出國報告（出國類別：研究）

赴韓國參加 2022 年網路犯罪對策國際研討會

服務機關：內政部警政署刑事警察局
姓名職稱：郭丁太 科長
陳彥宇 副隊長
葉泰志 副隊長
黃翰文 股　長
廖力緯 偵查正
楊承諭 警務正
林逸雄 偵查員
派赴國家：韓國
出國期間：111 年 8 月 30 日至 111 年 9 月 2 日
報告日期：111 年 11 月 30 日

摘要

隨著智慧型行動裝置發展、社群網路不斷演進，以及近年 Covid-19 疫情爆發下，網際網路與民眾生活已密不可分，網路犯罪與威脅亦不斷演進，相關網路隱匿技術也推陳出新，如暗網及洋蔥網路等，並結合虛擬貨幣，以其具去中心化、使用不受地域限制和容易匿名等特性，令偵查人員難以追查金流及真實身分；爰此，世界各國執法機構無不積極蒐集相關技術資訊、培育相關技術人才，研議相關抗衡之方法與技術，以及應對措施與規範。本次出國研習係屬本局為瞭解科技網路犯罪與相關專業技術人員培訓，經審查後同意派員韓國首爾參加 ISCR 2022 網路犯罪及執法應變策略國際研討會研討會，透過各國針對新型態網路犯罪執法經驗的交流，可以做為未來本國研擬相關執法對策之借鏡。

目次

壹、目的

許多智慧型行動裝置與社群網路不斷演進以及 Covid-19 大流行，網際網路與民眾生活密不可分，網路犯罪與威脅也不斷的演進，相關網路隱匿技術也推陳出新，如暗網及洋蔥網路等，並結合虛擬貨幣，以其具去中心化、使用不受地域限制和容易匿名等特性，令偵查人員難以追查金流及真實身分；爰此，世界各國執法機構無不積極蒐集相關技術資訊、培育相關技術人才，研議相關抗衡之方法與技術，以及應對措施與規範。本次出國研習係屬本局為瞭解科技網路犯罪與相關專業技術人員培訓，經審查後同意派員韓國首爾參加 ISCR 2022 網路犯罪及執法應變策略國際研討會研討會，透過各國針對新型態網路犯罪執法經驗的交流，可以做為未來本國研擬相關執法對策之借鏡。而本次 ISCR 2022 主題著重於：Covid-19 疫情大流行後的今天，面對新型態網路議題，例如布達佩斯公約、加密或幣、元宇宙、勒索軟體等網路犯罪議題及因應對策分析及實際案例分享。特此，規劃參加本場次研討會蒐集最新資訊、增進各國經驗交流，本次共邀請 95 個來自世界各國執法機關參加，會中更進行網路犯罪防制技術探討與交流；另本次並於會中增加 FBI 美國聯邦調查局調查「Trade Traitor」 攻擊加密貨幣交易所事件，發現號稱 APT-38 之網路攻擊者與朝鮮共和國勾稽之過程。

貳、過程

本次研習會於 8 月 31 日至 9 月 2 日共 3 日於韓國-首爾舉行。於 8 月 30 日(週二)搭乘中華航空航班，歷時 3.5 小時飛行至仁川。9 月 2 日(週五)搭乘中華航空返回臺灣進行防疫隔離 3 日。

表 1 出差人員行程表

日期	預訂行程	任務	停留日數
8 月 30（週二）	啟程 臺北-首爾	啟程赴韓國首爾（飛航時間估約 2 小時 30 分）	1
8 月 31 日（週三）	會議	參加研討會	1
9 月 1 日（週四）	會議	參加研討會	1
9 月 2 日（週五）	會議 返程 首爾-臺北	參加研討會 結束後返程(飛航時間估約 2 小時 40 分）	1
合計			4 日

ISCR 2022 網路犯罪及執法應變策略國際研討會

一、疫情時代下之網路犯罪觀點及對策

(一)國家的網路安全：

由 Anup B Kmuar 報告，講者是微軟的亞洲數位犯罪調查及分析團隊的主管，其過去曾擔任印度聯邦警察中央調查局的警官。其認為在俄烏戰爭的觀察中，他們發現網路攻擊也被視為交戰手段的一部分，在實體攻擊前兩年，就已經有持續不斷的網路攻擊，在實體戰爭開始後，網路攻擊仍然會持續，另外還有假訊息的相關攻擊。其定義為在「錯誤訊息」（Misinformation）以及「惡意訊息」（Malinforamtion）還有「故意的惡訊」(Disinformation)。

