

摘 要

第 11 屆 IAP 亞洲及太平洋地區會議於 113 年 11 月 27 日至 29 日在香港舉行，主題為「科技時代的有效檢控服務」，探討科技發展對刑事司法的影響及國際合作的重要性。與會者來自 28 個國家，討論涵蓋法律改革、數位證據取證、虛擬資產監管、人工智慧詐欺等議題。新加坡介紹應對數位身分詐欺的法律改革，荷蘭分享國際合作打擊網路犯罪的經驗，香港與歐盟則強調數位證據管理與 DeFi 監管的挑戰。此外，多國提及人工智慧在詐欺與犯罪中的應用，並強調技術發展對司法體系的衝擊。

本次會議強調國際司法合作的重要性，SEAJust 與 e-CODEX 等平台有助於加速跨境案件處理。數位轉型亦為討論重點，澳洲、韓國與菲律賓分享電子證據管理與遠端審訊經驗，以提升檢控效率並保護受害者。會議建議司法機關加速數位化，強化數據共享與跨國合作，確保司法體系能有效應對科技犯罪挑戰，維護司法公正。

目錄

壹、	前言.....	3
一、	國際檢察官協會(IAP)之簡介.....	3
二、	第 11 屆 IAP 亞洲及太平洋地區會議(下稱 IAP 亞太地區會議)在香港舉行	3
三、	本次會議主題：科技時代的有效檢控服務.....	4
貳、	第 11 屆 IAP 亞洲及太平洋地區會議內容.....	4
一、	113 年 11 月 28 日開幕儀式(Opening Ceremony).....	4
二、	113 年 11 月 28 日會議.....	5
(一)	國際檢察官協會業務重點說明.....	5
(二)	議程一 (Plenary 1)：為打擊科技犯罪推行法律改革的需 要、挑戰、成效及經驗分享.....	8
(三)	議程二 (Plenary 2) 從社交媒體、去中心化金融談到虛擬資 產.....	12
(四)	特別議程 (Special Plenary Session) 通過刑事事宜相互協 助加強國際合作，應對新挑戰.....	15
三、	113 年 11 月 29 日會議.....	18
(一)	議程三 (Plenary 3) 檢控網絡罪行的經驗分享—數位證據的 取證及處理.....	19
(二)	議程四 (Plenary 4) 法庭及檢察部門的數位轉型—科技發展 對刑事證據及法律程序的影響.....	22
參、	心得及建議.....	27
一、	數位時代司法挑戰與應對策略.....	27
二、	國際合作與司法互助的重要性.....	27
三、	數位轉型與法庭現代化的推動.....	28
四、	未來展望：強化司法數位化與國際合作.....	28

壹、前言

一、國際檢察官協會(IAP)之簡介

國際檢察官協會（International Association of prosecutors，下稱 IAP）是一個非政府、非政治之組織，是世界上第一個國際檢察官組織。其於 1995 年 6 月在維也納成立，其創立是因為跨國犯罪日益嚴重，特別是販毒、洗錢及詐欺犯罪，國際間普遍認為需要加強檢察官間的國際合作，提高相互幫助、資產追蹤及其他國際合作的速度及效率。中華民國檢察官協會於民國 98 年加入國際檢察官協會正式成為團體會員。

二、第 11 屆 IAP 亞洲及太平洋地區會議(下稱 IAP 亞太地區會議)在香港舉行



IAP 歷年聚集各國各級別檢察官，常見高階司法互助中央主管機關高階主管出席與會。第 11 屆 IAP 亞太地區會議於 113 年 11 月 27 日至 29 日在香港舉行，本次會議以個人會員及組織會員名義參加與會者多達 135 人，來自 28 個國家及領地¹。本屆 IAP 亞太地區會議由法務部國際及兩岸法律司檢察官陳玟君以組織會員名義參加，並與來自世界各國之檢察官交

¹ 除我國外，尚包含：丹麥、荷蘭、英國、澳洲、亞塞拜然、巴林、巴西、汶萊、中華人民共和國、香港、澳門、印度、印尼、科威特、馬來西亞、蒙古、巴勒斯坦、巴布亞紐幾內亞、菲律賓、沙烏地阿拉伯、新加坡、南韓、泰國、美國、越南、尚比亞、辛巴威等。

流及分享經驗。

三、本次會議主題：科技時代的有效檢控服務

Effective Prosecution Service in the Technological Age

本次會議主題為「科技時代的有效檢控服務」(Effective Prosecution Service in the Technological Age)，著重探討透過亞太地區檢控機關之國際合作，因應科技時代新型態犯罪趨勢，將科技納入刑事司法系統以促進偵查作為，亦討論如何在法律訴訟中正確取得、保存和呈現數位證據，以及數位化和人工智慧如何影響證據收集和分析。在此主題下，本次年會分為數個子題，包含：(一)為打擊科技犯罪推行法律改革的需要、挑戰、成效及經驗分享、(二)從社交媒體、去中心化金融談到虛擬資產、(三)通過刑事事宜相互協助加強國際合作，應對新挑戰、(四)檢控網絡罪行的經驗分享—數位證據的取證及處理、(五)法庭及檢察部門的數位轉型—科技發展對刑事證據及法律程序的影響。

貳、第 11 屆 IAP 亞洲及太平洋地區會議內容

一、113 年 11 月 28 日開幕儀式(Opening Ceremony)

本次主辦年會之東道主為香港特別行政區，其行政長官李家超(Lee Ka-chiu)於開幕致詞中表示，隨著科技的高速發展，網路空間成為犯罪的新領域，科技帶來的便利性與挑戰性並存，本次年會的主題針對科技偵查，正是針對科技時代的新型態犯罪，透過國際間檢察官的合作，強化數位電子卷證系統之應用，運用現代科技手段，提升偵查犯罪的效率與準確性，以創建更安全、更智慧的未來。

