公務出國報告 （出國類別：國際會議）

出席 2019 年網路犯罪研討會報告

姓名職稱、服務機關：

臺灣臺北地方檢察署檢察官 洪敏超

臺灣臺北地方檢察署檢察官 羅韋淵

派赴國家：美國華盛頓特區

出國時間：108 年 6 月 3 日至 10 日

報告日期：108 年 9 月 9 日

摘要

本次研討會係由美國國稅局犯罪調查處（IRS-CI）及世界銀行（World Bank，WB）舉辦，研討會日期為 2019 年 6 月 5 日至 7 日，會議地點為美國華盛頓特區世界銀行總部，以「全球協力追查金流並打擊網路犯罪（Connecting Globally to Follow the Money and Fight Cybercrime）」為主題，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，透過案例分享、以區塊鏈追蹤洗錢流向（Blockchain Tracing）之演練，提升與會者對此類犯罪之認識並提升偵查技巧。又主辦單位邀請來自超過 50 個國家之代表出席，筆者此行除了從會議中瞭解美國國稅局犯罪調查部門偵辦網路犯罪、以虛擬貨幣洗錢等基本概念及偵辦技巧外，亦於會議中與各國之網路、稅務犯罪調查人員交流，瞭解彼國之網路犯罪、洗錢案件之偵辦情形及困境，與會各國代表莫不認同網路犯罪、稅務及洗錢犯罪多涉及跨境，各國應積極互相合作、交換訊息，以攜手打擊網路犯罪等跨境犯罪。

目錄

照片目錄

壹、 目的

本次研討會係由美國國稅局犯罪調查處及世界銀行舉辦，以「全球協力追查金流並打擊網路犯罪」為主題，探討涵括虛擬貨幣、暗網、公開來源情報及社群網路等新興網路及金融犯罪議題，主辦單位邀請來自超過50個國家之代表出席，筆者此行除學習網路犯罪之相關新知外，於會議中與美國國稅局犯罪調查部門調查員、英國、荷蘭、開曼群島、墨西哥、日本等各國之網路犯罪調查人員交流，瞭解彼國之網路犯罪、洗錢案件之偵辦情形及困境，期待我國能與各國積極互相合作、交換訊息，以攜手打擊網路犯罪等跨境犯罪。

貳、 行前準備：

由於我國並非聯合國的會員國，所以以往由世界銀行等聯合國附屬組織所主辦的會議或活動，我國均未受邀而無從躬逢其盛。本次「2019 年網路犯罪研討會」是首次由 IRS 主動邀請我國參加該次會議，因此在有幸經蔡部長遴選奉派出國後，本於「知己知彼 百戰不殆」的精神，我們分別就主辦單位、會議主題、與會對象進行了事前的沙盤演練及對應分析。就主辦單位及會議主題部分，除了透過 IRS 與世界銀行的網站及公開發行刊物瞭解其業務內容及 IRS 犯罪小組的組織外，也針對該小組日前針對網路犯罪與洗錢防制（諸如破獲某暗網網站及與某情報分析公司合作）等相關新聞加以蒐集。我們在出發前也多次以電子郵件詢問主辦方相關議程、講者資料等細節，並就我國司法實務相關連之議題預先準備，並擬定可能的提問內容與國內案例分享。除了希冀在會議進行期間展現我國追緝網路犯罪高度專業能力以及完善的法律制度外，更希望能以此為契機爭取我國能見度，促進我國與其他國家或國際組織情資交換或司法互助等合作機會。

其次，由於本次會議邀請對象計有 50 餘國，而會議期間僅有 3 日，在有限

的時間下，為有效達成與國外執法人員結緣以爭取日後情資交換與司法互助機會，除了主辦方外，我們事前已就可能的與會國家或組織做成清單，並就其等與我國在緝毒、洗錢防制及網路犯罪方面業務往來的關連度高低及重要性程度加以分類。意即，具有較高業務往來性或重要性之國家或組織，均屬於優先的潛在合作對象。對於這些潛在合作對象，我們也以本次會議主題為主軸，就各該國家或組織近期發生或面對的議題進行網路資料蒐集，藉由彼此共同的議題為出發點集思廣益或分享經驗，並事先瞭解各國人士的偏好，依其所代表之層級準備對應且具有我國特色的小禮物，以符國際禮儀，並發展務實外交。在出發之際我們也承蒙了本部國際及兩岸法律司蔡秋明司長及本署邢泰釗檢察長的提點與指示，除了準備符合外交公儀的禮品外，也準備了適當數量的北檢重案實錄光碟與國外執法人員切磋與分享。

最末，在出發前也很感謝本部國際及兩岸法律司戎婕檢察官的協助與聯繫，讓我們事先能與法務部調查局駐華盛頓秘書藍家瑞及陳立偉先生取得聯繫，讓我們更進一步了解 IRS 及 WB 的職掌與業務範圍與近期涉外司法實務所關注的議題。

參、 美國稅務局犯罪調查處介紹

一、 任務

美國稅務局犯罪調查處（IRS Criminal Investigation，簡稱：IRS-CI）下有 4,200 位工作人員，其中約有 2,800 位為特別探員，負責調查稅務犯罪、洗錢及違反銀行秘密法、毒品案件金錢流向之案件。雖然其他美國聯邦機構也對於洗錢及違反銀行秘密法之案件有管轄權，但美國稅務局係調查違反稅務法律潛在犯罪之唯一聯邦機構。其中犯罪調查處之特別探員為了追查經濟犯罪，更是就回復