圖 1，烏俄戰爭中資訊戰手段類別

在俄國的網路威攝行動中，他們觀察到了有多種手段，如惡意程式、勒索軟體、商業詐騙、在 azure 上的濫用以及技術支援詐騙

等等手法。講者也提到了，某些身份以及密碼可能遭竊、某些安全裝置可能過時、未被維護或是有漏洞未能修補，這些都會對業或是組織造成潛在的安全疑慮。

另外在防範措施上，也有多種建議，如強化雲端防護、防止可疑的存取以及管理者們，應了解其在系統裡所使用的各種安全工具。

(二)網路犯罪預防大隊：

由 Floor Jansen 所提報，講者是荷蘭國家警察的高科技犯罪團隊副主管，其針對網路犯罪者進行剖繪以及分析，他認為網路犯罪行為，較難在犯罪中，遭到司法人員的干涉，比如正在搶劫的罪犯，可能剛好看到警察，而沒有搶劫或是中止其搶劫行為。但網路犯罪者，一般並不會在網路上遇到司法人員的干涉。

圖 2，淺在網路犯罪者特徵及活動軌跡

因此，其針對網路犯罪行為，提出了 4D 策略，「Deter」判斷哪

些人可能會是網路犯罪者;「Divert」分化其讓其不會組成駭客團體;「Degrade」降低其犯罪的危害;「Disrupt」干擾其犯罪，使其不會成功。

其認為如能依預防一般犯罪的方式，針對網路犯罪，依其 4D 的方式進行預防，可以收到其效果，講者並展示一個畫面，他說有一個駭客在遭到警察逮捕後，就自殺了，他認為這是其責任，並須用導引的方式，將年輕的駭客導引到對的方向，讓其不會誤觸法網。

(三)韓國警政署網路犯罪防制策略報告：

由 Byeong-gui Lee 提報，講者是韓國警政署下網路調查局的網路犯罪調查科的科長，其介紹了韓國網路調查局的歷史及組織架構，在韓國的警政署下面，共有四個局，調查局（主管經濟、貪污、特殊以及犯罪情資蒐研)、刑偵局(主管組織、性別、少年暴力犯罪)、網路調查局（主管網路犯罪調查、恐嚇調查以及數位鑑識)、國家安全調查局（主管國家安全管理、分析以及調查)。

在網路調查局的網路犯罪調查科下，有分兩個股，一個是網路犯罪調查股，一個是網路性騷擾調查股，分別就業管事項進行工作。在 Lee 的工作工，其中駭侵、DDoS 攻擊、惡意軟體、網路詐騙、網路經濟犯罪、人員定位、網路性別暴力、網路賭博、網路誹謗等等，均屬於網路犯罪；Lee 也分析了自 2017 年以來近 5 年的韓國網路犯

罪數據，其認為網路犯罪的模式正在改變，其一是匿名性，如暗網、虛擬資產、加密通訊、使用海外伺服器等等。第二是多元化，許多新型態的網路犯罪，或是共生犯罪的發生。第三是組織犯罪，網路犯罪不再是孤狼犯案，而是有組織並且分享其工具或是方法。

韓國的應對方式如下，第一建立特別的機關，如前段中提到的網路恐嚇調查科，另外在各省的警察局內，也增加了網路調查科。第二，在中央方面，組織團對來應對網路經濟、網路賭博、網路性暴力以及網路恐嚇案件，第三是強化調查人力，如僱用專業人員，提供教育訓練、以及工具設備。第四是強化國際合作。第五是強化犯罪預防以及災害復原，希望能將網路犯罪的狀況壓制到最低。

