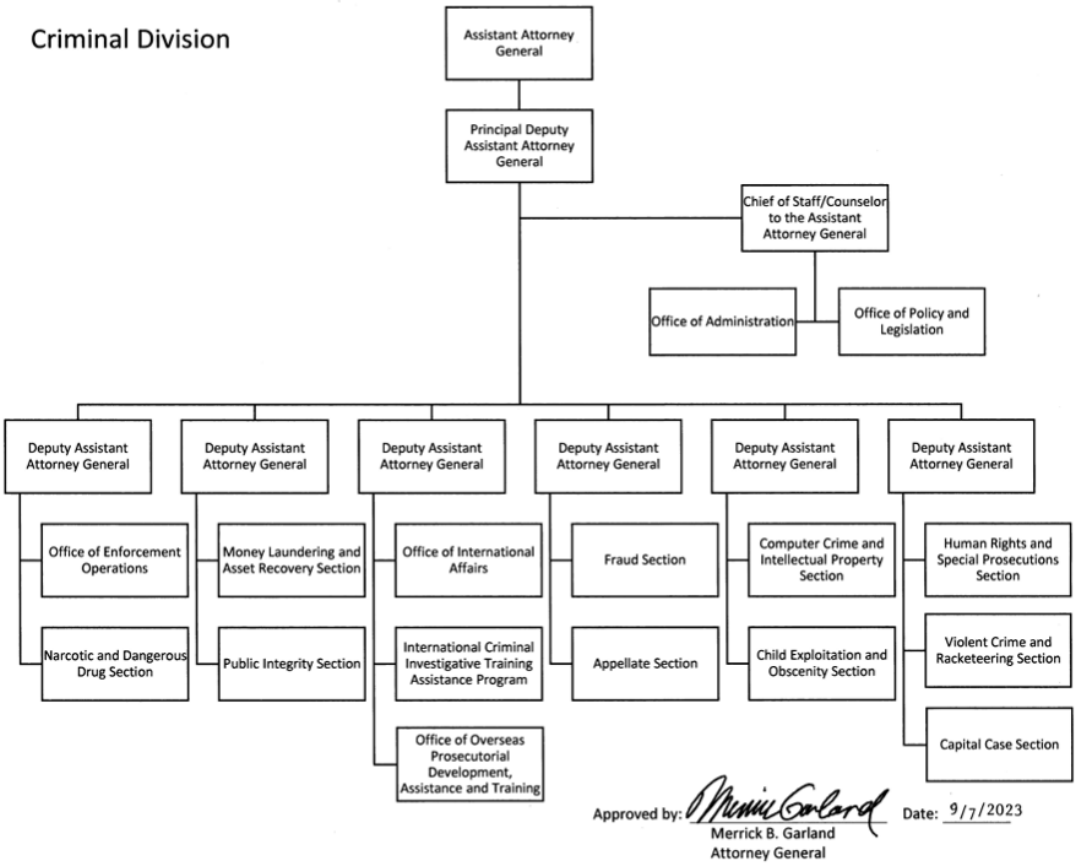


圖 17

[169] https://www.justice.gov/opa/pr/criminal-division-s-computer-crime-and-intellectual-property-section-celebrates-20-years (Last viewed: Nov,17,2023)

CCIPS 成立於 1996 年 10 月 13 日，其前身是 1991 年在該部門的一般訴訟和法律諮詢科下成立的一個由 5 名律師組成的「電腦犯罪小組」（Computer Crime Unit）。至 2016 年為止，CCIPS 的成員已增至 40 多名律師，此外還有 9 名組成 CCIPS 網路犯罪實驗室的數位調查分析師。部門律師定期進行複雜的調查；解決新興電腦和電信技術引發的獨特法律和調查問題、訴訟案件；為其他檢察官提供訴訟支援；訓練聯邦、州和地方執法人員；對立法提出意見並提出建議；促進網路安全；發起並參與打擊電腦和智慧財產權犯罪的國際努力。

CCIPS 與全國各地美國檢察官辦公室的檢察官合作，包括起訴經驗豐富的駭客，例如：對駭客 Albert Gonzalez 進行定罪，他與共犯滲透到了全國主要零售商的電腦網路，並竊取超過 4,000 萬個信用卡、金融卡號碼；Gameover Zeus 殭屍網路和 Cryptolocker 勒索軟體計畫的查獲，與俄羅斯涉嫌網路犯罪分子 Evgeniy Bogachev 的起訴；Megaupload.com 被取締並對其運營商 Kim Dotcom 提出起訴，罪名是涉嫌實施歷史上最大的全球線上數位盜版。該部門與美國聯邦檢察官辦公室和國際合作夥伴合作，在打擊 Tor 網路上託管的暗網市集的國際行動中發揮了核心作用。

CCIPS 在解決電腦犯罪和數位證據日益國際化的問題上發揮了變革性作用。於 1997 年，該部門協助建立了 G8 24/7 高科技犯罪網絡，該網絡為其他參與國建立了正式聯絡窗口，以便為涉及電子證據的國際調查提供緊急協助。自那時起，CCIPS 一直擔任美國的 24/7 網路聯絡窗口，協助對國外犯罪和恐怖事件做出緊急反應。

（九） 巴伐利亞邦數位犯罪中央檢察辦公室

巴伐利亞邦數位犯罪中央檢察辦公室[170]（Zentralstelle Cybercrime Bayern, ZCB），於 2015 年 1 月 1 日由巴伐利亞邦司法部成立於班堡高等

[170] https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/spezial_1.php (Last viewed: Nov,17,2023)

檢察署內，並有 18 位擁有技術及數位犯罪調查專業訓練背景之檢察官及 4 位鑑識專家。該辦公室負責邦內重大數位犯罪案件之調查，例如組織性網路犯罪、對重大經濟、金融部門之數位攻擊、網路勒索或網路詐欺，暗網非法交易或兒少色情等案件，亦支援重大數位犯罪的公訴工作。於 2020 年 10 月，更於辦公室內成立打擊網路性暴力及兒少色情專組，下有 8 個檢察官及技術專家負責重大網路性暴力及兒少色情案件的查緝。ZCB 亦負責在數位犯罪領域中，與德國其他邦或跨國執法單位間之合作協調，並研究新科技及社會趨勢以辨識新興數位犯罪態樣，並支援邦內司法人員有關數位犯罪專業知識之教育訓練，俾更有效打擊數位犯罪[171]。

班堡（Bamberg）高等檢察署檢察長 Wolfgang Grundler 及副檢察長 Thomas Goger 於 2023 年 3 月來臺，除拜會我國法務部外，更與法務部及所屬檢察機關進行三天的深度業務交流，分別舉辦交流論壇及研討會，包括首屆臺德檢察體系交流系列論壇。此為德國班堡高等檢察署繼 2022 年 7 月與法務部及所屬司法官學院、行政院洗錢防制辦公室共同舉辦「元宇宙與加密世界」國際研討會，分享「加密通訊資料取得之挑戰與法律界線」後，再度與我國交流並提供實務經驗，深化臺德檢察體系之合作，並強化執法機關跨國打擊數位犯罪之量能[172]。

（十） 日本打擊網路犯罪之部門

日本為迅速應對日新月異的通信技術、網絡犯罪、虛擬貨幣犯罪等造成的犯罪匿名化與跨境化，在於 2021 年 4 月，在最高檢察廳下設立「新興犯罪檢察小組[173]」（Japan Prosecutors unit on Emerging Crimes, JPEC, 日文為「先端犯罪検察ユニット」），小組成員則包括高等檢察廳及地方檢察廳對於科技、網路有專業，且具備海外留學背景的檢察官及檢察事務官，研究

171 2023 法務部臺德檢察交流系列論壇「檢察體系如何因應遽變中的數位犯罪」中之介紹。
172 https://www.moj.gov.tw/2204/2795/2796/166443/post (Last viewed: Nov,17,2023)
173 https://www.kensatsu.go.jp/content/001329255.pdf (Last viewed: Nov,17,2023)

新興犯罪資訊，偵查技巧並與私部門、學術單位合作，為檢察官提供此類新興犯罪偵辦之法律及實務建議、訓練及協助。在國際合作方面，該小組擔任網路犯罪檢察官非正式國際合作之聯絡窗口（關於 JPEC 的功能如圖 18）。而 JPEC 成員更積極參與國際會議，以強化網路犯罪之情資交換。

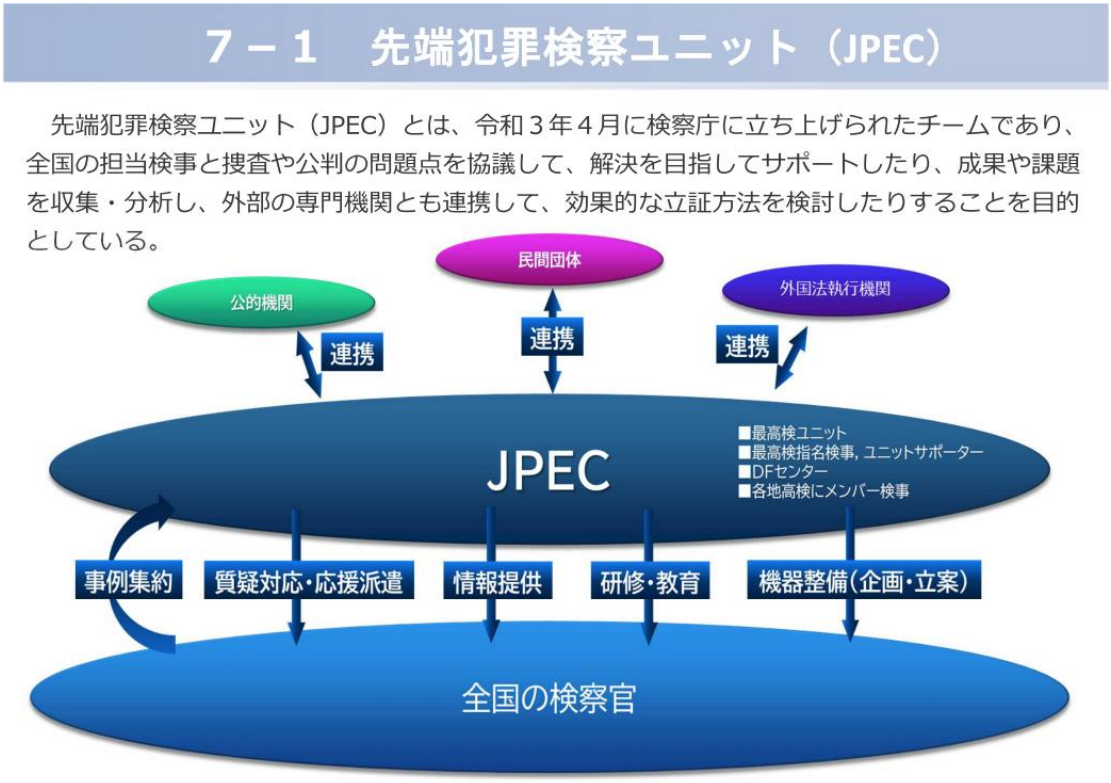


圖 18（來源：日本法務省刑事局「檢察廳對各種犯罪之因應」第 7 頁）

圖 19（來源：註 173 第 18 頁）

（十一） 韓國打擊網路犯罪之部門

由於利用虛擬資產進行的新型犯罪急劇增加，韓國最高國家檢察機關大檢察廳今年已撥款超過 9.86 億韓元（約 73 萬美元），指派金融監督院、金融情報機構和韓國交易所的金融專家，於首爾南部地方檢察廳成立「虛擬資產聯合調查小組」（Virtual Asset Joint Investigation Team），並於 2023 年 7 月 26 日正式啟動，舉辦牌匾揭幕儀式。這是韓國檢察機關首次設立專門的虛擬資產調查組織[174]。

「虛擬資產犯罪聯合調查小組」（由首席檢察官李正烈領導）正在開發追蹤系統以捕獲流向的虛擬資產。專門打擊虛擬資產（加密貨幣）犯罪。在上開預算中，有 7.78 億韓元（約 58 萬美元）是用於購買虛擬資產追蹤、分析設備的軟體許可證，有 2.08 億韓元（約 15 萬美元）用於綜合戰略計劃（ISP），旨在建立用來一個分析和追蹤虛擬資產非法交易的追蹤平台[175]。

（十二） 新加坡打擊網路犯罪之部門

新加坡總檢察署副首席檢察官王守仁認為：科技罪案主要有兩種形態，一是科技促成（technology-enabled），即與科技直接有關的犯罪，如駭入電腦系統等；一是科技輔助（technology-faciliated），即通過科技來協助完成的傳統犯罪，例如數位化偽造、網路騷擾和詐騙等，其更表示：所有檢察官須受科技罪案和數碼證據基本訓練。而新加坡總檢察署[176]自 90 年代後期注意到科技犯罪的趨勢，於是開始通過各種方式培養一組專注於科技罪案的檢察官，並在 2023 年正式成立了兩個專案小組來應對新挑戰，即科技罪案工作組（Technology Crime Task Force）和虛擬貨幣工作組

174 https://www.news1.kr/articles/?5120439 (Last viewed: Nov,17,2023)
175 https://tw.nextapple.com/blockchain/20230821/8C5DF3A1E69DEF69B7727BE9949C9859 (Last viewed: Nov,17,2023)
176 https://www.agc.gov.sg/resources/databases/newsitem/lianhe-zaobao-article-on-technology-crime-task-force (Last viewed: Nov,17,2023)

（Cryptocurrency Task Force）。科技罪案工作組主要應對電腦或科技輔助的罪案，以及處理數位證據等事項。虛擬貨幣工作組則專注於虛擬貨幣作為資產所引起的各種問題，包括協助新加坡警察部隊追蹤、查獲和處置這類資產[177]。

