

從警察機關觀點探討臺灣詐欺犯罪防制跨機關合作現況與挑戰

Interagency Collaboration in Fraud Prevention in Taiwan: Current Conditions and Challenges from a Policing Perspective

溫翎佑*

摘要

詐欺犯罪具有高度組織化、數位化與跨境化特性，使其防制工作已超出單一警察機關所能獨力因應之範疇。基此，本研究以警察機關觀點為出發，透過文獻分析與深度訪談法，蒐集並分析 20 位受訪者意見，包括中央警察機關管理人員、刑事警察大隊大隊長及直轄市分局長，旨在探討臺灣詐欺犯罪防制跨機關合作之運作現況、制度限制與政策精進方向。研究結果歸納出六項主要發現：第一，警察在防詐體系中承受過度期待，責任呈現高度集中化；第二，跨機關合作雖已制度化運作，惟多屬形式性安排，缺乏實質強制力；第三，金融與電信部門之合作機制相對成熟，但仍受法制規範與誘因不足之限制；第四，數位經濟與平台治理為當前制度體系之最大缺口；第五，檢察官科技偵查素養對案件推進與偵辦成效具有關鍵影響；第六，地方政府所推動之創新防詐策略雖具成效，惟缺乏制度化支撐。基於上述發現，本研究提出六項政策建議：第一，防詐策略應由事後執法導向轉向以被害人為中心之整合防制模式；第二，跨機關合作機制應強化以「目標承諾」(goal commitment)為核心之制度設計；第三，應重新定位警察於整體防詐治理體系中的角色；第四，主管機關應加速建立平台責任法制與風險內部化機制；第五，應建構制度化之跨機關情資共享與整合體系；第六，應強化檢察官偵辦詐欺案件之科技犯罪專業能力。

關鍵字：詐欺防制、跨機關合作、警察觀點

* 作者溫翎佑現職為臺灣警察專科學校行政警察科助理教授。

Abstract

Fraud has become increasingly organized, digitalized, and transnational in nature, placing its prevention beyond the capacity of any single police agency to address independently. This study adopts a police-centered perspective and employs literature review and in-depth interviews to collect and analyze the views of 20 participants, including senior officials from central police agencies, commanders of criminal investigation corps, and precinct chiefs of metropolitan police departments. The study aims to examine the current operation, institutional constraints, and policy improvement directions of interagency collaboration in fraud prevention in Taiwan. Six major findings are identified: (1) police roles in fraud prevention are subject to excessive expectations and a high degree of responsibility concentration; (2) interagency cooperation exhibits formal institutionalization but lacks enforceability; (3) collaboration with financial and telecommunications sectors is relatively mature but still constrained by legal frameworks and incentive structures; (4) governance of the digital economy sector represents the most significant institutional gap; (5) prosecutors' technological investigative literacy substantially influences case progression and investigative effectiveness; and (6) local innovative anti-fraud strategies demonstrate effectiveness but lack institutional support for sustainability. Based on these findings, the study proposes the following policy recommendations: (1) shifting from a post-incident enforcement approach to a victim-centered prevention strategy; (2) strengthening interagency collaboration through institutional designs that foster goal commitment; (3) redefining the role of the police within the anti-fraud governance system; (4) enhancing platform accountability regulations and mechanisms for internalizing risk within digital industries; (5) establishing an institutionalized interagency intelligence-sharing and integration framework; and (6) improving prosecutors' professional capacity in technology-enabled crime investigations.

Key words: fraud prevention, interagency collaboration, police perspective

壹、前言

警察及其他執法機構的工作，較少從「時代」的視角做審視。從歷史觀點來看，「時代」的劃分方式多元，其中較常見者，係依據人類所使用之工具或武器材料加以區分，例如石器時代、青銅時代與鐵器時代。進入 21 世紀後，人類社會多被視為邁入「數位時代」。過去約 70 年間，電腦與全球資訊網路的快速發展與普及，已對警務工作與執法模式產生深遠影響。此種影響具體體現在通訊方式的革新、大量資料庫之即時存取，以及各類數位科技設備的廣泛應用，包括視訊監控系統、指紋辨識、車牌自動辨識、人體掃描裝置、隨身攝影機、無人機與槍聲偵測系統等。(Nogala, Talmar, Pūraitė, Mészáros, Kokkinos, Fernandes, R. & Huikuri, 2022: 7)。但從另一個角度來看，犯罪者同樣也利用數位時代的工具從事犯罪。近年來，隨著詐欺犯罪手法日益組織化、數位化與跨境化，詐欺犯罪防制已不再是單一警察機關所能獨力因應的政策議題。臺灣防詐政策亦逐步由傳統以警政機關為核心的執法模式，轉向結合警政、金融監理、電信管理、數位平台與地方政府等多元行動者的跨機關協作模式。在制度設計層次，台灣已陸續建構包括 165 反詐騙專線、詐欺犯罪防制中心，以及行政院層級的打擊詐欺指揮中心統籌機制，期望透過跨機關資訊整合與政策協調，提升防詐工作的即時性與整體成效。然而，既有的跨機關合作文獻多半假設，跨機關合作與跨部門治理有助於提升政策效能，並因其強調包容性、協調性與公共價值，而可獲得較高的公共支持與正當性。然而，這些相關論述多停留於規範性層次，實證研究仍相對有限 (Lee & Kim, 2024: 2429–2431)。

基於此，本研究嘗試從第一線執行防詐工作的警察主管人員的觀點出發，檢視其如何看待傳統以警政機關為主導的防詐模式，以及在警政、金融、電信與數位平台等多元網絡共同參與下，跨機關合作機制應如何加以補強，方能具備實務上的可行性與組織內部的支持性。藉由納入警察人員的實務經驗與主觀認知，本研究期能為後續防詐政策在跨機關分工、權責配置與制度調整上，提供具實證基礎的政策建議。

貳、相關文獻回顧

近年來，對於詐欺防制的措施，由早期從犯罪成因、手法與運作管道之分析去發想，逐漸轉向以被害人為核心的路徑，關注被害人之心理脆弱性、其最初接觸犯罪者的途徑，以及從受害發生至察覺並中止受害的整體歷程，來規劃相關的防詐作為。顯示詐欺問題已難以僅從「犯罪行為本身」加以理解，亦突顯詐欺防制不可能單純透過追訴或逮捕犯罪者而加以根除，而必須採取跨網絡、跨部門的治理思維，從被害人視角出發，整合相關網絡共同介入，方能有效回應詐欺的風險管理。因此在文獻探討部分，本文將先探討詐欺犯罪特性，說明詐欺犯罪防制為何需要跨機關合作，其次分析我國詐欺犯罪防制合作現況，以及各國在跨機關詐欺犯罪防制的合作模式，以作為本研究之理論基礎。

一、詐欺犯罪特性與跨域合作之必要性

詐欺犯罪已逐漸成為數位時代中最具擴張性與變動性的犯罪類型之一。其運作結構不僅隨科技發展而快速演化，更融入通訊、數位平台與金融基礎設施之中，使傳統以刑事追訴為核心的犯罪防制模式面臨顯著挑戰。在此背景下，單純以案件偵破或起訴成果衡量防制成效，已難以全面反映詐欺犯罪對社會所造成之風險與損害。因此，就詐欺犯罪之核心特性欲加以防制，實有往跨域合作與減害導向思維發展之必要性，以下討論之。

（一）詐欺犯罪特性

近年來，詐欺犯罪已不僅是臺灣所面臨的治安問題，亦成為多數先進國家共同關注的重大犯罪威脅。相較於其他犯罪類型，詐欺犯罪通常具有跨國運作、分工細緻、倚賴數位科技，以及低成本、高報酬等結構性特徵，使其得以快速擴散並持續演化。此一特性亦使傳統以刑事執法與事後追訴為核心的犯罪偵查模式，逐漸顯現其侷限性。單一執法機關難以全面掌握整體詐欺行為的運作脈絡，亦難以及時因應其風險外溢效果。聯合國毒品與犯罪辦公室即指出，近年來以網路詐欺為核心的犯罪中心，已在東南亞地區形成高度工業化的運作規模，相關犯罪集團不僅持續向其他司法管轄區擴張，亦迅速多元化其犯罪業務，轉向發展支撐詐欺活動的關鍵基礎設施。其犯罪生態系統涵蓋線上賭博平台與軟體服務、加密通訊工具、虛擬貨幣與區塊鏈網路，以及非法線上市場等多元領域（UNODC, 2025:

3-5)。此發展趨勢，使詐欺犯罪集團得以在全球擴大受害者範圍，並大幅加重執法機關在偵查、溯源與追訴上的既有挑戰。

從犯罪防制的角度觀之，其核心目標不外乎兩項：一是預防犯罪的發生；二是在犯罪未能預防時，對犯罪行為人進行有效追訴。然而，臺灣詐欺犯罪自早期以實體接觸為主的金光黨手法，演變至今日高度數位化的犯罪型態，其運作結構、風險分布與影響範圍，已明顯超出單一機關，甚至單一國家所能獨立因應的範疇。詐欺犯罪防制逐漸呈現出仰賴跨機關、跨域合作與風險管理的防制趨勢。既有研究指出，網路犯罪至少具備五項特性，使現行執法體系在刑事追訴層面面臨困境。其一，網路空間本身高度複雜且快速演變；其二，網路犯罪與犯罪行為人具有高度跨國性，動搖以明確領土管轄權為基礎的實體犯罪偵查模式；其三，被害人樣態不明，缺乏精確且完整的被害數據；其四，眾多中介者在網路犯罪中扮演關鍵角色。由於網路空間的存取、維運與管理責任，分散於數量龐大的利害關係人之間，包括網際網路服務供應商、主機服務業者、搜尋引擎、社群媒體平台與線上交易市集等，其行為無論屬於被動或主動，皆可能在執法機關因應犯罪時，發揮緩解或加劇問題的效果；其五，執法人員對網路犯罪的角色認知與能力需求，已不同於傳統實體犯罪，普遍認為其需要新的技能、訓練，甚至全然不同的角色定位（Khan, 2024: 5-8）。在此脈絡下，網路詐欺活動可被視為一個成熟犯罪生態系統，其結合先進技術與有組織犯罪手段，形成一個高度獲利且適應性極強的犯罪產業。犯罪組織得以藉由既有洗錢網絡，以及加密貨幣與虛擬資產服務提供者的快速擴張，隱匿其鉅額不法所得（Amerhauser & Thi, 2025: 2）。