(四)Covid-19 疫情下網路犯罪與之關聯數據報告：

由 Heiko Lohr 報告，講者是德國網路犯罪科的政策服務股的股長，其認為在後疫情的時代，會有許多針對供應鏈的攻擊，其舉德國的例子，在 2019 年的時候有 12 萬餘件，2021 年的時候成長到了 14 萬餘件勒索軟體的攻擊，但是其認為相關數據隱含很大的黑數。另外其也提到了，現在的網路犯罪也服務化，很多服務稱為「Cyber Crime as a Service」(網路犯罪即服務)，換句話說，有心人士不用是專業人士，不須要什麼駭客技能，你可以取得一些勒索軟體，並寄發釣魚郵件給你想攻擊的企業，只要企業裡面有人開啟了惡意

連結，就會執行勒索軟體，完成攻擊。

在打擊方面，Heiko Lohr 也提到了自 2015 年開始對於 hydra market 的打擊，一個查獲了 7 千萬個使用者帳號，以及 2 萬個交易帳號另外也扣押了 550 個比特幣。因此他也提出跨國合作是非常重要的，他希望未來能強化國家之間的合作，如使用 24/7 窗口等等來更完善的保存資料，以利追查。

二、布達佩斯公約及網路犯罪國際對策

布達佩斯公約又稱網路犯罪公約（Cyber Crime Convention），其是自 2001 年所簽署的國際公約，一開始共有 56 個成員國，其主要所體現的精神如下：

(一)明訂要求各簽署國應立法對各類網路犯罪進行處罰，如非法存取、資料干擾、系統干擾、濫用、詐騙、兒少色情以及侵犯著作權等案件。

(二)另外簽約國應建立一個通訊聯絡窗口，其必須是 24 小時全年無休皆能聯絡與合作的機制。並且要能針對同樣簽署國的窗口，進行合作，調閱、保存及提供資料。

我國雖不是布達佩斯公約的成員國，但是我們同樣擁有 24/7 的窗口，而非成員國的請求以及資料的提供，並沒有相關強制力，甚至我國在法律面上，對於依布達佩斯公約來進行調閱的請求，也沒有相關的規

範可以依循，這是未來我們應強化的地方。另外講者也有提及，俄羅斯以及中國，似乎有意圖要組建一個類似的聯盟，但目前亦尚未成形。

在來自 Google 公司的講者中提及，Google 公司要保存或是提供資料必須依循美國的法令，另外是僅能提供使用者的資料，而非其所使用的內容。最後也提及，布達佩斯公約（Budapest Convention）即將有第 2 額外協定（The Second Additional Protocol），首先就是直接的合作，應提供使用者或是域名註冊者的資料。其次是在允許的情況下，提供網路連線資料（traffic data）。第三，在特殊的情況下，同意緊急的資料請求以及在允許的情況下，提供存放在電腦裡的資料。第四，提供緊急的 MLA 模式，加快處理時程。第五，允許跨成員國之間使用視訊聽證會。第六，跨國共組聯合調查團隊。以上六大要點是第二額外協定的相關規劃，從 2022 年 5 月已開始進行簽署，目前已有 22 個成員國完成國內立法，並進行簽署。

三、元宇宙及人工智慧科技演變之新型態威脅

(一)大規模人工智慧的未來發展：

由 Jung-woo Ha 報告，講者是 NAVER 公司的人工智慧實驗室的主任，其所展示的技術使做出圖像辨識，比如用 AI 辨識出哪些照片裡面有狗，甚至辨識出，所要找的狗在哪些照片裡。另外其也展示一種使用自然語言的程式編碼技術（Natural language to code），稱為「Copilot and

Alpha code」，另外該公司的 CLOVA 系列軟體，可以自動翻譯，或是可以用來做為長者以及兒童的保護機制來提供一般日常的運用。該公司目前已將 AI 技術融入人們的生活當真，未來也將會是這樣的趨勢。

(二)元宇宙及 AI 人工智慧的安全以及威脅：

講者 Dae-seon Choi 提到，未來在元宇宙的部分的安全，也是大家應該重視的議題，從實體到虛擬之間，使用 VR 或是電子設備做為橋樑來介接，但是相關威脅，如大腦駭侵、隱私入侵、基礎設施駭侵、機器人濫用、假訊息以及詐騙等等威脅以及攻擊，仍然有可能是元宇宙會發生的問題，甚至可能造成使用者在生理或是心理上的傷害。