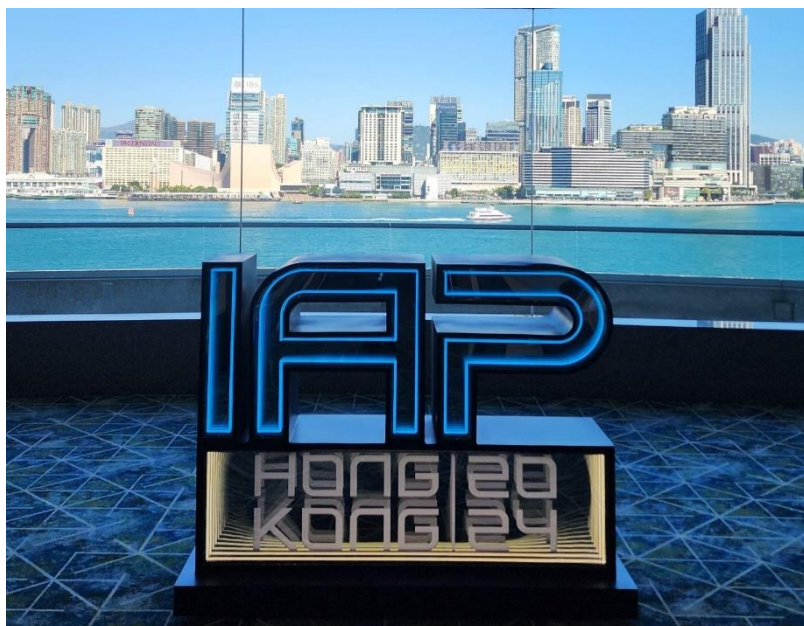
現任香港特別行政區政府律政司司長林定國(Paul Lam)則於開幕致詞中表示，科技如今已經滲透我們個人及職業生活各個層面，也不斷提升我們生活的品質和標準。然而，犯罪分子也同樣從中獲益。當今的罪犯在

實施犯罪時愈發倚賴科技，近年來，科技犯罪案件數量大幅提高，隨著科技的持續發展，我們必須互相分享知識和經驗，方能領先於網絡犯罪分子，提升我們在偵查、預防和調查科技犯罪方面的能力。本次會議的主題「科技時代的有效檢控服務」邀請我們共同思考如何在國際層面加強打擊科技犯罪的努力，並交流各種重要議題和最佳實踐，包括科技時代去中心化所帶來的挑戰、數位證據的處理，以及科技進步對犯罪證據和程序的影響等問題。

中國最高人民檢察院副檢察長童建明並強調，科技是一把雙刃劍，既為我們帶來福祉，卻也被不法份子用來犯罪，其分享三個科技犯罪的態樣，包含運用 AI 語音機器人技術之電信網路詐騙案件、利用虛擬資產跨境洗錢之案件、以數位方式侵犯商業祕密及智慧財產權等案件，檢察機關必須充分、靈活利用現代偵查手段，例如大數據、聲相鑑定等，方能有效應對這些新型犯罪挑戰，保障社會安全與法治秩序。其亦提到，雖然各國法治模式及檢察制度有差異，但對懲治犯罪，保障人權、維護穩定、促進發展的法治目標是一致的。

二、113 年 11 月 28 日會議

(一)國際檢察官協會業務重點說明



本場次由國際檢察官協會秘書長 (Secretary-General) Roel Dona、總顧問 (General Counsel) Shenaz Muzaffer 及網路犯罪國家高級顧問 (Senior National Advisor Cybercrime) Naomi Mohamedr 為與會人員介紹國際檢察官協會之重點業務。國際檢察官協會除促進國際間對打擊犯罪之合作外，亦旨在提升及建立國際檢察官執行業務之標準及原則，更呼籲國際間各政府應重視對檢察官們之保護及照顧義務。國際檢察官協會常見之合作夥伴包含聯合國區域間犯罪和司法研究所 (UNICRI)、聯合國安理會反恐怖主義委員會 (UN CTED)、聯合國教育科技及文化組織 (UNESCO)、歐洲理事會、席拉庫薩國際刑事司法及人權機構 (The Siracusa International Institute for Criminal Justice and Human Rights) 及世界銀行 (World Bank) 等。講者並介紹國際檢察官協會之幾項業務內容，包括：

1. 全球訓練學院(Global Training Academy,GTA)

全球訓練學院旨在為國際檢察官協會之個人或組織成員提供一貫及全面性的訓練課程及能力培養，且會與區域組織、國家單位組織、國際組織、各國家政府單位及私人單位等一同合作進行課程規劃。上開課程將著重在不同司法體系間均可適用之相關議題，例如：網路犯罪、貪腐、運輸毒品、金融情報機關之工作、審判權選擇、跨境及跨國犯罪等。

2. IAP 標準(IAP Standards)

IAP 提出檢察官之職業責任標準及基本職責與權利聲明，此項標準與聲明概述檢察官在職業行為、獨立性、公正性方面的義務，以及檢察官在刑事訴訟中的作用以及其與司法機構合作的義務。

3. 全球檢察官合作平臺(Prosecutors' International Cooperation Platform)

此平臺為各國檢察官們在國際間建立直接、有效且即時之聯繫管

道，常見之聯繫議題包含罪贓返還、國際司法互助、國際及跨境犯罪之罪犯引渡等。此平臺更建立相關議題之資料庫以促進各國檢察官間之合作。

4. IAP 專家網絡(IAP Specialist Networks)

為提升國際檢察官之偵查能量，IAP 集結了各種領域之專家，形成九大項專家網絡，包含：協會論壇 (Forum of Associations of Prosecutors, FAP)、反貪腐網絡 (Network of Anti-Corruption Prosecutors, NACP)、消費者保護網絡 (Prosecutors Consumer Protection Network, PCPN)、反恐怖主義網絡 (Counter Terror Prosecutors Networks, CTPN)、網路犯罪網絡 (Global Prosecutors E-Crime Network, GPEN)、國際刑事司法論壇 (Forum for International Criminal Justice, FICJ)、軍事犯罪網絡 (Network of Military Prosecutors)、性犯罪調查網絡 (Prosecuting Sexual Violence Network, PSV)、人口販運平臺 (Trafficking in Persons Platform, TIPP)。旨在透過提高效率 and 擴大覆蓋範圍來促進跨境打擊網路犯罪。此網絡將來自世界各國的檢察官聚集在一起，提供積極交流實務知識和專題討論的平台，期能成為跨國聯合網路犯罪行動的催化劑。

