出國報告（出國類別：研究）

2024 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：楊永富 副隊長
派赴國家/地區：韓國 / 首爾
出國期間：113 年 8 月 26 日至 8 月 30 日
報告日期：113 年 11 月 7 日

摘要

本報告介紹 2024 年 8 月 27 日至 8 月 30 日在首爾舉辦的「2024 年網路犯罪對策國際研討會」，該研討會由韓國警察廳網路安全局主辦，旨在促進全球執法機構間的合作，探討網路犯罪的最新趨勢與技術應對。會議議題包括暗網與資訊傳遞安全、網路安全執法治理、數位取證等，對提升全球網路犯罪防治能力具有重要意義。

本署派遣業務單位人員參與此次研討會，目的在於深化對全球網路犯罪趨勢的理解，增強跨國執法合作，並學習應對新興科技犯罪手法。參會的主要目標包括：掌握網路犯罪的最新模式，如暗網與加密貨幣犯罪、交流有效的執法對策、強化數位取證技術應用、以及建立國際間的合作機制，以便提昇應對跨境網路犯罪問題。

研討會中討論了多個關鍵技術和挑戰，其中包括零信任架構的應用，這種架構不依賴內部信任，而強調持續的身份驗證，對當前的分散式網路安全需求至關重要；人工智慧（AI）在數位鑑識中的應用，尤其是在大數據篩選和案件加速偵查方面的潛力；以及加密貨幣在犯罪調查中的挑戰與應對策略，AI 和數據科學算法能有效追蹤與分析比特幣等加密貨幣的交易。

此外，跨國合作與資料共享被視為打擊網路犯罪的關鍵，研討會強調全球執法機構的協作對解決跨國網路犯罪問題的必要性，並提供了推動國際合作與數據共享的具體建議。

總體來說，這次研討會展示了先進的數位鑑識技術和網路安全措施，強調了人工智慧、零信任架構與跨國合作的重要性，未來，國內執法機構應積極推動這些新技術的應用，加強對網路安全和數位鑑識專業人才的培養，並促進全球協作，以應對日益複雜的網路威脅。

目次

壹、目的

韓國警察廳網路安全局自 2000 年起，每年定期舉辦國際網路犯罪研討會，邀請各國派員至研討會進行交流，了解全球網路犯罪趨勢、新興科技犯罪手法，分享各國執法單位有效偵查對策，以共同解決各國面臨的跨境網路犯罪問題，本(2024)年 8 月 27 日至 8 月 30 日於首爾舉辦「2024 年網路犯罪對策國際研討會」本次研討會議程包括暗網及資訊傳遞安全、網路安全執法治理、數位取證的範圍等議題。

本署指派業務單位人員出席，主要是為了深入了解全球網路犯罪的最新趨勢與挑戰，並加強與各國執法機構的合作與交流，提升自身對跨境網路犯罪的應對能力。此次研討會提供了以下幾個關鍵目標：

了解全球網路犯罪趨勢與新興科技犯罪手法：網路犯罪手法日益多樣化與複雜化，研討會將有助於學習並掌握最新的犯罪模式，尤其是在暗網和加密貨幣等領域的應用，這些都是目前全球執法機構面臨的重大挑戰。

交流網路安全執法對策：與來自不同國家的執法機構代表進行交流，分享各自的偵查經驗與有效對策，這不僅能增強跨國合作，也能為處理日益嚴重的網路犯罪提供新思路與工具。

強化數位取證技術：隨著網路犯罪的複雜性增加，數位取證技術成為關鍵。通過研討會上的學術交流與實務分享，能了解如何應對數位取證中的挑戰，並學習新興技術在數位鑑識中的應用。

建立跨國合作機制：網路犯罪具有高度的跨國性，因此強化與國際執法機構的協作至關重要。此次研討會提供了一個平台，促進各國警察機構間的協作與信息共享，進一步加強全球網路安全治理。

期藉由參與此次研討會，提升對網路犯罪防制的專業知識，建立跨國合作關係，並借助新興技術提高自身的執法效能，以更提昇執法知能、應對未來網路犯罪帶來的各種挑戰。

貳、過程

本次研討會為來自不同國家及領域的專業人士提供了一個寶貴的交流平台，

無論是業界，還是政府機構的代表，都能夠在此共同探討最新的議題，分享最佳的實踐經驗，並就如何應對當前的全球性挑戰提出具體的解決方案。

(一)零信任及安全網路

Cloudflare 的高級經理 Smrithi Ramesh 在「零信任與更安全的互聯網」主題演講中，強調了零信任的概念及其在當前網路安全架構中的重要性。她首先介紹了 Cloudflare 的服務及其全球影響力，指出該公司每天攔截超過 1580 億次威脅，管理全球 20%的互聯網流量，這使其在監測網路威脅和提供安全洞見方面具有獨特的視角。

「零信任」是一種不斷驗證的安全模型，旨在應對傳統圍牆式安全模型的不足。隨著雲端服務和混合工作模式的普及，傳統的實體防火牆和代理過濾裝置無法應對當今分散且複雜的網路環境。因此，零信任架構強調「永不信任，總是驗證」的理念，無論用戶或設備是否在受信任的網路內，都必須持續驗證其身份和行為，確保網路安全。

Ramesh 還談到安全訪問服務邊緣（SASE）的重要性。SASE 是一種將零信任理念應用於更廣泛的網路安全策略的方法。她提到，傳統的網路防護模式已不足以應對當前的安全挑戰，特別是在人員分散的工作環境下，零信任和 SASE 的結合成為新的解決方案。

此外，她以 Cloudflare 在 2023 年 10 月的一次攻擊事件為例，展示零信任在即時威脅防禦中的成效。在事件中，攻擊者試圖破壞 Cloudflare 的網路，但零信任控制措施在兩分鐘內阻止了數據洩露。此案例突顯出情報和可視性在及時應對威脅方面的重要性。

Ramesh 分享了 Cloudflare 在 2024 年初對威脅趨勢的分析，揭示了 DDoS 攻擊、生成式 AI 和機器人流量等新興威脅的增長趨勢。她指出，在漏洞被公開後，攻擊者可在 22 分鐘內利用該漏洞，而當前的網路流量中有 31%來自機器人，其中 93%是惡意的。DDoS 攻擊依然是針對網頁應用的主要威脅，Cloudflare 在 2024 年上半年已防禦了 850 萬次 DDoS 攻擊。這些威脅隨著生成式 AI 工具的普及而更加複雜，使攻擊規模和頻率前所未有。