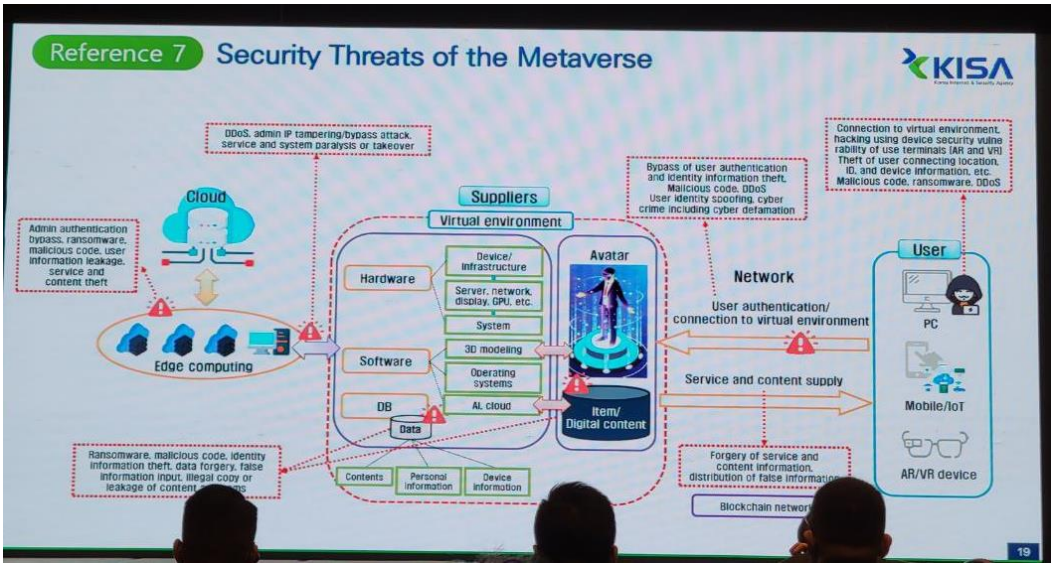

圖 3，元宇宙之安全與威脅示意圖

因此講者建議，首先要建立安全的元宇宙環境，其次是連結元宇宙的設備應該要有足夠的安全機制，最後就是立法應該要跟上，避免在元宇宙世界發生的犯罪，有無法可罰的狀況。另外講者也提到一些例子，

比如目前很多聲控的家電，使用者可以透過聲控的方式，開啟或是關閉燈光，而駭客則可以透過入侵使用者的音樂撥放設備，在音樂中插入指令，而控制相關聲控的家電。另外講者也很擔憂，未來人們的隱私，因為會存在元宇宙世界中，有可能會被入侵，然後遭到攻擊（加密勒索或是個資外洩）。這些是我們未來可能會面對，並且必須要去防範的問題。

四、網路攻擊及勒索軟體犯罪之演進

講者 Jeong-soo Ahn 提到，在資安事件的調查中，很多都是經由一些小部分，去拼湊出一支大象，比如某些程式是朝鮮網軍會留下的，某些來源是屬於某個伊朗或是俄羅斯網軍常用或是慣用的。經由多方拼湊，而找出幕後的攻擊者。