（二）跨域合作之必要

基於上述種種詐欺犯罪的結構性限制，將刑事追訴視為詐欺防制的主要手段，已無法回應詐欺犯罪對社會所造成的實質風險與損害。近年國際研究逐步指出，未來詐欺防制有必要從以追訴為核心的反應式執法，轉向以「減害」（harm reduction）為導向的風險管理模式。相關研究強調，詐欺防制不應僅關注是否逮捕犯罪者，更實際的作法反而關注是否能即時阻斷詐欺流程、降低被害人財損、縮短受害時間，並提供必要的被害人支持與協助（Anderson, March & van Burken, 2024: 488；Takefuji, 2023: 1；UNDP, 2025: 6；Fox-Mills, 2025: 1）。在此架構下，刑事追訴應被定位為整體防制措施中的一環，而非衡量防詐政策成效的唯一或首要指標。詐欺防制思維從追訴轉向減害，研究者認為是後續探討金融端阻詐、平

台責任設計、跨機關資料共享，以及被害人保護機制的基礎，亦是詐欺犯罪防制必須跨網絡合作的主要原因。畢竟當犯罪高度依附商業平台、金流與資訊基礎設施時，防制犯罪的難度勢必超出警察機關的專業範疇，而需仰賴多個公私部門共同參與。換言之，詐欺犯罪未來防制的關鍵，應是能否透過制度化的跨機關分工與責任配置，使掌握關鍵資源的網絡機關共同承擔防詐義務。研究者以為，此一發展趨勢同樣讓警察人員在詐欺防制體系中的角色產生轉變。

二、我國跨機關詐欺犯罪合作現況

考量整合政府與民間業者資源以共同合作的策略，已成為當前各國詐欺防制的趨勢。尤其在數位網路環境中，詐欺集團之運作模式與影響力顯著擴大（陳昱奉，2023：42）。目前我國詐欺犯罪防制之政策主軸，係以行政院提出之「新世代打擊詐欺策略行動綱領」為核心。在跨機關合作的架構方面，行政院於2023年正式成立專責單位，現為「打擊詐欺指揮中心」負責統籌、督導與協調各部會推動綱領之落實（嚴宏元，2023：49）。該綱領旨在整合跨部會資源，強化科技截堵能力，並健全相關法制基礎（嚴宏元，2023：52-53；內政部警政署，2023：1）。在政策架構上，綱領將詐欺防制區分為「識詐」、「堵詐」、「防詐」、「阻詐」與「懲詐」五大面向，並依序由內政部、國家通訊傳播委員會、數位發展部、金融監督管理委員會及法務部等主管機關負責相關業務。由此可見，我國詐欺犯罪防制體系係以跨部會分工與公私協力作為核心，政府所稱之「打詐國家隊」，即透過跨機關協作整合公私部門力量，以回應詐欺犯罪防制。

在法制層面，近年相關法規亦朝向強化平台責任與金流管制方向修正。例如，《證券投資信託及顧問法》已明定網路平台業者對投放假投資廣告應負連帶賠償責任，以強化投資詐欺之防制效果。為阻斷詐欺集團之帳戶來源，《洗錢防制法》亦修正增訂「人頭帳戶罪」，明確禁止無正當理由提供帳戶供他人使用，違者除先由警察機關裁處告誡外，於告誡後五年內再犯者將科以刑事責任。此外，行政院亦指定金融監督管理委員會為「具金融投資或支付性質之虛擬資產平台」之主管機關，以強化對虛擬資產及其交易平台之監管，降低其遭犯罪集團利用為洗錢工具之風險（內政部警政署，2023：2）。除政府部門外，民間亦逐步投入詐欺防制，例如數位信任協會之成立，其成員涵蓋資訊科技、資安、金融與區塊鏈等國內外機構等（GASA，2024：3）。然而，在跨機關合作網絡中，各網絡合作者所掌握之資源與權責並不對等，合作關係亦非完全對稱。隨著社會數位化程度提高，犯罪

樣態與行為人特性產生變化，亦產生諸多新的議題，例如潛在被害人應由何者負責保護、警察、其他政府部門、網路服務供應商與商業資安公司間的責任應如何劃分等問題，迄今仍存爭議（Leukfeldt, 2017: 1）。

從理論面觀之，跨網絡詐欺防制之推動，仰賴高度相互依賴之網絡合作者間進行複雜互動。然而，該等互動並非自然形成，而須透過制度設計，方能促成合作並維持運作（Bianchi, Nasi, & Rivenbark, 2021: 1582）。如何在各網絡合作者之間形成共識、完成決策並確保有效協調，往往面臨高度困難。我國的詐欺防制工作向來由警察機關擔任主責，由於警察機關、金融機構、電信業者、數位平台及地方政府之權責分工、組織目標與風險承擔程度各異，合作過程中容易產生協調成本與本位主義。即便中央已設置跨機關防詐平台或單一窗口機制，實務上仍可能出現任務擴張、功能重疊或責任歸屬不明等情形，使跨機關合作在形式上看似完備，但卻可能面臨諸多困境，此亦是本研究所欲探討的議題。

三、國際防制詐欺犯罪跨機關合作模式

研究指出，當社會問題超出單一組織或部門之能力範圍時，來自公共部門、私營企業與民間社會之行動者，往往必須透過制度化的夥伴關係共同回應（Henry, 2024: 745）。詐欺犯罪即屬此類典型案例。但研究同樣顯示，跨機關合作並非自然順暢運作。Waardenburg 等人（2020: 403–404）追蹤荷蘭八個打擊犯罪合作網絡的形成與運作過程，指出網絡合作常伴隨三類核心挑戰：(一)問題界定與解決困難、(二)合作歷程之管理，以及(三)多重關係下的問責機制建構。其複雜性源自專業人員同時承受來自不同制度體系之期待與角色要求，有時甚至彼此矛盾衝突。例如，長期強調合規與風險控管的公務人員，往往對資訊分享持保留態度；但合作機制又高度仰賴資訊流通與信任建立。Waardenburg 等人因此強調，成功關鍵不僅在於形式化架構或交流成本降低，更在於行動者是否發展出「兼容並進」（both/and）的治理思維，在程序合規與彈性合作之間取得動態平衡。類似的結果還有紐西蘭 2012 至 2017 年之旗艦級跨機關合作計畫研究。Scott 與 Merton（2021: 1638）指出，儘管跨機關合作本質上具有高度複雜性與執行風險，但在涉及警政、金融、電信與地方政府等多元網絡的議題上，往往是唯一可行的政策途徑。但早期研究將跨機關合作成功歸因於制度化溝通平台與明確資訊流通機制這類社會技術的設計；惟 Scott 與 Merton 後續分析發現，即便跨機關交流成本仍然存在，若各行動者對核心政策目標形成高度「目標承諾」（goal commitment），合作仍得以持續並產生

成效。研究者以為此一觀察對詐欺防制尤具啟示：當詐欺關鍵目標，如降低被害人財損或即時攔阻金流成為跨機關共同承諾時，跨機關合作的種種困境未必構成無法跨越的障礙。

在具體實踐方面，新加坡近年建立以「公私共同承擔責任、跨部門合作與專業培訓」為主軸的整合式模式（Khan, 2024: 13）。新加坡 2025 年上半年詐騙案件數確實較前一年同期下降（SPF, 2025: 1），其新施行措施包括《防制詐騙法》之施行、限制令制度、加密貨幣追蹤小組、銀行進駐反詐騙中心，以及金融管理局擴大「共同責任架構」（SRF）等。此類制度強調即時金流阻斷與資訊共享，並透過跨部門合作強化整體防制效能。歐洲國家亦有類似作法，Eurojust 與 Europol（2025）報告指出，面對數位證據大量增加與跨境資料存取困難，歐盟透過「電子證據一覽子計畫」及《數位服務法》等立法工具，簡化調查程序並強化跨國合作。同時，公私部門合作在資料共享與技術支援上扮演關鍵角色，但亦面臨法律與資料保護限制。另一方面，多國研究均指出，詐欺犯罪具有高度「黑數」現象。歐洲與英國調查顯示，網路詐欺之報案率顯著低於其他財產犯罪（Kemp et al., 2020:293；van de Weije et al., 2019）。報案行為除與犯罪嚴重程度相關外，亦受城市化與社會心理因素影響（Koning et al., 2025）。若僅依賴警政統計設計政策，恐難以全面掌握問題規模。英國「國家經濟犯罪被害人關懷小組」之經驗亦顯示，即時支援與風險教育對提升防詐意識具有實質效果（Home Office, 2025）。INTERPOL（2021）與世界經濟論壇（World Economic Forum ,2020）均強調，政府無法單獨擁有所需之全部技術與資源，私部門必須成為治理體系的一部分。整體而言，多數先進國家在詐欺犯罪防制的各個面向，已從傳統執法導向，轉向跨機關合作與公私協力模式。

參、研究設計與實施

儘管近年在「新世代打擊詐欺策略行動綱領」架構下，已逐步推動跨機關合作機制，惟警察機關仍為受理民眾詐欺報案之第一線政府部門，且多數防詐工作從過去 20 多年至今，實質上仍由其承擔。據此，為瞭解我國詐欺犯罪防制跨機關合作之實際運作情形，本研究以警察機關為分析起點，檢視臺灣在詐欺犯罪防制方面跨機關合作過程中之現況及其政策精進空間。研究方法上，除透過國內外相關文獻之整理與分析，作為調查工具設計之理論基礎外，並採半結構式深度訪談方式蒐集實證資料。以下分別說明本研究之研究對象與資料分析方式。

一、研究對象

本研究共訪談 20 位具實務經驗之受訪者。研究對象依職務性質與在詐欺犯罪防制體系中的角色位置，採目的性取樣方式區分為三類。第一類為中央主管機關現職或曾任相關職務之人員，主要掌握政策規劃與制度設計層面之經驗；第二類與第三類則為第一線執行機關主管，包括現任直轄市分局長及刑事警察大隊大隊長，著重其在跨機關合作實務運作中的經驗與觀察。本研究擬藉由不同職務的警察人員之觀點交叉比對，以呈現在警察機關角度中，我國跨機關防詐合作之樣貌。深度訪談分為兩階段進行：第一階段先訪談第一線執行機關主管，並以詐欺案件數較多的直轄市為主，經初步分析與問題彙整後，據以修訂訪談題綱；第二階段再訪談第一類人員，以進一步釐清制度設計與政策推動層面之議題。在樣本對象方面，第一類受訪者計 6 人，第二類與第三類各 7 人，共計 20 位受訪者，基本資料如下表 1。訪談期間為 2025 年 10 月至 12 月。