電腦證據、使用特殊設備以回復遭加密、鎖碼之電子資訊等有特別專長。而經由該處偵辦案件的定罪率，亦是所有聯邦執法機關中最高的，這也顯示該處之犯罪偵辦能力[1]。

二、 跨國案件之偵辦

跨國稅務案件之偵辦係犯罪調查處之主要任務之一，因為有許多藉由境外帳戶來逃稅的趨勢，藉由境外帳戶、信用卡、信託、境外公司、合夥以及其他方式來逃稅、洗錢、移轉毒品犯罪之金錢等，均是該處的調查重點，同時也與其他國家的執法機關分享資訊並協助發展經濟犯罪調查之技術，故其與其他國家間的合作就顯的極為重要，。而「追錢」(follow the money) 更是該處的強項，為了強化國際合作，該處也在部分外交使館或領事館設有專員，以有助於與外國執法機關迅速交換資訊[2]。筆者此行前，也與該處派駐在香港的專員取得聯繫[3]。

三、 販毒、運毒所得之追查

該處有一句名言：「不管收入的來源為何，都是可以被課稅的」(No matter what the source of income -- all income is taxable.)。該處成立於 1919 年，其中第一件毒品走私案件之偵辦即為 1920 年代在夏威夷的鴉片走私案，成功地讓走私集團主事者繩之以法。該處的毒品計畫目標為利用偵辦經濟犯罪之專

---

[1] 關於 IRS-CI 之任務介紹，可參見：
https://www.irs.gov/about-irs/criminal-investigation-ci-at-a-glance

[2] 關於 IRS-CI 之國際合作方面，請參見：
https://www.irs.gov/compliance/criminal-investigation/international-investigations-criminal-investigation-ci

[3] 可參見香港政府禮賓部之官網所列美國駐香港領事及人員名冊：
https://www.protocol.gov.hk/chi/consular/america/usa.htm

業，藉由調查、起訴並沒收資產，以瓦解販運毒品及洗錢集團[4]。筆者大部分時間均被指派在緝毒專組，對此十分有感，也看到了國內處理販毒或毒品運輸案件之盲點，依照過往經驗，通常係著重在毒品之查獲及犯罪者之訴追，但時常忽略販毒或毒品運輸所得之追查，美國稅務局犯罪調查處上開經驗提醒筆者追查毒品案件之金流與追查毒品一樣重要。不過以國內實務現況而言，檢察官及司法警察之時間、資源有限，在龐大案件壓力下，通常追查毒品及販毒被告已耗費相當之時間、資源，且緝毒專組檢察官仍須處理毒品以外之案件，恐難如同美國稅務局犯罪調查處一樣，專注在販毒或運毒所得之追查，也許國內可考慮成立一專責追查不法所得（包含販毒、運毒）之單位，雖然建置初期會花費相當之成本，但就如同美國稅務局犯罪調查處特別探員給予筆者之答覆：「專責追查不法所得之單位建置，雖然會花費成本，但成立後所追查並查扣之龐大犯罪所得，可以有部分用來充實並強化不法所得追查單位之能量，成為一個追查不法所得之正向循環」，實值參考。

四、　網路犯罪調查小組

自 2015 年起，犯罪調查處為因應伴隨稅務、財務及經濟犯罪而來的網路犯罪，成立了位在洛杉磯及華盛頓特區的網路犯罪調查小組（Cyber Crime Unit ，簡稱：CCU），網羅了特別幹員、專業人員及電腦工程師等，負責偵辦下列案件：商業電子郵件入侵、網路釣魚、竊取銀行帳戶、網路個人資訊買賣、使用虛擬貨幣之稅務問題、洗錢、暗網市集之所有人、管理者及大盤商、以虛擬貨幣、網路方式之洗錢、輸送金錢以資助恐怖組織等犯罪類型。該小組一樣秉持著「追錢」的宗旨，在 Silk Road、Mt. Gox、 Alphabay、 BTCe、Backpage.com 等案件之

[4]關於 IRS-CI 偵辦毒品案件之說明，可參見：https://www.irs.gov/compliance/criminal-investigation/narcotics-related-financial-investigations-criminal-investigation-ci

調查均有重要之貢獻[5]。

肆、 全球稅務執法聯合組織（J5）

一、 設立目的

全球稅務執法聯合組織（The Joint Chiefs of Global Tax Enforcement[6]，簡稱 J5）之成立目的係為打擊稅務犯罪之聯合執法機關。各國執法機關間會共同蒐集、分享資訊、展開行動並培訓處理稅務犯罪之執法人員。因境外機構及經濟工具被使用於稅務犯罪及洗錢，係有害於國家之經濟、財證及社會利益，故 J5 合作調查稅務犯罪、洗錢及從中得利者，J5 並致力跨國合作以降低虛擬貨幣及網路犯罪對於稅務機關之威脅，並累積相關數據及技術。

二、 成員

J5 成員包含了澳洲犯罪情報委員會（Australian Criminal Intelligence Commission ，簡稱：ACIC）、澳洲稅務局（Australian Taxation Office ，簡

---

[5] 關於 J5 之介紹，可參見：
https://www.irs.gov/pub/irs-utl/2018_irs_criminal_investigation_annual_report.pdf

