未來進行式－AI 金融詐騙

林書立*

摘　要

AI CYBER 世代是最充滿智慧的時代也是最愚蠢的時代，是信仰 AI 的時代也是懷疑 AI 的時代，是 AI 的光明季節也是 AI 的黑暗季節，更是希望的 AI 春天與絕望的 AI 冬天，AI 的正義與 AI 的犯罪都在奔向天堂的道路上，但也都在跌入地獄的深淵中，AI 的好壞在於誰能先一步使用。

科技工業的發展大量增加了人類的物質富裕，但也造成傳統社會秩序徹底的分裂，並帶來新的社會問題，個人與群體的社會疏離、城市的擁擠與冷漠、網路與 AI 的社交工程，使得真假越來越難辨識，Cyber Crime 成為犯罪活動猖獗的主因，透過電信與網路，犯罪集團利用人類的渴望，營造被害情緒價值的培養，使得網路詐騙成為詐騙快速蔓延的溫床。我們不能被騙不「貪」就是「笨」，否則，一旦認為自己不貪也不笨，就容易掉入詐騙的陷阱，現代的電信網路詐欺是「歹徒精心設計的劇本」，只有你想不到，沒有詐騙做不到，如果你還沒被騙，那是因為還沒遇到適合你的詐騙劇本，我們必須面對「只要疏於防護，就有可能犯錯」。

許多金融詐騙的情節都匪夷所思，雖然我們苦口婆心勸阻被騙的民眾，但被騙的民眾早已被犯罪集團洗腦，預告銀行行員會勸阻被害人，所以取款時，要先編好藉口，欺騙銀行員與警方，必要時就大鬧銀行櫃檯，因為詐欺集團早已編織未來的憧憬，取款成功後，脫離下流老人，共創人生，享受美好生活，因此攔阻的人，就是敲碎被害人美夢的「惡魔」，更是被害者最不願面對的事實。

眼見被害人的天使就在門外或網路等他，距離美好未來只剩最後的一哩路，敲醒他人美夢，白挨罵是當然的事，但是攔阻被害人的最後一道防線，必須受得住嚴重的炮火攻擊，因為我們攔阻擋下的不是一個人，而是一個家庭甚至是整個社會的將來與福祉。

* 銘傳大學犯罪防治學系助理教授

僅以本文獻給持續戮力敲醒被害人的防詐夥伴。遭到不清醒客戶謾罵不是恥辱，而是行善積德的承擔與奉獻，我們仍須保持「自反而不縮，雖千萬人吾往矣」的精神。

關鍵字：金融詐欺、科技犯罪、AI 犯罪防治運用、詐騙被害心理、社交工程詐騙、跨國金融犯罪

JEL **分類代號**：D18, K42

壹、前言

一、科技始終來自人性

「科技始終來自人性」是 1999 年知名電信公司家喻戶曉的名言，強調技術發展應以滿足人類生活、情感需求與便利為核心，而非單純追求技術指標，成為深植人心的經典科技人文詮釋，然而科技始終沒有人性，資通科技從電信走向網路後，高度的匿名性成為犯罪份子運用資通科技(ICT)進行一系列跨國科技犯罪的濫觴，聯合國毒品與犯罪署更於 2025 年在一篇有關全球犯罪趨勢的關鍵報告「Inflection Point(轉折點)」[1]中，具體指出以跨國電信網路詐欺為主的金融犯罪，已經來到死亡交叉，取代過去組織犯罪以跨國毒品犯罪為骨幹，成為當前跨國組織犯罪集團的新世代趨勢，金融詐欺科技犯罪不但成為全球組織犯罪的主流，東南亞的詐騙中心、地下金融和非法網路市場對全球產生巨大的影響，因為科技犯罪與地下金融已成為犯罪份子的幫兇，這份關鍵的全球犯罪趨勢報告等同宣告「科技始終沒有人性」。

二、形影不離是手機，無法消滅是詐欺

回顧 Covid-19 新冠疫情徹底改變了我們的世界，特別是原本就已經快速發展的物聯網時代，受到強制隔離的影響，讓越來越多人被迫放棄馬路走向網路，不管你懂不懂通訊科技，知不知道社群媒體，會不會用數位帳戶，現實生活的強制隔離措施，逼得每個人都得上網擷取資訊、上網聯繫溝通，甚至上網購物、上網交易，上網交友，不管你是嬰兒潮世代、X、Y、Z 世代，一直到數位原生的 α 世代，都一起加入到網路生活的新時代，於是原本還在工業 4.0 的物聯網時代，受到加速刺激蓬勃發展，從此「形影不離是手機，無法消滅是詐欺」不使用網路幾乎無法當現代人。