(二) 議程一 (Plenary 1)：為打擊科技犯罪推行法律改革的需要、挑戰、成效及經驗分享



1. 新加坡最近修法發展

此議程由新加坡總檢察署 (Attorney-General's Chambers) 刑事司 (Crime Division) 高級處長 (Senior Director) 韓儀 (Hon Yi) 介紹，隨著科技發展與網路犯罪的多樣化，新加坡近年來推動多項立法改革，以應對數位身分濫用、SIM 卡詐欺以及加密資產犯罪等挑戰。新加坡政府自 2003 年引進數位身分證制度 (Singpass)，所謂數位身分證，是新加坡公民和居民的一組數位身分，可透過此數位身分在線上和線下使用政府和民間部門之服務，包含納稅、申請許可、繳費、銀行、保險等服務。然因使用數位身分證辦理銀行帳戶、申請 SIM 卡過於便利，社會上開始出現數位身分證之濫用、偽冒身分申請 SIM 卡、租借數位身分證帳戶，並遭詐欺集團、犯罪集團收購後用以實行詐欺犯罪、收受贓款及洗錢。

關於數位身分證之濫用，新加坡政府修正電腦濫用條例 (Computer Misuse Act)，將轉讓數位身分證，或將數位身分證提供、散布與他人等犯罪行為納入規範，且規範修正後，行為人如因轉

讓、提供、散布數位身分證而獲得利益，或行為人未採取合理手段善盡查證義務，則推定行為人主觀上明知或可得而知其行為將幫助他人實行犯罪。

關於偽冒身分申請 SIM 卡之問題，新加坡政府修正 1906 年雜項犯罪（公共秩序及妨害）法（Miscellaneous Offences [Public Order and Nuisance] Act），將非法提供 SIM 卡與他人、非法提供個人資訊供他人申辦 SIM 卡、交易以他人身分申辦之 SIM 卡以供犯罪之用、為獲報酬而交易以他人身分申辦之 SIM 卡、為供犯罪之用而持有以他人身分申辦之 SIM 卡、幫助他人偽冒身分註冊 SIM 卡以供犯罪之用等犯罪行為納入規範。

最後，加密資產司法管轄權仍具挑戰性。新加坡法院在 Cheong Jun Yoong v. Three Arrows Capital Ltd 案件中確立，管轄權可根據加密錢包私鑰持有人所在地來界定。然而，犯罪分子可能不在該司法轄區內，仍需進一步的國際合作與法律調整。

這些法規的改革反映了新加坡在應對新興數位犯罪上的積極策略，結合立法、技術與執法手段，以提升網路安全與司法效能。

2. 運用人工智慧（Artificial Intelligence, AI）之電信犯罪—殺豬盤（Pig Butchering Scam）

此議程由澳洲新南威爾斯州檢察署（The Director of Public Prosecutions, New South Wales）檢察官（Crown Prosecutor）Liam Shaw 介紹，現今詐欺集團犯罪手法日新月異，其中包括濫用人工智慧（Artificial Intelligence, 下稱 AI）深度學習（deep learning）的技術，合成某（不一定存在的）人的圖像或影片、聲音，甚至塑造社群媒體，亦可用於聊天機器人，產生聊天訊息內容，

即所謂深度偽造（deep fake）。此技術遭詐欺集團用在「殺豬盤」詐騙，「殺豬盤」是一種長期培養受害者信任的投資詐騙，通常涉及假冒身分、情感操縱與高額詐欺犯罪所得。隨著 AI 技術的進步，執法單位在偵查與取證均面臨嚴峻挑戰，行為人利用深度偽造（deep fake）技術製造假身分，生成虛假證據，甚至操控影像與聲音，使傳統的身分驗證方式失效，此外，機器學習演算法可根據受害者行為模式調整詐騙策略，使被害人更易受騙，案件也因此更難追蹤。

在取證層面，AI 生成內容的識別難度較高，數位證據容易遭到篡改，使法庭舉證變得困難。此外，詐欺集團往往採用去中心化技術，如加密貨幣與暗網交易，使資金流向難以追蹤，進一步增加執法難度，由於這類犯罪具有跨國性，執法機構常面臨司法管轄權的限制，國際合作效率受阻。

為應對上開挑戰，國際合作至關重要，各國需建立共享數據資料庫與聯合執法機制，以提升跨境犯罪打擊能力，確保科技發展與執法手段同步提升，以有效遏制 AI 詐欺犯罪的蔓延。

3. 菲律賓打擊網路犯罪的挑戰與應對策略

此議程由菲律賓卡加煙省檢察官辦公室（Office of the Provincial Prosecutor of Cagayan, Philippines）檢察官 Steven M. Dayag 介紹，隨著科技發展，菲律賓的網路犯罪案件顯著增加，根據菲律賓國家警察（Philippine National Police, PNP）數據，2023 年共發生 19,472 起網路犯罪案件，比 2022 年增長 68.98%。2024 年第一季度，每天平均報告 49 起案件。此外，聯合國兒童基金會（The United Nations Children's Fund, UNICEF）報告顯示，20% 的菲律賓 12 至 17 歲網路使用兒童曾遭受網路性剝削與虐待（2022 年）。菲律賓也是全球「失蹤與受剝削兒童國家中心」