[6] J5 之標誌為：

其代表之意義可參見：
https://www.irs.gov/compliance/joint-chiefs-of-global-tax-enforcement

稱：ATO)、加拿大稅務局（Canada Revenue Agency，簡稱： CRA)、荷蘭財政資訊及調查處（Fiscale Inlichtingen- en Opsporingsdienst，簡稱：FIOD)、英國稅務海關總署（HM Revenue & Customs，簡稱：HMRC）及美國國稅局刑事調查處（IRS-CI)。

三、 工作內容

包含發展分享蒐集資訊之策略，以強化共同利益，並打擊稅務犯罪、網路犯罪及洗錢。執行上開策略及程序，實行聯合調查上開犯罪，並且有效地溝通。J5 雖甫成立一年，但已共同合作調查 50 件以上之跨境逃稅案件，實行超過百次的資訊交換，遠超過過去 10 年間的資訊交換次數，而 J5 彼此間交換資訊係透過 FCInet[7]（Financial Criminal Investigation Net）平台，該平台特別之處係在於沒有一個統一資料庫或管理機構，加入之成員間可連接彼此之資訊，以增進效率。其工作內容之一也包含為執法機關伙伴辦理網路犯罪之教育訓練[8]。

四、 J5 與本次會議

因為此次會議係由美國國稅局刑事調查處及世界銀行共同主辦，而該處同為 J5 成員之一，故本次會議第一天開場，即邀請由 J5 成員之代表致詞，共同宣示打擊稅務犯罪、網路犯罪及洗錢之決心，在結束致詞後，J5 成員代表亦在世界銀行大樓舉辦成立週年之記者會，說明其工作成果[9]（如圖 1)。

---

[7] 關於 FCIne，可參見：https://www.fcinet.org/index.php

[8] 澳洲稅務局關於 J5 之說明，可參見：https://ngm.com.au/joint-chiefs-of-global-tax-enforcement/

[9] 關於 J5 成立週年記者會，可參見：https://www.canada.ca/en/revenue-agency/news/2019/06/joint-chiefs-of-global-tax-enforcement-j5-conduct-media-availability.html

伍、 世界銀行簡介

「 世界銀行」(World Bank，WB)由國際復興開發銀行 (International Bank for Reconstruction and Development，IBRD)與「國際開發協會」(International Development Association，IDA)組成，是聯合國經濟及社會理事會下的國際金融機構[10]。 「 世界銀行」另外與「國際金融公司」(International Finance Corporation，IFC)、「多邊投資擔保機構」(Multilateral Investment Guarantee Agency，MIGA)及「國際投資爭端處理中心」(International Center of Settlement of Investment Disputes，ICSID)合稱為「世界銀行集團」(World Bank Group) [11]。世界銀行集團有 189 個成員國，員工來自 170 多個國家，並在 130 多個地方設有辦事處

依據世界銀行出版的「反洗錢與打擊資助恐怖主義參考指南(第二版)」[12]，世界銀行希望對各國提出建議，能根據該指南所介紹之國際標準及相關最佳做法，來建立和改善各自的法律和體系框架以及所採取的預防措施。主辦單位並提供了「Combatting Cybercrime : Tools and Capacity Building for Emerging Economies」一書予筆者，此書供各國就網路犯罪的立法與公司部門合作事宜提供了完善的參考資料。

---

[10] 可參見聯合國網站關於世界銀行或世界銀行集團之相關介紹：
https://www.unsceb.org/content/wb

[11] 關於世界銀行或是節銀行組織在聯合國系統下的分類及定位，請參見：
https://www.un.org/en/pdfs/un_system_chart.pdf。

[12] 可在以下網址下載：
http://siteresources.worldbank.org/INTAML/Resources/AMLRefGuideChinese.pdf

陸、 簡介世界銀行打擊網路犯罪之方法

一、 打擊網路犯罪之工具包

講者為世界銀行首席顧問 David Satola (World Bank Lead Counsel)，其介紹世界銀行（簡稱：世銀）為了使包括 internet 在內的各項技術能夠繼續作為促進經濟成長和發展的力量，必須採取某些措施以確保網際網路的安全以及網際網路中所傳輸的資料和通信的安全。因此世銀與其他參與機構[13]計畫並設計研擬了一套以新興經濟體為對象的工具包(Toolkit)，該工具包的設計除了旨在提昇發展中國家的政策制定者、立法者、檢察官、調查人員以至於個人，甚至整個社會打擊網路犯罪的能力外，更希望最終能藉此方式達成在政策、法律和刑事司法等方面的良好整合，用以建立對抗網路犯罪所需的有利環境。此外，該工具包還附有一個虛擬圖書館，由參與組織和其他組織提供相當豐富的素材及資源。正因該工具包希望藉由打擊網路犯罪以建立安全的網路環境，因此該工具包裡面除了整理既有相關案例以及法律的爭議的定義供作案例研習外，該工具包所著眼者，並不僅限於傳統的網路犯罪類型，更延伸至面向未來的新興技術，例如量子計算、區塊鏈技術、數位貨幣以及物聯網(the Internet of Things，IoT）等。

二、 工具包內容

該工具包也提供了評估工具組（Assessment Tool），分別從 Policy

[13] 除了世銀外，其他參與機構計有：the Council of Europe (CoE), the International Association of Penal Law (AIDP), the International Telecommunication Union (ITU), the Korea Supreme Prosecutors Office (KSPO), the Oxford Cybersecurity Capacity Building Centre (Oxford), the United Nations Conference on Trade & Development (UNCTAD), the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office on Drugs & Crime (UNODC).