[177] https://www.zaobao.com.sg/news/singapore/story20231017-1443667 (Last viewed: Nov,17,2023)

柒、 心得與建議

一、 培育專業人才

（一） 科技教育訓練

因網路犯罪、虛擬貨幣、通訊方式等新興科技應用之犯罪手法日新月異，且犯罪者使用新應科技在各式犯罪上亦層出不窮，犯罪者可能透過網路、加密通訊方式、虛擬貨幣來從事毒品、詐欺、重大經濟犯罪、洗錢、貪瀆、賄選等犯罪型態，堪認上開新興科技之基礎知識乃現代偵辦案件之基石，而我國檢察官多為法律係畢業，專業是法律，如何建構讓全體檢察官具備新興科技的基礎知識，例如：網路原理、IP 追查、駭客手法、區塊鏈、加密、虛擬貨幣、幣流分析、電腦及手機鑑識、通訊技術及原理等，讓檢察官可有效與司法警察溝通，迅速理解案情，並能以淺白方式說明給法院瞭解，實是未來的趨勢。

我國近年來檢察官處理案件壓力繁重，雖在大型地檢署設有專組，然而在案件數量龐雜，且除了黑金專組（大黑）可只處理重大黑金案件外，其他專組的檢察官除了要處理專組案件，也要處理一般案件，導致檢察官無暇進修，吸取最新科技知識，故如能推動修法，將公然侮辱（例如：在社群媒體或網路遊戲中謾罵等與公益較無涉之案件）、車禍過失傷害（尤其是在一定程度輕傷之情形，筆者時常處理車禍破皮瘀青而提告過失傷害者，但其實告訴人主要的需求是民事賠償）等除罪化，回歸民事程序處理。如認修法費時，可在不修法之情形下，進行真正的書類簡化（例如：在簡單案件直接引用移送書之犯罪事實，讓檢察官不用在剪下貼上修改）；切勿將心力放在枝微末節之事（例如：地檢署檢察官速偵案件的結案書類上的製作書類日期），將耗費在這些事情的文書往返、時間資源省下來，讓檢察官真正有時間精進專業知識，始為國家之幸。

又法務部近年來設有證照制度，例如：金融、政府採購、貪瀆等，可考慮加入科技偵查或電腦犯罪的項目。筆者於 2023 年 9 月間前往英國倫敦，參加國際檢察官會議擔任報告人，會中與荷蘭檢察官討論關於檢察官電腦犯罪職能之建立，荷蘭檢察官告訴筆者，在荷蘭關於網路犯罪的課程設有三個階段的教育訓練，因為荷蘭檢察官認為現今的案件幾乎都會遇到網路犯罪或與網路有關之犯罪，他們認為這是荷蘭檢察官必學的課程，筆者著實認同。

（二） 專業團隊

美國司法部早在 1991 年即成立電腦犯罪小組，嗣於 1996 年擴大轉型為電腦犯罪暨智慧財產權組，專門負處理重大複雜之網路犯罪案件。而近年成立虛擬貨幣執法小組（NCET），在今年美國司法部更宣布 NCET 併入電腦犯罪暨智慧財產權組成為常設單位，以因應重大虛擬貨幣犯罪。而虛擬貨幣犯罪常涉及不法金額龐大之洗錢、詐欺等犯罪，偵辦是類案件所涉及之知識、原理、追蹤技巧等均需受過訓練，始能有效偵辦。又此類案件常涉及跨境因素，如何向境外交易所調取資料，以進行進一步偵查，或如何與國外執法機關合作，亦為重點。亞洲鄰近國家如日本、南韓、新加坡皆陸續成立虛擬貨幣偵辦專業團隊，其中日本設於最高檢察廳之下，網羅對於網路犯罪專精且具有海外留學背景之檢察官及檢察事務官加入，近年也有與美國司法部合作破獲索尼生命保險公司員工涉及比特幣之亮眼案件；新加坡今年也在總檢察署下設立科技罪案工作組和虛擬貨幣工作組，均係在該國之最高檢察機關下設立專業團隊，可見其等對於科技犯罪之重視。而南韓也於今年宣佈成立「虛擬資產犯罪聯合調查小組」，並開發虛擬貨幣追蹤平台。以上可供我國參考。

二、 強化國際合作

（一） 積極參與國際合作與國際會議

在偵辦網路犯罪過程中，因為網路犯罪天生的匿名性及跨境性，國際合作相形重要。正式之國際合作需遵行司法互助程序，在我國係由法務部國兩司負責，檢察官在承辦個案上如有向國外請求之需要，均需透過國兩司，故檢察官宜熟悉司法互助程序，始能有效率地進行司法互助。又國際合作除了正式的司法互助以外，還有非正式的合作，例如警務合作、國際情資交換平台等，檢察官宜熟悉該等非正式國際合作模式，可更有效率地獲得情資。再者，在個別檢察官可以做到的是，在參與國際事務的過程中，多與國外之檢察官、執法機關交流，並留下聯絡方式，日後如有案件偵辦或外國法律制度的請教，也多一個機會及窗口可以請教，舉一個筆者個人的例子，筆者之前至泰國曼谷參加由美國國際執法學院（ILEA）開設之訓練課程，認識來自亞洲多國的檢察官及執法機關；復前往英國倫敦參加國際檢察官協會第 28 屆年會擔任報告人，也結識來自世界各地的檢察官；赴美期間參加全美網路犯罪會議及美國檢察官、執法機關組成之虛擬貨幣偵辦討論團體，均結識美方的執法機關及檢察官。日前國內某單位詢問筆者關於美國虛擬貨幣財產申報的問題，筆者即請教上開結識的友人，獲取最新的美方及其他國家的作法，供國內單位參考。

又我國為 24/7 之正式會員，檢察官於偵辦網路犯罪案件時，可多加利用該資源。此外，歐洲理事會於 2006、2007 舉辦網路犯罪相關會議，我國均有派員參與，實是最佳讓世界看見臺灣檢察官的專業能力的機會，也是讓臺灣有機會與世界接軌，尋求更多國際合作的可能性。可惜在此之後，從公務出國報告資訊網之資料看起來，似乎沒有（或甚少）有指派檢察官與會之機會，建議部裡可多尋求此等國際會議之與會機會，選派具有科

技、網路專業，並具有良好外語能力及實際偵辦經驗之檢察官與會，以期與國際上新興科技犯罪偵辦之潮流齊頭並進，以強化國際合作。

（二） 厚植語言能力

科技突破了國界的限制，犯罪集團使用科技犯罪也是沒有國界的，常常案件查一查就遇到跨境的因素，例如：境外 IP、境外交易所、境外網路服務提供者、境外帳戶、境外共犯等，均需要尋求國際合作的機會。而在與其他國家的檢察官或執法機關的溝通上，較為普遍還是使用英語，如果不具備良好的英語能力，則要如何達成與國外的檢察官、執法機關順利溝通？當然現在科技發達，書信文字尚可使用翻譯軟體或 AI 等科技協助，但人與人面對面溝通、參與國際會議的聽力、口說等即時應對，就要靠平時累積，才能溝通無礙，也才有後續洽談合作的可能。期許未來學弟妹們除了強化對於科技犯罪偵辦的專業訓練外，也能厚植語言能力，在這個犯罪沒有國界、地球是平的的時代，透過參與國際會議、司法互助等各式國際交流，讓世界看見臺灣檢察官的專業與打擊犯罪的決心。

捌、 附錄：哈佛見聞

一、 訪問學者報告（第一次）

期間：111 年 8 月 25 日至 12 月 11 日

（一） 前言

1. 109 年間之訪問學者申請：

筆者前於民國 109 年間經臺灣臺北地方檢察署檢察長之首肯，同意筆者向法務部申請赴外國法學院進修，同年 3 月間獲法務部選派至美國哈佛大學擔任訪問學者，旋向哈佛大學博克曼網際網路與社會研究中心(Berkman Klein Center For Internet & Society，下稱博克曼中心)遞交申請文件後，於 109 年 5 月間收到該中心之核准信函，同意筆者於 109 年 9 月 1 日至 110 年 8 月 31 日間至該中心擔任訪問學者，惟亦說明：因新冠肺炎（COVID- 19）疫情嚴峻，故哈佛大學校內之課程、活動多無法以實體方式進行，而改以視訊方式行之等語，於此之際，筆者慮及疫情仍屬嚴峻，乃進一步詢問博克曼中心是否能保留筆者之訪問學者資格至下一年度，惟博克曼中心說明：因訪問學者係採逐年申請、審核，故無法保留資格等語，筆者在考量赴美研究如僅能以視訊方式為之，恐影響研究之實益及效果，且慮及全球疫情嚴重，哈佛大學因而取消畢業典禮、該校校長亦染疫、全球口罩等防疫物資短缺等考量之下，僅能忍痛婉拒博克曼中心之邀約，而法務部亦考量疫情嚴峻，而同意讓該年度受法務部遴派之訪問學者得自行考量疫情狀況決定是否延緩計畫，筆者向法務部說明上開考量後，經法務部同意保留筆者之哈佛大學訪問學者資格至 110 年秋季入學。

2. 110 年度之訪問學者申請：

經漫長等待，且疫情似有稍稍趨緩之際，筆者於 110 年 2、3 月間準備再次向博克曼中心提出訪問學者之申請，然博克曼中心於 110 年 3 月 3 日

於其網站上公告略以：本中心暫停招收 2021-2022 年度之訪問學者，以因應現實狀況。本中心將調整並精進訪問學者計畫，並待未來校園生活狀態更明朗時，重新開放申請等語。筆者為求確認，進一步詢問博克曼中心執行長 Urs Gasser 先生及承辦人 Rebecca Tabasky 女士，經其等回信稱：很遺憾，因疫情之故，本中心做了困難之決定，將於下一年度暫停招收訪問學者，預計於 2022-2023 年重新開放等語。是筆者因學校政策因素而無從向該校申請訪問學者，嗣經法務部再度首肯保留筆者之訪問學者資格至 111 年度秋季。

3. **111 年度之訪問學者申請：**

又經過一年之漫長等待，博克曼中心重新開放訪問學者之申請，筆者再度遞交申請，於 111 年 5 月 12 日獲得該中心之回信，審核通過筆者之訪問學者申請，邀請筆者於 2022 年 9 月 1 日至 2023 年 8 月 31 日間至該中心擔任訪問學者，博克曼中心在歷經二年間的疫情影響而採線上交流後，終於即將重新開放實體交流，且在新的學術年度，博克曼中心亦重新調整其研究框架及精進相關計畫，該中心之原執主任 Urs Gasser 先生因至德國任教職[178]，而由 Sue Hendrickson 女士[179]接任該中心執行主任。筆者在睽違二年後，終於在 111 年 8 月間出發赴美，前往哈佛大學。

（二） 哈佛大學博克曼中心簡介

1. **緣起：**

自 1996 年哈佛大學法學院教授 Charles Nesson 與教授 Jonathan Zittrain 創立「法律與科技研究中心（Center on Law and Technology）」後，該中心即致力於電腦網際網路尖端議題研究。嗣於 1997 年， Berkman 家

[178] https://cyber.harvard.edu/story/2021-04/urs-gasser-embark-new-role-across-atlantic
[179] https://cyber.harvard.edu/story/2021-12/berkman-klein-center-welcomes-susan-hendrickson-executive-director

族捐贈美金 540 萬元予該中心以支持其研究，為茲紀念，該中心於 1998 年更名為：哈佛法學院博克曼電腦網際網路及社會研究中心（the Berkman Center for Internet & Society at Harvard Law School），並沿用迄今。博克曼中心之宗旨是在探索、認知電腦網際網路，包括其發展、動態、規範及標準，研究因電腦網際網路發展衍生之法律問題，進而分享其研究成果。該中心對於電腦網際網路相關議題研究，成果斐然，堪稱執世界之牛耳。具體地說，該中心目前進行研究之領域為教育及數位人文、AI 倫理與治理、科技及網路治理、網路健康、媒體、民主及公共揭露、網路隱私、科技與法律等重要議題。該中心創立迄今，曾至該中心研究之來自 40 餘國之訪問學者、研究人員、教職員等業超過 500 名，同時並有法學院學生參與相關計畫之實習。

2. **重啟社群媒體研究計畫（The Institute for Rebooting Social Media）：**

在面對疫情嚴峻之二年後，博克曼中心開設了為期三年之「重啟社群媒體研究計畫」，並針對該主題招募訪問學者，目的在於加速指出目前社群媒體最迫切面對之問題，包含假訊息（misinformation）、隱私洩露（privacy breaches）、網路騷擾（harassment）、及網路內容治理（content governance），藉由召集從業界、政府部門、私人團體及學術團體共同聚焦、研究，期能增進數位社群空間之狀態。

（三） 參與之講座、活動及報告

1. **博克曼中心之訪問學者討論**

迎新週：博克曼中心於 111 年 9 月 6 日起，舉辦為期一週之迎新週，因應美國疫苗施打率已高，且疫情趨緩之際，該中心於長達二年之視訊線上活動後，首次舉辦之實體活動，且今年適逢該中心成立 25 週年，故此次迎新週活動別具意義。除了今年度之訪問學者外，亦邀請以前年度之訪問學者「回娘家」共襄盛舉，除了讓訪問學者間可彼此認識交流外，亦可分

享彼此之近期研究議題及心得。期間討論網路巨頭之商業與人權、政府監控網路與資料之儲存、調取、社群媒體之現況等議題，其中令筆者頗感興趣者為「文化謙卑」（Cultural Humility）之主題討論，其義包含自我探索、批判，尊重他人之信仰、習慣及價值，並向他人學習之過程。經由上開主題討論亦令筆者對於該中心之多元、開放留下深刻印象。