(NCMEC) 通報最多疑似線上兒童性剝削案件的第二大國家，僅次於印度。

為了應對網路犯罪，菲律賓積極推動法律修正，並強化國際合作，當前的網路犯罪法律涵蓋非法存取、數據干擾、系統干擾、網路詐欺、網路身分盜用與網絡誹謗等犯罪行為，並特別針對「兒童線上性剝削與虐待 (Online Sexual Abuse and Exploitation of Children, OSAEC)」加強法規。

菲律賓執法機構在調查與起訴網路犯罪時，採取了多種科技偵查手段，包括數位鑑識分析、跨國司法互助與各類網路犯罪專用搜索令，例如：電腦數據揭露令，要求提供用戶資訊與數據、電腦數據監聽令，允許執法機構監聽、記錄、監控網路通信內容、電腦數據搜索與扣押令：授權搜索、扣押與檢驗電腦數據。

此外，菲律賓司法部設立網路犯罪辦公室與網路犯罪調查與協調中心，加強公私部門合作，並要求網路服務提供商、支付系統業者共同打擊網路犯罪。透過持續強化法規、技術與國際合作，菲律賓政府積極應對日益嚴峻的網路犯罪挑戰。

4. 法律改革對抗科技犯罪的需求、挑戰與經驗分享

此議程由荷蘭國家檢察署 (Public Prosecutor's Office) 國家網路犯罪檢察官 (National Cybercrime Prosecutor) Koen Hermans 介紹，由於科技犯罪日益嚴重，各國需不斷更新與完善法律體系，以有效打擊網路犯罪。

過去，全球執法機構曾成功執行大規模行動，例如 2013 年「Blackshades」行動，該行動涉及 19 個國家合作，逮捕 90 餘名嫌犯，並進行超過 300 次搜查。此案例顯示國際合作在打擊網路犯罪中

的重要性。

2024 年的「Endgame 行動」進一步提升打擊網路犯罪的全面性，不僅專注於逮捕與起訴，還包含受害者通知、心理戰（PsyOps）、錯誤資訊澄清（Disinformation）及經濟制裁等手段，以全面遏制網路犯罪活動。

然而，打擊科技犯罪仍面臨諸多挑戰，例如：法律框架不足，缺乏明確的法律來規範「犯罪中斷行動」與「受害者通知機制」、全球法律差異，各國法律與執法方式不同，但面對的科技犯罪挑戰卻相似，也影響了跨國合作的效率。未來，各國需加強國際合作與最佳實踐經驗交流，建立統一的法律框架，以應對快速變化的科技犯罪威脅。

(三) 議程二 (Plenary 2) 從社交媒體、去中心化金融談到虛擬資產

1. 巴西司法系統的技術挑戰與應對策略

此議程由巴西里約熱內盧公共檢察署 (Public Ministry of the State of Rio de Janeiro, Brazil) 資深檢察官 Fabrício Rocha Bastos 介紹，巴西的司法系統正在經歷數位化與去中心化的轉型，雖然提高了效率，但也帶來了許多挑戰。講者並舉出三個案例，探討巴西執法機關所面臨之挑戰。其一為比特幣法老案，此為巴西的重大加密貨幣詐騙案，此案揭示了去中心化金融體系下資產追蹤的困難，犯罪分子利用海外帳戶及加密通信，讓傳統的執法手段難以有效應對。

其二，為 X 社群軟體（前推特）在巴西的暫時封鎖，巴西政府對 X 社群軟體的短暫封鎖事件，凸顯了數位平台內容監管的挑戰，政府

該如何在保護言論自由與防範虛假資訊和仇恨言論之間取得平衡，成為法律上的難題。

其三，為雷納百貨公司為勒索軟體攻擊案件，這起對巴西知名零售企業的網路攻擊事件，顯示了企業基礎設施的脆弱性，並突顯出強化網路安全及數據保護政策的必要性。

巴西司法系統面對的挑戰包括加密貨幣與其匿名性，由於區塊鏈技術的去中心化特性，使犯罪分子得以隱匿身分，增加了司法機關追蹤資產與執法的難度，此外，去中心化的社交媒體平台跨越國界，使巴西的法規難以有效管理違規內容與網路犯罪。再者，從零售業到銀行業，巴西面臨日益增長的網路安全風險，司法系統亟需提升應對能力。最後，數位證據的儲存分散化、跨國案件的法律適用性等問題，亦使得電子證據的合法性與可採信度受到挑戰。

為解決上開問題，政府應建立明確的加密貨幣及去中心化平台法律定義，並且強化投資者與消費者保護機制，亦應制定有效的反洗錢及「了解你的客戶」(Know Your Customer) 法規，以防範非法資金流動。並改善數位資產凍結與回收機制，加強跨國司法協作。採用先進的數位鑑識技術，提高調查效率。並建立國際資料共享平台，以應對不斷變化的技術挑戰。除了技術上的創新，更應建立更強的政府、執法機關與私營企業間合作機制，推動資訊共享與聯合執法，在推動技術應用的同時，確保隱私、透明度與公平性，避免科技濫用導致的法律漏洞與人權問題。

2. 數位證據蒐集之挑戰

此議程由荷蘭公共檢察署 (Public Prosecution Office, Netherlands) 高科技犯罪資深國家檢察官 (Senior National

Prosecutor on Hightech Crime) Esther Baars 介紹在歐盟範圍內收集數位證據的挑戰與解決方案，尤指涉及社交媒體、去中心化金融（DeFi）和虛擬資產領域，並強調如何應對去中心化技術時代的變化與挑戰。

數位證據的蒐集，在現代刑事案件中至關重要，因為有 85% 的犯罪案件涉及數位資訊。然而，此過程面臨諸多挑戰，包括跨境調查的法律與技術障礙，導致取證程序冗長且複雜，執法機關和司法機構均需要更高效的工具來確保取證的速度與可靠性，以應對數據存取與司法管轄權的限制。