她還強調了 Cloudflare 的 Radar 功能，這是一個可視化工具，能夠幫助企業

和執法機構監測和了解網路安全態勢，並應對針對亞洲國家和執法機構的攻擊趨勢。根據 Cloudflare 的數據，91%的網路攻擊始於電子郵件，該公司也積極追蹤垃圾郵件的來源，以提高針對這類威脅的應對能力。

總結來說，Ramesh 指出，零信任不僅對於企業，對政府、小型企業乃至個人用戶都具有重大意義。零信任不是單一產品，而是一種理念，透過「永不信任，總是驗證」的原則，網路安全可以更有效地應對數位轉型帶來的挑戰。她呼籲大家共同努力，以建立一個更安全、道德的互聯網。

(二)應用人工智慧加速案件偵查

Cellebrite 亞太區董事總經理 Mark Fitzsimons 在「AI 於調查中的應用」演講中強調，AI 技術正迅速革新數位調查，能幫助執法機構更快速地解決案件並發掘證據。他首先指出，Cellebrite 的各種 AI 驅動產品如 Premium、Guardian 和 Pathfinder，都在加速數據管理和分析、幫助用戶管理複雜數據等方面發揮關鍵作用。例如，Premium 可以從手機提取數據，Guardian 則便於證據管理與分享，Pathfinder 則專門處理大量的數位數據。

Fitzsimons 表示，AI 技術已廣泛應用於人們日常生活中的許多場景，如創意設計、串流媒體推薦、人臉辨識和網購等。但他也提醒，AI 同時被犯罪分子利用，生成 Deepfake（深度偽造）視頻、釣魚攻擊及社交工程攻擊等方式來實施犯罪，這些發展也給執法部門帶來新的挑戰。

他進一步說明，AI 並不會取代調查人員的角色，而是輔助工具，能夠加快調查進度和提升效率。隨著數位足跡的增加，尤其是手機中大量數據的增長，AI 可以快速篩選出潛在證據，讓調查人員聚焦於更高層次的分析。例如，在一宗涉及兒童性剝削的案件中，AI 技術協助篩選了 35TB 的數據，並識別出關鍵證據，使得犯罪嫌疑人最終被定罪 12 年半，這說明 AI 能夠在協助執法及促進司法公正方面發揮顯著作用。

AI 在調查中的應用範疇廣泛，包括協助調查人員尋找與毒品相關的數據或回溯特定歷史紀錄，甚至能在國際恐怖主義威脅方面提供自動翻譯，幫助理解外語資訊。此外，Pathfinder 的光學字符識別（OCR）技術能從影像中提取關鍵字，並進行相似圖像比對。例如，可以將監控影像中嫌疑人的衣著特徵與手機中的數

據比對，協助更迅速地鎖定嫌疑人。

Fitzsimons 建議，執法機構應推動小範圍測試項目，測試 AI 在調查中的潛在應用效果，並設計相關政策以確保技術的合理應用。他呼籲執法部門和技術專家密切合作，共同探索並推廣 AI 技術，以便在未來的案件調查和犯罪對抗中更有效地發揮作用。

總結來說，Fitzsimons 的演講闡述了 AI 在數位調查中的潛力與價值。他強調，AI 並非取代人類，而是強化調查過程的工具，能夠加快案件解決速度、提升調查質量並更有效地應對數位犯罪威脅，從而幫助執法機構維護正義與社會安全。

(三)人工智慧在 DFIR 工作整合的運用

HSI（美國國土安全調查局）的 James Greenmun 在演講中，深入探討 AI 技術如何融入數位鑑識（DFIR）流程，從概念驗證到工作流程整合的過程。他首先介紹了 HSI 的部門架構，並分析了當前數位鑑識的現狀。隨著 AI 技術的迅速發展，數位鑑識在存取性和隱私保護上也有所突破，尤其在翻譯、轉錄、影像與影片轉文字、圖案及標誌識別等方面。這些技術的應用讓調查工作更加高效，並加強了數據透明性與準確性。

Greenmun 指出，AI 在鑑識調查中的應用帶來了全新的可能性，例如透過語義搜索技術，調查人員可以基於概念而非僅限於關鍵字來搜尋資料，大幅提升效率。他強調，精確性和透明性是數位鑑識的基石，因此在測試這些 AI 技術時，需確保數據準確且具備隱私保護。他提到語音轉文字工具（如 Whisper）以及影像與影片轉文字、標誌檢測等技術的實踐應用，這些技術能有效處理不同來源的數據。

HSI 的概念驗證項目還包括與受害者識別實驗室的合作，利用影像識別技術來拯救孩童，例如透過識別校徽、運動隊服等圖像特徵以協助個化受害者。然而，Greenmun 坦言，這些 AI 模型的訓練和部署成本高昂，因此 HSI 正努力擴展這些技術在整個鑑識團隊中的應用。

AI 在數位鑑識中發揮著強大的輔助作用，但其挑戰同樣不可忽視，特別是 AI 模型可能出現「幻覺」錯誤，導致錯誤資訊的生成，這可能對鑑識結果產生負面影響。此外，Greenmun 提到惡意應用 AI 的現象，例如生成式 AI 模型（如 Stable

Diffusion）被用來製造虛假的兒童虐待圖像，可能誤導鑑識團隊並浪費調查資源。為此，HSI 正致力於開發偵測此類 AI 生成圖像的技術，以便鑑識過程中的線索更加可靠。

Greenmun 最後強調，AI 與現有鑑識工具的整合是未來數位鑑識的重要趨勢，HSI 正著手建立能處理語音、文字和影像的統一平台。AI 技術能讓數位鑑識的處理過程更加高效、精準，不僅協助揭露案件真相，也能在應對 AI 生成的惡意圖像時提升防範能力。透過小範圍測試並制定相關政策，HSI 希望能更深入地探索並推廣 AI 在鑑識調查中的應用，最終建立一個更健全的數位鑑識工作流程。

(四)加密貨幣的犯罪跡證識別及提取

印度中央調查局的警察總監 Pravin Mandloi 聚焦於利用 AI 和機器學習工具協助數位鑑識人員應對加密貨幣的調查挑戰。隨著加密貨幣成為犯罪活動中資金流動的重要方式，數位鑑識領域的專家們需要新的方法來迅速識別、追蹤並提取與犯罪相關的加密資產。