訪問學者報告：於迎新週之後，訪問學者固定每週均舉辦小型研究會，會內可自由發表與網路相關之研究主題，進而讓訪問學者間可彼此討論學習。筆者於第二週即進行發表，主題為「社群媒體之詐欺案例」（Social media scam case），介紹筆者前實際偵辦之網路愛情詐騙（Romance scam）案例（簡報檔詳見附件「Social Media Scam Case」），詐欺集團藉由 facebook 搭訕被害人並與之培養感情後，指示被害人將款項經由比特幣 ATM 轉為比特幣而發送至詐欺集團控制之錢包地址。筆者向與會者說明臺灣在追查方面之困境，例如：社群媒體資料調閱時間限制、隱私保障及調閱資料之法律基礎、科技公司多設置於境外等因素，另在防制詐欺方面，對於社群媒體假帳號之偵測、詐欺案例之宣導及其他社群媒體本身之防制措施等面向，亦引起熱烈之討論。此外，對於端對端加密（End-to-end encryption，縮寫：E2EE）之通訊軟體之資料無法調閱，可能對於公共利益、犯罪追查上帶來困境乙節，亦有所討論，根據筆者研究，最著名之案例即為「Signal」，Signal 是由 Signal 技術基金會和 Signal Messenger LLC 開發的跨平台加密訊息服務。Signal 經網際網路傳送一對一及群組訊息，因為採用端對端加密之技術，故 Signal 通訊軟體之伺服器並不留存用戶之對話訊息、群組名單、聯絡人、貼圖、暱稱等資訊，而僅僅留存帳號設立時間及最後使用時間，是自 2016 年起，美國執法機關為偵辦刑事案件，而陸續依據聯邦大陪審團調取紀錄之傳票（Grand jury subpoena）、搜索票（Search warrant）、法院命令（court order）等向 Signal Messenger LLC 調取

用戶資訊，惟均遭其以 Signal 使用端對端加密技術且未留存用戶資料為由，而無從提供[180]。而對於端對端加密之人民隱私需求，及犯罪調查之公共利益兩端如何權衡，實屬兩難，為了突破端對端加密技術之犯罪偵查困境，美國司法部亦表示：科技公司應在其加密產品和服務的設計中加入機制，使政府能夠以適當的法律授權行事，可從該加密通訊中讀取可閱讀及可用格式的數據[181]。惟此一提議受各科技公司及人權團體以侵害隱私及人權為由而大力反對，究竟人權保障及公共利益如何取捨，有待持續關注及不斷地公共辯論，期能找到平衡點。

在動盪時代下之社群媒體治理：於 2022 年 11 月 14 日，博克曼中心邀請 META 公司負責內容政策之副總裁 Monika Bickert 女士，在哈佛法學院奧斯汀大樓[182]（Austin Hall）進行對談，針對社群媒體如何因應各國政府對於言論內容之管制及兼顧言論自由之保護等重大議題進行討論，當數位時代訊息傳遞快速、方便，假訊息或不法內容亦藉由社群媒體快速傳遞，甚至影響公共利益，在各國政府紛紛立法要求臉書等社群媒體下架涉及假訊息或不法內容言論之際，臉書為求兼顧尊重各國政府之法規及訊息之公開透明，在依各國政府法規下架不法內容之言論時，同時會在頁面標註下架內容之原因及法律依據。另在新冠肺炎疫情期間亦有諸多關於疫情之不實訊息流竄，臉書之因應作法係透過 AI 辨識訊息，如偵測到該等訊息為有關新冠肺炎者，則當用戶欲轉傳連結時，會自動跳出警語，提醒用戶該訊息內容涉及新冠肺炎，並偵測其來源及製作時間，讓用戶選擇繼續轉傳或是放棄轉傳，使用戶有更多時間思考是否轉傳及內容來源之正確性。雖然

[180] https://signal.org/bigbrother/
[181] https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety
[182] 奧斯汀大樓建於 1881 年，為美國知名建築師 Henry Hobson Richardson 所設計，外型為歐洲中世紀一種以半圓拱為特徵的建築風格，稱為羅馬式建築，係哈佛大學法學院首座專用之授課大樓，亦為美國法學院首座專用授課大樓，可參：https://en.wikipedia.org/wiki/Austin_Hall_(Harvard_University)

Monika Bickert 女士亦表示 AI 偵測之正確性非百分之百，但仍可見 META 公司對於使用科技防制假訊息之努力。

2. **哈佛大學甘迺迪學院（John F. Kennedy School of Government, Harvard Kennedy School,或 HKS）之系列講座：**

由於筆者之研究主題為「打擊網路犯罪法制及國際合作之研究」，而現今網路犯罪中涉及虛擬貨幣者日益增加，故虛擬貨幣議題對於網路犯罪之研究者誠屬不可忽略。筆者前偵辦多起虛擬貨幣相關犯罪案件，因而對於區塊鏈基本原理、虛擬貨幣之追查技巧、扣押、監管趨勢、交易所資料調閱等花費諸多時間研究，而哈佛甘迺迪學院對於虛擬貨幣、區塊鏈、web3.0 等議題開設系列講座，筆者就參加心得簡要記錄如下。

第一場之主題為「Congress and Crypto: What Happens Now?」（議會與虛擬貨幣：現在發生了什麼事?），主講者為哈佛大學法學教授 Howell E. Jackson 及甘迺迪學院 M-RCBG 數位資產政策計畫主任 Timothy Massad，Timothy Massad 同時為前任美國商品期貨交易委員會（Commodity Futures Trading Commission）主席。此場講座從美國證券交易委員會（SEC）對於比特幣之性質認定談起，其認定基礎為美國最高法院所提出之「Howey Test」[183]之四項判準：(一)投資人出資、(二)出資於一共同事業、(三)投資人分享報酬、及(四) 報酬主要取決於發起人或第三人之努力。而比特幣之產生係基於區塊鏈「挖礦」機制而產生，不屬於投資契約，故非屬證券。然而其他基於在區塊鏈上佈署智能合約而產生之代幣（Token），因屬於由中心機構或公司發行，甚至可能進行 ICO（Initial Coin Offering）之募資程序，即有機會被認定為證券。如某虛擬貨幣經認定具有證券性質者，即歸由 SEC 所管轄，如不具有證券性質而具商品性質者，則可能歸由商品期貨交

[183] 關於 Securities and Exchange Commission v. W. J. Howey Co.，可參見：https://www.law.cornell.edu/supremecourt/text/328/293

易委員會所管。而在 2022 年 11 月間爆發世界知名虛擬貨幣交易所 FTX 破產事件，引發全球虛擬貨幣投資者及政府機關一片譁然，Timothy Massad 認為對於虛擬貨幣交易所（平台）需要有更強而有力之規範，包含更大的透明度、避免利益衝突、成立保護消費者基金等。

在我國，亦引發立委質疑政府未保障境外交易所在台用戶權益，就此，金管會表示：FTX 交易所係在境外，並非經本會核准設立的機構，相關商品也係在境外提供，投資人應自行評估風險。而 FTX 在日本設有子公司，在臺則無，日本及新加坡的相關監理措施也未及於境外交易所等語[184]。於 FTX 破產效應仍發酵之際，可以預期的是各國政府對於虛擬貨幣交易所之監管力道勢必加強，而加強虛擬貨幣交易所之監管力道，對於犯罪偵查而言應有所助益，蓋關於虛擬貨幣之流向調查，因為虛擬貨幣錢包地址有其匿名性，在經過公開帳本、公開資源或商用軟體之幣流追查過程，如查知該等虛擬貨幣流經中心化交易所者，極有可能透過向交易所調取資料，而查知與該錢包地址相關之人。然而，各國執法機關可能都面對同一難題，即虛擬貨幣交易所常選擇監管力度較低之國家註冊登記，甚或低調而未公開期註冊登記地，在此情形下，執法機關勢必面對跨境調取資料之難題，筆者雖曾於實際案件中有向境外交易所成功調取資料之經驗，然亦曾遭遇境外交易所以其登記在歐洲地區為由，要求筆者行司法互助或提供歐洲調查令，而使案件偵辦卡關。又就虛擬貨幣之查扣而言，因犯罪集團可輕易使用電子錢包程式移轉虛擬貨幣，如一律透過司法互助程序請求他國協助查扣該國虛擬貨幣交所之涉案虛擬貨幣者，則恐耗費時日，緩不濟急，是對於境外交易所之虛擬貨幣查扣，是否能透過建立如國際間之國家金融情報中心（Financial Intelligence Unit，簡稱：FIU）、「艾格蒙聯盟」[185]

184 https://www.fsc.gov.tw/ch/home.jsp?id=2&parentpath=0&mcustomize=news_view.jsp&dataserno=202211230002&dtable=News

185 https://egmontgroup.org/

或電腦緊急應變團隊（Computer Emergency Response Team，CERT[186]）等非正式之情資交換，即為現今網路犯罪、詐欺、洗錢等犯罪偵查之要務。

3. **哈佛大學法學院教授之面談**

William P. Alford 教授：其現為東亞法律研究計畫（East Asian Legal Studies Program）主任，對於臺灣、中國之法律及法制史有所鑽研，並關注身心障礙人士之法律保障，曾任國際特殊奧運（Lead Director and Chair of the Executive Committee of the Board of Directors of Special Olympics International）執行委員會主席，William P. Alford 教授為人客氣和藹，熱心提供筆者關於電腦犯罪領域有所涉獵之教授名單及聯絡方式，並推薦筆者可參加費正清中國研究中心（Fairbank Center for Chinese Studies）所舉辦之研討會[187]。

Alex Whiting 教授：其現為哈佛法學院之客座教授，目前是海牙科索沃專家檢察官辦公室[188]的副專家檢察官（Deputy Specialist Prosecutor at the Kosovo Specialist Prosecutor's office in The Hague.）。從 2010 年到 2013 年，他在位於海牙的國際刑事法院 (Office of the Prosecutor at the International Criminal Court，ICC) 檢察官辦公室工作。於 2002-2007 年，Alex Whiting 教授曾是海牙前南斯拉夫問題國際刑事法庭 (International

[186] 自 1988 年起，各國家和地區為因應網路犯罪興起，紛紛建立電腦緊急應變團隊，如日本的 JPCERT/CC、德國的 CERT-BUND、英國的 UKCERT、美國的 US-CERT。1990 年，應急回應與安全組論壇（FIRST）成立，到 2012 年 8 月初，該論壇已成為超過 57 個國家，264 個成員參與的國際性組織。而臺灣亦成立「台灣電腦網路危機處理暨協調中心」（Taiwan Computer Emergency Response Team，TWCERT），為提升臺灣整體資安防護能量，TWCERT/CC 在數位發展部指導下，推動企業資安事件通報協處、產品資安漏洞通報、惡意檔案檢測服務及舉辦資安推廣宣導活動等重點工作，並透過與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，提升國家整體資安聯防能量，共同維護臺灣整體網路安全。

[187]「費正清中國研究中心」（Fairbank Center for Chinese Studies）是哈佛大學成立的研究中心。該中心建於 1955 年，稱為「東亞研究中心」，第一任所為費正清。後來為了紀念費正清而改名為「費正清東亞研究中心」（Fairbank Center for East Asian Research）。在哈佛大學成立 Edwin O. Reischauer Institute of Japanese Studies 與韓國研究所後，該中心於 2007 年改名為「費正清中國研究中心」，以彰顯其中國研究的特長。該中心培養了眾多漢學研究人才，出版了大量的中國相關文獻，是美國漢學研究重鎮之一。可參：https://fairbank.fas.harvard.edu/about/history-of-the-fairbank-center/

[188] https://www.scp-ks.org/en

Criminal Tribunal for the Former Yugoslavia，ICTY) 的首席控方律師。在前往海牙前南斯拉夫問題國際法庭之前，他擔任了十年的美國聯邦檢察官，先是在華盛頓特區的民權司刑事科（Criminal Section of the Civil Rights Division）工作，然後在波士頓的美國檢察官辦公室工作，專注於有組織犯罪和貪腐案件。由於 Alex Whiting 教授一方面在哈佛法學院任教，一方面在海牙科索沃專家檢察官辦公室任職，故其需時常往返美國及荷蘭海牙，其向筆者分享海牙科索沃專家檢察官辦公室係為處理於 1998 年間，在科索沃境內所發生對科索沃或南斯拉夫公民所犯之反人類罪、戰爭罪而設。

Christopher T. Bavitz 教授：其現為博克曼中心下之網路法診所（Cyberlaw Clinic）管理主任，其專精於網路著作權法律議題，近期亦在博克曼中心講授 AI 生成作品可能引發之著作權法之問題，研究領域皆為最新之網路法律議題。Christopher T. Bavitz 教授給與筆者關於網路犯罪領域相關議題研究方向諸多建議。

4. **研究主題擇定**

法務部指派予筆者研究之題目「有關打擊網路犯罪法制及合作之研究」，此題目鍥合筆者之研究興趣，且筆者前也有處理網路犯罪、資安案件、網域扣押案件等實際經驗，復對於網路詐欺透過虛擬貨幣洗錢案件稍有心得，平時對於網路犯罪、科技偵查相關議題深感興趣，而網路犯罪之領域甚廣，可能之研究議題包含：暗網（Darkweb）偵查、網域扣押、「特洛伊之盾行動[189]」（英語：Operation Trojan Shield）、虛擬貨幣追查實務及跨境交易所資料調取、端對端加密通訊軟體之偵查困境與突破等偵查實務議

[189]「特洛伊之盾行動」（Operation Trojan Shield），係執法機關藉由特定通訊軟體商之配合，3 年來動員全球 17 個國家的 9000 名執法人員，監控在 100 個國家內 1 萬 2000 支手機傳送的 2700 萬則訊息，追蹤 300 多個組織犯罪集團的活動。於 2021 年 6 月間全球同步執法，逮捕黑幫幹部 800 多人，查獲 250 個軍火庫、8 噸古柯鹼、22 噸大麻，以及折合超過 4,800 萬美金（新台幣 13.3 億元）。可參：https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