表 1 受訪談對象基本資料表

代碼	服務單位	職稱	服務年資(至 2025 年)
A1	北部大學犯罪防治系 (前於刑事警察局服務)	助理教授	36 年
A2	北部縣市警察局	局長	35 年
A3	刑事警察局	主任	25 年
A4	刑事警察局	秘書	28 年
A5	刑事警察局	科長	27 年
A6	刑事警察局	隊長	18 年
B1	南部縣市警察局	分局長	30 年
B2	南部縣市警察局	分局長	28 年
B3	中部縣市警察局	分局長	36 年
B4	北部縣市警察局	分局長	27 年
B5	北部縣市警察局	分局長	35 年
B6	北部縣市警察局	分局長	27 年
B7	北部縣市警察局	分局長	30 年
C1	北部縣市警察局	大隊長	24 年
C2	北部縣市警察局	大隊長	21 年
C3	北部縣市警察局	大隊長	30 年
C4	南部縣市警察局	大隊長	25 年
C5	東部縣市警察局	大隊長	23 年
C6	北部縣市警察局	大隊長	32 年
C7	警政署所屬警察機關	大隊長	19 年

二、資料分析方式

本研究之訪談資料採逐字稿整理後進行質性分析。分析程序以主題分析 (thematic analysis) 為主要方法，並參考紮根理論之編碼邏輯進行資料處理，以建構我國跨機關防詐合作運作態樣之分析架構。依據紮根理論框架下循序漸進之編碼過程，使研究發現能由資料中逐步生成，而非預設結論。另在資料分析過程中，研究者採取持續比較法 (constant comparison)，反覆比對不同受訪者之觀點，以辨識共通性與差異性，當新增訪談內容未再產生實質性新概念時，即視為理論飽和已達成。最後，為提升研究之信度與效度，本研究採多重資料來源交叉驗證，除訪談資料外，亦輔以政策文件、法規資料與相關文獻進行比對分析。在研究過程

中，研究者亦持續進行自我反思，檢視自身在警政與防詐議題之既有立場與經驗可能對資料詮釋造成之影響，並透過反覆回顧逐字稿與分析備忘錄，以降低主觀偏誤。透過上述程序，本研究力求在分析深度與解釋嚴謹性之間取得平衡，以增進研究結果之可信度。

肆、資料分析與討論

在「新世代打擊詐欺策略行動綱領 2.0」中，政府係以「識詐、堵詐、防詐、阻詐、懲詐」作為五大面向。在此架構下，警察機關主責「識詐」工作；於「堵詐」（電信端）、「防詐」（數位經濟產業端）、「阻詐」（金融端）及「懲詐」（司法系統端）等面向，亦有協作的角色，且有正式聯繫機制。本文即以此跨機關協作架構為基礎，聚焦警察機關於跨部門網絡合作中的運作樣態與執行困境，並從警察機關視角出發，分析其與上述各面向之互動關係

一、應重視跨網絡合作以提升打詐有效性

大部分的受訪者都提到，警察機關在防詐體系中多數扮演執行端角色，真正能影響整體詐欺犯罪成效者，仍是政策層級的跨部會合作與制度設計。受訪者 B1 認為，若僅依賴警察機關的短期專案或執法強化，往往無法有效處理詐欺犯罪結構性問題，應由中央層級整合金融、平台與電信資源，建立長期性的金流關聯分析與責任分工機制。此種觀點與前述文獻所提的國際趨勢不謀而合，受訪者 A1 表示詐欺防制的核心並非單純加強取締，而在於透過政策或法制規範工具提供者，例如社群平台、金融機構與電信業者，使其共同承擔預防責任，因此跨機關合作不僅僅是在政府部門間，還包括公私協力的部分。受訪者 B6 指出，跨網絡合作的重要性與詐欺犯罪產業結構的高度分工密切相關，詐欺集團已由過去「一條龍」模式轉變為高度分包化運作，金主、機房、車手與洗錢體系分散於不同國家與產業節點，使警方往往僅能在金流末端進行處理。因此若缺乏跨國與跨產業合作機制，單一執法機關難以有效打擊整體犯罪鏈。

打詐策略就警察機關內部多只能在執行面精進；政策面需要跨部會與平台、金融、電信共同負責。…由中央層級推動金流關聯分析與平台責任機制，整體成效才會上來。(B1-11-6)

打擊詐欺的重點不是只一再考慮「提升偵查、加強取締」，而是要從政策面下去著手…提供詐欺工具的這些社群平台要有一定的義務、要求跟管控；金融端要把「壞人的帳戶」找出來。英國現在也開始加強對空殼公司的管理。在整個打詐上，國外做的東西其實很多。(A1-14-1)

詐團裡面還有工程師，什麼東西都有…他們現在分包式，台灣是車手團，車手

團完了之後，還有洗錢集團…我們在偵查能夠做的，大概就是剩錢不讓出去而已。
(B6-11-3)

受訪者 A2 認為，近年詐欺案件數量出現下降趨勢，與跨網絡合作機制逐步形成密切相關。特別是在《詐欺犯罪危害防制條例》施行後，跨機關合作的制度化程度有所提升，使得網絡平台合作、資訊共享等面向開始發揮效果。受訪者 B3 則從反面指出，部分新興犯罪領域管理遲滯，凸顯出跨網絡合作的重要性。例如虛擬貨幣監管過去長期缺乏明確主管機關，導致制度責任分散，影響政策回應速度。B3 認為，近年行政院推動跨部會合作方向正確，但關鍵仍在於能否將協調結果轉化為可執行之制度工具。

我自己觀察詐騙數字下降，一方面是詐防條例上路之後，機關的合作發揮功效…第二個就是國際的大環境也有受到影響。(A2-1-2)

虛擬貨幣的主管機關是誰？這個問題我 103 年就跟他們反映，前一陣子才聽說金管會要接，如果十幾年前就有人願意站出來負責，現在很多問題早就解決了…行政院做跨部會協調方向是對的，但重點在於協調完要有「實際、能執行的政策」。
(B3-12-3)

二、與電信網路端的堵詐合作

在與電信業者配合方面，由於詐欺犯罪防制條例已經賦予相關配合的義務，因此多數受訪者表示在法源的依據上較沒有問題，實務上第一線的偵查人員認為電信業者的作業配合度高，但另一方面電信業者配合政府打詐政策所提供的服務均要收費，受訪者批評其是將防詐工作視作生意，而未擔負企業的社會責任。

(一) 第一線的作業配合度高

受訪者 C7 表示，電信業者在日常偵查支援上被視為高度可靠的合作夥伴，尤其在門號資料與通聯相關資訊調閱上，因此在警察需要快速取得個案資料的情境下，電信端確實能提供即時、效率性的配合，且已形成電子化流程，比起受金管會管理較嚴格的銀行業者，電信業者的彈性較高，作業程序較簡便。

電信業者他們調資料速度最快；我要調個電話門號資料，越快越好嘛。這塊

我們是有電子化流程的。最近銀行的配合度也比較高。最重要的就是這兩類業者啦。只是銀行還受制於金管會——常常是銀行想做，金管會說不可以。(C7-7-3)

(二) 惟業者仍可能以成本與經費作為協商籌碼

但另一方面，受訪者 A6 同時對電信端的合作動機抱持高度批判，認為業者把防詐視為生意，每推行一項新措施就要求政府支付額外費用。這使合作關係更接近「在商言商」。A6 對電信業者要求政府付費的合理性提出強烈質疑，典型例子是跨境詐騙電話語音提示「這是國際來電」竟被要求投入數千萬的預算。

電信業者把防詐視為一門生意，我要求電信業者配合做什麼，他就要求政府機關付他錢。舉個例子：跨境詐騙電話語音提示「這是國際來電」，光這個就要幾千萬的預算。不合理啊，然後每推行一個策略他就要一次錢…但問題是：業者收這個錢合理嗎？(A6-23-1)

此外，受訪者 A6 指出，《詐欺犯罪危害防制條例》施行後，雖已提供與電信業者合作之法源基礎，惟制度建立後仍面臨執行效率與經費負擔問題。A6 認為，電信業者憑藉關鍵基礎設施與技術優勢，將部分防詐措施轉化為議價服務，使政府除制定政策外，仍須持續向業者「購買」其執行功能。A6 進一步主張，部分源頭防詐作為應屬企業社會責任，不宜全由政府承擔；且業者執行效率時有延宕，甚至藉此要求追加經費。本研究認為，此現象反映電信業者「公共安全責任」與「商業營運邏輯」之界線未明。電信端雖具降低詐欺防制外部成本之能力，其投入誘因仍以事業經營為導向，而主管機關之態度亦可能外溢至其他治理領域。然依前述 Scot 與 Merton (2021:1638) 之研究，跨機關合作能否持續並產生成效，關鍵仍在於各行動者對核心政策目標形成高度「目標承諾」。

目前 165 在跟電信或平台合作時，法源上沒什麼問題。我要講的「不方便」，比較像是他們會推拖啦、效率不好，他們是「有錢才要做事」。…我覺得就不對，這該是他們「社會企業責任」的部分，就不應該再叫政府掏錢。(A6-23-5)

(三) 目前需補強之監管漏洞為建立境外門號實名驗證機制

受訪者 C2 指出，隨著網路詐欺犯罪興起，當前電信面向之防制困境已出現轉變，境外詐欺來電已非主要問題，反而是詐欺車手在國內大量使用境外門號作

為犯罪工具。此類門號雖可於我國正常通訊與上網，惟於偵查過程中，常因無法確認登記人身分，且缺乏入境紀錄與使用者資料之勾稽機制，致使偵查關鍵環節受阻。C2 並觀察，近期查獲之詐欺車手幾乎皆持有境外門號，且多為香港與泰國號碼開頭，顯示此一漏洞已成為詐欺集團普遍運用之犯罪工具。受訪者 B1 亦表示，早期即存在透過收購 SIM 卡或使用人頭門號規避責任之情形，顯示單純形式性之實名制度難以有效發揮監管功能，亟需明確界定責任歸屬與管理機制。受訪者進一步建議，應建立境外門號使用之實名驗證制度，例如透過線上身分認證、護照資料比對或入境紀錄查核等方式，填補現行監管灰色地帶，並及早建構可落實之跨機關管理機制，而非僅於事後追捕。

今年查獲的四千八百多名詐欺車手中，幾乎人手一支境外門號…建議通傳會應要求所有境外門號在我國境內使用時，必須完成線上身分驗證，至少比對護照號碼或入境紀錄後方可啟用，以補足實名查核的漏洞。(C2-8-3)

我二十年前在機場也遇過導遊帶團，離境時去現場收 SIM 卡…以前路上違規看板滿留的連絡電話都是人頭卡。把卡丟了找不到人就沒事，跟本無法開罰…現在看到問題才開始討論誰管，真的慢了。(B1-11-3)