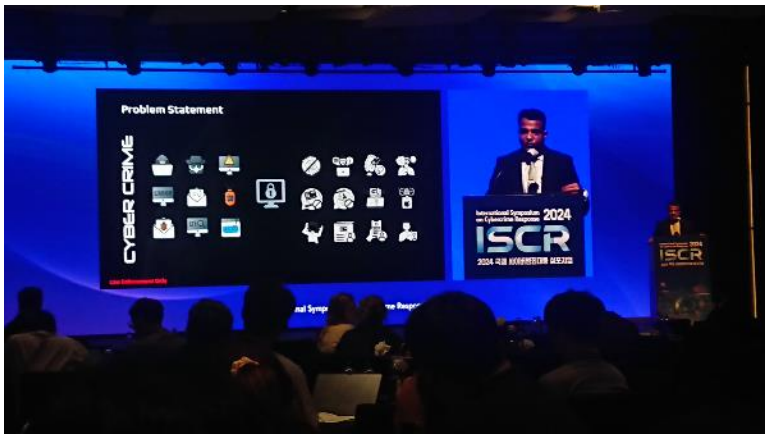
Mandloi 指出，加密貨幣的廣泛應用增加了調查的複雜性。以比特幣為例，犯罪組織會將資金轉換成不同幣種，如從比特幣轉為美元，再轉為瑞波幣等，使追蹤過程更加困難。他列舉了聯邦犯罪、網路詐騙、電話中心詐騙和恐怖融資等六大犯罪類型，強調加密貨幣與去中心化金融技術的結合如何助長犯罪集團的運作。例如，ISIS 利用比特幣捐款的方式來籌集資金，並通過圖表展示了從 2016 年到 2024 年加密貨幣在恐怖活動資金流向中的增長趨勢。為應對這一挑戰，執法人員需要 AI 工具協助追蹤資金來源和去向。

Mandloi 展示了如何利用 AI 和數據科學算法自動分析加密貨幣交易數據，並揭露嫌疑人活動的可視化數據網路。這些工具可以快速掃描大量數位證據，提取如加密貨幣錢包地址和 QR 碼等信息，協助執法人員辨識資金流轉模式。他也介紹了在詐騙監控中的應用範例，利用監控儀表板及時監測嫌疑人的交易，從而讓犯罪分子難以隱藏資金流向。

此外，他談到新興的加密貨幣技術帶來的挑戰，例如閃電網路和去中心化金融（DeFi），這些技術使加密貨幣的轉移速度和便捷性提升，同時也增加了追蹤難度。他指出，加密通訊和隱形水印技術也讓數位鑑識更為複雜，因此 AI/ML 工具

成為解決之道。這些技術能夠在海量數據中進行意圖解析、快速識別犯罪組織的數位足跡。

最後，他分享了案例研究，展示 AI/ML 工具在實際偵查中的應用效果，例如在烏克蘭和俄羅斯戰爭期間偵測到的詐騙比特幣地址。這些工具的運用展示了 AI/ML 技術在數位鑑識領域的重要性，提升了識別與追蹤加密貨幣犯罪的效率。Mandloi 總結道，隨著數位犯罪手段不斷演變，未來執法機構需更多地依賴 AI 和數據分析工具，以應對日益增多的加密貨幣犯罪挑戰。



說明：加密貨幣犯罪案分析

(五) 「終局計畫」案例分享

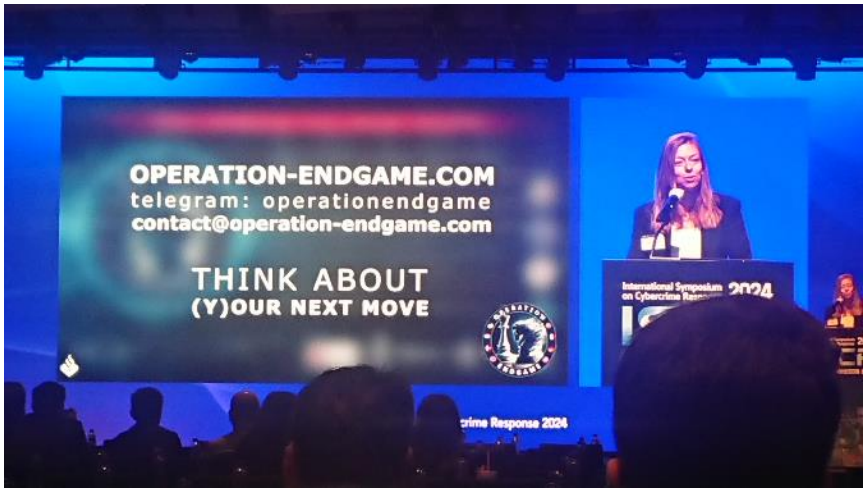
荷蘭警察數位協調員 Fieke Miedema 介紹了「終局計畫」的執行過程及成效，該行動旨在清除惡意程式對網路生態的威脅，並由多國聯手進行，是迄今針對初始訪問機器人網路和勒索軟體的最大行動之一。本次行動涉及荷蘭、德國、法國等國的協作，以及來自美國、加拿大和英國的支援，歐洲刑警組織和其他信息技術支持機構也為行動提供了關鍵協助。

Miedema 指出，勒索軟體已成為嚴重的國際問題，其年支付金額高達 11 億美元，為此「終局計畫」的重點是對抗初始訪問機器人網路，這些網路通常用於幫助犯罪分子發起勒索軟體攻擊。行動過程中，各國以並行調查方式進行跨境資訊共享，利用了歐盟相互支援協議和布達佩斯網路犯罪公約，讓合作無縫銜接。數據共享和國際協作的建立是行動成功的關鍵，並依靠私營機構提供的技術和情報支援，這些企業能封鎖犯罪活動並向受害者發出通知，協助執法部門有效控制犯罪活動。

行動過程採用了多層面的策略，包括從打擊犯罪者、阻斷基礎設施、監控財務活動等方面入手。Miedema 分享了針對犯罪者的手法，例如針對藏匿於非合作國家的犯罪分子，將其信息告知其周圍人員，試圖透過公開其身份來增加壓力。在基礎設施方面，終局計畫針對機器人網路的控制伺服器進行打擊，利用了「誘導網」來幫助受害者清除惡意軟體並斷開與攻擊者的連結。這種方式減少了攻擊者的掌控力，雖然部分伺服器會復活，但長期干擾仍對犯罪活動產生了顯著影響。