題。此外，在國際法制方面，網路犯罪公約（Convention on Cybercrime (ETS No. 185)，又稱布達佩斯公約）於 2001 年在法國史特拉斯堡由簽約國簽署後，嗣於 2003 年 1 月 28 日增加「利用電腦系統犯種族主義或仇恨行為犯罪之附加議定書」（First Protocol on Xenophobia and Racism (ETS No. 189)），又於 2022 年增加「第二項附加議定書」（Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)），關於「第二項附加議定書」涉及國際間之強化合作及對於數位資訊之傳遞議題亦值介紹。

對於上開各項偵查實務、國際條約等議題均與網路犯罪相關，實值研究，惟範圍甚廣，故筆者目前刻蒐集並閱讀相關國外文獻、資料，並期報告方向與國內實務相關且能供國內偵查機關參考。

（四） 2022 年全美州檢察長會議-首都論壇

2022 年全美州檢察長會議定於 2022 年 12 月 6 日至 12 月 8 日在華盛頓特區舉辦，今年我國法務部受邀組團參加，筆者亦加入團隊前往協助並參與（如圖 20（會場照片））。除了在會議上協助翻譯外，亦陪同部內訪團至美國數執法機關、華盛頓特區檢察長辦公室參訪並交流意見。

圖 20（會場照片）

（五） 國內會議

參與臺灣高等檢察署舉辦之虛擬貨幣資料調閱與查扣相關問題研商會議：於美國東部時間 2022 年 12 月 5 日晚間 9 時起，參與上開會議，並於會前提供關於實際偵辦經驗中，境外虛擬貨幣交易所之資料調閱實際調閱成功情形，及協助彙整交易所聯絡方式、所需文件、格式、調閱情況，並於會中分享個人調閱過程之經驗。

二、 訪問學者報告（第二次）

期間：111 年 12 月 26 日至 111 年月 2 月 25 日

（一） 旁聽課程

1. 關於旁聽選課程序：

哈佛大學法學院開放給訪問學者旁聽課程，而旁聽課程需先填寫「旁聽申請單」（AUDIT PETITION[190]），送交該門課程之教授簽名同意後，將申請單交回哈佛大學法學院註冊辦公室（Office of Registrar），待審核通過後即可正式旁聽該課程。而申請之時程十分緊湊，2023 年之冬季學期申請期限至 1 月 4 日，秋季學期申請期限至 1 月 27 日，筆者冬季學期申請旁聽 Alex Whiting 教授[191]開設之「刑事程序法：偵查」（Criminal Procedure:

[190] https://hls.harvard.edu/wp-content/uploads/2022/08/Audit-Request-Form-AY2023.pdf （Last viewed 2/3/2023）

[191]

Alex Whiting

Visiting Professor of Law from Practice

2022-2023

Alex Whiting 教授前擔任美國聯邦檢察官十年，其後於 2002 年至 2007 年至前南斯拉夫問題國際刑事法庭 (International Criminal Tribunal for the Former Yugoslavia (ICTY))擔任檢察官。2010 年至

Investigations）課程；2023 年春季學期申請旁聽 Ioannis Kalpouzos 教授[192]開設之「國際刑事法」（International Criminal Law），及 Antonia M. Apps 教授[193]開設之「白領犯罪法律及程序」（White Collar Criminal Law and

2013 年在國際刑事法庭（International Criminal Court）擔任檢察官，現於海牙科索沃檢察官辦公室擔任副專家檢察官（Deputy Specialist Prosecutor at the Kosovo Specialist Prosecutor's office in The Hague），並同時於哈佛大學法學院擔任客座教授，詳細介紹可參見：https://hls.harvard.edu/faculty/alex-whiting/ （Last viewed: 2/3/2023）

192

Ioannis Kalpouzos 教授專精於國際公法、國際刑法、戰爭法、人權法等領域，近期專注研究新型武器科技與法律之議題，並為全球法律行動網路（Global Legal Action Network (GLAN)）之共同創辦人。詳細介紹可參見：https://hls.harvard.edu/faculty/ioannis-kalpouzos/ （Last viewed: 2/3/2023）

193

Antonia M. Apps 教授現為美國證券交易委員會紐約辦公室主任（Director of the New York Regional Office, Securities and Exchange Commission）。前為美國聯邦檢察官及全國認可之訴訟律師，對於刑事及民事訴訟均有深厚經驗，前曾於紐約南區檢察署刑事部擔任檢察官七年以上，處理諸多受到高度關注之證券詐欺及內線交易案件，包括：S.A.C. Capital Advisors, L.P 對沖基金之案件。其亦為證券及商品詐欺小組成員，負責調查重大經濟犯罪，包含：投資詐欺、會計詐欺、仲介詐欺、操縱市場、不動產抵押擔保證券（RMBS）及擔保債權憑證（CDOs）之衍生案件、洗錢案件等。其擔任律師職業期間，曾代表金融機構、公司參與規範執行之程序、白領犯罪調查、複雜之商業訴訟及內部調查。其具有超過 15 年之訴訟實務經驗，被認為是傑出、聰明又注重細節之律師，且在白領犯罪領域具有精準判斷及分析技巧之能力。詳細介紹可參見：https://hls.harvard.edu/faculty/antonia-m-apps/ （Last viewed: 2/3/2023）

Procedure）、Timothy Edgar 教授開設之「資訊安全及網路衝突之法律問題」（Legal Problems in Cybersecurity and Cyber Conflict）。

2. CANVAS 課程系統簡介：

哈佛大學設置 CANVAS 課程系統，提供學生可自該系統內查看已選修之課程名稱、課程綱要、上課教室、日期、課程教材、該課程之同學基本資訊、圖書館資源等，若教授有要公告之事項，亦會顯示在該系統內[194]，而要使用該系統必須先向校方申請「Harvard Key」帳號、密碼，並透過選修、旁聽申請，進入該系統後始能查看相關課程訊息，雖然關於此系統之申請、進入算是比較細節的事項，但對於有心選修上課的訪問學者而言，如果可以熟悉系統操作，則可更快進入學習狀況。以下就旁聽課程簡要記錄如下：

（二） 法學院「刑事程序法：偵查」

Criminal Procedure: Investigations 此堂課開設在冬季學期，密集於星期一至五每日上午 9 點至 12 點半上課，上課教室位於哈佛法學院奧斯汀樓

194 CANVAS 系統頁面如下：

（Austin Hall，建於 1882 年，乃哈佛法學院最古老的建築[195]）。此堂課程之指定教材為：R. Allen, J. Hoffman, D. Livingston, A. Leipold, and T. Meares, Criminal Procedure, Investigation and Right to Counsel (4th ed. 2020)，Alex Whiting 教授以其豐富之聯邦檢察官之經歷，從美國憲法第四修正案[196]、第五修正案及最高法院諸多判例為基礎，討論基於保障人民之財產權、隱私權，原則上須具備合理懷疑（probable cause），且取得法院核發之搜索票，始得進行搜索，但美國最高法院亦建構出諸多例外。

195

196 The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

課堂上[197]除了傳統的搜索外，亦討論到現今網路數位時代中，對於數位證據之蒐集該如何適用傳統之刑事程序法理論，例如美國國會與美國前總統川普（Donald Trump）在 2018 通過了可釐清海外資料存取的雲端法案（Clarifying Lawful Overseas Use of Data Act or the CLOUD Act[198]），該案肇因於美國司法部於 2013 年時因調查一起運毒案件取得了法院的搜索票，要求微軟提供存放於愛爾蘭伺服器上的客戶資料，而微軟則提出上訴，認為美國沒有權力漠視其他國家的主權而強制存取放在他國的資料。Cloud Act 允許美國執法機關向法院申請存取美國業者「境外資料」的合法權力，但業者同樣可以根據境外國家的隱私法令來挑戰這些搜索票；此外，美國政府亦可與其他國家達成雙邊協議，以互相存取置放於彼此國家的資料。時任美國司法部長 Bill Barr 與英國內政大臣 Priti Patel，在 2019 年 10 月 3 日簽

197 實際上課情形：

198 https://www.congress.gov/bill/115th-congress/house-bill/4943

署了全球首個雲端法案協議[199]，將使得雙方的執法機構在獲得適當授權的情況下，向對方的科技公司索取各種重大犯罪事件的電子資料，諸如恐怖主義、兒童性虐待及網路犯罪等。根據協議條款，在獲得適當的法院授權之下，執法部門可直接向對方國家的科技公司請求存取電子資料，將調取資料的時間縮短至幾周或幾天。而依以往之司法實務，就算是藉由司法互助（Mutual Legal Assistance）協議，也經常需要幾個月的時間才能取得資料，故上開基於雲端法案之協議，大大加速了執法機關調取電子記錄之速度。

在網路數位時代，電腦犯罪及其他各式犯罪，透過利用網路、科技的發達，已然無國界限制，以筆者實際偵辦網路犯罪之經驗來說，追查來源IP、電子郵件或諸多通訊軟體使用者資料是偵辦跨境電腦犯罪不可或缺的第一步，而諸多科技公司係屬境外公司，其用戶相關資料之儲存伺服器亦未必在該公司登記國，而可能在第三國，目前法務部雖業已與 Google、微軟、META（臉書）、LINE 等公司就關於資料調取部分有所協議，固對於案

199

協議全文可參見美國司法部網站：
https://www.justice.gov/ag/page/file/1207496/download#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes

件之偵辦有所助益，然 google 及 META（含 Instagram）部分，並未提供通訊內容（例如：Gmail 電子郵件內容、Google Play 消費內容、信用卡卡號、臉書私訊內容等）的選項，而僅分別提供用戶註冊資料及請求送達後往前回溯 90 日、30 日之登入 IP 記錄，如能擴及「通訊內容」[200]，則必能對於案件之偵辦極大助益。

美國實務上[201]，依據電子通訊隱私法（Electronic Communications Privacy Act，ECPA）Title 18, United States Code, Section 2701 to 2713[202]對於數位服務提供者之資料調取分為：A.基本註冊者資料（Basic subscriber information）、B.其他非內容相關資料（Other non-content information）、C.通訊內容資料（Content and precise location information）。

關於 B.及 C.之區別，以 Gmail 為例，電子郵件之主旨及內容屬於「通訊內容資料」，而 Email headers，包含信件日期、時間、寄件、收件地址即屬於「他非內容相關資料」。上述 C.「通訊內容資料」之調取門檻最高，需執法機關或檢察官向治安法官（Magistrate Judge）證明該用戶之資料具有相當理由（Probable Cause）係與犯罪有關，於取得法院令狀後，始得調取。

上述 A.「基本註冊者資料」包含：客戶姓名、地址、電子郵件地址、電話號碼、通話記錄（Historical call logs）、使用服務類型及期間、註冊時之 IP 及近期之登入、登出之 IP、帳單及付款記錄。執法機關欲調取此類資料，可直接發電子郵件或者發出大陪審團傳票（Grant Jury Subpeona）向業者調取，而無須經過法院許可，但實務上業者依法[203]會通知該用戶有執法

[200] 惟關於通訊內容之調取，一般而言需要向法院聲請搜索票，並經司法互助程序為之。
[201] 以下說明整理自美國司法部電腦犯罪及資產犯罪組 (Criminal Division's Computer Crime and Intellectual Property Section, CCIPS)資深顧問 Ryan Dickey 於 111 年 5 月 11 日之視訊演講及簡報檔（刑事局邀請美國國土安全調查署(HSI)111 年 5 月 11、12 日網路犯罪偵查線上訓練）。
[202] https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121
[203] 18 U.S. Code § 2703 - Required disclosure of customer communications or records.