Framework、Legal Framework、Substantive Criminal Law、Procedural Criminal Law、e-Evidence、Jurisdiction、Safeguards、International Cooperation 及 Capacity-building 等 9 個面向及 115 種指標進行評估。Policy Framework 包括國家戰略和政策以及與民間部門合作非法律性質的事務； Legal Framework 包括國家法律以及該國家是否有締結相關條約; Substantive Criminal Law 著重在於那些被定義為刑事犯罪的行為；Procedural Criminal Law 則著重於調查事項；e-Evidence 側重於網絡犯罪脈絡下數位證據的證據能力和處理方式；Jurisdiction，重點在於如何界定犯罪的管轄權;Safeguards 側重於三個要素：正當法律程序、資料保護和言論自由；International Cooperation 重點在於引渡以及正式和非正式的司法互助（MLA）; Capacity-building 考慮機構（如執法培訓學院）和人才培育，側重於偵查、起訴和審理的培訓需求等。此評估工具考慮了政策和立法，以及實際案例並彙集國際實務，且結構與工具包章節的結構相似，如能參考該工具包，可以對正在評估的面向有更深入的闡明和理解。上開工具包及評估工具均可自世銀網站免費下載並使用，且會定期更新[14]。

柒、 虛擬貨幣(Virtual Currency)介紹與追蹤

一、 講者簡介

此專題之講者有：James Daniels 、Eric Hergert、John Golinvaux 等三人，講者 James Daniels 及 Eric Hergert 均為 IRS-CI 之特別探員，James Daniels 並受指派擔任 FBI 犯罪調查小組，並且是該小組關於網路犯罪方面的專案經理，專責在虛擬貨幣及暗網的調查。Eric Hergert 則是在西雅圖辦公室擔任西部網路犯罪小組之成員（如圖 2），專精於身份竊盜、退稅詐欺及處理與虛擬貨幣有

[14] 可自以下網址下載：http://www.combattingcybercrime.org/

關之案件。John Golinvaux 則是 Excygent 公司的高級網路犯罪分析師，Excygent 公司負責與 IRS-CI 合作並支援網路犯罪的鑑識與分析，John Golinvaux 在編制上隸屬於 IRS-CI，主要工作內容在於透過數據與各種來源清報的分析來進行網路行為的追蹤。

二、 課程內容

（一）虛擬貨幣概述：虛擬貨幣(Virtual Currency, Digital money) 僅以數位形式存在而不具實體，但它與傳統貨幣具有相同的特徵，意即可以持有、移轉及兌換成其他貨幣，也可以當作支付工具使用（課程現場如圖 3）。在虛擬貨幣中，加密貨幣應用了區塊鏈及去中心化的技術，這意味著沒有任何監督機關得以監管加密貨幣在網路上的所有活動，如此一來也造成了加密貨幣的使者大幅增加。截至 2019 年 2 月，已有超過 2000 種加密貨幣在市面上流通[15]。

（二）截至 2019 年 8 月，市值最高的前 10 種加密貨幣依序為 Bitcoin 、Ethereum、XRP、Bitcoin Cash、Litecoin、Binance Coin、Tether、EOS、Bitcoin SV 及 Monero[16]。其後講者即就當前市值較高的加密貨幣介紹其概況，並說明各種加密貨幣之取得方式(諸如挖礦、現金購買及以他種加密貨幣兌換)，茲僅就上述加密貨幣的特徵擇要敘述如下：

（1） Bitcoin:錢包地址由 25-36 位字元組成，起始數字為 1 或 3；

（2） Ethereum:錢包地址由 42 位字元組成，起始 2 位字串為 0x；

（3） XRP（Ripple）:錢包地址由 34 位字元組成，起始字母為 R；

（4） Bitcoin Cash:與 Bitcoin 同，錢包地址由 25-36 位字元組成，起始數字為 1 或 3；

[15] 詳細內容請參照：https://coinmarketcap.com/zh-tw/all/views/all/

[16] 資料來源：https://coinmarketcap.com/

（5） Litecoin:錢包地址由 33 位字元組成，起始字母為 L 或 M；

（6） Monero:錢包地址由 95 位字元組成，起始數字為 4。

（三）講者另外也針對電腦設備或行動電話中儲存上開加密貨幣之電子錢包路徑位置加以介紹，例如 Windows 作業系統之路徑通常為\Document and Settings\UserName\Application Data\ClientName”（Xp）、”\Users\<username>\Application Data\Roaming\ClientName”（win7、10）’、”\Users\<username>\Documents”、”\Users\<username>\Local\Google\Chrome\User Data\Default\Local Storage;Linux 作業系統之路徑通常為~/.bitcoin/,須在利用”ls －a”指令查詢；

MAC 作業系統之路徑通常為~/Library/Application Support/ClientName；

Android 作業系統之路徑通常為/data/data/<package_name

至於對電子錢包內加密貨幣的扣押方式則可以透過將該錢包的種子「*Seed*」儲存在執法單位的電子錢包，或以 mnemonic converter 將之轉成私鑰匯出，避免遭押的電子錢包內之密貨幣被移轉外，針對前綴為『xprv』類型的私鑰，亦可以相同方式達成扣押之目的，唯一不同之處在於後者轉換私鑰之程式須利用 xprv converter 進行。