三、與數位經濟產業端的防詐合作

缺乏完整專法與主管機關權責不明，是數位經濟產業合作端所面臨的最主要問題。綜合受訪者觀點，對於目前防詐體系中的雲端缺口，主管機關仍有很大的發揮空間，以下分析之。

(一) 受訪者認為平台應負義務轉嫁由政府承擔且未能落實風險管理

依據《打詐行動綱領 2.0》規範，防詐工具應透過公私協力機制開發。受訪者 A1 表示，目前較具體作法為警察機關與數位發展部建置爬蟲工具、彙整可疑連結後，再轉交平台或第三方服務商下架。然而 A1 反覆指出，現行數位詐欺下架與偵防流程已呈現「政府取代平台應盡之責」的扭曲現象，其間政府額外投入的人力、技術與成本，均本應由平台內部負擔。A1 批評當前合作模式形同政府代為執行平台應盡之內容管理責任，並主張數發部角色應為督促平台履責，而非直接介入執行。A1 指出，平台收取廣告費，管理成本卻由數發部與警察吸收；且政府要

求下架越多，詐團反而需投入更多廣告費，使平台除無須承擔責任外，還可藉此獲利。受訪者 C4 引述國外報導指出，國際平台每年自詐騙廣告獲利龐大，應加強規範其自我審查責任；C3 與 B1 亦認為，現行對平台之裁罰未能有效促使其建立主動審查機制。

說穿了，不管是數發部也好、警察也好，很多時候是在幫平台做本來他們應該做的事情…比方說以前在講「藍勾勾認證」，藍勾勾是要繳錢的…你既然有收錢幫人家掛藍勾勾，那仿冒的假帳號就不應該再出現了…本來就是企業自己的責任。(A1-5-2)

網路廣告平台業者他就該自己做分析，這才是核心問題。我們有裁罰嗎？這又是第二個 bug。(C3-3-2)

每年從詐團的廣告獲益了 500 億美金嘛…以他們的科技跟技術，絕對有辦法可以過濾掉這些跟詐騙有關係的東西，但反正我賺到錢就好了啊，這不是我的責任。我們修法可以在這一塊多課予一些責任。(C4-8-3)

平台必須對非法投資廣告管理負責，要負社會責任，不能只賺錢不管內容。民眾詐騙資來源的源頭不管，後面的電信與金融機關也不管，不能只叫警察收拾還要扛治安不好的結果，沒有道理。(B1-5-3)

目前不同平台在防詐工作上的推動成效不相同，受訪者 A1 提到 Google 透過第三方 G2 機構完成廣告主實名審核，詐欺廣告量明顯低於 Meta；而 Meta 目前雖宣布跟進，惟仍仰賴政府提供「白名單」協助辨識真人帳號，顯示仍被動依賴公部門。A1 進一步表示，若是平台能夠在發現詐欺廣告時，可以將廣告主身分、付費方式等資訊提供，則警察機關還可以做溯源，更為根本的解決詐欺廣告的來源。受訪 B1 認為平台既然能把廣告受眾投放做得極精準，就應有能力在演算法階段做風險控管。B1 表示甚至可以考慮以海外集體訴訟的方式對平台施壓，要求其必須遵守臺灣的法律及配合警察機關的資料調閱。簡言之，受訪者認為應該把屬於平台的風險控管成本還給平台，且只有平台業者最了解自己的產品安全風險在於何處，而政府的職能本應就放在標準制定、監督與制裁，才能避免公部門持續背負私部門風險外部化的沉重成本。

現在看起來，Google 上面的詐騙廣告數量，大概只有臉書的十分之一，因為

Google 有找一個 G2 的機構幫忙做審核認證…臉書仿冒名人的投資詐騙好像是有變少一點，但我覺得那多半是數發部在努力用「白名單」，不是平台自己主動過濾…你收了廣告費，真的出事，你要把錢從哪裡來這件事交出來。(A1-7-1)

找國際律師在海外提訴訟…若在演算法階段就能安插反詐宣導，甚至配合 DNS 層級的阻擋，點了也連不上，那就更好了。現在平台的演算法對廣告投放做得那麼精準，對打擊犯罪卻不見得配合。(B1-7-4)

(二) 應透過具成本效果之罰則設計促使業者內化風險控管責任

政府如何運用制度規範促使大型數位平台調整商業流程並承擔防詐責任，成為訪談過程中受訪者頻繁提及的議題。資料分析顯示，受訪人員認為，唯有「明確的法規要求」結合「具時效性與嚇阻力的裁罰機制」，方能對平台形成實質約束；凡缺乏即時性或裁罰力度不足的規範，往往容易被平台與詐欺集團各自利用而流於形式。受訪者 C2 即指出，其所服務的縣市在透過程式協助下架詐欺廣告過程中，促使中央依《詐欺犯罪危害防制條例》對 Meta 未於 24 小時內下架廣告開罰 250 萬元。其後 Meta 派員拜會地方政府，顯示裁罰確定性能改變平台態度。受訪者 A6 亦指出，Meta 在遭裁罰後，下架效率已提升至通報後 2 小時內完成，另外現行蝦皮購物禁止張貼帳號或 QR Code 的有效防詐作法，亦源於過去曾遭裁罰經驗，凸顯平台的配合往往源於法制壓力與執法力道。

未依限下架者，我們會通報數發部裁罰…Meta 在 7 月份的時候，還特別從總公司派亞洲總部的人來拜會市政府。(C2-4-2)

目前對這種平台上的廣告，我們通報，他 2 小時內就可以下架，這是有明顯改善的。臉書之前被罰過，罰了之後確實有差。(A6-6-2)

進一步而言，多數受訪者指出，若平台能將風險管理納入服務流程，將有助於顯著提升防詐成效。受訪者 A6 舉例，在高風險對話情境中主動攔阻連結或帳號傳遞，以及導入 MID 驗證機制強化行動支付安全，皆屬能有效壓縮詐欺操作空間之關鍵措施。然而，此類機制多仰賴業者自律，如何透過制度化規範促使其落實，成為重要課題。對此，受訪者 A1 建議，可要求投資廣告設置保證金、建立延遲付款機制，或依全球營收比例課以裁罰責任，以改變平台既有商業邏輯。受訪者 C6 指出，現行平台廣告收益與罰鍰金額差距甚大，目前的罰則難以改變業者行

為。受訪者 B1 進一步指出，可參考英國對數位平台課予之監管責任與規範，透過具實質制裁效果之制度設計，提高業者投入資源強化風險管理之誘因。受訪者 A4 及 C2 都提到，現行制度過度聚焦事後補救責任，對平台事前審查與風險控管缺乏明確處罰機制，形成監理落差，應透過制度設計促使平台將風險成本內部化。

「投放投資廣告」是特許行業，要有牌照才能做。所以人家要投放投資廣告的時候，你至少要先收一筆保證金。如果在這期間，被通報為詐騙而下架，那保證金就沒收；以後這筆錢可以拿來補償被害人、或轉作防詐基金，甚至可以規定在特定情況下，平台要連帶負一些賠償責任。(A1-6-1)

現在的罰則大多是在處理事後補救，但我們現在真正需要強化的是事前審查。事前風險管理如果做不好，要有相對應的罰則。目前最大的問題就是一事前做不好，幾乎沒有明確的處罰機制。(A4-3-4)

蝦皮上平台不讓你貼帳號、貼連結，那這就是「做到一個點」…所以像蝦皮詐騙就減少非常多，因為它禁止丟連結，這就是業者願意做詐騙就會少。(A6-5-3)

政府可以參考英國的作法。兩年前他們討論，對於外資平台要課以企業社會責任，要管制實名制度與下架，不配合就裁罰，似乎可以罰到全球營收的一定比例。(B1-5-2)

廣告面你根本沒有一個完整的數據可以掌握，源頭也查不到。我們現在能做的，大概就是「下架」而已，你找不到那些人，實務上也很無力。(C2-4-3)

數發部罰款加起來可能有上千萬，但是 Meta 賺幾十億…他的犯行跟你罰他不成比例，就是你的處罰概念，不要只有繳錢，你要讓他痛苦。(C6-7-6)

整體而言，訪談資料一致顯示，當前平台管理關鍵在於監理制度須重新設計，導向賦予業者事前風險管理的責任。若缺乏明確法制授權與積極執法態度，政府將難以有效促使平台落實防詐責任，亦將削弱整體打擊網路詐欺之政策效能。

(三) 受訪者多認為數發部監理角色不足且有法制空白的結構性問題

承上，對平台的監理是防詐重要的一環，多數受訪者對數位發展部在詐欺犯罪防制上的角色抱持高度期待，惟實務上卻普遍感受其作為仍顯不足。受訪者 C2 指出，數發部對網路平台業者的管理仍屬鬆散，不僅缺乏明確裁罰權限，亦未建立統一窗口統籌警政與司法需求，導致數位端防線未能有效啟動，恐形成詐欺犯

罪防制上的缺口。受訪者 C4 以實務案例說明此一結構性問題。其指出，當第一線警察機關依「打詐綱領 2.0」要求數發部協助時，卻遭對方以「某縣市警察機關已自行開發偵測工具」為由，反向發函要求其他警政單位自行處理、退出支援。此舉被受訪者解讀為數發部反向推責，顯示部會間缺乏明確權責共識，致使第一線警察人員持續被迫補位、承擔可能非其專業之工作。

數發部對網路平臺業者的管理仍屬鬆散，該部與警政及司法機關在跨部會協作上也欠缺統一窗口。亟需數位網路主管機關正視且投入資源建立合作網絡。(C2-7-3)

警政署有提出來請數發部來幫忙，但是後來數發部發現某一個縣市警察機關，他們也有辦法做，就發一個公文就跟你講說，哪個縣市他們都可以自己做，這個就不要 pass 給我們了…不能因為我多做，你就把你的本職工作丟出來。(C4-11-7)

數發部就是說：你們辦案、你們要查資料，都要考量到產業的發展…我們希望不是把詐騙問題都檢討警察，要看是哪邊的問題就該檢討。(C5-7-4)

拉數發部進來是最好的…數位方面的，因為這是我們國家政策。…我們臺灣對於這些國際的社群媒體好像不太敢得罪。(C6-7-2)