機關調取該用戶資料[204]。上述 B.「其他非內容相關資料」之調取雖然需要向法院申請令狀，但證明門檻明顯低於 C.「通訊內容資料」。

關鍵字搜索票（Keyword warrant）之爭議[205]：於 2020 年 8 月 5 日在科羅拉多州丹佛市（Denver）發生了一起造成五人死亡的縱火案件，警方為尋找犯罪嫌疑人之身分，向法院聲請「關鍵字搜索票」：亦即透過向 Google 公司請其提供用戶之網路搜尋記錄，用以過濾並發現在縱火案發生前一定時間內，有哪一些用戶曾透過 Google 搜尋功能以「縱火地址」為關鍵字搜尋。法院最後核發關鍵字搜索票，警方持之向 Google 公司調取相關記錄，幫助警方過濾並特定三名青少年為嫌疑人。在此引發之法律爭議為：此「關鍵字搜索票」係由 Google 公司從大規模的用戶資料中過濾出相關用戶，而過濾出的用戶不一定就是犯罪嫌疑人，尚包含其他單純以該關鍵字搜尋而不涉及犯罪之用戶，這樣的搜索票聲請是否符合「相當理由」（probable cause）及「特定」（particularity）之憲法第四修正案的要求[206]？其中一名嫌疑人之律師主張：上開關鍵字搜索票係屬大規模的釣魚搜尋（a massive fishing expedition）侵害了成千上萬不相關人民的權利及隱私，故主張上開證據係屬非法取得，應予排除。然丹佛地方法院法官 Martin Egelhoff 否決了上開主張，其說明：上開搜索可類比於從一堆乾稻草中尋找一根針，雖然乾稻草可能很龐大，且其內含有諸多資訊，但不代表在該乾

[204] 一般而言，而法機關多不希望業者通知用戶，因為該用戶本身是犯罪嫌疑人，若經業者通知，則可能會影響偵辦計畫，在此情形下，美國執法機關可向法院申請法院命令（Court Oder: Nondisclosure Oder），禁止業者通知用戶。

[205] https://www.theverge.com/2022/7/1/23191406/denver-arson-google-keyword-warrant-challenge-constitutional-fourth-amendment-privacy

[206] 參見哈佛大學法學期刊：Geofence Warrants and the Fourth Amendment, 134 Harv. L. Rev. 2508, MAY 10, 2021. (https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment/)

草堆中搜尋特定目標即意味著有違「過寬限制原則」[207]（overbreadth）。此案目前由科羅拉多州最高法院審理中，值得後續觀察。

此外，與關鍵字搜索票有關者，且為美國執法機關偵查案件常用的令狀為「地理圍欄搜索票」（Geo-fence warrant），要求科技公司提供特定期間內、在一定地理範圍內使用手機、平版、電腦等網路電子設備的用戶資訊（例如：用戶的 google 歷史定位資料、GPS、藍芽、上網 IP、基地台位置、WIFI 強度等），Google 公司從 2016 年起即開始提供美國執法機關上開資料，且年年增長[208]。此種搜索票常用於群眾犯罪或其他需要特定犯罪嫌疑人身分之用途。在我國偵查實務上，亦曾有因偵辦重大運輸、販賣毒品案件，為追查某經過某地點之不明嫌疑人之身分，而由檢察官依據通訊保障及監察法第 11 條之 1 第 3 項之規定依職權調取通信記錄，由電信公司提供某特定時段內，某地點可連接到之基地台之所有門號通話及上網紀錄，再從中過濾之。雖調取之對象並非科技公司，而係電信公司，然二者均有調取範圍廣泛及對象不明確之疑慮，就此法律疑慮，宜盡早深入研究並研擬說帖意見，以因應未來可能會產生之法律質疑。

與我國制度之比較思考：我國對於科技公司或電子資訊儲存單位之資料調取，似無如上所述美國執法機關使用「地理圍欄搜索票」之經驗，如未來偵辦案件上，有需要對於境外科技公司調取用戶的歷史定位資料、GPS、藍芽、上網 IP、基地台位置、WIFI 強度等資料，因目前諸如 Google、Meta 等公司並未提供我國檢察官或執法機關上開資料，可研擬其

---

207 “I liken this search to looking for a needle in a haystack,” he said. “… And the fact that the haystack may be big, the fact the haystack may have a lot of information in it, doesn’t mean a targeted search in that haystack somehow implicates overbreadth.” See: https://www.techdirt.com/2023/02/03/colorado-supreme-court-to-hear-challenge-of-reverse-keyword-warrant-served-to-google/

208 於 2018 年間，美國執法機關共向 Google 公司發出 941 個請求，2020 年間增長至 11033 個請求。請見：https://www.wired.com/story/geofence-warrants-google/ 。又除了 Google 公司外，Apple、 微軟、Uber、Lyft（美國常見的計程車叫車服務，類似於 Uber）都有收過美國執法機關對其等提出之 Geo-fence warrant。

法律依據（例如:刑事訴訟法第 133 條、第 136 條、第 138 條）、法律程序（是否需搜索票？調取票？檢察官許可？），如遇該等公司拒絕，有何手段因應？如需進行司法互助程序，其相關程序、實例、例稿為何等議題，亦值進一步思考。

（三） 法學院「國際刑法」

本課程（International Criminal Law）介紹並討論國際法律系統如何面對並處理國際重大犯罪，聚焦於：國際刑法與國際法之關係、種族滅絕罪（Genocide）、危害人類罪（crimes against humanity）、戰爭罪（war crimes）、侵略罪（the crime of aggression）、國際刑法之加害者與被害人、國際刑事法院對於內國法及國際刑事司法管轄及執行等議題。

（四） 法學院 2023 年春季工作坊

「重塑金錢：中央銀行、虛擬貨幣及經濟的力量」（Reinventing Money: Central Banks, Cryptocurrency, and the Power of Finance）：此系列工作坊將從 2 月初持續進行至 3 月底，上課地點在法學院 Hauser 大樓[209] 102

209

教室，此工作坊係由哈佛大學法院博士候選人 Dan Rohde[210]所發起，內容探討身處在金融創新的時代，近期發生二起重大金融事件（UST 脫鉤及 FTX 事件），數位支付及個人化的科技發展創新令我們重新思考：我們創造錢的過程及及使用錢的方式！關於金融（含虛擬貨幣），人民對於政府開始有了新的要求，而中央銀行也重新思考其任務[211]，尤其是關於氣候變遷及綠色

210

Dan Rohde
S.J.D. Candidate
drohde at sjd.law.harvard.edu

Dissertation

A Legal History of the Bank of Canada, 1934-1967

211 我國中央銀行總裁楊金龍表示：基於促進普惠金融、維護央行在支付體系之角色、因應數位支付未來趨勢，我國央行亦開始研究、試驗行「央行數位貨幣」(Central Bank Digital Currency，CBDC)，研究階段有四：技術研究階段、試驗階段、先導計畫試點階段、全面上線階段，目前央行業於 111 年 6 月間完成第二階段之試驗。可參見：楊金龍，央行貨幣的支付功能與 CBDC 的發行（https://www.cbc.gov.tw/tw/dl-177989-65adf5960c2b4e26902bd881570e68c8.html ）

經濟（green finance）。此工作坊從錢的歷史為起點，探討當代的貨幣改革及央行數位貨幣政策[212]。

[212] 課表如下：

Workshop Schedule - All Sessions are Wednesdays at 1:30-3:30pm

1	Feb 8, 2023 - 1:30-3:30	What is Money? (And Why Should You Care?)

Part 1 - Reinventing Money Then

2	Feb 15, 2023 - 1:30-3:30	Government Money: Money as a Colonial Project
3	Feb 22, 2023 - 1:30-3:30	Private Money: The Invention & Politics of Commercial Banks
4	Mar 1, 2023 - 1:30-3:30	"Independent" Money: The Invention of Commercial Banks

Part 2 - Reinventing Money Now

5	Mar 8, 2023 - 1:30-3:30	Reinventing Public Money: CBDCs, E-CASH and Postal Banking
6	Mar 22, 2023 - 1:30-3:30	Reinventing Private Money: Cryptocurrency
7	Mar 29, 2023 - 1:30-3:30	Reinventing Central Banks: Central Bank Independence and Green Finance

（五） Berkman Klein Center 訪問學者交流[213]

Berkman Klein Center[214]於 2023 年 2 月 16 日特別邀請哈佛大學法學院教授 Charles Nesson 跟訪問學者們分享其對於陪審制度的體悟。Charles

[213] 筆者目前即在 Berkman Klein Center 擔任訪問學者，該中心亦將筆者之經歷及照片刊登於官網上（https://cyber.harvard.edu/people/wayne-lo ）：

Wayne Lo

AFFILIATE

SHARE TO

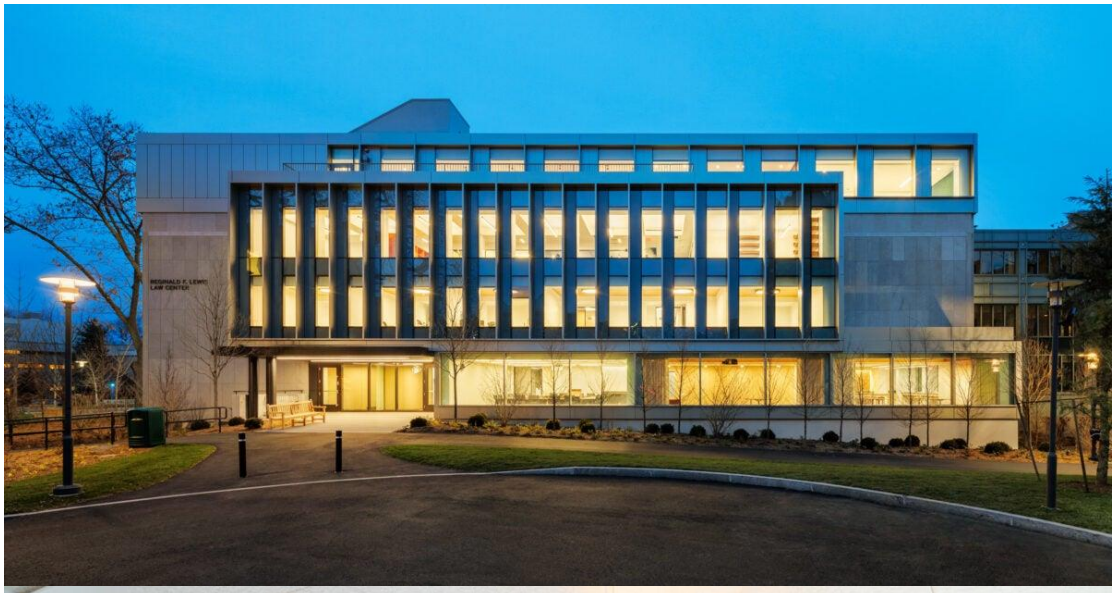
TECHNOLOGY & THE LAW | JUSTICE, EQUITY, & INCLUSION | MEDIA, DEMOCRACY, & PUBLIC DISCOURSE

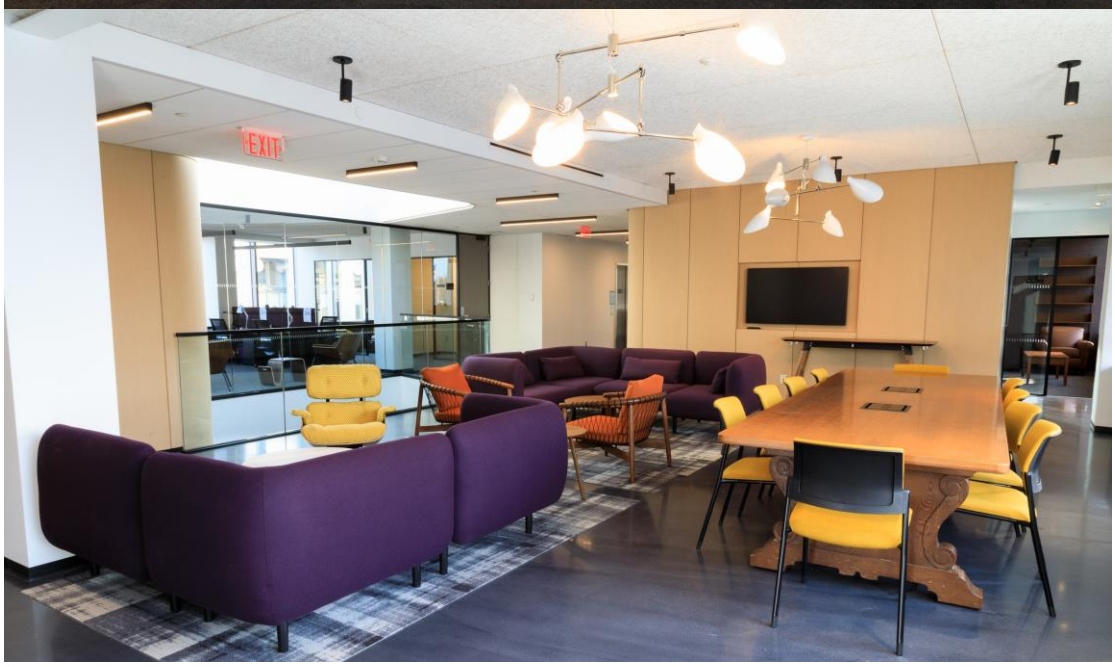
EMAIL

Wayne (Wei-Yuan) Lo is currently a Taiwanese public prosecutor at Taipei District Prosecutors Office and has been a prosecutor for 11 years. Wayne specializes in cyber crimes, cryptocurrency crimes, money laundering crimes, and telecom fraud. Nowadays, when criminal groups have cooperated across the border, the law enforcement agencies need to work together tighter. So Wayne also helps the Ministry of Justice of Taiwan to deal with mutual legal assistance cases to practice international cooperation.