歐盟已制定相關監管架構，以因應上開挑戰。其中，E-Evidence（電子證據）法規（2023/1543）與指令（2023/1544）規範了任何在歐盟提供服務的數據供應商，要求其設立聯絡辦公室，並確保遵守基本權利與執行政序。此外，e-CODEX（電子司法交流）法規（2022/850）則提供一個數位平台，促進執法機構、檢察機構與私營部門之間的法律信息共享，加速跨國司法合作。

數位取證與法律體制的發展，均需要法律與技術專業人士的合作。透過協作，專業人士可以共同提出問題，以推動政策變革，並產生有效的解決方案，確保執法機關能夠應對不斷變化的技術環境。而司法部門、技術專家與私營機構的公私協力合作，將能更有效地打擊與數位資產相關的犯罪行為。

3. 香港的數位資產監管

此議程由香港金融管理局貨幣管理部數位金融科主管（Head of Digital Finance Division, Hong Kong Monetary Authority）Ernest Ho 介紹香港數位資產的生態系統、監管架構及未來發展，重

點涵蓋虛擬資產、穩定幣發行以及對法律執法的影響。

數位資產具透明、去中心化、不可更改及全天候運作等特性，並透過分散式帳本技術（如區塊鏈）運行。其交易可分為用戶間直接交易（P2P）及透過中介機構進行交易。隨著市場發展，監管需求日益增加，香港已建立相關法規以維持金融穩定並保障投資者。

穩定幣因其價格穩定特性，可用於跨境支付及數位資產交易，但亦帶來金融與貨幣穩定、用戶保護等風險。香港擬規定發行人須持牌，滿足儲備管理、穩定機制、財務要求（最低資本 2500 萬港元）及風險管理標準，確保穩定幣具足夠資產支撐，並可按面值贖回。監管當局將擁有廣泛的執法權力，包括罰款、吊銷牌照、公開譴責，甚至刑事懲罰，以防範違規活動。

此外，數位資產的跨境與去中心化特性對檢察機關也構成挑戰，司法機構需加強與國內外監管機構、執法部門的合作，共享情報，以有效應對數位資產相關犯罪。

(四)特別議程 (Special Plenary Session) 通過刑事事宜相互協助 加強國際合作，應對新挑戰



1. 區域司法合作網絡的角色：SEAJust

此議程由韓國法務部國際刑事事務處處長(Director of the International Criminal Affairs Division, Ministry of Justice, Republic of Korea) Kim Hyungwon 介紹東南亞司法合作網絡（下稱 SEAJust）的角色與影響。SEAJust 成立於 2020 年，由聯合國毒品與犯罪辦公室（UNODC）支持，旨在促進東南亞地區國家在刑事司法互助（MLA）與引渡方面的非正式合作。目前該網絡擁有 22 個成員，包括東盟國家、韓國、日本、美國、法國等。

隨著韓國與其他國家的刑事司法互助案件數量迅速增加，SEAJust 成為提升跨境司法合作效率的重要平台。韓國現已簽署 35 項雙邊刑事司法互助條約及 36 項雙邊引渡條約，並正積極擴展司法合作網絡，以加快刑事案件處理速度。SEAJust 的核心功能包括建立中央機構間直接溝通管道、提供法律與技術培訓、分享最佳實踐以及促進數位證據與資產追蹤合作。

講者介紹了數起通過 SEAJust 協調的成功案例。例如，在與泰國的合作中，SEAJust 幫助韓國檢方獲取 E 航空公司及 X 公司的財

務紀錄，進而證實貪污與挪用公款的指控。在柬埔寨，一名韓國直播主被發現死亡，SEAJust 加快了韓國與柬埔寨執法機構之間的溝通，使得相驗程序及調查迅速展開。此外，在 Kwon Do Hyeong 加密貨幣逃犯案件中，SEAJust 促成了韓國、新加坡、塞爾維亞和蒙特內哥羅之間的情報共享，協助追蹤與引渡進程。

展望未來，SEAJust 計劃加強與歐洲司法網絡（European Judicial Network, EJN）、CASC 等其他區域司法合作機構的聯繫，並應對日益增長的數位犯罪、洗錢與網絡詐騙問題。隨著全球司法合作的深化，SEAJust 期望能擴大影響力，促進國際司法互助與執法協作。

2. 加強國際合作：刑事互助與應對新挑戰

此議程由汶萊總檢察署副檢察官（Deputy Public Prosecutor, Attorney General's Chambers, Brunei）Siti Khalillah Hussin 介紹如何透過刑事司法互助機制加強國際合作，並應對當前司法挑戰。汶萊的刑事互助框架主要依據 2005 年《刑事事項互助令》（MACMO），並輔以 2006 年《引渡令》和 2012 年《犯罪資產追回令》（CARO）。MACMO 適用於所有外國，並基於雙邊條約、東盟刑事互助條約（ASEAN MLAT）以及互惠原則提供司法協助。

汶萊可提供的司法協助包括獲取證據、錄取證人陳述、安排證人出庭、查詢和識別個人、搜索與扣押財產、追蹤資金流向等。然而，由於不同國家的法律體系存在差異，刑事互助請求的處理往往面臨挑戰。例如，在某些情況下，因「雙重犯罪原則」（Dual Criminality）未能達成一致，請求可能遭到拒絕。此外，與國際及區域性執法機構的溝通不足，也可能導致請求處理延誤。

講者列舉了多個案例來說明刑事司法互助的重要性。在 2023 年 9 月，汶萊向某國提出請求，要求提供涉及洗錢案件的銀行紀錄與相關人員的資訊，然而該國認為該犯罪所得來源（如性交易）在其司法管轄區內並不構成犯罪，因此拒絕提供協助。為了突破困境，汶萊透過亞太區追討犯罪所得機構網絡（ARIN-AP）與相關官員協商，尋找可行的解決方案。

另一個案例涉及 2018 年一起司法官員貪污案，涉案金額超過 1575 萬汶萊元。涉案人員將資金轉移至多個國家，汶萊因此向不同國家提出刑事司法互助請求，包括要求凍結資產、調取銀行紀錄、安排證人出庭作證等。透過這些合作，汶萊成功追回部分非法所得，並將其歸入國家犯罪資產追回基金。