私營機構的協作在行動中至關重要，Miedema 提到他們與「Have I Been Pwned」等公司合作，建立「Check Your Hack」網站，讓用戶檢查是否受駭客影響。此外，他們向主機代管商發送多個下架請求，有效減少犯罪者的操作空間。總體來看，行動成功關閉了多個惡意系統如 IcedID、Smoke Loader 和 Bumblebee 等，為打擊勒索軟體活動提供了新模式。儘管部分伺服器會間歇性復活，但終局計畫的成功標誌著國際網路治理的新起點。

這次行動也揭示了惡意駭客的活躍，例如來自北韓的駭客組織，自 2009 年起不斷對全球政府和基礎設施發動攻擊，並逐漸將勒索軟體變為牟利的工具。Miedema 指出，國際社會只有透過持續協作才能有效遏制此類跨國犯罪行為。未來，她希望有更多國家和機構加入這場全球性的網路治理行動，以共同應對網路犯罪的挑戰並保護網路安全。



說明：「終局計畫」案例分享

(六)保護數位環境：有效執法參與網路安全的策略

在 ISPR 會議上，幣安公司的副主管 Nils Andersen-Röed 分享了加密貨幣的挑

戰，及其在執法和網路安全中的角色。Andersen-Röed 有多年處理暗網和加密貨幣相關案件的警察經驗，他描述了執法部門在對抗數字犯罪中所面臨的變化，並概述了加密貨幣在當前金融犯罪中的位置。

加密貨幣因其去中心化特性和匿名性，被越來越多的犯罪分子利用來洗錢、詐騙和掩蓋犯罪資金來源。比特幣等加密貨幣波動劇烈，讓追蹤變得困難。即便如此，Andersen-Röed 表示，實際上加密貨幣中的犯罪資金比重並不高，根據估算，加密貨幣犯罪僅佔加密貨幣總交易量的 0.3%-0.4%，而傳統金融體系中的犯罪資金約為 2-5 兆美元。

在處理加密貨幣犯罪中，公開的區塊鏈提供了透明度，讓追蹤交易成為可能。通過分析區塊鏈地址和交易紀錄，調查人員可以部分地追踪到犯罪資金流向和交易模式。部分企業也致力於研究區塊鏈地址，嘗試將其與實際持有人建立聯繫。雖然這些分析工具無法掌握所有地址，但它們可以提供重要的線索，為調查提供基礎。

然而，Andersen-Röed 指出，犯罪分子已經開始利用更複雜的技術，如 VPN、Tor 網路、API 攻擊等，來掩蓋行蹤。部分犯罪組織甚至運用東南亞客服中心的運營模式，建立完整的犯罪鏈條，並且加密貨幣詐騙的形式多樣，包括愛情詐騙和假投資詐騙等。這些組織還會通過賭博平台和轉移服務，使資金流轉過程更加隱蔽，增加執法機構的追踪難度。

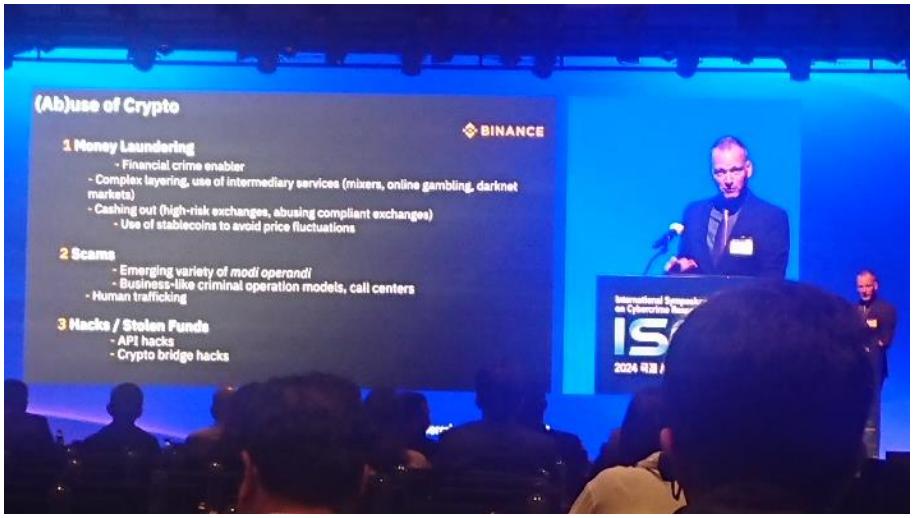
Andersen-Röed 也談到，幣安公司作為全球最大的虛擬資產服務平台之一，擁有超過 2 億個用戶帳戶，因此經常是執法單位調查的對象。為了應對日益增長的需求，幣安公司在 19 個國家取得了監管許可，並加強了與各國執法機構的合作，致力於打擊加密貨幣犯罪。幣安公司也提供了資源，如幣安公司 Academy，為用戶和執法人員提供加密貨幣的基礎和高階知識。

此外，Andersen-Röed 指出，犯罪分子已經開始運用 AI 生成虛假身份和賬戶，使追蹤變得更加困難。AI 技術的進步為執法帶來新挑戰，這需要調查人員掌握數位調查工具並接受相應訓練，提升調查能力。

在討論透明度和執法配合方面，Andersen-Röed 強調，幣安公司始終配合各國的執法機構。為協助執法機構更快識別犯罪資金，幣安公司接受合法請求來協助查找可能涉及犯罪的帳戶，但無法全面公開所有用戶地址。對於這些挑戰，他

建議執法單位使用商業追踪工具並與交易所進行合法的協調。

總結而言，Andersen-Röed 的演講突顯了加密貨幣在犯罪領域的快速發展和跨國合作的必要性。加密貨幣帶來了更便捷的資金流動，但其匿名性和數位特性也增添了調查難度。隨著數字金融的持續發展，執法機構將需要加強網路安全措施、增強數位調查能力並與加密貨幣平台保持密切合作。