因此，當問到在跨機關合作上，目前最需優先強化合作關係為哪個對象時，多數受訪者都提到數發部與國家通訊傳播委員會（NCC），且兩者重要性相當，均是與網路平台相關的主管機關。進一步而言，受訪者 A4 直指當前平台監理產生困境的根本原因，在於我國缺乏一套完整的平台專法或母法架構。其指出，相較金融體系尚有《銀行法》等完整法制工具，主管機關得以多元手段監理風險；平台端則僅依賴《詐欺犯罪危害防制條例》中零星條文，執法工具極其有限，導致即便發現業者未落實風險管理，也難以找到具體法源做裁處。此一問題亦同樣存在於第三方支付與虛擬資產等新興數位經濟領域。受訪者 C6 亦指出，當前跨網絡合作打詐中，與數發部的合作是最為薄弱的一環。相較之下，經濟部反而展現較高配合度。整體來看，多數的受訪者認為，數發部對於法律現存缺口消極以對，僅希望警察承擔制度漏洞所衍生的風險；而平台業者之所以不配合，關鍵在於「無利可圖」且法律並未明確規定。

現在的狀況是全部查詢、投單都透過警政署出去…連 Google、LINE 都還要跑現場才能調資料，太原始了。但數發部不要。業者不配合的原因又是什麼？無利可圖，還有法律沒有規定他們「必須」要建這種管道。(A6-23-3)

幾乎所有部會都需要加強。但若真的要分層級，我會認為最優先需要強化是數發部與 NCC，而且這兩個單位的重要性是平等的。(A3-1-3)

像銀行有《銀行法》及配套規範，主管機關可以用很多工具處理未落實風險管理者；但平台這邊，常常只有《詐防條例》裡幾條規定提到平台責任，工具非常有限。…第三方支付、虛擬資產也是類似狀況。(A4-3-8)

受訪者觀察，主管機關並非是沒發現現行平台監理法制存在許多空白處，導致實務上無法強迫平台業者落實風險管理責任，而是主管機關不願積極處理。受訪者 A3 指出，除在平台廣告管理及相關義務執行上積極度不足，對平台業者之規範與督導相對寬鬆，且還對違規行為裁罰意願偏低，難以形成有效的嚇阻效果。甚至第一線執行的警察機關報請內政部嘗試推動裁罰案件，還常遭遇主管機關以法律解釋空間、規範定義不明確等理由加以阻擋、處處限制。A3 甚至形容此種情形為「抵制」，反映跨部會間在權責認知與政策立場上的落差，原應由主管機關主導的監理機制，反而成為推動執法的阻礙。總結而言，受訪者認為當前業者自律不足的源頭，來自於主管機關監理角色的消極，在缺乏明確法制授權與積極執法態度下，要求平台落實防詐責任無疑是緣木求魚，這樣的情形亦削弱政府整體防詐政策的實質效能。

我的看法是：平台端風險管理並沒有做到位，但主管機關的推動力也不夠。針對廣告、平台應做事項、以及相關義務的執法規範，我覺得並沒有非常積極。甚至我們這邊推動裁罰的案件也很有限，原因是會受到主管機關的「抵制」。他們會用很多法律上的解釋去卡住你，或者以「定義不清」來降低執法強度。(A3-3-5)

其實具體的修法方向，就是把「偵查實務中遇到的瓶頸」寫進法律。比如說 Gmail、Google 的資料不給警察調…回到很簡單的「平等原則」—你給其他國家什麼，就要給我們什麼。(A6-23-3)

四、與金融端的阻詐合作

詐欺犯罪離不開金流，由於阻詐的需求，金融機構是警察機關最早開始合作的對象之一，因此雙方的合作已成常態化，從中央至地方的警察機關均已與金管會及當地銀行等金融機構建立聯繫機制，不過在合作成效上，受到金融機構內部管理差異，有不同的配合度，但整體而言，金融機構的配合確實有一定的影響力，近來詐欺集團的金流多已從 ATM 轉向虛擬貨幣與第三方支付，也由於詐欺犯罪的洗錢手法不斷變化，不少受訪者提出未來與金融端的合作要進一步朝向資料共享方向努力，才能夠突破現行追金流的速度與規模受限的瓶頸，以下分析之。

（一）合作已常態化，但成效受金融機構內部差異左右

受訪者普遍肯定警銀合作在「實體攔阻」層面已相當成熟，且第一線互動頻繁。受訪者 A2 與 C4 均表示，整體運作「基本上沒有問題」。然而，實務上攔阻成效仍高度受金融機構內部推動力度、組織文化及第一線行員個人風格影響。受訪者 A2 指出，各金融機構對實體攔阻詐欺之重視程度仍存在差異，甚至在部分攔阻失敗個案中，特定機構曾占較高比率。不過，透過拜訪、提醒及上級關切後，其配合度確有提升。例如透過每月打詐記者會公開點名表現優良及待改善之金融業者，經媒體揭露後，原態度較為消極者亦轉為積極配合警察機關。此外，受訪者 A6 觀察指出，若銀行高層曾具警職背景，對警察機關之防詐需求通常較能理解與支持。研究者認為，上述現象顯示警銀合作並非僅憑制度建立即可自然產生成效，而仍高度依賴金融機構內部管理條件，包括教育訓練、督導機制、組織文化及是否納入績效考核等，方能使行員主動攔阻行為成為常態化之工作項目。

每一家金融機構的態度還是不太一樣，內部推動的力度、公司文化、個人風格也不同…當時我們攔阻失敗的案件裡有超過一半是郵局發生的…他後來被上級關心之後就更積極了，願意跟我們一起配合。(A2-8-1)

臺灣要不要建立「全國金融異常交易資料庫」或「警政與金融聯合風險評分系統」，我的答案是：非常有必要，而且非常需要。只有這樣，銀行才會真正配合警政單位在防詐上的要求。(A3-4-5)

這幾年我們推動電子化調閱之後，拿到的資料已經是可以直接統計、分析的格式，這對實務幫助很大…跨行即時警示、共享可疑帳戶資料，也早就有制度。(A4-4-1)

警察有在的網銀安全級別都高一點。元大、台新也算。這可能警察過去把觀念帶進去。警察去金融業當資安長，我覺得對打詐影響超大…因為他們知道有問題找誰、我們也知道各銀行窗口是誰，所以互動很好，溝通也順。(A6-8-1)

目前在跟銀行的調閱跟合作的部分大概沒有什麼問題啦…金管會已經有盡量去配合，警政署又有推動線上調閱。(C4-2-5)

金融端防詐合作之成效亦可從另一面向觀察。多位受訪者指出，當金融機構與警察合作密切時，臨櫃匯款之實體攔阻趨於嚴格，ATM 提領限制亦隨之提高，且警方積極查緝面交車手，使詐欺金流管道受到壓縮。在此情況下，詐欺集團逐漸轉向網路金融及虛擬貨幣等較難攔阻之新型態模式。受訪者 B1 進一步指出，第三方支付已成為新興防詐缺口，並以其承辦案件經驗說明，早在 3 年前即發現部分第三方支付業者可能淪為金流中轉甚至共犯，直至近期政府始逐步加強相關監管。此一現象顯示，詐欺金流攔阻之跨機關合作不應侷限於傳統銀行體系，尚須擴展至「準金融」領域，包括第三方支付與虛擬貨幣等，亦即涉及數位經濟產業之監理問題。

因為我這邊盯得滿緊的，所以慢慢地他的匯款、提領、交付的情形都下降很多，就變成是用網路金融、購買虛擬貨幣那一類。(A2-9-2)

現在比較頭痛的是第三方支付。這部分最近才開始管比較嚴。我三年前辦過一家公司因為洗錢角色嚴重才收押，我們調金流時現場找不到錢，當時以為只是廠商，其實是共犯，甚至在公司搜索到地檢署來調閱資料的公文。(B1-11-4)

很多青壯年他們使用數位支付工具很頻繁，很熟悉操作。他知道怎麼用、怎麼提升額度、怎麼綁約定帳戶，就很容易被詐騙集團一步一步引導騙走那麼多錢。(A6-18-1)

(二) 制度瓶頸在於提升金流追蹤速度與規模

多數受訪者均強調，詐欺偵辦的核心在於「速度」。受訪者 B1 指出，警察人員在追查過程面臨高度時間壓力與執行困難。雖然受訪者 C2 與 C5 表示，近年已透過「投單平台」以線上調閱方式提升資料調取效率，但受訪者 A1 與 A6 仍以澳洲情資中心及新加坡警銀聯防機制作為對照，認為其關鍵在於制度設計能將防詐工作與金融監理緊密結合。這兩國的制度是透過安排多家銀行代表實體進駐

同一場域，使警方於發現異常交易時，得即時啟動鎖卡與金流追蹤機制，並連動金融監理權限，對不配合者可直接處以行政裁罰。澳洲還整合線上報案系統與情資中心，使民眾可直接上傳完整案件資訊，由具偵查權限之單位即時承接處理。此種設計不僅有助於警方溯源偵辦，也能降低民眾反覆詢問案件進度所衍生之行政成本與不滿。相較之下，臺灣雖在前端攔阻與帳戶凍結等措施上具一定成效，但在後端追蹤與情資整合之制度化方面，仍存在明顯不足。

澳洲指定六家主要金融機構進駐情資中心，「這是你家的客戶，你就負責凍結你那一家的帳戶，把那一金流資料抓出來」，六家都在現場，合作起來非常快。新加坡的警銀聯防也是一樣…這是立即合作的優點。(A1-26-2)

我去過新加坡，那個中心的重點其實也就是可以馬上調資料。但新加坡有一個好處是：他可以「直接罰」，哪個業者做不好，會直接反映在他的評比上。這個才是有殺傷力的地方，金融監理直接聯動。(A6-3-2)

大致上有分「警示帳戶」跟「非警示帳戶」兩類：如果是「非警示帳戶」，就要由警察局層級投單，已經被列警示的分局可以分局直接投，再送到金融機構調閱。(C2-5-4)

以前我們就知道，你匯一百萬出去，大概十分鐘之後就會分散到十個戶頭…金流在跑的速度很快這十家再丟出去可能又變成二十家，一直下去你要警察怎麼查?(B1-11-5)

多位受訪者指出，當前詐欺偵查在金流追查方面仍受限於資訊整合不足。受訪者 B1 與 C2 均建議，應建立類似警政查詢系統之關聯式分析平台，以整合金融機構資料並強化金流即時掌握能力。B1 指出，詐欺偵辦的關鍵在於第一時間保全被害人資金，因此當民眾完成首筆匯款並報案時，金融端應具備即時分析資金流向之功能，透過系統自動進行關聯運算，迅速提供完整金流路徑，甚至可藉由輸入被害人基本資訊即同步帶出相關帳戶與交易資料。B1 進一步說明，此一需求源於詐欺資金流動速度極快且跨境追查困難。雖金融監理機關掌握相關帳戶與匯款資訊，但現行跨機關合作模式仍存在效率不足問題，使警方在金流追查上持續面臨時間與規模之限制。另受訪者 B4 亦建議，為降低詐欺集團提領效率，可於 ATM 提款導入生物辨識機制，以強化資金控管與即時攔阻能力。整體而言，上述意見均凸顯現行詐欺偵查體系，在金流即時整合與科技運用層面仍有精進空間。