（四）講者除了介紹區塊鏈的原理、應用，各礦池及哈希算力分佈[17]外，也以 Bitcoin 為例，也就如何獲得 Bitcoin 及設定錢包以進行移轉或自提款機存提 Bitcoin 等加以說明。此外，講者亦就加密貨幣的 IPO（Initial Coin

[17] 哈希算力意思是每秒能計算幾個單位的 Hash 值。常見的算力單位層級包括 MH/s、TH/s、GH/s，1 MH/s = 1,000,000 H/s，1,000 MH/s = 1 TH/s，1,000TH/s = 1 GH/s = 1,000,000 MH/s。

Offering，首次代幣發售）[18]及其所涉及之詐欺問題與過往案例做了充分而詳細的介紹。

（五）關於虛擬貨幣的追蹤工具可以分為付費版本及免費版本 2 類，付費版本計有：Chainalysis、CipherTrace、Eliptic 及 Neutrino 等；免費版本則可以利用 WalletExplorer.com、Blockchain.info 及 BlockExplorer.com 等網站進行查詢。至於如果要進行網域域名（Domain Name）或 IP 位址（IP Address）查詢，除了向來常用的 WHOis 查詢網站外，也可利用付費工具 DomainTools 或利用 DomainBigData.com 網站進行免費查詢，若是查詢網站歷史資料，亦可在「Wayback Machine」網站進行查詢。至若要對暗網進行調查，講者亦介紹了可以與 Flashpoint 公司[19]合作，利用該公司提供的平台服務或API，以取得該公司在暗網獲得之相關情資，進而進行分析，或使用 Accurint 公司[20]之付費服務取得調查對象之公開資料與記錄。

（六）講者亦即提及如有需要，對於個人持有加密貨幣之「任何識別信息」，包括任何加密貨幣餘額，錢包地址，甚至是登錄時間和信息，通信和交易細節，亦可以透過向大陪審團申請令狀之方式，以獲取 Apple、Microsoft 和 Google 的記錄（包含完整申請下載歷史）以證明特定人確實持有加密貨幣帳戶，間接證明該人有使用特定加密貨幣之事實。

（七）在加密貨幣市場上另存在一種提供分散的聯合支付方式的加密貨幣交易商（exchangers，或稱 Mixers、Tumblers），由於其等所提供的服務可以就一種或數種加密貨幣分散匯出，導致混淆加密貨幣原始的交易地址，致實

---

[18] 指某個團體、企業、組織或個人在區塊鏈上發行代幣（Token），並募集虛擬貨幣（例如：ETH、BTC）所進行的融資活動，詳情可見杜宏毅、宋倬榮，區塊鏈之書，頁 139 以下，該書可自 https://www.facebook.com/download/preview/326797697894094 免費下載。

[19] https://www.flashpoint-intel.com/

[20] https://www.accurint.com/

務上追查不易。對於加密貨幣交易商之行為，講者係借用金融業者所使用的「KYC」（Know Your Customer，認識客戶）概念出發，亦即從反洗錢的角度觀之，加密貨幣交易商與金融業者一樣，必須在提供金融商品或服務前，了解客戶的身份，藉此評估風險承受能力後，才能提供合適的商品給客戶。且必須要遵守「AML」（Anti-Money Laundering，洗錢防制）之規範，如其客戶有可疑舉止，應該提出可疑交易報告（Suspicious Activity Report，SAR）。從而，如加密貨幣交易商之言語或行為透露其對於交易對象或客戶並不了解或拒絕了解，此時即可認定該加密貨幣交易商與其客戶間，有共同犯罪之犯意存在，於我國法制上，此等主觀犯意的認定，則較近似於刑法所稱之「不確定故意」，此等他山之石，殊值參考。

捌、 暗網案例介紹：xDedic

一、 講者簡介

講者 Justin Allen 現為佛羅里達洲坦帕市 IRS-CI 之特別探員，並受指派擔任 FBI 電腦犯罪任務小組，其專注於基於經濟犯罪動機之網路犯罪，包括暗網市集、論壇、防彈主機代管服務供應商（Bulletproof Hosting Providers[21]）

二、 案例內容

（一）xDedic 介紹（如圖 4）

xDedic 是一個惡名昭彰的暗網市集，自 2014 年起開始營業，主要運

[21] 所謂 Bulletproof Hosting Providers 係指某些網域或網頁代管業者，縱容渠等之客戶上傳或散佈不法資訊，例如：垃圾郵件、網路賭博或色情資訊等，可參見：https://en.wikipedia.org/wiki/Bulletproof_hosting