三、拼一次富三代的邪惡科技帝國

強制隔離不僅加速資通科技的發展，同時更加速了詐騙產業鏈的發展。原本就已透過 VoIP（Voice over Internet Protocol）的語音傳輸通話技術進行的詐騙，進化到以跨國電信網路為詐欺犯罪的 Cybercrime，隨著疫情的隔離，有更多不懂網路可以轉化電信顯示號碼的人，因為相信了電信網路的隱匿與偽冒而受到詐騙，大量而快速移轉的金額透

[1] Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia/April2025, United Nations Office on Drugs and Crime (UNODC).

過跨國網路與虛擬資產的移轉，資金安全地滑進詐欺集團的手中。而隨著不懂網路匿名的犯罪者，容易遭到警方的逮捕，經過移送與寬鬆的告誡及裁罰後，也更進一步的學習網路匿名技術、購置境外假帳號、假網頁、假粉絲團與人頭門號、人頭帳戶與虛擬貨幣，學不來的，就用外包，新的詐騙犯罪開始招募專案工程師、社群小編、網路演算廣告、個人幣商，建立跨國機房、跨國水房、跨國假廣告投放，至於快速累積的大量犯罪所得，透過跨國洗錢中心，發展出數位貨幣的保證到款、保證安全，於是又回到必須招募更多人來犯罪，祭出保證致富、保證安心、拼一次，富三代的邪惡科技帝國，不斷快速累積的大量財富，使得詐欺的邪惡帝國採購了最新的軟、硬體設備，在科技犯罪的支撐下，網路科技金融犯罪成為獲利最快、風險最低、成本效益最高的金融犯罪。

四、犯罪學的噩夢「低成本、低風險、高報酬」

當資通科技（ICT）正以 AI 技術為核心，藉由更快速的 6G、物聯網（IoT）與半導體來推動智慧化與跨產業整合的同時，基於 AI 自動化的資安信賴體系，如果無法被有效發展建置，那麼缺乏實名制的犯罪技術升級，金融詐欺犯罪將面臨源於古典犯罪學理論的理性選擇理論(Rational Choice Theory, RCT)最不利的防制犯罪的情境–「低成本、低風險、高報酬」。

理性選擇理論由 Cornish 和 Clarke 於 1986 年提出，他們沿用 Becker 的「主觀期望利益理論」來探討犯罪議題，理論是基於經濟理論中的「預期效用」原則，預期效用原則是指人們將根據他們期望選擇最大化的利益或效果，並用最低的成本或最少的損失的程度做出理性決策，犯罪者在行為前大部分會有或多或少的規劃與準備，即便是短暫準備也算，此過程可稱之為「有限之理性」（許春金，2007）。理性選擇理論核心假設為：犯罪人具備自由意志，會透過衡量犯罪的利益與成本（風險）來決定是否採取行動，在預備犯罪者「有限理性」與「自利」及犯罪經濟學的「低成本」考量下，當前的金融詐欺犯罪刑事司法戰局成為「不易抓、難起訴、高再犯」，反而吸引更多猶豫的族群，評估後選擇投入金融詐欺。

除了依據理性選擇理論，犯罪預防將處於不利地位外，如依據我國犯罪學家黃富源教授，引入的「明恥整合理論」（Theory of Reintegrative Shaming）[2]進行分析，當前詐

[2] 澳洲犯罪學家 J. Braithwaite 提出明恥整合理論整合了標籤理論、犯罪副文化理論、控制理論、機會理論、學習理論等諸理論中互補而共存的部份。以控制理論來探討初級偏差行為的產生，以標籤理論來了解二級偏差行為何以形成，並以犯罪副文化理論說明二級偏差行為為何可持續，再以其他理論加以補充說明。參閱 Braithwaite, J. (1989), Crime, Shame and Reintegration. New York: Cambridge University Press；以及，黃

欺科技犯罪這種充分利用資通與 AI 科技特性，讓犯罪者可以透過科技躲在第三國的鍵盤後面進行犯罪，犯罪者不但看不到被害人的痛苦，不易被抓也不易被判有罪，更不易感覺到犯罪的羞恥感，在缺乏「羞恥」（shame）以及「復歸」（reintegration）的概念下，犯罪者不易停止犯罪，反而在集團以及收益的鼓舞下，越來越投入這一類的犯罪，最終越來越多人加入，技術越來越升級，產業規模越來越大，成為橫掃世界的金融詐騙帝國。