我們都很希望像警政查詢系統做成關聯式分析平台。比方說查車牌，查戶籍，只要打上名字或身分證號丟進去，我查一查，相關資料就跑出來了…但目前金管會把這些工作都留給警察機關做，我覺得最沒有效率。(B1-11-6)

電影演真的，就是第一時間錢進去，然後各地車手拚命把錢領出來。錢一進去到這個帳戶，這個帳戶就會再往下分散到其他人頭帳戶，去把錢領掉。(B4-5-6)

我們比較希望達到的狀況，就是資料庫能夠直接串接警示帳戶，有授權的狀況下，我們像查前科一樣，登入系統，就可以直接把資料叫出來看。對我們來講，時間會省非常多。(C2-5-5)

(三) 未來合作的趨勢在風險被害人的資料管理，需賴法規修訂

在警銀合作的下一步發展上，訪談資料顯示，實務運作的主要瓶頸已由「合作意願」轉向「資料管理與法源基礎」。受訪者 B5 指出，當前阻詐盲點在於資料無法跨機構連通：同一被害人短期內可能於多家銀行連續匯款十餘筆，但第一線行員僅能掌握本行零星紀錄，無法辨識被害人其實已處於高度受害風險情境。此一觀察與 A2 所提之「阻詐金鐘罩」概念相呼應，即透過跨行資料整合及即時風險控管，針對已深陷詐騙情境的被害人採取限制措施。然而，多位受訪者亦提到，此類作法的最大障礙在於個資法與資料共享缺乏明確授權，金融機構因擔憂法律責任而不敢進行資料介接。

我剛講阻詐金鐘罩牽涉到被害人的個資問題，這就必須透過修法去處理…要推全國性，就一定會碰到個資保護問題，要靠條例去解。(A2-4-1)

我們遇到的挫折是：短期內連續這麼多筆密集被騙，代表是短期內深陷其中的行為。可是當我們去跟中國信託行員接觸聯繫時，只看得到中國信託個人的資料，他不知道台北富邦那邊已經被騙了十幾筆了，再上面一層其實是沒有連通的…現在還是怕違反個資法。(B5-2-6)

現在銀行自己也在做辨識異常金流，我們和銀行在這方面也很密切。但資料庫的串接在法律上本來就有限制。(C7-8-2)

金融機構一直在講，他們願意相互介接資料，問題是沒有明確法源依據，他們會害怕個資責任。所以第一步一定是修法，把資料共享的法源補齊。(A3-4-2)

刑事局其實都有訂好一定的做法，資料也有給，但金融機構不見得會照單全收…金管會也沒有統一訂定要怎麼做。(A6-18-2)

受訪者 A1 強調，阻詐工作涉及制度設計與政策選擇。其引述新加坡經驗指出，透過立法允許對「持續受騙」之被害人帳戶採取暫停或扣押措施，可有效避免跨行轉移資金之漏洞。整體而言，訪談資料反映，未來警銀合作的核心挑戰是如何建立合法且具強制力的資料管理模式；若缺乏制度化法源支撐，跨行風險辨識與即時阻詐仍難以發揮效能。

其實跟銀行合作一塊是使用像「鷹眼」那種 AI 類型的工具…提早標記「這個帳戶可能有問題」，然後先做風險控管。…新加坡有立法，把已經知道的『好人帳戶』，可以申請『扣押、暫停』下來。(A1-9-1)

我們比較在意的是你明知道有問題，怎麼還會放他匯？你光關懷提問之後，怎麼不再跟我們講？(A2-8-2)

可以給的資料其實還很多。因為法律沒有規定要保留，所以他根本沒有留，這些問題就只能個別去協商。但那是很瑣碎的事啊，我們就是需要這種瑣碎的東西。(A6-9-3)

五、與司法系統端的懲詐合作

依據我國刑事訴訟法，檢察官是唯一的偵查主體，因此警察機關在偵辦詐欺案件最常接觸的對象就是檢察官，但是詐欺案件的偵辦牽涉到高度科技偵查技能，許多受訪者皆反映法院及檢察官的科技偵查素養及對偵查工具的理解，均直接影響到詐欺案件偵辦的進度與成效。另外在調查局體系中，洗錢犯罪防制目前是該局的業管，詐欺犯罪的犯罪所得的匯出往往牽涉到洗錢犯罪，然而在金流追查中，調查局的洗錢資料庫並未與警察機關系統有任何的嫁接，若要取得相關資料用以偵辦詐欺犯罪困難度較高。最後，對於跨境犯罪問題，受訪者指出國家層級的司法互助不足，是跨境追查詐欺犯罪的主要缺口，以下敘述之。

（一）檢察官科技偵查素養及對偵查工具的理解影響案件進度與成效

詐欺案件的破獲速度是關鍵因素，然而在保障人權的框架之下，警察機關許多的偵查手段必須要經過司法系統的審查才能夠進行。其中請領相關核准票據必須要經由身為偵查主體的檢察官，但當檢察官對於科技偵查素養不足時，極可能會影響案件的進度。受訪者 C3 不願意對檢察官的科技偵察能力多做評論，但認為

檢察官既然是偵查主體，對於詐欺案件的偵辦應該要比警察更為積極，科技偵查的能力不應需由警察教授。受訪者 C7 無奈表示，警察人員為偵辦詐欺案件努力學科技偵查手段，判斷到要抓幕後操縱者時，卻要先「教會」檢察官才能夠請到票據。因此偵辦的警察人員即便掌握門號、IP 或錢包地址，也可能因檢方「看不懂」而延宕。受訪者 C4 也指出相同的困境，表示不能只有警察人員要加強科技偵查的能力，法官與檢察官也要瞭解相關的常識。同一脈絡也延伸到對警察筆錄效力與重複程序的不滿。這些都在在顯示於詐欺這類高度技術化犯罪中，偵查實作能力的警察端與具權限的檢方端已產生落差。

各位有看到哪個檢察官在第一線執行？誰才是偵查主體？檢察官他對科技偵查了解嗎？no comment。檢察官是訴訟法上的主體，當然他應該自己會科技偵查。(C3-7-2)

有一個很大的問題就在於，警察一直在提升這一方面，但法官跟檢察官沒有。所以我們在辦案上面要請搜索票、做財產的扣押，我還要跟他解釋我是怎麼去追出這個東西…如果你檢察官不懂，我要怎麼跟你討論？法務部跟司法院這一邊的，我覺得他們的進步的幅度比較有限。(C4-13-2)

我跟你講，我認為檢察官不應該有偵查權。尤其是詐欺…我要查這個門號過去的使用紀錄、當時在哪邊騙人，現在還要開票才能夠拿到網路歷程。…你遇到爛的檢察官，你就不用辦了…他們自己也搞不懂科技偵查，很多我還要教他。(C7-7-1)

就是把我打好的筆錄電子檔送給檢察官啊，這就是另外很奇怪的地方，檢察官叫我們要問一次，那到底他是偵查主體還是我們？(B7-9-5)

受訪者 A1 指出，詐欺案件具有高度即時性與跨境特性，但在現行架構下，警察須層層報請指揮偵辦，導致黃金時間流失。在案件量已超出司法體系負荷的情況下，程序卻未能因應案件性質而調整。受訪者 C7 則是援引韓國 2023 年取消檢察官偵查權改革，主張參考多數國家，包括日本與德國的做法，讓警察人員也有偵查權，可以解決現行警察機關與檢察系統間的窘境。研究者以為，警察機關承擔破案與社會期待壓力，卻未獲得相應的案件主導權，在詐欺犯罪這類講求追查速度的案件中，重重的限制極易使案件出現遲滯。

詐欺這一塊，不管是追 IP、追跨國，全部都是在跟時間賽跑。等你報完、審完、核完，很多黃金時間就過了。如果整個司法體系本身就已經撐不住這種案件量，那至少在「詐欺、小金額案件的追蹤與主導」上，你就應該適度地授權警察，而不要什麼都等檢察官指揮，至少讓分局長以上可以直接偵辦。(A1-4-2)

很多國家都是「單一偵查」。至少韓國就是檢察官沒有偵查權…德國跟日本這兩國的檢察官都是輔助而已。警察都可以自己去調取或跟法院申請搜索票。(C7-7-2)

Meta、Google 目前只給法務部調，不給警察調。這在我看來就是差別待遇。而且法務部並不是偵查第一線，你在那邊搶這個東西要幹嘛？法務部會主動發動搜索嗎？不會啊。警察也不會隨便搜索，我們是要申請的。(A6-23-4)

(二) 洗錢金流情資掌握在調查局未能與警察機關高度配合

金流是詐欺偵辦的核心，但除了追查被害人的資金流向之外，詐欺集團為了洗錢也有金流的出入。在許多國家詐欺與洗錢防制是由相同機關負責，但是在我國的現行制度下，洗錢的情資與分析屬於法務部調查局負責，警察端缺乏可直接運用的整合平台，受訪者 A3 與 B3 都提到若是想查詢這方面的情資，警察機關並沒有一套能直接運用的系統。受訪者 A1 則對洗錢端資源封閉稍有抱怨，認為調查局通常不願意將掌握的資料提供出來。

你洗錢握著這麼多資源不願意提供出來，他們就是很堅持…現在他會吐一些出來啦。但 SSTR 通報一些案件還是在他們啦。他要給你看多少就給你看多少。(A1-4-1)

調查局的大額通貨交易資料，從 92 年開始建立但調查局就是不給。你是一個 FIU 機構，掌握那麼多金融情資，如果願意分享給警方，其實對打擊犯罪很有幫助。(A3-2-2)

要什麼資料都得去調查局經濟犯罪防制中心拜託人家調 data，人家願意給你操作你才看得到…現在最大問題就是金流。…要從根本解決，就是把金流這一塊「切」出來好好管。(B3-12-5)