作模式為由數個犯罪集團出售或購買遭駭客入侵的伺服器，而駭客通常使用 Client tools、RDP（Remote Desktop Protocol） patch 或 Socks proxy 等方式，入侵並控制伺服器，該黑市共有來自 174 個國家的 7 萬餘台伺服器在販售，由 416 名不同的經銷商提供。其中，受影響最嚴重的十個國家分別為：巴西、中國、俄羅斯、印度、西班牙、義大利、法國、澳大利亞、南非和馬來西亞。在臺灣、中國大陸、和香港，總計也有超過 100 家知名大型企業和 ISP 的伺服器受到感染並在 xDedic 地下黑市出售，這一些遭感染控制的伺服器包括政府單位、醫院、主要都會之公共運輸設施、會計師事務所及法律事務所、學校，甚至包含機場。在入侵行動成功後，攻擊者就可無聲無息的銷售伺服器的存取權限，啟動整個業務流程的運轉。欲購買上開遭駭資訊之網路罪犯者，最低僅需支付 6 美元，就可依價格、地理位置、作業系統等條件，在 xDedic 上搜尋到遭控制之伺服器，查看該伺服器的所有資料，或用其作為實施進一步攻擊的平台，包括發動針對性攻擊、惡意軟體攻擊、DDoS 攻擊、釣魚攻擊、社交工程攻擊以及廣體攻擊等[22]。xDedic 的管理者為了躲避追查，相關交易均使用比特幣。具稱 xDedic 提供之詐欺犯罪之金額超過 6,800 萬美金。而且根據現有證據都顯示，地下黑市是由使用俄語的網絡罪犯所營運。

（二）調查情形

1. 聯合調查團隊

於 2016 年間由民間的防毒軟體公司出具報告揭露 xDedic，之後美國佛羅里達中區檢察官辦公室、FBI、IRS、聯邦電腦犯罪小組（Federal Computer Crime Unit）、聯邦檢察官辦公室、比利時偵查法官

---

22 https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07191218/xDedic_marketplace_ENG.pdf

（Investigating Judge of Belgium）、烏克蘭國家網路警察及德國聯邦刑事調查局、歐洲刑警組織等執法單位進行合作調查，於 2018 年年初，上開調查單位之主事者在海牙見面開會，並簽署了聯合調查團隊協議（Joint Investigative Team agreement[23]）

2.查獲過程

於 2016 年起，比利時聯邦檢察官辦公室開始利用特別的偵查技術，發現躲在 xDedic 後面的犯罪設施並取得幾個重要的犯罪伺服器之數位備份（digital copies），在歐洲刑警組織及烏克蘭國家網路警察協助分析上開資訊後，找出該網站之管理者位於烏克蘭[24]。2019 年 1 月 24 日，調查小組同步搜索位在烏克蘭的 9 個處所，扣押數個 IT 系統，並逮捕了 3 名烏克蘭嫌犯。美國方面也依據法院之命令扣押了 xDedic 暗網市集之網域名稱，此後如有欲連上 xDedic 網頁者，均會被導向下列官方頁面[25]，並

[23] 關於 Joint Investigative Team (JIT)，可參見：
https://www.europol.europa.eu/activities-services/joint-investigation-teams

[24] 關於此案查獲過程，可參見：
http://www.eurojust.europa.eu/press/PressReleases/Pages/2019/2019-01-28.aspx

[25]

顯示該市集已遭扣押並下架，與 xDedic 有關之犯罪均告終止[26]。此案例也正式宣告網路犯罪者並非可自犯罪調查及處罰中豁免。

（三）後續發展

因 xDedic 幕後的組織成員尚未全數破獲，也許是考量此案尚在持續偵辦中，所以講者並未就偵查技巧有過多著墨，筆者於會場舉手提問道：是否可能僅透過 IP 追查，而查到躲在暗網幕後的人，講者回答稱：如果僅是透過 IP 追查是十分困難的，同時必須透過金流等多方面追查，而 xDedic 案中係因某位嫌犯的女朋友透過網路繳納信用卡帳單而露出馬腳，讓調查人員有跡可尋。

（四）附帶說明

附帶一提，本次研討會所提及之案例及偵辦技巧，因尚涉及後續偵辦

[26] https://www.europol.europa.eu/newsroom/news/xdedic-marketplace-shut-down-in-international-operation

部分，故在研討會上講者並未鉅細靡遺地說明案件細節，而僅係提出梗概，供作參考，而會場之工作人員亦提醒與會之成員，不要就現場播放之投影片拍照。筆者當然是入境隨俗，遵守會場之規定。雖然會場工作人員在一開始時有說明會將會議投影片電子檔於會後寄送予與會者，但也僅限於較不涉及案例之基礎說明部分。

玖、 心得及建議

一、 網路犯罪與洗錢

根據防制洗錢金融行動工作組織(FATF)40 項建議中的第 3 項建議，各國應依據維也納公約、巴勒莫公約（the Vienna Convention and the Palermo Convention）為基礎，將洗錢行為罪刑化，並應擴大洗錢罪及於所有重大犯罪，涵蓋最大範圍之前置犯罪。而依第 36 項建議，各國應在合宜情形下簽署並實施 2001 年歐洲議會有關網路犯罪公約（the Council of Europe Convention on Cybercrime），因此，執法機關在查緝各項犯罪時，實應同時注意被告或關係人之行為是否有涉及違反洗錢防制法之規定，以為資金之追查及不法所得之沒收，避免該等不法所得轉輾轉作為他種犯罪之資本，造成更大危害。

二、 建置追錢之專責機構

網路犯罪、區塊鏈之技術、虛擬貨幣之蓬勃發展，犯罪者也利用該等技術來洗錢或從事不法用途，執法機關實有必要針對最新之網路犯罪趨勢加以研究，並與其他國家互相交流學習，強化國際合作，以因應網路犯罪無國界及日新月異。而「追錢」係美國國稅局犯罪調查處之成立主要目的，專責追查不法所得之單位建置，雖然會花費成本，但成立後所追查並查扣之龐大犯罪所得，可以有部分用