回應金融詐欺犯罪的議題，雖然犯罪被害人關心的是被騙的錢能不能拿回來？但是基於國家政策甚至是刑事政策的立場而言，更重要的是如何控制詐欺犯罪？如何降低巨量詐欺犯罪幾乎癱瘓刑事司法的傷害？如何讓詐欺不要一再犯罪？如何用科技與法律壓制詐欺？如何擬定整體 AI 發展策略與制定 AI 犯罪預防的刑事政策？恐怕才是更值得關注與探討的議題。

貳、罪與罰的跨國難題

一、這是最好的時代，同時也是最壞的時代

英國作家狄更斯在 1859 年出版的《雙城記》（A Tale of Two Cities）描述：「這是最好的時代，同時也是最壞的時代」，成為經典諺語，雖然這是一部以法國大革命為背景所寫成的小說，事實上也反映出工業革命對於社會治安的整體影響。工業革命通常會大量增加了人類的物質富裕，但也造成傳統社會秩序徹底的分裂，並帶來了新的社會問題，如污染、個人與其群體社會的疏離、城市內的擁擠、和童工的出現。這是犯罪活動猖獗的一個重要原因，也正因如此，工業化時期的英國意識到英國在工業化的進程中，犯罪活動猖獗，犯罪率持續上升，侵犯財產犯罪成為犯罪的主要類型，青少年犯罪不斷增長並呈低齡化趨勢。貧困、糟糕的城市環境，傳統管理制度失效，缺乏有效的警察制度來抑制和打擊犯罪，於是 1829 年，時任英國內政部長的皮爾爵士（Sir Peel）在倫敦蘇格蘭場（Scotland Yard）創立現代化的警察，取代原本混亂的志願式治安體系。

富源（1992），明恥整合理論－一個整合、共通犯罪學理論的介紹與評估，警學叢刊第二十三卷二期，頁 93-102。

二、《犯罪不值得》（Crime Does Not Pay）

工業革命讓過去農村生活的英國開始城鎮化，但工業革命對社會帶來改變的同時，不僅使得當時社會風氣改變，也為犯罪帶來了巨幅的改變，大量犯罪增加，英國經濟和社會迅速而廣泛的轉型反映在刑法、犯罪行為以及兩者之間錯綜複雜的關係中，[3]於是1860 年英國維多利亞時代起，英國開始有了「Crime Does not Pay」的諺語，意為「犯罪(代價)不值得」，勸阻人們不要去犯罪。自 1885 年犯罪學三聖之一的拉斐爾(Raffaele Garofalo)[4]創造了「犯罪學」以來，各國不斷研究各種犯罪的成因，期待增加定罪的刑罰可以減少犯罪的發生，此一時期罪與罰成為犯罪學追求的研究重心，但諾貝爾經濟學獎得主加里・貝克爾(Gary Becker)[5]卻在 1968 年的《罪與罰：經濟分析途徑》文中提出，犯罪經濟學模型或許能提供金融詐欺犯罪更清晰解釋，亦即犯罪者是理性選擇者，在合法與非法活動之間計算成本與收益。當守法成本遠高於違法預期效益(被逮概率乘以刑罰懲罰度)時，只要利潤空間夠大，犯罪的冒險便不會斷絕。因此，一個人會成為罪犯不是因為他本來就是罪犯，而是因為這個人有著和其他人一樣會有的選擇權，而在他的情景選擇中，犯罪的預期收穫高於可能受到的定罪與懲罰。

Crime Does not Pay 這句諺語也在 1920 年代以後開始在美國流行，1942 年更推出《犯罪不值得》（Crime Does Not Pay）從真實案例改編的系列漫畫，[6]專門描述目無法紀和無法無天的重大犯罪事件。有許多觀點指出流行的原因與當時美國黑幫活動盛行難以控制犯罪有關，使得媒體開始大幅報導犯罪被捕的新聞。

---

[3] Crime and Justice in Eighteenth- and Nineteenth-Century England/ Douglas Hay/Crime and Justice , The University of Chicago Press 1980, Vol. 2 (1980), pp. 45-84

[4] 拉斐爾・加羅法洛（Raffaele Garofalo，1851 年-1934 年）是 19 世紀末義大利著名的犯罪學家，與隆布羅索（Cesare Lombroso）和費里（Enrico Ferri）並列為義大利實證主義犯罪學派（刑事人類學派）的代表人物。被稱為犯罪學三聖。他提出「自然犯罪」概念，主張犯罪是違背人類同情心（pity）和誠實心（probity）本性的行為，並強調心理缺陷對犯罪行為的影響。

[5] 加里・貝克爾在所著《犯罪與懲罰經濟分析法》（crime and punishment: an economic approach）研究中，把誘因經濟模型用於分析預防犯罪方面，同時提出犯罪行為合乎理性並對誘因作出反應的論點。他更主張恢復死刑，並挑戰種種假設”非理性”行為的犯罪理論，在法律及經濟學研究方面另辟蹊徑。

[6] Mitchell, Kurt; Thomas, Roy (2019). American Comic Book Chronicles: 1940-1944. TwoMorrows Publishing. p. 170.