受訪者 B3 反覆強調，釐清犯罪金流去向係詐欺案件偵辦之核心關鍵。其指出，現金與虛擬資產之金流追查耗時甚鉅，且在缺乏明確主管機關統籌管理下，虛擬貨幣已逐漸成為詐欺犯罪所得的重要洗錢管道。隨著詐欺集團運作模式由單純資金流動轉變為「資通流」整合型態，偵查工作難度顯著提升；若未能結合即時且有效之情資分析機制，將難以形成實質打擊能力。此外，現行制度在功能分工上，將上游犯罪偵查（詐欺）與下游金流處理（洗錢防制）分屬不同權責體系，亦被多位受訪者視為瓶頸。受訪者 A6 即指出，詐欺與洗錢業務分散於不同機關負責，易造成追查中斷。受訪者 C2 則表示，洗錢防制中心雖掌握可疑交易資料，但警方須經多層程序始得調取，且難以符合即時偵查需求。另受訪者 A5 指出，在跨境情資運作上，若未由調查機關主動啟動協查或進行情資共享，相關資訊往往停留於單一機關，進一步削弱跨境追查效率。

像這些「高額交易下架」之類的機制，實務上感覺速度還是沒有那麼快。其實是調查局這邊比較需要加強的。收到國外情資之後，你有沒有去做相關作為？如果你查不出來，有沒有把它 pass 給其他執法機關？(A5-24-3)

這一切很無厘頭—「洗錢」跟「詐欺」被硬生生拆開，結果就是：警察沿著金流追到最後，追不下去。(A6-4-2)

虛擬貨幣常常要查半天，人力少、案件又多…中央從來沒有想過要怎麼管這些金流，問題當然只會越來越嚴重。…以前我們是查人流，詐騙後來演變成查「資訊流」。但在調查局那邊才有完整的資料庫…只能一直去拜託人家給資料。(B3-12-6)

調查局底下的洗錢防制中心，確實會彙整 50 萬以上的可疑交易，但是那些資料還是要我們正式調查、提請求，他們才會提供。實務上跟我們直接合作的比較少。(C2-7-4)

（三）國家層級司法互助不足是跨境案件追查的主要缺口

訪談結果顯示，地方第一線偵查機關在詐欺案件辦理上，主要合作對象集中於地檢署與金融機構。受訪者 C4 指出，涉及跨境案件時，通常須透過刑事警察局國際科轉介處理。然而，受訪者 A6 明確反對將跨境詐欺偵查停滯之責歸因於第一線偵查人員，並將問題提升至國家層級能力不足之結構性議題。其指出，若僅以「查至境外金流即難以續辦」作為理由，實際上是將制度性限制轉嫁於基層

人員；真正關鍵在於主管機關能否建立有效的司法互助與國際合作機制。A6 進一步以新加坡已與逾百個國家簽署司法互助協議為例，質疑我國在國際對接能力上的不足。整體而言，受訪者意見顯示，跨境詐欺偵辦之瓶頸不僅涉及科技偵查與情資掌握能力，亦與法務與外交體系在國際犯罪合作支持不足密切相關。

目前那跟合作的單位，你如果以一般偵查人員在第一線遇到的，就是跟地檢署，然後跟銀行調閱一些資料…跨境的話，還是跟刑事局國際科。(C4-3-2)

境外辦不下去不是這些辦案同仁的問題，是「為什麼你不能跟國際對接」的問題。法務部到底在幹嘛？…新加坡那麼小的國家，都能跟一百多個國家簽司法互助協議。你如果想合作，是用合作取代競爭、取代意識形態的競爭。但台灣沒有。(A6-3-1)

伍、結論與建議

一、研究發現

本研究透過文獻探討與深度訪談，綜整我國詐欺犯罪防制跨機關合作現況與挑戰，主要研究發現如下：

（一）警察在防詐體系中承受過度期待，責任呈現高度集中化

臺灣過去多將詐欺犯罪防制責任交由警察機關，然文獻顯示，各國多採跨機關合作策略以提升防制成效。我國近年亦朝此方向發展，將詐欺防制區分為五大面向，由不同機關在共同政策框架下推動。然而訪談分析發現，第一線警察普遍認為現行體系對其角色寄予過高期待，致使責任高度集中。雖然政策上將「識詐宣導」定位為內政部主責事項，但在實務運作中，警察實際承擔的工作範圍遠超於此，除宣導外，尚須負責即時阻詐、案件偵辦、跨機關協調及被害人關懷等多重任務，使基層警力長期處於高負荷狀態。從警察角度來觀察，無論政策論述或社會期待，打詐成效過度依賴警察，忽略詐欺犯罪本質上涉及金融、電信、數位平台與司法等多元網絡，屬跨域合作議題。本研究認為，此種責任過度集中現象不僅造成分工失衡，亦使警察在資源有限下難以兼顧任務品質。

（二）跨機關合作雖多屬形式性安排，缺乏實質強制力

研究發現，從第一線警察人員觀點而言，跨機關合作在實務上常面臨權限不足、資訊掌握不對等、行政程序遲滯，以及機關本位運作與平台配合度有限等問題，致使合作機制多流於形式，難以形成具體且穩定的運作效能。整體來看，我國雖已建立跨部會合作機制，但合作成效多仰賴個別機關意願與第一線人員的關係網絡，缺乏合作的強制性。以中央防詐體系為例，刑事警察局，包括 165 專線在內，長期扮演關鍵樞紐角色，透過與金融、電信等機關進行系統介接，促成跨部會資料交流；然跨部會間的資料授權、系統整合與合作法制基礎，整體仍有待持續精進。

（三）金融與電信部門之合作機制相對成熟，惟仍受法制規範與誘因不足之限制

臺灣過去多將詐欺犯罪防制責任交由警察機關，然文獻顯示，各國多採跨機關合作策略以提升防制成效。我國近年亦朝此方向發展，將詐欺防制區分為五大

面向，警銀與警電合作已具一定穩定基礎，但跨行資料共享與源頭管控仍有不足處。受法源限制與商業誘因影響，金融機構跨行資料整合不足，致即時風險辨識與阻詐效能受限，難以形成完整預警體系。此外，電信業者多將防詐措施視為可議價服務，顯示其公共安全責任尚未制度化。整體而言，與金融與電信相關行政機關與業者的跨域合作仍有資料共享法源不足等問題。

（四）數位經濟產業與平台治理為當前防制體系最大缺口

研究顯示，警察人員認為目前詐欺犯罪防制跨機關合作的關鍵制度缺口，在於數位經濟產業端「源頭阻斷」法制設計尚未完備，尤其對網路平台、第三方支付及虛擬資產業者仍欠缺明確且具強制力之規範，未能清楚界定其事前風險控管義務、事後資料提供責任及相應裁罰機制，致使業者防詐投入程度不一。整體而言，防詐體系最顯著的結構性弱點即在於數位平台責任法制不足，平台對詐欺風險之事前管理義務不明確、監理工具有限，致使政府機關實際承擔大量原應由平台負責之風險管理成本，形成責任外部化現象。

（五）檢察官科技偵查素養對案件推進與偵辦成效具關鍵影響

在司法體系端的懲詐合作方面，由於檢察官為唯一偵查主體，資料分析顯示，其對科技偵查工具與數位證據分析的理解程度，實質影響案件推進速度與整體偵辦成效。隨詐欺犯罪日益科技化與跨境化，案件常涉及區塊鏈追蹤、虛擬貨幣金流分析及平台資料調閱等專業技術；若承辦檢察官對相關工具與技術缺乏基本認識，將直接影響搜索票核發、強制處分判斷與證據評價的即時性與精準度等，進而延宕偵辦進程。此外，詐欺犯罪多與洗錢金流相伴，但相關情資主要掌握於法務部調查局體系，與警察機關間的資訊共享仍未暢通，致使追查效率受限，易造成線索中斷或重複作業。

（六）地方政府所推動之創新防詐策略雖具成效，惟常缺乏制度化支撐

研究亦發現，地方警察機關透過科技應用與跨局處合作展現多項創新的詐欺防制策略，對即時阻詐具實質效果。然而，訪談資料亦顯示，此類創新多依賴地方首長支持、議會關注及特定人員的專業能力與關係網絡，缺乏穩定的制度化支撐。一方面，相關科技工具的建置與維運需仰賴地方經費與技術資源，其他縣市未必具備相同條件，導致出現區域差異；另一方面，中央尚未建立統一的作業流

程與法制授權，使地方創新成果難以系統性複製與擴散。整體而言，地方的詐欺防制策略創新雖能在短期內補足跨機關合作缺口、提升阻詐即時性，但若未納入中央層級的制度設計與資源配置，仍難以轉化為可長期運作的全國性防制措施。

二、研究建議

依據研究發現，本文提出以下制度建議：

（一）防詐策略應由事後執法導向轉向以被害人為中心之整合防制模式

詐欺犯罪因具組織化、數位化與跨境化等特質，若將防制策略與資源配置集中於事後追查與刑事處理階段，通常難以有效降低整體被害發生率及追回被害人損失。從國際經驗觀察，新加坡等國已逐步發展以「保護潛在被害人資產安全」為核心之制度設計，透過暫停帳戶、延遲匯款與風險預警機制，將防詐重心由事後執法轉向守護可能受害者。因此，本研究認為，未來防詐策略應由傳統執法導向，逐步轉型為以被害風險管理為核心的政策模式，透過法制化資料共享基礎、建構跨機關即時預警系統等措施，建構以被害人為中心的防制策略，方能從結構面有效降低詐欺犯罪之整體危害。

（二）跨機關合作應強化以「目標承諾（goal commitment）」為核心之制度設計

研究發現，我國防詐合作多停留於形式性協調，實際運作仍高度依賴個別機關意願與人際網絡，顯示跨機關合作尚未建立穩定之制度基礎。參考 Scott 與 Merton 的研究指出，即便跨機關交流仍存在成本，只要網絡成員對核心政策目標形成高度「目標承諾」（goal commitment），合作仍可持續並產生成效。本研究據此認為，或可透過建立跨機關共同績效指標及制度化責任分攤機制等方式，促進形成跨機關防詐之共同目標，作為行動之基礎。

（三）應重新定位警察於整體詐欺防制體系中的角色

警察機關在臺灣詐欺治理體系中扮演不可或缺的核心角色，然本研究深度訪談結果與文獻所得的結果類似，即詐欺犯罪的防制成效取決於跨部門與公私協力的完整程度，警察無法以單一機關之力解決跨境化、組織化與科技化的詐欺問題。若仍以警察機關為打詐的核心，僅能在犯罪鏈末端進行有限處理。研究顯示，當前防詐體系呈現警察責任過度集中之現象，影響警力負荷，唯有透過跨機關、公