汶萊的刑事互助機制在國際執法合作中發揮了重要作用，尤其是在打擊貪污、洗錢和跨國犯罪方面。未來，汶萊將繼續透過 ASEAN MLAT 與國際司法合作網絡深化合作，確保司法互助請求能夠更有效地處理，並進一步強化打擊跨國犯罪的能力。

三、113 年 11 月 29 日會議

(一)議程三 (Plenary 3) 檢控網絡罪行的經驗分享—數位證據的取證及處理



1. 公共採購中的網絡犯罪：斐濟數位證據案例研究

此議程由巴布亞紐幾內亞獨立反貪委員會特別法律顧問兼副執行董事 (Special Counsel and Deputy Executive Director Legal, Independent Commission Against Corruption, Papua New Guinea) Rashmi Aslam 介紹斐濟一起涉及政府財務系統 (FMIS) 的網路犯罪案件，以及如何透過數位證據進行偵查與起訴。該案件涉及公共工程部 (PWD) 帳務部門多名公務員，他們與私人公司勾結，偽造購買交易，非法獲取財務利益。案件主謀為帳務部門主管，擁有認證詐欺審查師資格，並設計了一套精密的作案手法。

案件揭示了技術雖然能提升透明度與效率，但同時也可能被有組織的白領犯罪集團利用。當時，斐濟尚未頒布專門的網路犯罪法，也沒有專門的數位證據收集程序，因此調查人員只能依賴傳統刑事程序。透過專家證人協助，調查人員成功還原犯罪現場，重建 101 筆虛假交易，涉案金額達 36 萬斐濟元。

犯罪模式包含幾個關鍵特徵，嫌犯選擇碳粉和墨盒作為採購項

目，因為此類物品使用廣泛且較不易引起懷疑。所有交易金額都設定在 2,800 至 2,999 斐濟元之間，以規避 3,000 元的審查門檻。原本年度預算僅 600 元，卻在半年內報銷了 36 萬元，明顯暴露了貪污行為。

在數位證據收集過程中，調查人員發現大部分紙本文件已被銷毀，只能依賴政府財務系統內的數據。每筆交易涉及 8 名公務員，他們需通過 7 個主要面板和 12 個子面板進行操作。系統記錄了超過 1200 個數位足跡，顯示每位嫌犯的登入時間、操作內容和變更細節。這些數據最終成為主要證據，並由金融分析師及資訊科技（Information Technology, IT）專家提供解釋。

最後，審判歷時兩個月，所有被告均被判有罪，主謀被判處 12 年監禁，其他被告則被判 3 至 12 年不等的刑期。隨後，帳務部門的其他涉案人員均認罪，並與主案件合併判刑。部分私人公司仍在受審中。

2. 遠端直播兒童虐待：挑戰與機遇

此議程由荷蘭公共檢察署（Public Prosecution Office, Netherlands）兒童性剝削專案組（OSEAC/TSEAC）成員 Nicole Smits 和 Linda van den Oever 發表，探討遠端直播兒童虐待（Live Distant Child Abuse, LDCA）的現象、挑戰以及應對策略。這類犯罪涉及犯罪者透過社交媒體或網路平台聯繫中介，支付費用後觀看並指示受害兒童遭受性虐待。此類案件在全球迅速增加，尤其在 COVID-19 疫情後更加猖獗，例如 2022 年菲律賓就有近 50 萬名兒童遭受剝削製作性虐待影像，並且平均受害時間長達兩年。

遠端直播兒虐通常通過 Skype、Facebook、WhatsApp 及成人交

友網站進行，交易付款方式主要為 PayPal 及其他金流服務。犯罪模式通常由女性中介（如家人、朋友或鄰居）提供兒童受害者，而觀看者則多為來自歐美國家的男性。這種犯罪極具隱蔽性，受害兒童往往在熟悉的環境中遭受親近者的虐待，並長期受到心理創傷。此外，由於這類犯罪不僅源於貧困，更因可快速獲利，因此虐待行為往往長期持續，每名兒童每天可能面對多名買家。

執法機構的調查面臨諸多挑戰，主要包括難以即時發現犯罪行為、直播內容不會自動存檔、端對端加密技術阻礙監控、以及受害者及中介的定位困難。如果數據設備遭到扣押，數據量過於龐大，需耗費大量人力篩查。此外，保護個人隱私的相關法規，限制了國際間資訊共享，使案件調查更加困難。

目前，遠端直播兒虐案件主要可以透過數種管道發現，包括在查獲兒童性虐待材料（CSAM）時發現相關聊天紀錄或影像、逮捕中介後追蹤交易紀錄、金融機構通報可疑交易（如 PayPal 及 Skype 付款紀錄），或在暗網流傳的新影像中識別受害者與犯罪者。國際合作對於打擊此類犯罪至關重要，執法機構應加強受害者識別、金融交易追蹤及跨國救援行動，並推動網路平台承擔更多監管責任，以減少此類犯罪的發生。

3. 加密貨幣之調查與起訴

此議程由香港警務處網路安全及科技罪案調查科（CSTCB）網絡情報組主管 Rachel Hui Yee-wai 介紹，探討虛擬資產的特性、監管框架及詐騙案件的調查與起訴挑戰。隨著加密貨幣市場的擴展，虛擬資產已成為投資與交易的重要工具，其去中心化、無國界、匿名性及不可篡改等特性，使其既具創新潛力，但也帶來監管與執法的挑戰。

在香港，虛擬資產監管主要依據《打擊洗錢及恐怖分子資金籌集條例》(AMLO)，目前已有 3 間虛擬資產交易平台 (VATP) 獲得許可。此外，香港政府正研究對穩定幣和場外交易 (OTC) 市場實施監管，立法提案正在進行中。從 2021 年至 2024 年 8 月，警方共接獲 2,924 宗與虛擬資產相關的請求，並凍結了 3.039 億港元的資金。在 2024 年 1 月至 8 月期間，57.8% 的虛擬資產案件與網路投資詐騙有關。