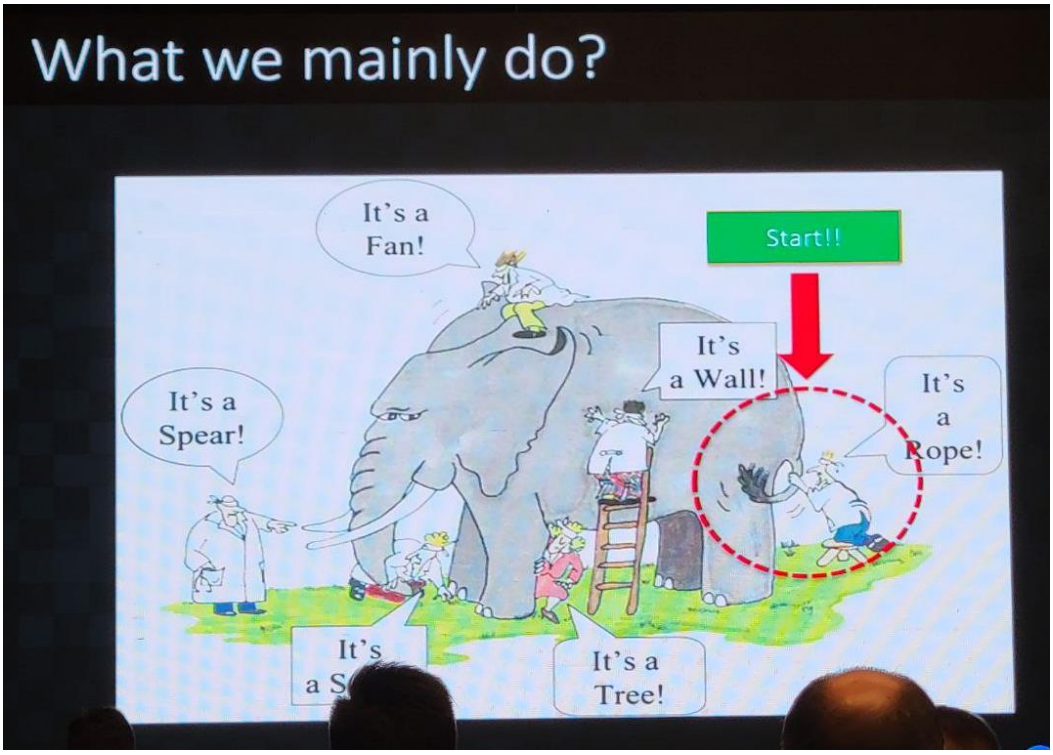

圖 4，資安事件還原示意圖

在 IoC（入侵指標，Indicator of Compromize）部分，講者認為應儘可能包含 6W，也就是 when, where, how, what, who 以及 why，以這個方式來進行的話，可以有效地偵測勒索軟體，比如每一種勒索軟體都有的行為就是產生加密檔案，刪除未加密的檔案，如果以行為模式來做，當電腦開始有大量這樣的異常行為的時候，如果可以用自動化的方式偵測並中止此一行為，可以有效防範勒索軟體。另外企業或是機關的資料，可能遭到重複的攻擊(Double Extortion)，比如先將個資進行外洩販賣（Data exfiltration）後，再以資料加密(Data encryption)進行勒索。

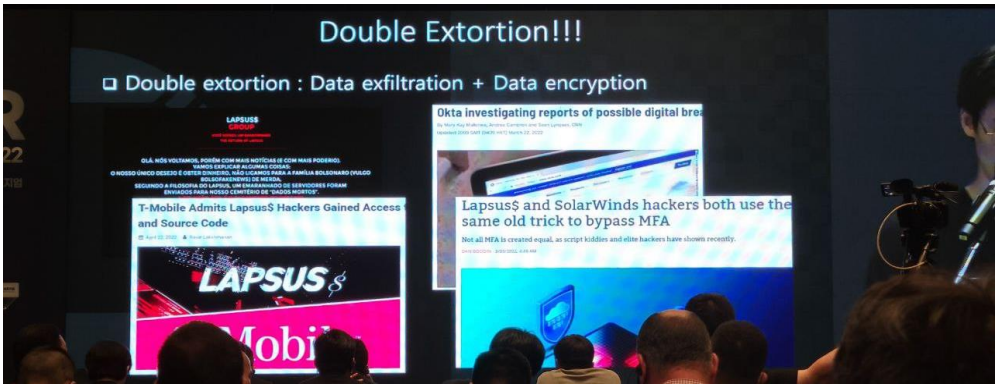

圖 5，重複的攻擊(Double Extortion)

另外講者也提到有關客群組的特徵值，如常對臺灣發起攻擊的中國網軍「Mustang Panda」其常會在程式碼中塞入其簽名，又稱為「junk code」如下圖。

圖 6，簽名示意圖

另外在 IR（資安事件應變，Incident Response）部分，資安應變在司法機關以及公司之間有不同的目的，客戶想要的是確認這個感染是否已經被清除，而司法機關主要是專注於追查駭侵的來源。另外講者觀察到一些趨勢，如在雲端伺服器上的威脅，以及最大宗的是利用社交郵件來進行攻擊。也可以善用第三方資訊，如國際合作交流、網路開源情資等等來進行駭客的追蹤與分析。