私協力的網絡合作，並將刑事追訴定位為整體防詐策略之一環，而非唯一手段，方能有效提升整體詐欺防制效能。

（四）主管機關應加速建立平台責任法制與風險內部化機制

本研究認為，對於數位經濟產業管理，應盡快建立完整數位平台監理法制，明確界定相關事前風險管理義務、資料提供責任及裁罰機制，並導入具效果之罰則設計，使平台將防詐成本內部化，從結構上改變以收益為優先之商業邏輯。具體措施例如：明確法制化平台控管義務，包括廣告審查、異常行為監測與詐欺內容即時辨識機制；導入成本內部化監理工具，如全球營收比例罰鍰、保證金制度與過失連帶賠償責任等，另外主管機關的監理權限亦應加強，可建立數位平台專法或整體監理架構。

（五）應建構制度化之跨機關情資共享與整合體系

行政院已於 2023 年成立專責之打擊詐欺指揮中心，刑事警察局亦於 2025 年 11 月正式設置法制化之「詐欺犯罪防制中心」，其政策目標均在於透過組織正式化提升指揮層級與整體偵防量能。然而研究顯示，當前跨機關合作效能仍受限於資料共享法源不足、系統整合落差與行政程序遲滯，影響即時風險辨識與追查效率。因此，本研究認為，未來除應建置全國統一之防詐情資整合平台，促進金流、通訊與案件資訊即時共享外，亦須同步補強跨機關資料交換之法源依據，降低法律責任疑慮，使金融、電信與執法等機關得以進行風險資訊即時流通。

（六）強化檢察官偵辦詐欺案件之科技犯罪專業能力

本研究認為，未來除持續強化警察機關之科技偵查能力外，亦應同步提升檢察官對數位證據與科技工具之專業理解。隨著詐欺犯罪高度結合網路、電信與金流科技，應同步提升檢察官對相關技術的掌握。故建議透過在職訓練、專業課程及跨機關交流機制，強化檢察官對科技偵查工具、金流分析方法與新興詐欺手法之認識，以提升檢警合作之效率與默契。另研究亦發現，洗錢金流情資多集中於調查局體系，惟與警察機關之資訊共享仍有強化空間，致影響案件整合追查效能。建議進一步檢討並完善雙方情資共享制度，包括即時通報機制、權責分工與保密設計等，以加強跨體系合作並縮短偵辦時程。透過同步提升檢察官科技專業能力並強化警調情資整合，將有助於提升詐欺案件偵辦品質與效率。

參考文獻

一、中文部分

GASA (2024)。亞洲詐騙報告臺灣篇 2024。取自

https://www.gasa.org/_files/ugd/7bdaac_13f7eb8d194b4aa1a2f160e6d0517eaa.pdf (搜尋日期：2026/02/21)。

內政部警政署 (2023)。警政統計通報 (112 年第 50 週)。取自

<file:///C:/Users/PC/Downloads/11250+112%E5%B9%B41-10%E6%9C%88%E8%A9%90%E6%AC%BA%E6%A1%88%E4%BB%B6%E6%A6%82%E6%B3%81.pdf> (搜尋日期：2026/02/22)。

陳昱奉 (2023)。打擊網路詐欺之公私協力治理。《當代法律》, 20, 36-43。

嚴滋元 (2023)。詐欺犯罪現況與策略。《當代法律》, 20, 44-53。

二、英文部分

Amerhauser, K., & Thi, A. (2025). Compound Crime: Cyber Scam Operations in Southeast Asia. Global Initiative Against Transnational Organized Crime.

Retrieved from

<https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf> [Accessed 21/Feb/ 2026]

Anderson, M., March, E., & van Burken, C. B. (2024). Exploring the Roles Played by Trust and Technology in the Online Investment Fraud Victimization Process. *Journal of Criminology*, 57(4), 488–514.

Bianchi, C., Nasi, G., & Rivenbark, W. C. (2021). Implementing Collaborative Governance: Models, Experiences, and Challenges. *Public Management Review*, 23(11), 1581–1589.

Eurojust & Europol (2025). Common Challenges in Cybercrime 2024. Eurojust and European Union Agency. Retrieved from

https://www.europol.europa.eu/cms/sites/default/files/documents/Common_Challenges_in_Cybercrime_2024.pdf [Accessed 21/Feb/ 2026]

- Fox-Mills, L. (2025). Best Practices for Fraud Prevention Whitepaper. Moody's Analytics. Retrieved from <https://www.moody's.com/web/en/us/site-assets/ma-kyc-best-practices-for-fraud-prevention-whitepaper.pdf/> [Accessed 21/Feb/ 2026]
- Henry, L. A. (2024). Navigating Disruptive Times: How Cross-Sector Partnerships in a Development Context Built Resilience During the COVID-19 Pandemic Outbreak. *Business & Society*, 63(4), 745–773.
- Home Office UK (2025). Experiences of Victims of Fraud and Cyber Crime. Retrieved from <https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-d-cyber-crime/experiences-of-victims-of-fraud-and-cyber-crime> [Accessed 21/Feb/ 2026]
- INTERPOL (2021). National Cybercrime Strategy Guidebook. Retrieved from <https://www.interpol.int/> [Accessed 21/Feb/ 2026]
- Kemp, S., Miró-Llinares, F. & Moneva, A. (2020). A. The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research* ,26, 293–312.
- Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws*, 13(4), 44. Retrieved from <https://doi.org/10.3390/laws13040044/>[Accessed 21/Feb/ 2026]
- Koning, L., Junger, M., & Veldkamp, B. (2025). Reporting Fraud Victimization to the Police: Factors That Affect Whether Victims Report. *Psychology, Crime & Law*, 1–29. Retrieved from <https://doi.org/10.1080/1068316X.2025.2468347> [Accessed 21/Feb/ 2026]
- Lee, S., & Kim, M. (2024). Public Perceptions of Cross-Sector Collaboration and Sector Bias: Evidence from a Survey Experiment. *Public Management Review*, 26(8), 2429–2451.
- Leukfeldt, E. R. (2017). *Research Agenda: The Human Factor in Cybercrime and Cybersecurity*. Eleven International Publishing. Retrieved from https://securitydelta.nl/media/com_hsd/report/141/document/Research-Agenda-The-Human-Factor-in-Cybercrime-and-Cybersecurity.pdf [Accessed 21/Feb/

- 2026]
- Nogala, D., Talmar, A., Pūraitē, A., Mészáros, B., Kokkinos, M., Fernandes, R., & Huikuri, S. (2022). *European Law Enforcement Research Bulletin: Special Conference Edition No. 5*. European Agency for Law Enforcement Training.
- Scott, R. J., & Merton, E. R. K. (2021). When the Going Gets Tough, the Goal-Committed Get Going: Overcoming the Transaction Costs of Interagency Collaborative Governance. *Public Management Review*, 23(11), 1638–1660.
- Singapore Police Force (SPF). (2025). *Mid-Year Scam and Cybercrime Brief 2025* [Press release]. Retrieved from <https://www.police.gov.sg/> [Accessed 21/Feb/ 2026]
- Takefuji, Y. (2023). Case Report on Enormous Economic Losses Caused by Fraud from Japan to the World. *Journal of Economic Criminology*, 1, 100003. Retrieved from <https://doi.org/10.1016/j.jeconc.2023.100003> [Accessed 21/Feb/ 2026]
- United Nations Development Programme (2025). *Anti-Scam Handbook v2.0: Collective Response and Tools to Safeguard Development*. UNDP Policy Centre. Retrieved from https://www.undp.org/sites/g/files/zskgke326/files/2025-05/undp_anti-scam_handbook_v2.0.pdf/ [Accessed 21/Feb/ 2026]
- United Nations Office on Drugs and Crime (2025). *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*. UNODC. Retrieved from https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf/ [Accessed 21/Feb/ 2026]
- van de Weije, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of Reporting Cybercrime: A Comparison Between Identity Theft, Consumer Fraud, and Hacking. *European Journal of Criminology*, 16(4), 486–508.
- Waardenburg, M., Groenleer, M., de Jong, J., & Keijser, B. (2020). Paradoxes of Collaborative Governance: Investigating the Real-Life Dynamics of Multi-Agency Collaborations Using a Quasi-Experimental Action-Research Approach. *Public Management Review*, 22(3), 386–407.
- World Economic Forum (2020). *Shaping the Future of Cybersecurity and Digital Trust:*

Partnership Against Cybercrime. World Economic Forum. Retrieved from <https://initiatives.weforum.org/partnership-against-cybercrime/home/> [Accessed 21/Feb/ 2026]

附錄-研究工具

一、第一階段訪談題綱

- (一) 您在辦理詐欺案件時，最常與哪些單位合作？(如檢察官、法院、金融機構、通訊業者等)？跨機關間是否有情資分享機制？您認為警察機關在偵辦層出不窮的詐欺案件，最大的困難在哪裡？
- (二) 就您觀察，防詐工作目前是否有形成合作網絡？如有，合作模式大致為何？您認為目前防詐工作最欠缺何機關或團體的投入？為什麼？
- (三) 您認為應如何加強與其他單位（如金融機構、電信業者、網路平台、地檢署、社政機構等）的合作以提升整體打詐效能？目前運作存在哪些問題？您認為可以如何調整？
- (四) 就您觀察，現行法律是否足夠支持跨機關的合作與資料調閱？您覺得提升司法網絡合作防制詐欺的關鍵會是什麼？如果未來要修法，您認為最需要補強的是哪一塊？
- (五) 就您看法，現行打詐政策最需要改善的部分為何？
- (六) 您的職稱、警察機關服務年資？

二、第二階段訪談題綱

- (一) 您認為目前臺灣詐欺防制網絡(165、刑事局、銀行業者、社群平台、電信業者)中「制度性缺口」有哪些？在跨部會合作或整體反詐策略上，您認為有哪些國家的模式值得我國參考或借鏡？
- (二) 如果臺灣要比照英國 NFIB 或新加坡 ASC 建立『國家級詐欺防制中心』，在您看來，現行法制與機關任務分配最需要做哪些調整？您認為臺灣在組織架構上應採取何種模式，才能有效整合金融、警政、電信與社群平台的防詐功能？
- (三) 現行《詐欺犯罪危害防制條例》或其他法規，是否足夠支持跨部會資料調閱與合作？如果未來要修法，您認為哪一部份最需補強？
- (四) 就您的觀察，目前社群平台詐欺(FB/Google/YouTube/LINE)處理的瓶頸是什麼？您認為社群平台是否有做好相關的風險分析及管理？應如何改善？基於國內外經驗(如英國 Online Safety Act、新加坡 IMDA)，您認為臺灣下一

階段應如何更具體規範平台義務？

- (五) 就警方的偵查與阻詐需求而言，您認為現行金管會的防詐措施哪些有產生正向效果？哪些仍不足？
- (六) 您如何看待目前警察在詐欺防制中的角色？哪些工作原本不應由警察負責，現在卻由警察承擔？
- (七) 您的職稱、警察機關服務年資？