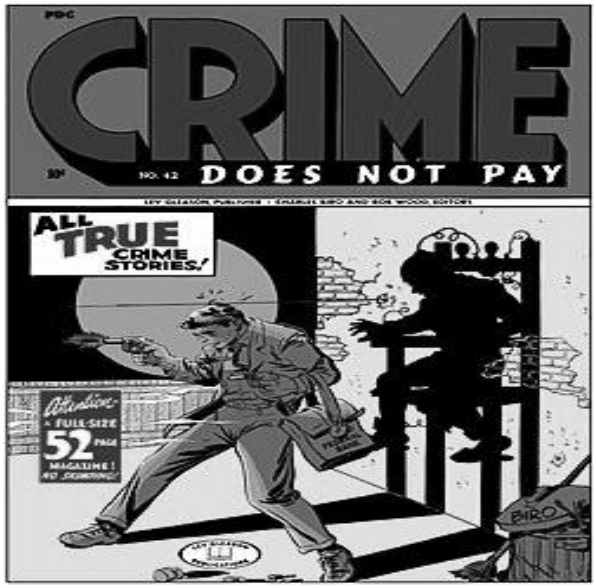


圖 1　《犯罪不值得》（Crime Does Not Pay）成為英國諺語，1942 年更成為美國第一部依據「真實犯罪」改編的系列式漫畫。

資料來源：《犯罪不值得》第 42 期（1945 年）封面，Uploaded：5 October 2021
https://www.comics.org/issue/234818/cover/4/

「犯罪不值得」(亦有翻譯為犯罪不償命)成為英、美流行諺語，是因為它強化了社會規範、正義和道德秩序，常常起到警示作用，告誡人們非法活動最後會帶來高風險，強調犯罪不可避免會垮台，最後得不償失，成功引起大眾與媒體關注當時難以控制的犯罪問題，在媒體開始大幅報導的效應下，當時受到矚目的犯罪最後大都呈現「付出犯罪代價」的結果。

事實上犯罪行為就算不會傷害自己，也一定會傷害他人，當前跨國電信詐欺犯罪看似不易被抓，不易被判重刑，但是這種跨國犯罪，付出的代價，不是只有用罪與罰來看待，因為這樣的犯罪已經成為高度分工的組織犯罪，一旦涉入，就算沒有被各國刑法懲罰，但後續想要脫離這些犯罪份子，幾乎就是難以醒來的噩夢，因為組織性犯罪，本質就是利用暴力來達到目的，要理解這種行為將付出慘痛代價，通常難以最基本的罪刑法定主義或同理心與道德感衡量。通常唯有親身經歷過這樣的組織犯罪，體驗加入容易，脫離困難的人，才能深切體會罪犯的邪惡本質，然而，此時多數為時已晚。

三、罪與罰的跨國難題

俄國犯罪心理學名著《罪與罰》描寫一名來自聖彼得堡的貧困大學生，為了生計殺死一個不道德的典當商，他說服自己，如果犯罪是為了消除障礙成為「不平凡」的人，那就是他的正義。然而，後來他深受困惑、偏執和厭惡的折磨。不斷在心中與內疚和恐懼鬥爭，面對自己的內在和因果，罪惡感使他不堪重負，以至於身心患病。最後他開始懺悔，決定接受法律制裁，不再疏遠社會。因為一切辯護都騙不了自己。