說明：保護數位環境議題分享

(七) 跨國資料請求的治理

在 Nima Binara 的演講中，他以私人企業 Google 法律顧問的身份，探討了跨國政府對數據請求的治理問題，並強調了隱私與執法需求間的微妙平衡。Binara 指出，隨著數位化的普及，全球各國執法機構對電子證據的需求不斷增加，特別是在網路犯罪與常規犯罪的調查中，私營企業如 Google 常常擁有關鍵證據。這種數位證據依賴不僅提升了企業數據披露的請求數量，也加深了法律規範的複雜性，尤其在跨國數據請求方面。根據 Google 的透明報告，2023 年僅上半年，Google 收到超過 20 萬份政府數據請求，顯示了這一趨勢的劇烈增長。

Binara 進一步討論了跨國數據請求的挑戰。以美國法律為例，Google 作為美國公司，無法隨意披露用戶數據，特別是在涉及 ECPA《電子通訊隱私法》規定的情況下。只有在存在生命威脅的緊急情況或兒童安全問題（如人口販運、兒童性剝削）時，美國服務提供商才可依照美國法律回應非美國執法機構的數據請求。這種限制促使部分國家考慮採取單邊行動來獲取數據，然而，Binara 認為，應以多邊協議來解決跨國調查中的數據需求，以避免隱私權侵害和法規衝突。

接著，Binara 談到當前數據治理領域的國際進展，強調了《布達佩斯公約》第二附加議定書的貢獻，該議定書允許簽約國加速數據分享，並提供緊急情況下的數據披露管道。他稱此為跨國數據協作的積極信號，同時指出，私營企業在制定過程中扮演了建議角色，這促使該協議在實踐上更具實效。此外，歐盟的電子證據法規、經濟合作與發展組織（OECD）的數據訪問指引和聯合國的網路犯罪公約也引起全球關注，尤其是在數據共享和人權保障方面。

此外，Binara 還提到美國的《雲法案》協議，這些協議允許美國服務提供商在特定條件下直接回應其他司法管轄區的數據請求，如英國和澳大利亞。這些協議的簽署需基於兩國皆具備足夠的隱私和公民自由保護，並限定適用於重大犯罪。這些協議呈現了一個重要轉變，即多邊合作已成為有效數據治理的必要條件，且私營企業仍有權拒絕不合理請求。

最後，Binara 展望未來，認為在數據治理領域中的多邊協議將是關鍵，並相信政府應扮演規範制定的主導角色，而非將此責任交給私營部門。Google 期待未來在這些框架中，與全球利益相關方合作，找到長遠且具效益的解決方案，以平衡公共安全與個人隱私。

(八) 國際刑警組織減少網路犯罪全球影響的方法

國際刑警組織（INTERPOL）在全球網路犯罪打擊工作中，通過跨國合作、技術支持與預防犯罪等多方面策略，致力於降低網路犯罪對全球的影響。Peter STANIER，在一次關於此議題的演講中，分享了國際刑警組織如何結合各國政府、私人部門及國際機構的力量，有效因應日益複雜的網路犯罪威脅。

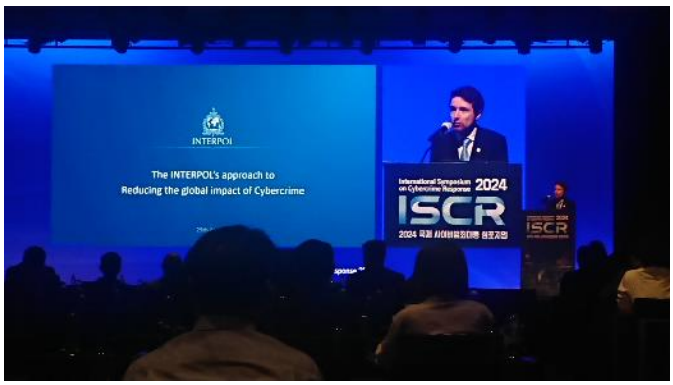
首先，國際刑警組織充分認識到網路犯罪的跨國特性和多變性。網路攻擊模式和特性常在各國之間快速傳播，因此，全球合作顯得尤為重要。國際刑警組織積極協助各會員國，並與世界經濟論壇、聯合國等機構合作制定政策，提升全球網路安全治理水平。例如，布達佩斯公約促進了成員國間的法律協調與合作，奈及利亞等國也在國際刑警組織的協助下加入了該公約，以應對跨國網路犯罪的挑戰。此外，國際刑警組織針對網路犯罪舉行跨國行動，特別是在非洲和亞洲進行針對性的打擊，以確保不同地區的犯罪威脅得到有效應對。

在行動層面，國際刑警組織不僅協助會員國進行緊急應對，也在大型行動中

發揮領導作用。例如，針對商業詐騙的「Operation Jackal 3」行動和南美的「Operation River」行動都展示了國際刑警組織與私人部門密切合作的成果。此外，名為「Gangster Web」的調查行動更是其中之一的重要案例，該行動持續四年並涵蓋 20 多個機構，致力於打擊勒索軟體犯罪，顯示了國際合作在網路犯罪防治中的必要性。

國際刑警組織的工作還涉及到對網路犯罪根源的研究與預防。自 COVID-19 疫情以來，全球的網路犯罪活動顯著增加，尤其對醫療機構的攻擊。國際刑警組織因此與私人部門合作，協助全球醫療系統應對威脅，並發布威脅評估報告，幫助會員國及時瞭解如勒索軟體、數據洩露等主要風險。此外，國際刑警組織透過能力建設和專業訓練提升各國的應對能力，這包括針對勒索軟體的模擬演練，以及提供加密貨幣犯罪偵查的平台培訓，幫助成員國提升網路安全防護水準。

在全球網路犯罪治理中，國際刑警組織始終堅守中立，尊重各會員國的數據主權與需求，並以透明、公平的方式分享信息。它致力於讓不同文化背景和法律體系的成員國在治理網路犯罪時都能有效協作。在此過程中，信任和協作至關重要。STANIER 強調，國際刑警組織將持續推動跨國調查和行動，期望能夠透過全球社群的緊密合作，全面提升網路安全並有效打擊網路犯罪威脅。



說明：國際刑警組織分享打擊網路犯罪策略

參、心得及建議

ISCR 2024 研討會聚焦於零信任安全、人工智慧（AI）、數位鑑識、加密貨幣調查及國際網路犯罪治理等議題，展現當前數位安全領域的挑戰和創新解決方案。本心得將探討零信任架構的實踐、AI 技術在調查中的應用、加密貨幣犯罪追蹤的進展，以及國際合作在網路犯罪對抗中的重要性。