五、虛擬通貨犯罪-網路詐欺及釣魚犯罪

(一)虛擬通貨的追蹤以及分析：

Coinbase 的 Loenzo Zen 表示，Coinbase 可以配合司法機關的調閱，並且可以協助扣押於該交易所的虛擬通貨資產。

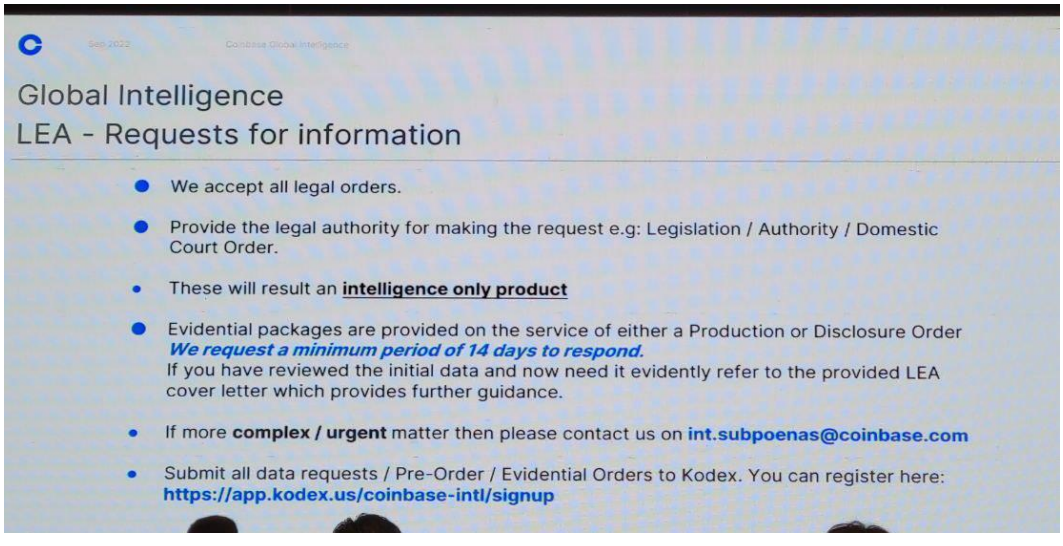

圖 7，Coinbase 配合執法機關事項

在調閱方面，司法機關可至網頁「https://app.kodex.us/coinbse-intl/signup」進行調閱，另外如果有更複雜的需求（如幣流追蹤、分析）等等服務，該公司亦可指派專人協助分析。其所提供之聯絡窗口為「int.subpoenas@coinbase.com」。