來充實並強化不法所得追查單位之能量，成為一個追查不法所得之正向循環。專責追查不法所得單位之建置，或係我國可以思考的一個方向。

三、 勇於發言及主動出擊

此行為筆者之一（羅韋淵）首次造訪美國，雖然筆者平日對於語言學習十分有興趣，只要有時間就會報名由司法官學院開設之各項英文口說、聽力及寫作課程，並參加臺北地方法院開設之英文班，在國內也參加過數場國際研討會，但終究是第一次出國參加研討會，心中難免緊張，於是在行前特別請教參與國際會議經驗豐富的粟威穆學長及陳昱奉學長，學長十分熱心地提點我應該注意的事項，並鼓勵我勇於發言，讓我獲益良多

在第一天會議開始前，筆者初到會場，不知道會場是否能夠拍照，為求謹慎，便詢問一位 IRS 在現場之工作人員，該工作人員也無法確認，便熱心地幫筆者詢問其他工作人員，後來得到的答覆是可以，而且該工作人員還熱情地邀筆者一起在會場自拍（Selfie，如圖 5），筆者二人也在會場合照留念（如圖 6），拍照後筆者與該位工作人員閒聊，並自我介紹筆者係來自臺灣的檢察官，而該位工作人員 Jean Brown 則係 IRS 犯罪調查部派駐在芝加哥之機要專員，此次因 IRS 舉辦本次會議而特別到華盛頓特區幫忙現場事務，隨後並透過 Jean Brown 的引介，

而與 IRS 犯罪調查部國際事務組之組長 Janine Meriweather 女士（如圖 7：右二為 IRS 犯罪調查部國際事務組組長 Janine Meriweather 女士），其係 IRS 犯罪調查部派駐在香港之探員 David Lum 之直屬主管，因為日後有可能遇到與 IRS 犯罪調查部合作之機會，所以筆者也與 Janine Meriweather 女士交換名片，Janine Meriweather 女士也笑稱：如有與 David Lum 溝通上有問題的地方，可以直接找她等語，雖然是一句玩笑話，但也讓筆者切身體會「見面三分情」，及從會議現場之當面交流或閒談中，一點一滴建立起對彼此之信任，均有助於日後之合作。

在會議過程中，二位筆者均提出自己對於主題之觀點，並舉手提問，而在中場休息時間，也積極與他國與會成員相互交流。午餐時間係採自費的自助餐方式，用餐地點在世界銀行大樓之員工餐廳內，夾菜時來自開曼群島的皇家警察 Khalesiah Barboram 女士（如圖 8）邀請筆者二人一同用餐，席間輕鬆聊天，Khalesiah Barboram 女士並介紹開曼群島之地理位置，對於筆者提及開曼群島為有名的避稅天堂一節，Khalesiah Barboram 女士亦說明以往的確如此，但隨著全球反避稅浪潮興起，開曼群島因應國際反避稅壓力及歐盟之要求，已於 2019 年 1 月修改法律，規定註冊企業必須「證明」在當地有實際的經營活動，違反規定者，將視規定與情節輕重不同而予以處罰。讓筆者體會到國際上對於稅務事項之重視，及歐盟經濟力量之強大。

此次會議雖邀請 50 餘國之代表出席（如圖 9），但東方臉孔之與會成員甚為少見，除了筆者二人外，僅有來自日本國稅廳調查查察部之代表二人，在會議中場的咖啡休息時間，筆者二人跟與會各國成員均圍成圈圈相互聊天，但日本代表未參與大家的聊天，筆者即主動向前以有限的日語跟日本代表打招呼並自我介紹，日本代表也訝異筆者能說些簡單的日語，而因為簡單的日語也開啟了我們的話題，聊天中得知原來日本國稅廳與美國 IRS 關係良好，美國 IRS 每年均會邀請日本國稅廳人員參加研討會，今年也不例外，而日本國稅廳下之調查查察部，亦具有犯罪調查權限，與 IRS 的設置相同，筆者也好奇目前在日本是否有遇到透過虛擬貨幣或暗網的稅務案件，日本代表也直言稱此目前對於日本亦屬非常新興之議題。

四、 心得總結

由於本此會議是由 IRS 與世界銀行聯合主辦，會議會場是在世界銀行的大樓內，進入會場都要經過層層安檢，除了要出示識別證掃描 QR code 以外，也要將隨身行李送入 X 光機及通過金屬探測器檢查始能進入。在會議前一天感謝法務部調查局駐華府法務秘書藍家瑞先生及陳立偉先生在我國駐美國台北經濟文化代

表處的接待(如圖 10),我們並抽空參訪了喬治城大學(Georgetown University)、美國最高法院、林肯紀念堂及雙橡園（如圖 11)。

本次出國參加會議除了感謝部長及蔡秋明司長事前的勉勵,預先就我國相關網路犯罪查緝實務案例做成簡報與摘要與國外執法單位分享外,也就暗網查緝技術與各國現今面臨的困境向講座請教與分享,藉由他山之石來了解我國與國外執法人員的尺短寸長之處。透過講座的案例分享,我們發現其實國內執法人員的偵查技術與能量與他國相較尚屬伯仲之間,經驗比國外執法人員甚至更加豐富,僅在於跨境取證或司法互助的合作機會較困難而已。然而,即使彼此國情不同,此行除了更加提高我國在國際上的能見度外,在網路犯罪無遠弗界的今日,大家都有未來強化彼此雙邊或多邊合作的共識。在這段會議期間,深感於我國駐外單位在外交實務的辛勞與努力,也非常感謝本部國際及兩岸法律司能與 IRS 合作,促成本次我國首度參與 IRS 與世界銀行合辦的會議,希冀將來能有更多參與此類會議的機會。