[214] Berkman Klein Center 於 2022 年下旬從舊址（23 Everett Street）遷入位於法學院院區的 Lewis International Law Center building（Lewis Hall）的 4 樓及 5 樓，嶄新及寬敞明亮的空間，讓訪問學者齊聚一堂交流學術，照片如下：

Nesson 教授現年 84 歲，係美國知名法學教授，在法學院教授美國陪審制度（the American Jury），其亦係 Berkman Klein Center 於 1997 年之創始人之一[215]。Charles Nesson 說明陪審團制度之精神即在於對國家機構的不信任，而將刑事案件之判斷交由來自四面八方的人民，透過不同的一般人民的智慧激盪出正確的判斷。筆者也特別跟 Charles Nesson 說明臺灣於今年正式實施國民參審制度，雖與美國的陪審制有異，但已是納入一般人民與





215 https://hls.harvard.edu/faculty/charles-r-nesson/

職業法官一同做出事實認定之判斷，期待能做出更正確的判斷，實現司法正義。筆者於交流後在會場內與 Charles Nesson 教授合照留念[216]。

（六） 哈佛大學甘迺迪學院[217]

（John F. Kennedy School of Government, Harvard Kennedy School, 或 HKS）課程、講座：除了法學院以外，筆者較常參與的課程係哈佛大學甘迺迪學院所開設之課程及講座，茲就所參加之課程分述如下：

[216]

[217]約翰·F·甘迺迪政府學院（John F. Kennedy School of Government, Harvard Kennedy School, 或 HKS）是世界頂尖的公共政策學校，也是美國哈佛大學的研究所之一。學院可授公共政策、公

1. Belfer Center for Science and International Affairs

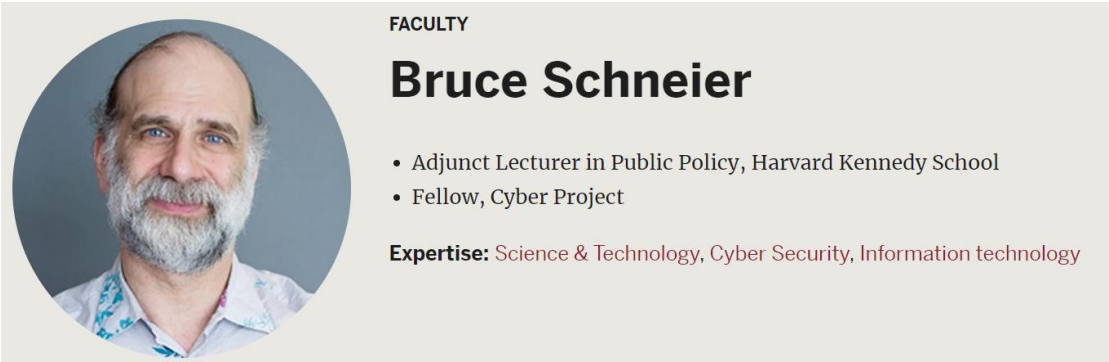
Belfer Center 之任務為對於現今國際安全、科學、技術、環境政策及國際事務等交錯議題，增進政策相關知識，並就上開議題研究、教學及提供訓練[218]。該中心於本學年邀請諸多 AI 人工智慧之研究者舉辦系列研討會，因筆者此行研究主題為網路犯罪相關，故參加該中心於秋季學期關於 AI 議題之系列研討會（AI Cyber Lunch Series：Explores AI and Algorithm Regulations and Practices[219]），其中 AI 及密碼學專家 Bruce Schneier 教授[220]發

共管理和國際發展等學位，也進行各種與政治和政府有關的研究。實際建築外觀如下：

218 https://worldwide.harvard.edu/belfer-center-science-and-international-affairs-0

219 https://www.belfercenter.org/publication/series-explores-ai-and-algorithm-regulations-and-practices

220



表之主題「AI 駭客來了」（The Coming AI Hackers），討論當 AI 系統學習如何駭入人類的經濟、社會及政治體系，我們應如何因應等諸多先進有趣之議題[221]。另電子隱私資訊中心副主任（Deputy Director at the Electronic Privacy Information Center）Caitriona Fitzgerald[222]則發表「AI 規範之現況」（The State of AI Regulation）。目前春季研討會仍持續進行中[223]。

2. Mossavar-Rahmani Center for Business and Government

Mossavar-Rahmani Center 致力研究於現今世界面臨的重大挑戰並分析政策，其視野涵蓋從在地問題到全球性問題[224]。該中心針對虛擬貨幣及 WEB3.0、區塊鏈等議題舉辦系列講座，因現今網路犯罪與虛擬貨幣相關犯罪密不可分，且筆者對於虛擬貨幣之犯罪偵查、政策研擬之相關議題持續關注，故筆者亦持續參與該系列講座，包含：「國會與虛擬貨幣：現在發生了什麼事？」（Congress and Crypto: What Happens Now?[225]），由美國期貨及商品交易委員會（Commodity Futures Trading Commission）前主席 Timothy

Bruce 教授與筆者同為 BKC 之一員，其為人十分機智、幽默及熱情，筆者在美期間適逢教授搬新家，教授也邀約筆者至其新家吃飯。

221 https://www.belfercenter.org/event/ai-cyber-lunch-bruce-schneier-coming-ai-hackers

222

223 相關議題及主講人可參見：https://www.belfercenter.org/program/science-technology-and-public-policy#!ai-cyber-lunch-series

224 https://www.hks.harvard.edu/centers/mrcbg/about/mission-history

225 https://www.youtube.com/watch?v=wglUgr-EqNk&t=1084s

Massad[226]介紹美國對於虛擬貨幣之定性爭議（證券、商品、期貨？）、主管機關之路線之爭（SEC？CFTC？）相關議題，此議題在美國目前爭激烈討論中，未有定案，而在 LUNA UST（號稱算法穩定幣）發生嚴重脫鉤及 FTX 交易所爆發危機後，唯一有共識者係虛擬貨幣應加強監管，又因虛擬貨幣之流動係屬全球性，我國國人雖在臺灣，但亦可在境外交易所、去中心化交易所等購買、投資、質押虛擬貨幣，造成監管難題，而犯罪者利用上開特性，直接騙取虛擬貨幣，或將不法所得轉化為虛擬貨幣再轉至境外交易所，造成偵查困難，國內亦有立法委員要求應設置專責主管機關之倡議，站在犯罪防制、追查、投資人保障之角度，確實宜訂立規範監管，且宜參考國際上之規範模式[227]，例如：FATF 之指引、歐盟加密資產市場監管法（草）案（The Markets in Crypto-assets Regulation，MiCA[228]）、美國立法討論趨勢等，訂立與國際潮流一致或相近之標準，俾利於日後之國際合作、資訊交換、甚至是簽署相關協議。其他議題包含：「元宇宙：新東西，但是

226

Congress and Crypto: What Happens Now?

Harvard Law School Professor Howell Jackson and Timothy Massad, Director of the M-RCBG Digital Assets Policy Project and former chairman of the Commodity Futures Trading Commission, discussed the current state of crypto regulation and the various ways that Congress is considering changing it. Will Congress

227 誠然，站在法務部或檢察官之立場，係著眼在犯罪偵查，故提升虛擬貨幣偵辦之知識及實務經驗乃屬第一要務。而虛擬貨幣（含虛擬貨幣交易所）之監管業務，似較與金融、證券、期貨、銀行相關，然因犯罪集團近年從事詐騙、洗錢及各式犯罪過程中使用虛擬貨幣之案例日增，如能有較完善之監管法規，則對於後續之犯罪偵辦亦能有幫助。至於監管機關係定一單一機關，或者區分不同功能、取向而分散式由不同機關依其職能負責，則屬仁智互見，惟一旦設立監管機關，則相對應之人力資源、對虛擬貨幣之基礎知識、教育訓練等則必須補足，否則形式上定監管機關、監管法規，如果人力資源不充足，亦無法達成效果。

228 https://blockcast.it/2023/01/02/how-will-mica-impact-the-web3-industry-in-europe/

讓老問題更嚴重」（The Metaverse: Cool New Stuff, Even Worse Old Problems[229]）、「最高法院接手 Section 230[230]」（The Supreme Court Takes Up）。Section 230 法案原本是要解決 ISP（網路服務提供）業者對於其用戶於網路上之（仇恨、色情、騷擾、假訊息等不法）言論需否負責之爭議，而以此法豁免 ISP 業者之民事責任，然時至今日，出現越來越多的網路平台業者、社群媒體等，諸如：Google、Youtube、Facebook、Instagram 等，其等並非傳統的 ISP 業者，其等是否負有何種注意義務？如果其等放任用戶刊登不法或不當言論，是否仍能引用上開法條作為豁免責任之依據，即生疑義，特別是美國上一次總統大選發生俄羅斯利用社群媒體散布假訊息欲影響選舉之事件後，此議題更受到關注及討論。又例如：Youtube 透過演算法而「推薦」用戶觀看之影片，如涉及不法訊息（例如散布恐怖主義），則 Youtube 是否仍能援引上開規定而主張豁免責任[231]？相關訴訟案件業經上訴至聯邦最高法院，最高法院將於 2023 年 2 月 21 日至 22 日舉行聽證程序及辯論，值得持續關注。又此議題與我國去年由 NCC 推出之數位服務中介法產生之爭議十分相關，雖然該法係屬行政管制，且引起網路平台業者以侵害言論自由為由反彈，但站在檢察官之立場，在現今數位網路時代，就刑事案件偵辦亦多會涉及向網路平台業者調取資料、請網路平台業者及時下架含有非法內容（例如：兒童色情、毒品等）之網頁，其實與檢方工作息息相關，亦值檢方研究關注。

229 https://www.youtube.com/watch?v=kkrfr7-hfdw

230 法條內容為：「電腦互動服務提供者或用戶，對於由他人提供之資訊，不應被認為是出版者或演講者」（原文："No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." (47 U.S.C. § 230(c)(1)).

231 https://www.brookings.edu/blog/techtank/2023/01/31/the-supreme-court-takes-up-section-230/

3.「進入 WEB 3:從零到發行虛擬代幣」

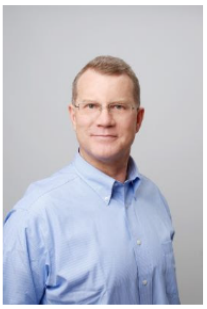
此課程（Intro to Web3--From Zero to Token Launch）係由甘迺迪學院邀請麻省理工學院（MIT）Steve Derezinski[232]講授區塊鏈、虛擬貨幣之基礎知識及原理，並手把手教學虛擬貨幣錢包移轉。Steve Derezinski 係在麻省理工學院數位研究室（MIT Media Lab）教授區塊鏈議題，且指導 MIT Bitcoin Club，為區塊鏈及虛擬貨幣領域之專家。於 2/9 課程講授去中心化自治組織（Decentralized Autonomous Organization，DAO）及實際發行虛擬代幣。雖然筆者對於虛擬貨幣犯罪偵辦有濃厚興趣並小有心得，於出國前也在國內各司法警察機關講授追查虛擬貨幣技巧，但參與此課程係從區塊鏈基礎知識出發，並涉及 DAO、「幣圈」發幣[233]、去中心化交易所等現今熱門議題，結合實務偵辦經驗及上開課程之技術面學習，令筆者收穫豐富。

三、 訪問學者報告（第三次）

期間：112 年 2 月 26 日至 5 月 25 日

因部裡指派予筆者之研究報告題目為：「打擊網路犯罪之法制與國際合作之研究」，故在此期間仍持續研究網路犯罪相關議題，在學校研究方面，

232



Steve Derezinski

Steve has taught Blockchain Ventures at MIT Media Lab, Babson and MIT Bitcoin club, and has been involved in Blockchains since 2016. The workshop is based on the semester-long classes he taught. He has an S.B. in mechanical engineering from MIT and an MBA from Sloan.

233 實務上亦可能涉及違反銀行法非法吸金或詐欺等案件。

筆者在 2023 年春季學期申請旁聽「網路安全及網路衝突之法律問題」（Legal Problems in Cybersecurity and Cyber Conflict），參加甘迺迪學院舉辦之「第四屆哈佛大學韓國安全高峰會：阻止北韓以竊取虛擬貨幣方式獲取歲入」（4th Korean Security Summit at Harvard: “Korea – An Oracle of Global Trends"：Curbing North Korea's Revenue Generation from Crypto Theft）。另筆者亦自費報名參加 2023 全美網路犯罪會議（2023 National Cyber Crime Conference），並取得完訓證明。此外，針對虛擬貨幣之追查技術，筆者亦取得受美國司法部採用、國際知名區塊鏈分析公司 TRM Labs 之專業認證。又因美國司法部於 2021 年 10 月間成立國家級的虛擬貨幣執法團隊（National Cryptocurrency Enforcement Team, NCET），筆者特別透過視訊會議，向該團隊中之司法部檢察官 C. Alden Pelker 請益關於虛擬貨幣追查、扣押之相關議題。茲將詳情分述如下：

（一） 哈佛大學之相關課程參與：

1. 法學院課程：「網路安全及網路衝突之法律問題」

此課程之教授為 Timothy H. Edgar[234]，其係前國家安全與情資、資安專家，曾於美國公民自由聯盟[235] (American Civil Liberties Union)任職。於 2009

234

Timothy Edgar

Lecturer on Law

Spring 2023

Download image

Timothy H. Edgar is a former national security and intelligence official, cybersecurity expert, privacy lawyer and civil liberties activist. He teaches at Brown University and Harvard Law School.

另關於 Timothy H. Edgar 教授之介紹，可參見：https://hls.harvard.edu/faculty/timothy-edgar/。

235 美國公民自由聯盟是一個美國的大型非營利組織，總部設於紐約市，其目的是為了「捍衛和維護美國憲法和其他法律賦予的、這個國度裡每個公民享有的個人的權利和自由」。聯盟透過訴訟、推動立法以及社區教育達到其目標。

年美國總統歐巴馬宣佈成立一個新的國家安全會議之職務「特別致力於保護美國人民之隱私及權利」，Timothy H. Edgar 教授亦經延攬而進入白宮工作，負責資安及人民隱私保護之議題。

此課程首先廣泛介紹當前世界面臨之網路議題，世界其實正在面臨網路戰爭，這種新型態的無煙硝的戰爭，站在美國國家政策的角度而言，應該著重於攻擊或者是防守？此外，關於網路犯罪，美國主要之規範係「電腦詐欺及濫用法案」（The Computer Fraud and Abuse Act ，CFAA），此法案主要是針對駭客行為，亦即未經授權或逾越權限而侵入電腦之行為，由於此法案之規範範圍極廣，除了傳統上之駭客行為外，亦有民間公司以之作為對付白帽駭客之工具（白帽駭客一般係指資訊安全研究者，透過各種網路技術，查找各大公司網路漏洞，並提報予該公司）。又部分國家甚至以國家之力培植「政府駭客」，例如北韓朴鎮赫（Park Jin Hyok）即為由北韓政府資助的名為“ Lazarus Group（或 APT 38） ”的駭客團隊的成員，並為北韓政府幌子公司 Chosun Expo Joint Venture（又名 Korea Expo Joint Venture）工作，以支持北韓政府的惡意網路行動。Chosun 隸屬於 Lab 110，後者是北韓軍事情報部門的一個部門。朴鎮赫被指參與了 2014 年入侵索尼影視娛樂公司（Sony Entertainment Pictures）的網路攻擊，及 2017 年的“Wannacry”網路駭客攻擊（加密被害人之電腦資料並勒索比特幣），該次攻擊令英國衛生服務電腦系統出現全國性癱瘓。上開案件業經美國司法部分別於 2018 年、2021 年 2 月間起訴朴鎮赫及其他共犯，起訴罪名包括：非法入侵電腦（computer fraud and abuse）、銀行詐欺、電匯詐欺（conspiracy to commit wire fraud and bank fraud）等罪嫌[236]。而美國掌管國

[236] https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and、https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and （最後瀏覽日期：05/25/2023）

家安全事務的助理司法部長約翰·德默斯（John Demers）在宣布起訴時表示：北韓傾國家之力扶植駭客而竊取數以百萬的資產，儼然成為一個打著犯罪旗幟的集團等語[237]。

除了上開議題外，就電磁紀錄之搜索與扣押、加密通訊軟體與科技之協助、資料外洩之相關法律責任、保險機制、資訊安全相關規範、關鍵基礎設施（critical infrastructure）與資訊分享之規範、美國聯邦貿易委員會（FTC）就資訊隱私之相關規範爭議等網路資訊安全重大議題，亦於課堂上有深入的介紹與討論。

據報載「臺灣近期多處頻傳的「炸（詐）彈恐嚇案」，警方經過警方清查 IP，發現都是來自境外，目前鎖定是一名中國籍張姓學生所為，這 2 年來他利用網路匿名寄出恐嚇信，多達上百封，造成我國警、調就勞師動眾調查，民眾也會恐慌，耗費多社會成本[238]。而 IP 追查及相關網路服務提供業者（ISP）如位於境外，除了可循海峽兩岸共同打擊犯罪及司法互助協議請求外國協助外，因為境外 ISP 業者之 IP 登錄資訊保存期限長短不一，為免證據遭刪除，世界上第一個針對打擊網路犯罪的公約「網路犯罪公約（Cyber-crime Convention）」[239]即應運而生，其中第二次增修條款（Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)）[240]，特別針對網路服務

---

[237] The regime has become a criminal syndicate with a flag, which harnesses its state resources to steal hundreds of millions of dollars.