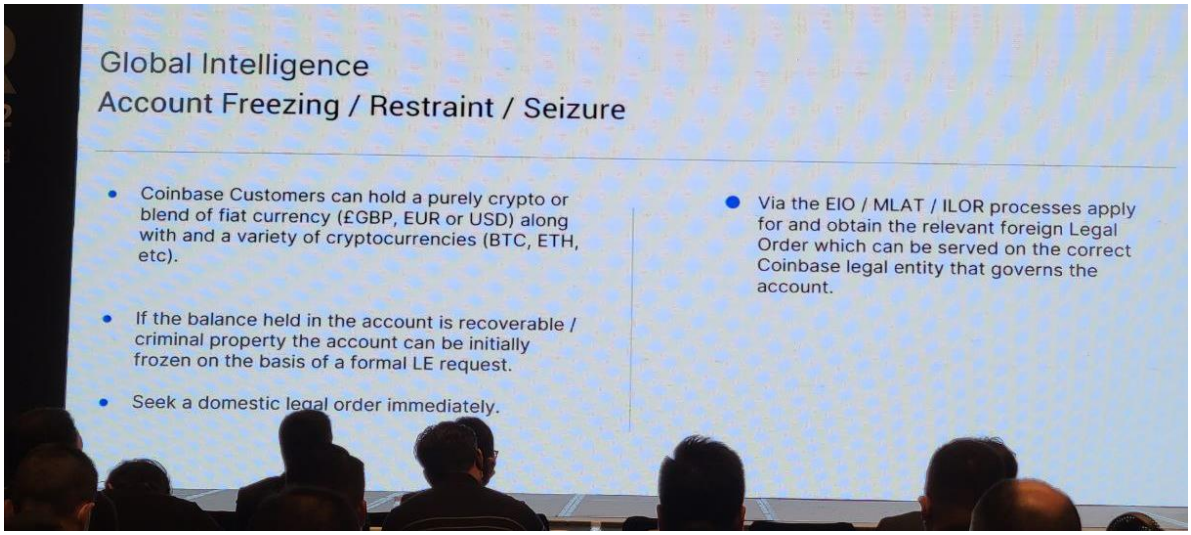

圖 8，Coinbase 窗口聯繫資料

根據 Chainalysis 的會中報告，位於莫斯科某一棟聯邦大樓，該址所申請的交易所帳號，常常涉及許多高風險錢包，可請我國 VASP 業者協助留意清查。另外其也提出有關朝鮮網軍常使用之特徵值，如常攻擊之對象、竊取之目標，以及虛擬通貨幣流還有出金之模式等等提供參考。如在朝鮮網軍常使用之幣流出金模式，就是常先以冷錢包轉至混幣器，再到交易所或是場外交易（OTCs）出金。

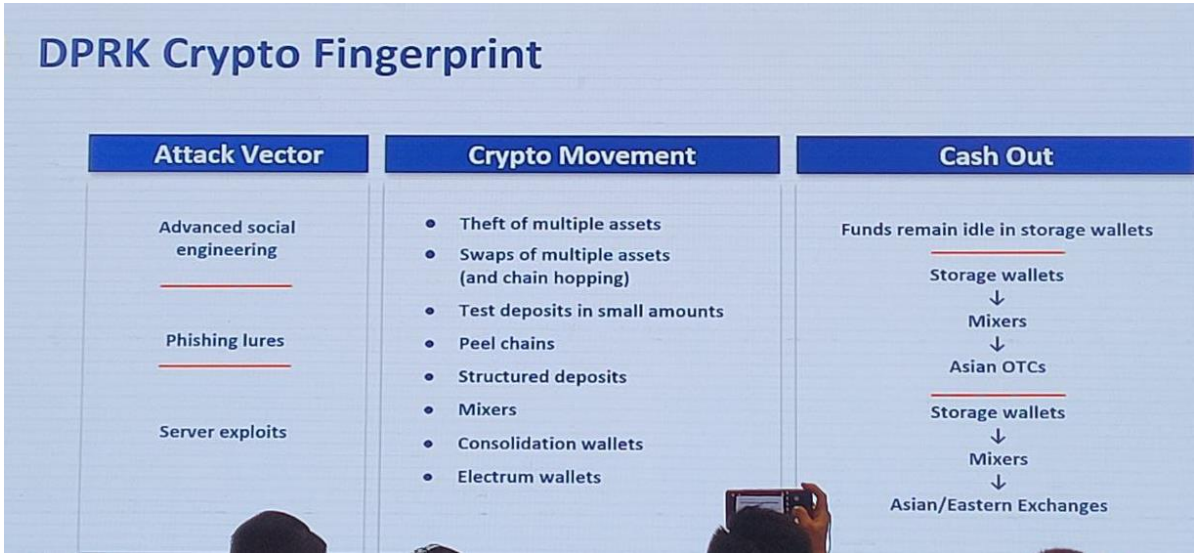

圖 9，朝鮮網軍攻擊路徑特徵

在英國的國家犯罪署（National Crime Agency）則認為，勒索軟體已走向服務化（Ransomeware as a Service）相關工具以及指引，均可以在市集中買到，相對於傳統的勒索軟體犯罪，其已走向個人化、獨立化以及大量化的攻擊。

(二)詐騙犯罪以及釣魚網址犯罪：

韓國律師 Jung Chul Kim 說明現行韓國也有很多投資詐騙，在 2022 年，共有 5 萬 2 千餘人被害，總損失金額達 70 億韓元(約合新臺幣 1.75 億)，另外在釣魚網址部分，先以網路公開情資（如臉書、領英等工具）鎖定交易所的高階管理幹部，再以高薪的方式，假裝是獵人頭或是新創公司等等，引誘在交易所的高管進行跳槽面試，最後再用釣魚郵件的方式，夾帶惡意檔案引誘高管開啟或點擊惡意連結。在取得高階主管之電腦主控權後，盜取該交易所之虛擬通貨。