講者並分享一件涉及 1 億 6 千萬 USDT (泰達幣) 的詐騙案件。詐騙者透過取得受害者的恢復密鑰 (Recovery Seed) 來竊取資金，受害者資金被迅速轉移到新的錢包內，導致無法追回。警方及時介入，並透過與泰達公司合作，成功凍結 1 億 3 千 3 百萬 USDT。此外，案件調查過程中，警方與香港大學的計算機科學及金融專家合作，分析 USDT 交易機制與價格波動，並透過技術部門追蹤資金流向，最終成功對 3 名被告追訴詐欺。

然而，加密貨幣犯罪調查仍面臨多重挑戰。由於匿名性，詐騙者能輕易隱藏身分，增加調查難度。部分詐騙涉及混幣器 (Mixer) 或幣種交換 (Swap Coins)，使資金追蹤幾乎不可能。此外，各國對加密貨幣的監管標準不同，跨境司法合作仍存在障礙。未來，執法機構需加強國際合作，並提升對新興技術的應對能力，以更有效打擊虛擬資產相關犯罪。

(二)議程四 (Plenary 4) 法庭及檢察部門的數位轉型—科技發展對

刑事證據及法律程序的影響



1. 破解數位證據的密碼：將數位鑑識引入法庭

此議程由巴布亞紐幾內亞獨立反貪委員會（Independent Commission Against Corruption, ICAC）法律執行總監 Belinda Hughes 介紹數位鑑識在現代刑事調查與法庭訴訟中的重要性，透過數位證據來加強執法效能，提高法庭審判的透明度與準確性，最終促進對貪腐與犯罪活動的打擊。

目前，數位證據已涉及近 90% 的刑事案件，然而傳統司法體系仍難以適應此一變化。在巴布亞紐幾內亞的一宗毒品走私案中，法院仍透過實物證據進行審理，也就是將 611 公斤古柯鹼運送至法庭內，作為審理之核心，然而，許多犯罪活動已轉向數位化，傳統證據收集與展示方式已不再堪用，司法機構需將數位鑑識技術納入辦案流程。

數位鑑識是鑑定、獲取、處理、分析及報告電子數據的科學領域，常見的數位證據來源包括電腦、智慧型手機、雲端儲存、外部硬碟等。這些數據可透過搜索令、通知或受害者與證人授權來獲取，並在案件審理過程中作為關鍵證據。隨著司法機構日益數位化，法庭也

開始採用例如高解析度顯示器、音響系統、互動標註工具及遠端視訊來提升審理效率，使數位證據能夠更直觀地呈現給法官與陪審團。

未來，專業的數位鑑識團隊將成為司法體系不可或缺的一部分，負責從行動設備、操作系統、網路流量、雲端儲存及檔案系統等領域收集與分析證據，並確保數據的完整性及法庭可受理性。透過這些技術的發展，司法機構將能更有效地追蹤與起訴數位犯罪，確保司法正義在數位時代得以落實。

2. 澳洲聯邦檢察署的數位轉型計劃

此議程由澳洲聯邦檢察署（Commonwealth Director of Public Prosecutions，CDPP）代理副署長 Christina Choi 探討該機構在數位化轉型方面的舉措，以應對當前法律環境日益增長的證據量與案件複雜性。澳洲聯邦檢察署自 2016 年起開始落實電子證據摘要（e-Brief）計畫，致力於為所有聯邦調查機構提供標準化的電子證據摘要，取代傳統的紙本證據管理模式，提升檢控效率與精確性。

隨著數位證據數量的增長，澳洲聯邦檢察署進一步開發了證據管理解決方案（Evidence Management Solution），以應對證據規模與複雜性的挑戰。透過上開系統，檢察機關可以更有效地組織、存取及審查電子證據，確保訴訟過程的流暢與透明。此外，澳洲聯邦檢察署亦引入了電子審判系統（eTrial Solution），該系統允許陪審員透過安全、個人化的數位平台查閱證據，提高庭審期間的證據呈現效率與司法公正性。

澳洲聯邦檢察署的數位轉型涵蓋從電子證據摘要的落實、數位證據的審查，到電子化證據展示的完整流程，確保檢察機關能夠適應現代司法環境的技術需求。未來，澳洲聯邦檢察署計劃進一步探索

生成式 AI (Generative AI) 在檢察體系中的應用，以自動化部分證據處理流程，提升檢察官的工作效率，並加強司法系統的數位化能力，確保司法公正能夠與科技進步同步發展。

3. 韓國司法數位化轉型：促進司法可及性

此議程由世界銀行(World Bank)高級法律顧問兼韓國大檢察廳 (Korea Supreme Prosecutors' Office) 檢察官 Min Suk Kim 介紹韓國司法體系數位化轉型的經驗，並分析如何利用技術提升司法可及性與效率。世界銀行的核心目標是終結極端貧困與促進共享繁榮，其中司法數位化是支持政府機構推動改革、加強政策執行、提升治理效能的重要手段。

隨著全球司法需求的增長，韓國推動了司法數位化計畫，以資訊科技縮小司法資源分配的不均衡，提高訴訟服務範圍與運作效率。韓國刑事司法資訊系統 (KICS) 是數位化改革的重要成果之一，該系統每日處理 230 萬宗案件，可共享 400 種資訊，連結 70 個司法機構，並提供電子案件提交、即時文件分發及線上查詢等功能。此外，KICS 允許用戶查閱犯罪紀錄、執行電子簽章及透過行動設備處理搜查令，減少了對紙本文件的依賴。

韓國的電子訴訟 (e-Litigation) 改革首先從專利案件開始，也為電子訴訟系統的推廣奠定基礎，透過逐步推動數位化，法庭克服了司法機關內部的抗拒，確保系統能夠符合法律標準、增強數據安全性，並採取透明的稽核機制來提高信任度。