[238] https://news.ltn.com.tw/news/politics/breakingnews/4305777 （最後瀏覽日期：05/25/2023）

[239] 於 2001 年 11 月由歐洲理事會的 26 個歐盟成員國以及美國、加拿大、日本和南非等 30 個國家的政府官員在布達佩斯所共同簽署的國際公約，自此《網路犯罪公約》成為全世界第一部針對網路犯罪行為所制訂的國際公約。而《網路犯罪公約》制定的目標之一是期望使國際間對於網路犯罪的立法有一致共同的參考標的，也希望國際間在進行網路犯罪偵查時有一個國際公約予以支持，而得以有效進行國際合作。另因該公約係在布達佩斯簽訂，故又稱布達佩斯公約。

[240] https://www.coe.int/en/web/cybercrime/second-additional-protocol

提供業者的相關資訊之請求協助程序予以明訂，甚至增加以電子傳輸請求之制度，供簽約國適用遵循，以突破網路犯罪證據之易消逝性。雖然我國尚非公約簽約國，然亦可於進行司法互助案件時參考該公約之機制精神，甚或依國際刑事司法互助法第 2 條之規定[241]，寬認該公約及增修條款為「其他相關法律」而適用之，以增進正式、非正式司法互助之效率。

G8 24/7 NCP （Network of Contact Points）Network：G8 高峰會以實際行動防制高科技犯罪議題，始於 1997 年發表的「八國司法部長會議公報」，其中揭示了 10 項行動方案，首要任務就是要求各國相互合作打擊網路犯罪，並應指派官方性質的全天候單一窗口，建立高科技犯罪執法情資之連繫管道。G8 所轄「高科技犯罪分項工作組」（Subgroup on High-Tech Crime）旋即在美國司法部刑事司「電腦犯罪暨智慧財產組」（簡稱 CCIPS）主導下，號召各國加入這個全名為「高科技犯罪執法情資聯絡窗口全天候聯防組織」（24/7 Network of High-Tech Crime National Points of Contact），至今已有 50 個會員國。我國於 2003 年 10 月透過美國司法部推薦，以臺灣名義正式加入，成為第 35 個會員國[242]（中國香港亦為會員

[241] 有關國際間之刑事司法互助事項，依條約；無條約或條約未規定者，依本法；本法未規定者，適用刑事訴訟法及其他相關法律之規定。

[242] 張紹斌、吳炳標，出席歐洲理事會網路犯罪公約委員會合作打擊網路犯罪國際研討會出國報告，第 27 頁至 31 頁。另據該報告所載，G8 24/7 聯防組織分別於 2004 年 3 月、2006 年 10 月，以「聯盟會議」名義舉辦兩次技能研習會（Training Conference），目的在增進會員間偵防網路犯罪之合作效率及辦案技巧，訓練對象以各會員國內承辦網路犯罪國際偵防合作業務之政府官員為限。法務部均派員參訓等語。經筆者查詢，法務部於 2006 年 10 月間，指派時任臺灣臺北地方檢察署檢察官朱應翔（現已離職）、時任法務部資訊處檢察官孫治遠參加「參加第二屆網路犯罪聯盟會議」，可參見：https://report.nat.gov.tw/ReportFront/ReportDetail/detail?sysId=C09600684 。惟自該次會議以後，該聯盟會議是否有持續邀請我國是參加、我國是否有指派檢察官參加等節，不得而知。筆者認為如能積極主動聯繫該聯盟，爭取參加相關會議之機會，並指派具有電腦網路專業及外語能力之檢察官與會，除了能提高臺灣能見度以外，對於跨境網路犯罪之合作偵辦，必能有所助益。

之一，中國至仍今未加入[243]）。而我國目前之窗口設於警政署刑事警察局科技研發科內之專責人員，經筆者瞭解，近年每年我國向他國透過此管道請求之數量甚少。

2. **甘迺迪學院部分：**

「第四屆哈佛大學韓國安全高峰會：阻止北韓以竊取虛擬貨幣方式獲取歲入」（4th Korean Security Summit at Harvard: “Korea – An Oracle of Global Trends"：Curbing North Korea's Revenue Generation from Crypto Theft[244]）。此高峰會的第三天特別邀請美國財政部海外資產控制辦公室（Office of

---

243 會員名單可參見美國 The Organization of American States 網站：https://www.oas.org/juridico/english/cyb_pry_G8_network.pdf

Members of the G8 24/7 Network (as of December 2007)

AUSTRIA	GERMANY	MALTA	RUSSIA
BELGIUM	HONG KONG, CHINA	MAURITIUS	SINGAPORE
BRAZIL	HUNGARY	MEXICO	SOUTH AFRICA
BULGARIA	INDIA	MOROCCO	SPAIN
CANADA	INDONESIA	NAMIBIA	SWEDEN
CHILE	ISRAEL	THE NETHERLANDS	TAIWAN
CROATIA	ITALY	NEW ZEALAND	THAILAND
CZECH REPUBLIC	JAMAICA	NIGERIA	TUNISIA
DENMARK	JAPAN	NORWAY	UNITED KINGDOM
DOMINICAN REPUBLIC	REPUBLIC OF KOREA	PAKISTAN	UNITED STATES
ESTONIA	LITHUANIA	PERU	
FINLAND	LUXEMBOURG	THE PHILIPPINES	
FRANCE	MALAYSIA	ROMANIA	

244

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

Research Experts Programs &

CONFERENCE – *Harvard Faculty, Fellows, Staff, and Students*

4th Korean Security Summit at Harvard: “Korea – An Oracle of Global Trends"

RSVP REQUIRED PAST EVENT

Tue., Apr. 11, 2023 - Thu., Apr. 13, 2023

Taubman Building - Allison Dining Room, 5th Floor

Foreign Assets Control, U.S. Department of the Treasury，OFAC）之主任 Andrea Gacki、韓國慶熙大學講座教授（亦為前聯合國裁軍事務高級代表）KIM Won-soo、區塊鏈分析公司 TRM Labs 調查專員（前 FBI 探員）Nick Carlsen、區塊鏈分析公司 Chainalysis 之網路犯罪調查專家 Ashley Chafin-Lomonosov，共同探討防制北韓透過網路犯罪盜取虛擬貨幣之議題。OFAC 主任 Andrea Gacki 提及：駭客將所盜取的虛擬貨幣移轉至駭客集團持有之錢包地址，依照區塊鏈之特性，在未取得該錢包地址私鑰之情形下，無從阻止該錢包地址上之虛擬貨幣移轉，遑論是扣押，然而目前 OFAC 係使用制裁之方式，亦即，將該駭客集團相關之錢包地址納入制裁目標，請各國依防制洗錢、資恐、資武擴之相關規定，令各國內之虛擬貨幣交易所或個人禁止與受到制裁之錢包地址有所往來，以此方式達成圍堵該錢包地址之目的[245]。此外，對混幣器 Tornado Cash 之洗錢行為，OFAC 亦首次將該虛擬貨幣之智能合約（Smart Contract）納入制裁名單[246]。在在足見美國對於新興科技使用於逃脫制裁、犯罪之防堵政策之落實，及國際合作之重要性。

此會議舉辦地點為甘迺迪學院 Taubman Building 五樓之 Allison Dining Room，該空間為一古色古香之圓形空間，講者坐於前方面對聽眾，而聽眾則圍坐於該場地，中間留一走道通往講台，如有提問者，則需走上講台前面對講者提問。筆者一方面為了讓臺灣檢察官可以在國際舞台上被看見，同時彰顯專業度，遂鼓起勇氣於提問時間走向前向講者及全場聽眾介紹自己係來自臺灣之檢察官，就虛擬貨幣錢包地址之透明度與犯罪趨勢之關係詢問 TRM Labs 及 Chainalysis 之區塊鏈分析專家，二位專家均認為雖然錢包地址上之資訊在區塊鏈上均屬公開透明，然犯罪者仍可利用日新月異之混

245 https://home.treasury.gov/news/press-releases/jy1498
246 https://home.treasury.gov/news/press-releases/jy0916

幣器、去中心化金融（DeFi）、跨鏈橋等新興科技以逃避追查，故犯罪趨勢不會因為區塊鏈之透明特性而下降。

有幸在哈佛甘迺迪學院此古色古香之場地與眾多專家對談，並讓全場知道臺灣的檢察官亦瞭解並關注此國際上之重要議題，實屬有幸（會議照片如下，筆者之提問亦登上哈佛大學甘迺迪學院之 Youtube 官方頻道[247]）。

247 https://www.belfercenter.org/event/4th-korean-security-summit-harvard-korea-oracle-global-trends#!day-3-agenda

（二） 全美網路犯罪會議

1. 會議內容

此網路犯罪會議（National Cyber Crime Conference）係由麻州檢察長辦公室主辦[248]，係屬全國性之網路犯罪會議，每年舉辦一次，今年係第 12 年，內容包括對於檢察官、執法機關對於網路犯罪及數位證據相關之訓練，為全美最大偵辦網路犯罪討論之盛事，今年舉辦期間為 2023 年 4 月 25 日至 27 日，地點在 Four Points by Sheraton Norwood，報名費用為每人美金 450 元，筆者認為機會難得，且主題切中筆者之研究題目，遂自費報名參加。而此會議嚴格限制需具有檢察官、調查人員、鑑識人員等執法人員始能與會，筆者在向主辦單位說明係來自臺灣的檢察官後，主辦單位即接受筆者之報名。而會議內容包含網路犯罪偵查、數位鑑識、執法技巧、如何在法庭呈現數位證據、IoT（Internet of Things - Rethinking Digital Threats）、社群媒體偵查技巧、暗網（Darkweb）介紹、偵查實際案例、手機追蹤、撰寫數位證據之聲搜書教學、虛擬貨幣追查、區塊鏈證據之證據能力及法庭應用等近百場課程。教授課程之講師為檢察官、FBI 探員、國土安全部犯罪調查部門（HSI）之探員、美國緝毒局（DEA）、鑑識人員等眾多專業講師。課程之上課方式為同一時段在不同教室開設不同課程，參與者可依自身興趣選擇參加課程，且大部分課程均有錄影存檔，就算對於同一時段的複數課程有興趣而只能擇一，對於同一時段的其他課程亦可事後在網站上觀看，觀看權限開放三個月。

2. 暗網課程

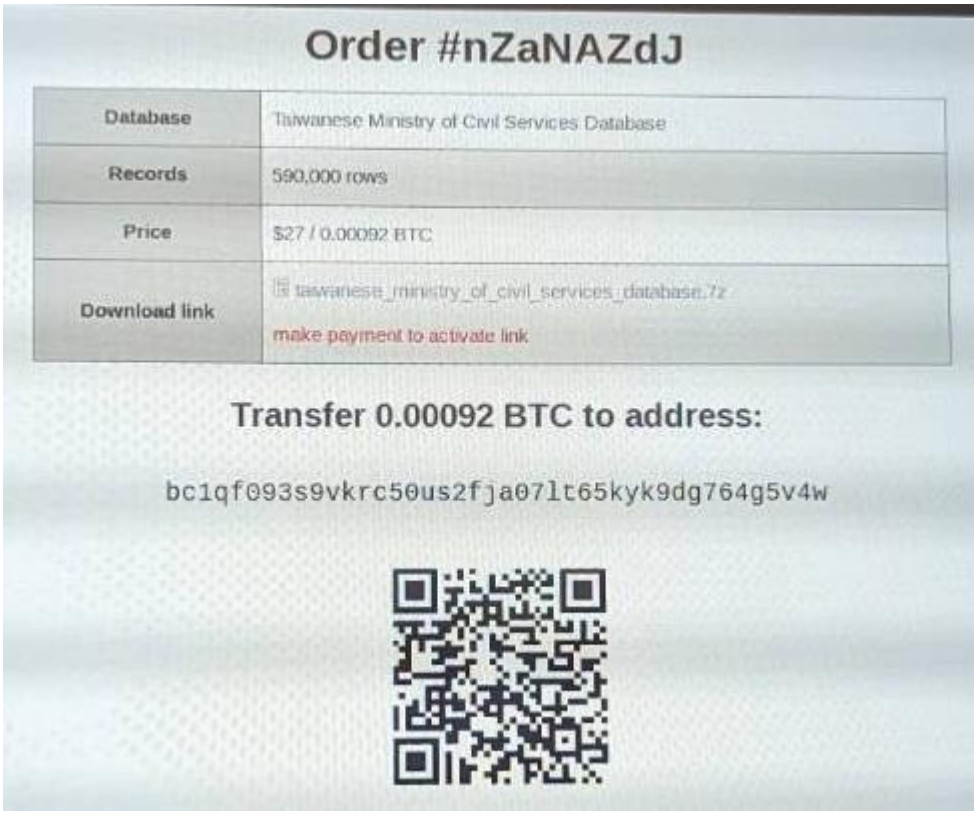
課程內容多係以實務出發，介紹實際網路犯罪案例，其專業度及實用度令筆者獲益良多，我國檢察官如能定期參與，對於提升網路犯罪之知識