一、零信任與安全架構的革新

零信任架構被提出作為應對當前複雜網路挑戰的核心解決方案，強調「永不信任，總是驗證」的理念。隨著雲端技術的廣泛應用和混合工作模式的興起，傳統的圍牆式安全模型已顯得不足。零信任的核心在於持續檢驗用戶及設備的身份和行為，並通過實時監控和威脅檢測技術，防禦 DDoS 攻擊及惡意流量。

透過整合零信任與安全訪問服務邊緣（SASE），企業能更高效地應對數位威脅。例如，某案例中零信任架構成功在短時間內阻止數據洩露，展示了其即時防禦能力。此外，利用工具進行威脅可視化與分析，幫助組織更準確地應對垃圾郵件和攻擊源。這表明零信任不僅是一種技術，更是一種應對數位轉型的安全文化。

二、人工智慧在數位調查中的應用

AI 技術被廣泛運用於數位調查中，以提升效率和精確性。AI 工具可快速處理海量數據，篩選出關鍵證據。例如，在處理大規模數據案件時，AI 能加速篩選過程並快速定位嫌疑人，為執法單位爭取寶貴時間。

此外，語義搜索和影像分析技術進一步提升了 AI 的應用範圍，能從照片中提取如校徽或特徵服裝等關鍵資訊，幫助定位案件相關方。然而，AI 技術也存在風險，例如誤判或生成不實資訊，這要求執法單位保持高度的準確性和透明度。

另一挑戰是 AI 技術的濫用，例如犯罪分子利用生成式 AI 製作深度偽造（Deepfake）內容或假冒影像，干擾調查工作。為應對這些挑戰，執法單位需開發識別 AI 生成內容的技術，確保調查方向的正確性。

三、加密貨幣犯罪的調查與技術進步

加密貨幣因其匿名性和去中心化特性，成為犯罪分子資金流動的重要工具，例如用於恐怖融資或詐騙。AI 和機器學習工具能自動分析加密貨幣交易模式，快速揭露資金流向。執法人員可藉此識別錢包地址及其相關交易，提升犯罪追蹤效率。

然而，隨著技術的進步，如閃電網路和去中心化金融（DeFi），加密

貨幣的調查變得更加複雜。一些案例顯示，犯罪分子利用新技術掩蓋資金流動，但透過工具分析，執法人員能成功追蹤犯罪行為，例如識別虛擬貨幣詐騙地址。

儘管加密貨幣犯罪佔總交易量的比例較低，但執法單位仍需應對犯罪分子使用匿名技術的挑戰。為此，調查機構與私人企業合作，開發監控與分析工具，同時教育公眾如何識別加密貨幣詐騙行為。

四、國際合作在網路犯罪治理中的作用

針對跨國網路犯罪的治理，國際合作成為關鍵。一些成功案例顯示，執法單位通過協作打擊勒索軟體攻擊的基礎設施，並幫助受害者恢復正常運作。數據共享和公私合作在其中發揮了重要作用，例如建立供用戶檢查是否受駭客影響的平台。

此外，針對國家支持型犯罪組織如駭客團隊的威脅，國際協作更顯重要。僅憑單一國家無法有效應對此類威脅，唯有整合多國力量並共享技術資源，才能形成強而有力的防禦機制。

五、技術進步與倫理挑戰的平衡

與會者一致認為，技術的進步在提供便利的同時，也帶來隱私與道德挑戰。例如，AI 與加密技術既可促進執法效率，也可能被濫用於非法活動。因此，執法單位與私人企業需要攜手制定相關規範與政策框架，確保技術被負責任地應用於犯罪調查與預防。

ISCR 2024 揭示了數位安全領域的多重挑戰與創新應對策略，涵蓋零信任架構的實踐、AI 在調查中的應用、加密貨幣犯罪的追蹤及國際合作的重要性。這些討論反映了技術進步對安全防禦的助力，也強調了全球協作與倫理考量在未來數位安全治理中的角色。隨著網路環境日益複雜，技術、政策和合作的結合將是構建更安全數位生態系統的關鍵。

結論與建議

在當前數位時代，隨著網路威脅和數位犯罪的日益增長，執法部門須採取有效的策略來應對這些挑戰。多位專家在不同領域的演講中提出了針對現代網路安

全問題及數位犯罪的解決方案，並強調了人工智慧（AI）、區塊鏈技術、數位鑑識（DFIR）等領域的應用。以下是關於執法策略的關鍵建議：

1. 強化零信任安全架構

隨著雲端服務的普及和混合工作模式的出現，傳統的圍牆式安全模型已不再適應現代的網路環境。零信任架構應運而生，這種架構強調「永不信任，總是驗證」的原則，即使用戶和設備位於受信任的網路內，也必須持續驗證其身份和行為。執法部門可採取零信任模式來確保內部系統不會被未經授權的訪問者突破。此外，結合安全訪問服務邊緣（SASE）策略，將零信任與更廣泛的網路安全策略結合，進一步增強系統的防護能力，這對於防範來自外部和內部的複雜威脅至關重要。

2. 運用人工智慧提升調查效率

AI 在數位調查中的應用已經顯示出顯著的潛力，特別是在處理大量數據的過程中。AI 技術可以快速篩選和分析潛在的證據，幫助調查人員提高工作效率。例如，AI 可用於識別手機數據中的關鍵證據，或是對比影像資料來定位嫌疑人。在具體的案件中，AI 能夠協助分析數百 TB 的數據，並且篩選出關鍵證據，這樣調查人員能夠聚焦於更高層次的分析。此外，AI 也能在協助揭露犯罪行為方面發揮重要作用，例如透過深度偽造視頻或社交工程攻擊等手段進行的網路詐騙，AI 可以幫助執法機構提高對這些技術的識別能力。

3. 數位鑑識中的 AI 整合

在數位鑑識領域，AI 技術的應用可以大大提升資料處理的效率和精準度。AI 可以進行語音轉文字、影像辨識、圖像標誌檢測等工作，並且通過語義搜索技術讓調查人員能基於概念而非單純的關鍵字來檢索資料，這樣能加速案件的調查進程。然而，AI 的應用也需要謹慎，因為 AI 模型可能會出現錯誤或「幻覺」現象，對鑑識結果產生影響。因此，執法機構需要對 AI 技術進行嚴格測試和驗證，並且在部署時確保數據的準確性和隱私保護。