司法數位化的推行面臨文化與政治層面的挑戰，例如不同機關間的權力平衡、數據共享的隱私顧慮等。因此，韓國採取聯邦式資訊架構 (Federated Information System Architecture)，確保各機構在

共享資訊的同時仍保有獨立決策權，避免單一機構對系統過度主導。此外，透過嚴格的角色存取控制（RBAC）和定期稽核，確保資訊安全並維護機構間的信任關係。

4. 重塑與利用科技：促進受害者保護的證據收集與起訴——菲律賓兒童網路性剝削案件的應對策略

此議程由菲律賓國際正義使命團（International Justice Mission，下稱 IJM）資深首席律師 Maranatha Praise D. Ladringan 介紹如何利用科技來強化對兒童網路性剝削與虐待（Online Sexual Abuse and Exploitation of Children，下稱 OSAEC）案件的調查、證據收集與起訴。雖然網際網路為兒童權利的實現帶來了新的機會，但同時也革新了性暴力的運作模式，使得犯罪行為更為隱蔽與難以偵查。

IJM 於 2021 年 3 月與諾丁漢大學（University of Nottingham）人權實驗室合作啟動 OSAEC 研究計畫，致力於發展受害者保護機制與最佳實務做法。其中，菲律賓政府制定了《反兒童網路性虐待與剝削法（RA 11930）》和《擴展反人口販運法（RA 11862）》，授權執法機構在特定條件下，無需法令授權即可進行通訊監控，以攔截犯罪行為。此外，遠端視訊審判的推行，減少了受害者親自出庭面對加害者的心理壓力，尤其是在案件涉及家庭成員、親屬或熟人時，這項措施可降低受害者的二次傷害，讓他們能夠更自在地陳述事實。

OSAEC 犯罪的特點在於使用數位平台作為媒介，而這也為執法帶來了挑戰。許多通訊軟體和設備廣泛使用端對端加密技術，使第三方機構（包括執法單位或平台供應商）無法讀取通訊內容，從而影響關鍵證據的取得。因此，菲律賓政府允許在滿足一定條件下，執法機構

能夠無需法令授權，針對涉嫌犯罪對象進行監控，以確保即時干預的可能性。

此外，遠端視訊審判不僅能保護兒童受害者，還能提升跨國司法合作。例如，透過視訊審判，國際執法機構的官員可以在自己的國家內認證證據，以強化在菲律賓進行的訴訟。同時，在針對國外買家的起訴案件中，遠端視訊審判可允許菲律賓的證人為外國法庭提供證詞，確保犯罪者即使在境外也能被追究責任。

這些創新做法展現了執法機關如何重新奪回科技的力量，將原本被犯罪者濫用的技術轉化為受害者保護的有力工具，幫助他們順利進入司法程序，並確保正義得以伸張。

參、心得及建議

一、數位時代司法挑戰與應對策略

本次會議聚焦於科技時代的司法挑戰，包括數位證據取證、加密貨幣監管、網絡犯罪偵查以及人工智慧在詐欺與偽造犯罪中的應用。透過與各國檢察官及法律專家的討論，可以清楚了解到，全球司法體系均面臨數位化帶來的挑戰，而法律框架與執法技術的更新往往落後於犯罪手法的進步。特別是在數位證據的採集與可採性方面，各國均遇到來自技術與隱私法規的挑戰。因此，未來在執法與司法層面，應更加強調科技工具的應用，例如數位鑑識、區塊鏈數據追蹤、端對端加密破解技術等，以應對新型犯罪模式。

二、國際合作與司法互助的重要性

此次會議提供了與各國司法機關交流的寶貴機會，顯示跨國合作在打擊網絡犯罪、追蹤非法資金流動及進行司法互助方面的重要性。尤其在數

位資產犯罪、網絡性剝削案件及去中心化金融（DeFi）犯罪的調查過程中，各國執法機關若無有效的跨境合作機制，將難以追蹤犯罪者並進行起訴。本次討論的 SEAJust 司法合作網絡與歐盟 e-CODEX 系統，提供了值得借鑑的跨國司法合作模式。建議未來可進一步與國際檢察官協會（IAP）及其他司法合作機構強化聯繫，透過共享專業知識、技術合作及司法互助機制，提高國際間對科技犯罪的應對能力。

三、數位轉型與法庭現代化的推動

許多國家已開始導入電子案件管理、線上審訊（如遠端視訊審判）、電子證據管理系統（如韓國 KICS 與澳洲 eTrial Solution），顯示數位轉型已成為全球司法機關的趨勢。這些技術不僅提升了訴訟效率，也有助於改善受害者保護機制，例如菲律賓的遠端視訊審判，讓 OSAEC 受害兒童無需親自面對加害者即可提供證詞，減少二次傷害。建議我國司法體系參考這些數位化改革，持續推動電子案件管理、數位證據審查機制及遠端審訊技術，以提升辦案效率，並確保在科技時代下的司法正義。

四、未來展望：強化司法數位化與國際合作

隨著科技的迅速發展，未來的司法體系將更加依賴數位工具來提升偵查與起訴的效率。本次會議展現出各國在數位鑑識、區塊鏈監管、人工智慧應用及網絡犯罪防治等領域的進展，顯示出司法數位化已是全球趨勢。我國應積極參考這些國際經驗，推動司法機關與執法單位的數位轉型，例如建立跨機構的電子證據共享平台、導入 AI 技術輔助數據分析，並加強與國際執法機構的合作，以應對日益增長的跨國科技犯罪。此外，司法數位化不僅限於提升技術能力，還需兼顧人權保障與隱私保護，確保科技在司法體系中的應用能夠符合法治原則，並促進更公平與高效的執法環境。未來，我國可考慮積極參與國際司法合作組織，如 SEAJust、e-CODEX 等，並透過雙邊與多邊協議深化跨境執法合作，進一步強化科技時代下的司法效能與正義實現。