壹拾、 會議照片

圖 1：J5 代表週年記者會合照

圖 2：與虛擬貨幣主題之講者 IRS-CI 特別探員 Eric Hergert 之合照

圖 3：會議及課程現場

圖 4：會議投影片現況（因此案尚有後續偵辦，故僅提供封面）

圖 5：與 IRS-CI 機要專員 Jean Brown 之合照

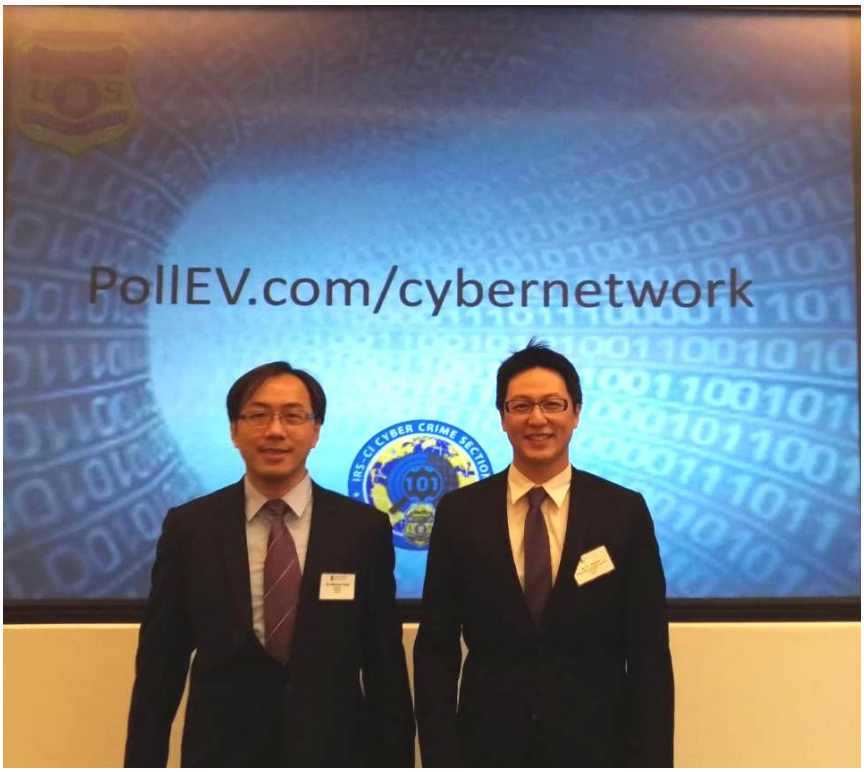

圖 6：筆者二人於會場之合影

圖 7：右二為 IRS 犯罪調查部國際事務組組長 Janine Meriweather 女士

圖 8：中間為開曼群島的皇家警察 Khalesiah Barboram 女士，右一為 IRS 打擊網路犯罪計畫主管，亦為虛擬貨幣、暗網基礎介紹之講者 James Daniels

圖 9 會後與會成員團體合照

圖 10：拜訪駐美國台北經濟文化代表處

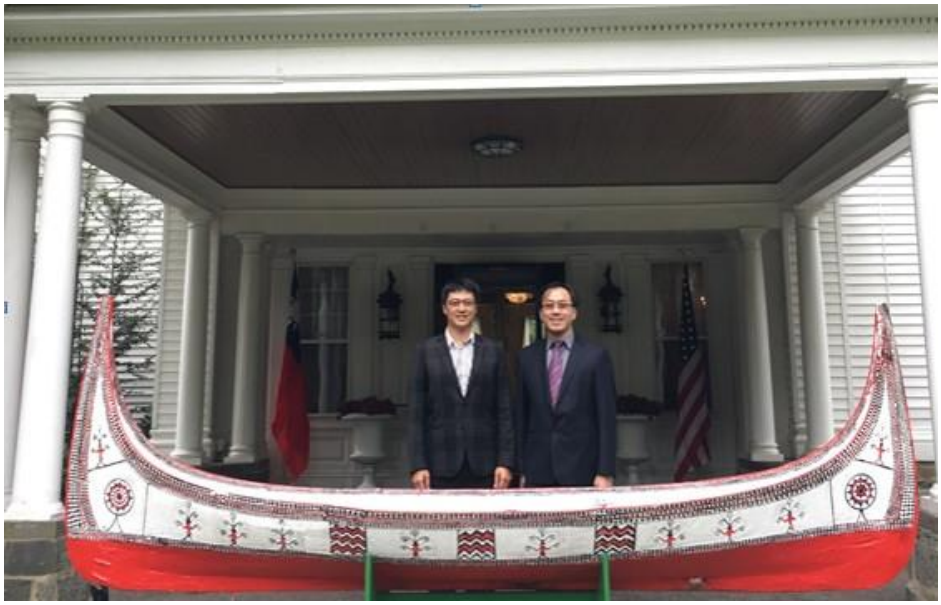

圖 11：筆者二人於雙橡園前之合影