4. 加密貨幣與區塊鏈技術的挑戰

加密貨幣的去中心化和匿名性使其成為犯罪分子進行洗錢、詐騙和資金掩飾的工具。儘管加密貨幣的交易在總體交易量中占比不高，但由於其流動性高和匿名性強，依然是數位犯罪的熱點之一。執法機構可以利用區塊鏈技術的公開透明性來追蹤加密貨幣的交易，分析區塊鏈交易紀錄及錢包地址，從而揭露犯罪資金流向。對於新興的加密貨幣技術，如閃電網路和去中心化金融（DeFi），執法機構需要採取更複雜的數據分析手段來識別和追蹤資金的流動。

5. 提高執法與私營部門的合作

現代數位犯罪已經跨越了國界，國際間的合作顯得尤為重要。執法機構應加強與私營企業的合作，利用它們的技術和情報支援來打擊犯罪活動。企業在數位安全領域的專業知識，特別是在監控和封鎖惡意軟體、偵測不法交易等方面，能為執法部門提供及時有效的幫助。此外，私營部門的資源可以協助監控網路犯罪行為，並向受害者發出通知，進一步加強跨國協作，提升打擊網路犯罪的效率。

6. 強化跨國合作以應對勒索軟體等網路威脅

勒索軟體的蔓延已經成為全球範圍內的重大威脅，並且常常涉及到跨國犯罪集團。各國政府和執法機構應加強合作，進行跨國信息共享，共同應對網路犯罪。以「終局計畫」為例，這一行動透過多國協作、信息共享和技術支援，成功打擊了勒索軟體的攻擊並清除了網路生態中的威脅。這類合作模式可以作為未來跨國打擊網路犯罪的範本，強調了執法部門、國際機構和私營企業之間的協同作戰。

7. 應對 AI 生成的惡意內容

隨著生成式 AI 技術的發展，犯罪分子已經能夠利用 AI 技術製作虛假圖像或視頻來掩蓋犯罪事實。AI 生成的惡意內容在數位鑑識過程中帶來了新挑戰，特別是在兒童虐待圖像的偽造方面。執法機構需要發展 AI 檢測技術，以識別這些由 AI 生成的虛假證據，並且增強對 AI 技術的監控，確保不會被不法分子所利用。

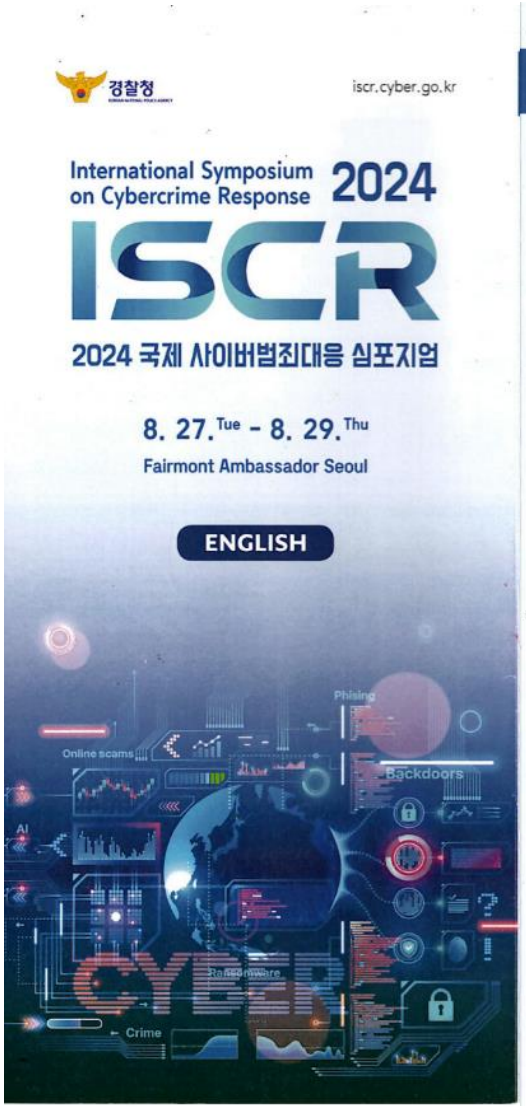
8. 推動數位安全教育與技能訓練

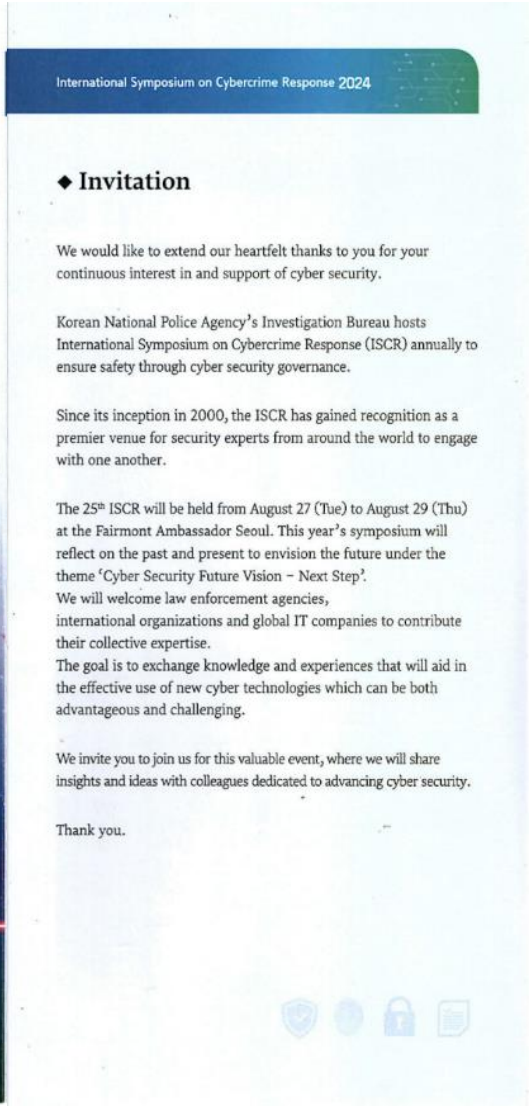
隨著技術的不斷發展，執法機構的專業知識和技能必須與時俱進。對於數位安全和加密貨幣等領域，執法人員需要接受專業的培訓，掌握最新的數位調查工具和技術。此舉將有助於他們提高應對各類新興威脅的能力，從而能夠更有效地維護公共安全並打擊數位犯罪。