緊接著由 Binance 公司講師 Jarek Jakuboek 介紹現行有關虛擬通

貨之詐騙手法，其聲稱目前有很多偽冒網址的攻擊，如駭客會申請「xn--binanc-l4a.com」之域名，然後在轉回 unicode 的時候，會轉成「binance.com」，以此誘騙受害者上當，並作釣魚網頁，騙取受害者之幣安帳密。

而另一種常見的手法是買谷歌的廣告，將其詐騙網址放到蒐尋後之第一個，另外也有觀察到偽冒名人的投資詐騙，比如製作假的馬斯克請大家一起來投資這個虛擬通貨，或是交友詐騙（其稱為 pigbutchered）等等手法。

而在 TRM 公司的介紹中，其為新成立的幣流追蹤公司，簡報者 Chris Janczewski 表示，其有組成一個調查團隊，部分成員為前 FBI 或是美國秘勤局的探員，專長為進行幣流追蹤以及分析，其可以找出跨鏈洗錢，在會後有向其詢問並索要名片及聯繫後方式，Chris 表示於臺灣尚無相關代理商，但其幣流追蹤軟體可先行提供本局試用，故本局於返國後，已先行電子郵件詢問其相關試用事宜，後續將持續進行聯繫。

最後是由在美國聯邦調查局 FBI 探員 Kevin Rodriguez 分享其調查著名的交易叛徒（Trade Traitor）事件，其中提到駭客組織 APT-38 利用長時間有計畫之攻擊，並運用多種入侵的手法，如前所述，利用獵人頭的理由，騙取交易所高管的信任，並成功引誘其點擊釣魚連結並入侵其電腦後，盜取該交易所的虛擬通貨，該局把是類案件稱為交易叛徒

（Trade Traitor）。另外在該次的盜竊案中，其相信攻擊來源係來自朝鮮網軍（APT-38），其於盜竊後，採用了相關複雜的洗錢方式，結合了跨鏈以及混幣器的機制，目前有部分的犯罪贓款遭到查獲扣押，另外還有 40%的虛擬通貨尚在鏈上。

六、智慧財產權的保護與分析

韓國近年因影劇及電影事業快速掘起，因此對於智慧財產權相當重視，該國會由警政署統一相關案件，並依案件的地區性分給各省的警察局去做查處以及扣押。另外其對於惡意域名，如偽冒網址、盜版網址的封鎖以及扣押，亦行之有年，目前已是相當成熟的作法，值得我國借鏡。

參、心得及建議

一、心得

參與 ISCR 2022 網路犯罪及執法應變策略國際研討會，除能了解世界各國執法機構與網路業務相關業者，針對新型態網路犯罪議題之因應措施及執法案例分享外，並針對虛擬通貨、元宇宙、AI 人工智慧以及勒索軟體等資恐議題進行分享與討論。此外，各國皆傾向陸續加入布達費斯公約(網路犯罪公約)，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，針對網路管理設施能設置相同標準，即時分享網路犯罪偵查情資，並於國際間在進行網路犯罪偵查時予以支援，蒐集情報形成資料

庫後，再用系統分析及整合。

未來網路將成為人民生活不可或缺的要素，物聯網將使未來世界與網際網路更密不可分，各類智慧型產品如智慧家電、無人駕駛車等，與各式雲端服務結合，然而網路帶來的便利與快速伴隨著是日新月異的網路犯罪問題，相關資通訊偵查技術至後續數位鑑識等一連貫技術，皆需本國投入技術發展及人才培訓，結合現有的硬實力與軟實力，提升相關偵查能量，以期面對未來資通訊技術的多變及挑戰。

二、建議

參加此類國際研習，可瞭解世界各國面對網路犯罪之因應策略，並了解其資通訊技術精進之程度，以及相關法令規範發展之趨勢，不僅了解國際間最新策略，提升國內刑事科技與犯罪偵查能量，並能與會各國執法機關建立跨境打擊犯罪、情報資訊交換等國際合作管道。ISCR 網路犯罪及執法應變策略國際研討會議每年皆有舉辦，建議每年派各業務相關科室至少 1 人以上前往參訓，以充分吸收最新相關策略、技術及成功經驗，並結合國內現有資通訊能量，因應網路科技快速進步時代之來臨。

圖 10、本次參訪人員合照