[248] https://www.mass.gov/service-details/national-cyber-crime-conference

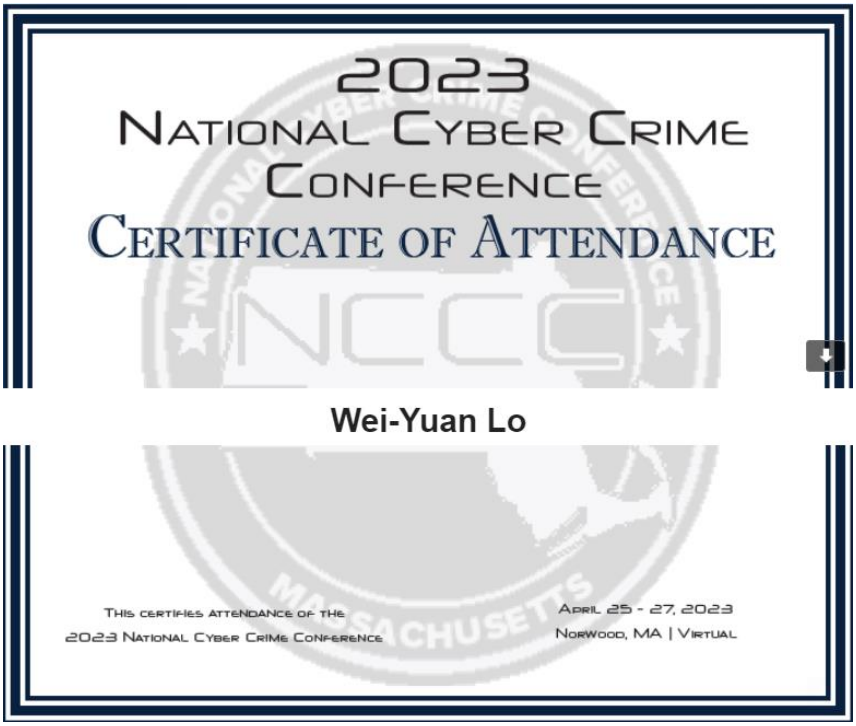
有絕大之幫助。關於課程筆記刻正整理中，日後如有機會將另做分享。茲舉一「暗網」（Introduction to the Dark Web）課程說明之，本課程講師為國土安全部資深調查人員，同時為聯邦執法訓練中心網路部門之訓練講師[249]，因為是採電腦實機上開，講師除了暗網基礎知識、瀏覽器設定、搜尋引擎介紹外，更讓參與者親自使用筆電上暗網，進入暗網市集查看非法物品之買賣情況，實屬難能可貴之機會，筆者本來在第二天的下午前往該教室參加，但因人數爆滿而無法進入，所幸講師告知隔日上午有開一門同樣的課，才讓筆者有幸於隔日上午參與。筆者在進入暗網市集後，特別以關鍵字「Taiwan」搜尋，而確實查找到我國 2019 年戶政資料遭放上暗網兜售，賣家則要求比特幣付款，相關實際頁面如下：

[249] Law Enforcement Training Advisor, Cyber Division，Federal Law Enforcement Training Center.

2016	SubaGames Database
2014	Sumo Torrents Database
2015	Super Stresser Database
2021	SuxxTO Database
2015	SweClockers Database
2017	Sword Fantasy Online Database
2021	SWVL Database
2019	Taiwanese Ministry of Civil Services Database
2021	Tamodo Database
2012	Taobao Database
2017	Taringa Database



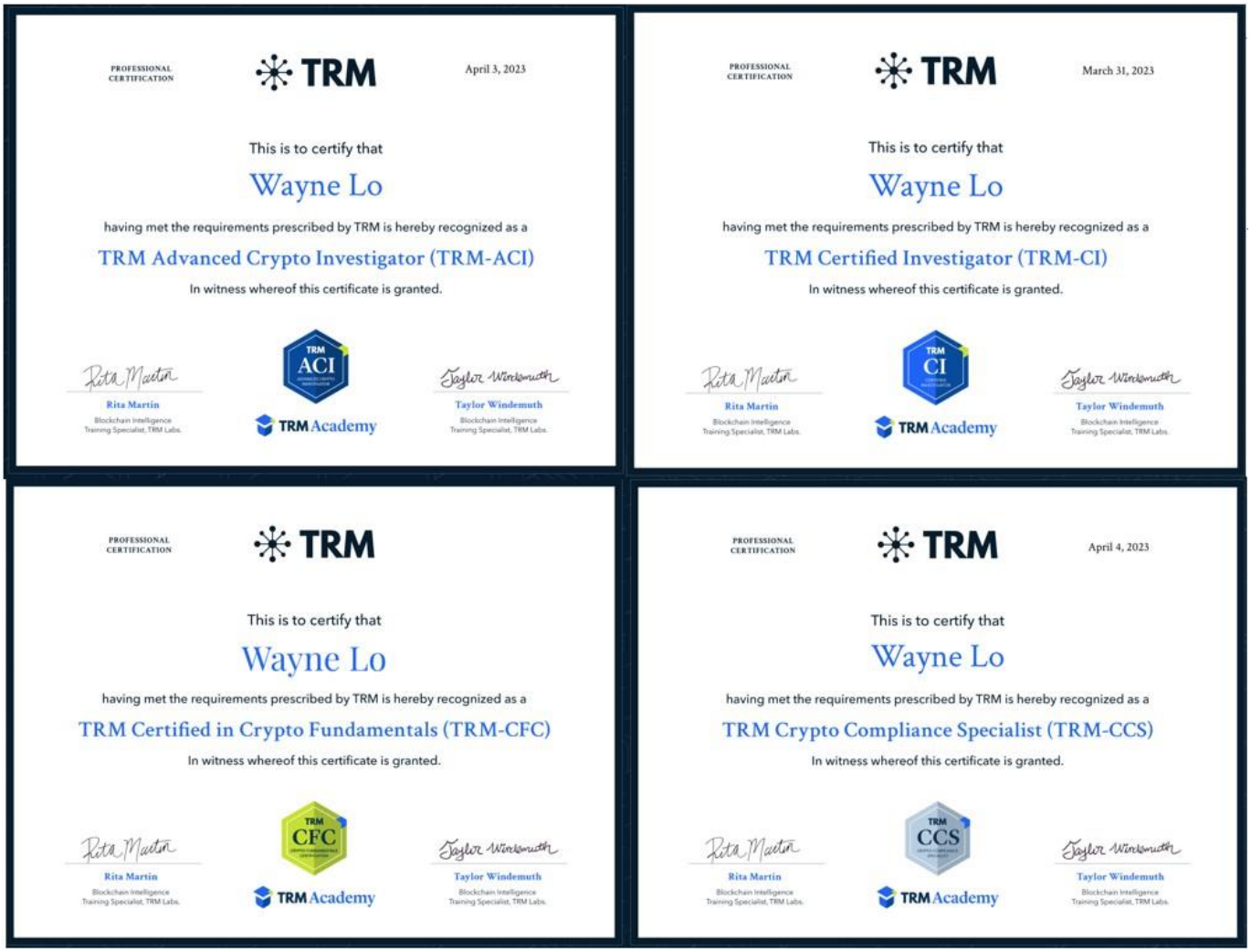
筆者於全程參訓後，亦取得 2023 年之全美網路犯罪會議之參訓證明如下：



（三） 區塊鏈分析公司 TRM Labs 之虛擬貨幣追查認證

關於虛擬貨幣之追查，基於區塊鏈公開帳本之特性，除了以區塊鏈瀏覽器及免費工具可查詢錢包地址之相關幣流外，亦可使用商用工具以增進效率，尤其是錢包地址之資料庫可協助識別錢包地址之歸屬，有助於進一步向虛擬貨幣交易所調閱 KYC 及交易資料，以及視覺化功能更可幫助爬梳、整理相關幣流，協助觀察及理解。

TRM Labs 係屬國際知名區塊鏈分析公司，其開發之區塊鏈分析工具目前為美國司法部及眾多執法機關所採用，我國高等檢察署亦有採購該商用工具。筆者在美期間通過上 40 餘小時之專業課程並通過考試，而取得 TRM 虛擬貨幣基礎認證（TRM-CFC）、虛擬貨幣調查人員認證（TRM-CI）、高階虛擬貨幣調查人員認證（TRM-ACI）及虛擬貨幣法遵專家認證（TRM-CCS）。相關證書如下：



（四） 與美國司法部虛擬貨幣執法團隊檢察官之視訊會議

美國司法部為因應虛擬貨幣犯罪日增，且影響層面廣大，特於 2021 年 10 月宣佈成立國家級的虛擬貨幣執法團隊（National Cryptocurrency Enforcement Team, NCET），成員由司法部電腦及智慧財產小組（CCIPS）之檢察官、反洗錢及資產追討小組（MLARS）和資安專家組成，並 2022 年 2 月 17 日指派檢察官 Eun Young Choi 為該團隊主管。NCET 領導來自全美各地檢察官辦公室相關團隊，以識別、調查、針對虛擬貨幣交易所、基礎設施提供商、以及其他濫用虛擬貨幣和相關產品實施或促進犯罪活動的實體，並對全美各地之檢察官提供虛擬貨幣相關之訓練及協助。又因應全球化之虛擬貨幣犯罪趨勢，建立全球合作、夥伴關係亦為 NCET 之任務之一 。此外，日本檢察界為因應新興科技、網路犯罪及跨境犯罪之偵辦，日

本最高檢察廳於 2021 年 4 月間設立「新興犯罪檢察官小組 」(先端犯罪検察ユニット、Japan Prosecutors unit on Emerging crimes、JPEC)，其主要任務為與私部門及學術部門合作蒐集、分析情資，提供檢察官法律與實務建議、訓練與協助，以及國際合作（同時為電腦犯罪檢察官之非正式合作管道)，其成員係從各級檢察廳具備科技、電腦專長，且需具備海外留學相關經驗之檢察官中挑選，目前成員共約 80 人。JPEC 於 2021 年 12 月與美國聯邦調查局（FBI）合作偵辦「索尼生命保險公司」員工透過虛假交易，將正在辦理清算手續的海外子公司向美國銀行帳戶非法匯款約 170 億日元換成「比特幣」之案件，透過雙方合作，由東京地檢署取得該比特幣的相關密碼，以違反「有組織犯罪處罰法」等罪名起訴該員工。他山之石，可以攻錯，我國在面對新興科技犯罪的挑戰時，可參酌上開國外之經驗，厚植檢察官科技辦案能力，並培養國際合作之經驗，以建立專業檢察官團隊。

筆者對於美國司法部之虛擬貨幣執法團隊十分感興趣，特別邀請該團隊之檢察官 C. Alden Pelker，透過視訊對談，筆者在請益過程獲益良多，相關會談要點如附件（不公開)。

（五） 最後三個月之計畫與展望

筆者此趟赴美之行迄今已過了 9 個月，剩餘 2 個多月就要回國，剩下的時間除了在 5 月 31 日至 6 月 2 日，奉法務部指派至佛羅里達州清水市參加「國際人口販運調察官協會（IAHTI)」舉辦之「國際人口販運會議」外，預計聯絡麻州檢察長辦公室、麻州之地方檢察署[250]或其他執法機關，

[250] 筆者於 2023 年 8 月 2 日參訪位在波士頓市中心的 Suffolk District Attorney's Office，跟二位負責偵辦兒童性侵害及人口販運的檢察官、Forensic Interviewer（臺灣譯為司法詢問員，其為針對兒童、性侵害被害人詢問之專業人員）會談，了解他們的 child abuse case 的處理流程，並參訪他們關於兒童受害人的談話室（裡面竟然還有狗狗喝水的水盆，原來是顧慮到有些受害人如有寵物陪伴，較可減輕壓力)，他們對於台灣的性侵減述程序及國民參審都表示很有興趣，雙方互動熱切。最後他們請我拍攝他們的兒童保護宣導活動 Now you see 照片（該活動旨在讓倖存者能夠談論他們的經歷，並為他們的韌性和力量感到自豪。最重要的是，《Now you see》的照片和文字幫助我們所有人擺脫了經常圍繞並導致虐待兒童的沉默和秘密)，筆者欣然同意。翌日他們把筆者的合照放上 Suffolk DA's Office 活動官方 Ig，介紹我是來自臺北地檢署的檢察官，還 hashtag 標注臺灣，感覺做了一場國民外交（如圖 21)。

尋求有無參訪之機會，期待與美國檢察機關、執法機關能有更深入之交流。此外，亦會利用最後之時間，持續撰寫並完成「打擊網路犯罪之法制及國際合作之研究」報告。

圖 21