總結來說，隨著技術的進步和數位威脅的多樣化，執法部門需要不斷創新和強化應對措施。通過加強零信任安全架構、利用 AI 技術加速調查、強化跨國合作等方式，執法機構可以更加高效地應對現代網路犯罪的挑戰。

附錄

「2024 年網路犯罪對策國際研討會」議程表





Programs

Date	Time	Program	
Day 1 (8. 27.)	12:00~13:00	Welcome Reception	
	13:00~14:00	Pre-ceremony Event	Keynote Address 1 by Pedro VERDELHO, Chair of the Committee of Cybercrime Convention (T-CY), Council of Europe
			Keynote Address 2 by LIM Jong In, Special Advisor to the President for Cyber, Office of the President
	14:00~14:30	Opening Ceremony	
	14:30~15:30	Coffee Break	
	15:30~16:30	Open Session	1. Next Step: Future Vision of Cyber Safety
	16:30~17:30		2. Korean Society's Cybercrime and Global Response
Day 2 (8. 28.)	09:30~11:30	Closed Session	1. Dark Web and Secure Messaging App : Hideout for Criminals
	11:30~13:00	Lunch Break	
	13:00~15:00	Closed Session	2. Double-edged Sword of Hyper-connectivity : Expanded Network with Heightened Vulnerability
	15:00~15:20	Coffee Break	
	15:20~16:50	Closed Session	3. Expanding the Scope of Digital Forensics and Transcending its Limitations
	18:30~20:30	Welcome Banquet for Overseas Law Enforcement Officers	
Day 3 (8. 29.)	09:30~12:30	Closed Session	4. Establishing Governance of Law Enforcement for Cybersecurity (10:50~11:10 Coffee Break)

Download Open Session Files

Please scan the QR code to download open session files.

International Symposium on Cybercrime Response 2024

Pre-ceremony Event & Opening Ceremony (8.27.Tue)

Time	Program
13:00~14:00	Pre-ceremony Event Keynote Address 1. Pedro VERDELHO | Chair of the T-CY, Council of Europe 2. LIM Jong In | Special Advisor to the President for Cyber, Office of the President
14:00~14:06	Opening Announcement
14:06~14:10	Opening Remarks CHO Ji Ho | Commissioner General, KNPA
14:10~14:13	Opening Video
14:13~14:20	Congratulatory Remarks
14:20~14:24	Congratulatory Video Message 1. Ghada WALY | Executive Director, UNODC 2. Jürgen STOCK | Secretary General, INTERPOL
14:24~14:30	Celebratory Performance

Day 1 (8.27.Tue)

Time	Program
Session 1 : Next Step: Future Vision of Cyber Safety	
15:30~16:00	UAM Cyber Threat and Future Public Safety YOON Donghwan | Senior Research Engineer, KIAST
16:00~16:30	Intelligent Malicious Script Detection Technology KIM Jungtae | Principal Researcher, ETRI
Session 2 : Korean Society's Cybercrime and Global Response	
16:30~17:00	Digital phishing Response System to Minimize User's damage in Korea LEE DongYeon | Director of Digital Yser Damage Response Division, KISA
17:00~17:30	The Way Forward: The FBI's Evolving Cyber Strategy Brett LEATHERMAN | Deputy Assistant Director, FBI

Day 2 (8.28.Wed)

* Closed Session will be disclosed only to the law enforcement members with prior approval

Time	Program
Session 1 : Dark Web and Secure Messaging App : Hideout for Criminals	
09:30~10:10	Investigating illegal scam/spam activities using SNS, Telegram and SIM boxes detection Alexander QUIGNON | Regional Director of Korea, Cognyte
10:10~10:50	Shutting down an anonymity tool for criminals: The 911 S5 disruption William HALL | Assistant Deputy Chief, U.S. Department of Justice
10:50~11:30	Uncovering Evidence in the Shadows of the Dark Web: Reveal The Onion KIM Jaeki | Director, Threat Research & Intelligence Center, S2W

Day 2 (8.28.Wed)

* Closed Session will be disclosed only to the law enforcement members with prior approval

Time	Program
Session 2 : Double-edged Sword of Hyper-connectivity : Expanded Network with Heightened Vulnerability	
13:00~13:40	Suggesting customized guidelines based on analysis of top LLM threats PARK Junyoung | Engineering Manager of Global Platform Dev, NAVER Cloud
13:40~14:20	Zero trust and a safer internet Smrithi RAMESH | Senior Manager Outreach- APJC, Cloudflare
14:20~15:00	TBD John CRAIN | Senior Vice President & CTO, ICANN
Session 3 : Expanding the Scope of Digital Forensics and Transcending its Limitations	
15:20~15:50	AI in Investigations: Accelerating Case Resolution and Uncovering Evidence Mark FITZSIMONS | Managing Director for APAC, Cellebrite
15:50~16:20	From AI Proof of Concept to DFIR Workflow Integration James GREENMUN | Program Manager, HSI
16:20~16:50	Identification and Extraction of Crypto Currency Artifacts AI/ML-Toolkit for Investigators | Digital Forensic Examiners Pravin MANDLOI | Superintendent of Police, Central Bureau of Investigation, India

Day 3 (8.29.Thu)

* Closed Session will be disclosed only to the law enforcement members with prior approval

Time	Program
Session 4 : Establishing Governance of Law Enforcement for Cybersecurity	
09:30~10:00	A Case Study of Operation 'Endgame' Fieke MIEDEMA | Digital coordinator, Politie, Netherlands
10:00~10:20	Recent Cyberterrorism Trends and Proposals for Response Strategies LEE Seungwoon | Section Chief of Cyber Terror Response Division, KNPA
10:20~10:50	Securing Digital Landscapes: Strategies for Effective Law Enforcement Engagement in Cybersecurity Nils ANDERSEN-RÖED | Deputy Head of Financial Crime Compliance, Binance
11:10~11:40	Governance of Cross-Border Data Requests: A Private Sector View Nima BINARA | Counsel, Google LLC
11:40~12:00	International Response Against Exploitation (InaRAE) for the Removal of CSAM HAM Young-wook | Director of Cybercrime Investigation Division, KNPA
12:00~12:30	INTERPOL's approach to reducing the global impact of Cybercrime Peter STANIER | Cybercrime Intelligence Officer, INTERPOL