但如今，我們面對的是更複雜的跨國網路詐欺，在新興的 AI Cyber Crime 背景下，高度運用科技，不但看不到被害人，還將犯罪行為跳脫到第三國，不在居住地犯罪，而是透過電腦資通科技，甚至是 AI 智慧科技來幫助一系列犯罪，使得跨國虛擬犯罪難以向上追查，這種 AI 的金融犯罪，無論是詐欺、洗錢，不斷編纂美麗的藉口，把每個犯罪成員的罪責劃分，「我只負責領錢」、「我只負責寫劇本」、「我只負責開發程式」、「我只負責找據點」、「我只負責提供材料」、「我只負責找人頭」、「我只負責把風」、「我只負責投放廣告」，不但淡化每個人的罪責，也淡化每個人的罪惡感，每個人都看不到被害人的慘劇，每個人都聽不到被害人的哭喊，跨國網路詐欺與洗錢被描繪成「不偷不搶上班族」，沒有罪惡感、很酷、很刺激、很賺錢，已經有數百萬人在從事的活動，因為確實有利可圖，只要不被抓，犯罪幾乎遠比誠實勞動賺得多。

四、犯罪就是一場賭局，籌碼不是刑期高低，而是定罪的機率

如果想依循過去犯罪學的「罪與罰」讓罪與罰相當，似乎難以嚇阻，因為網路技術讓跨國詐欺的執法合作困難，犯罪者來自 A 國，犯罪地在 B 國，而被害人卻在 C 國，首謀卻在 S 國的遊艇度假，因此不斷提高首謀的最高徒刑，根本無法嚇阻，因為追蹤斷鏈、證據斷鏈、被害斷鏈，單純依靠道德與教條或嚴厲修法來勸誡人們遠離詐欺犯罪越來越無效，因為想要犯罪的人，一旦發現教條的另一面是不易被抓，不會重判，這種勸誡的效果就會立刻瓦解，產生教條效應（Dogmatism），換句話說修法增加犯罪最高處罰的刑罰，不一定能有效嚇阻犯罪，想要犯罪的人，計算的犯罪成本，不是只有司法天秤兩邊的罪與罰，真正更令犯罪者受到威懾的是，可能會受到定罪的概率，而不是懲罰刑度本身，換句話說，罪犯本身就是風險的博弈賭徒，犯罪成本的衡量標準不是刑罰的高低，而是被抓捕的風險機率，以及進入刑事司法大漏斗後，實際遭到懲罰的犯罪風險分析。

換句話說，罪犯本身就是風險的博弈賭徒，犯罪成本的衡量標準不是依據守法人「罪與罰」的思考模式，而是先考量被抓到的機率，其次才考量定罪懲罰的風險機率，因此

犯罪率不是取決於警方的效率和打擊犯罪的付出成本，而是取決於犯罪者判斷實施犯罪的風險分析。

五、AI 的正義與犯罪都一起在奔向天堂的道路上，也都在墜入地獄的深淵中

當前我們面對 AI CYBER 世代，是最充滿智慧的時代也是最愚蠢的時代，這是信仰 AI 的時代也是懷疑 AI 的時代，那是 AI 的光明季節或 AI 的黑暗季節，那是希望的 AI 春天還是絕望的 AI 冬天，AI 的正義與 AI 的犯罪都在奔向天堂的道路上，也都在跌入地獄的深淵中，AI 的好壞在於誰能先一步使用。

參、全球科技犯罪時代

一、網路詐騙傳播像病毒，入侵金融像癌症

財經主流雜誌富比士（Forbes）2022 年 5 月以新英文字「Scamdemic」一詞來形容詐騙不斷變種與擴散的現象，具體描述了詐欺災情嚴重程度已達到重大瘟疫般的地步。詐騙手法一直圍繞著人們的「慾望」、「恐懼」與「急迫」，使得網路詐騙像傳染病毒一樣不斷變化，不斷編造一個又一個故事，經由跨國網路與最新 AI 科技來騙取人們財產，因為科技的網路詐騙有如流刺網，橫掃網路上的大小金額，從 QR-CODE 騙取幾百元到殺豬盤騙取上億元，大小通吃，各有專長各有領域，錢來得廣、來得多、來得快，可以迅速投入最新設備，運用最新的軟硬體，精緻化原本詐騙腳本。聯合國毒品與犯罪署（UNODC）更於 2025 年 4 月 21 日發布的專文「Cyberfraud in the Mekong reaches inflection point」(湄公河地區網路詐騙活動已達轉折點)指出，網路詐騙規模已擴大至全球，「網路詐騙就像癌症一樣，永遠不會消失」。[7]雖然各國當局在自己領域內努力防治，但詐騙不斷轉移，猶如癌症一般，UNODC 呼籲各國要攜手合作，才能有效打擊跨國網路詐欺犯罪。

[7] https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html

圖 2　聯合國毒品與犯罪署（UNODC）2025 年 4 月 21 日專題報告指出，隨著亞洲各國打擊力度加大，犯罪集團正將詐騙深入最偏遠、最脆弱、最無防範意識的區域。

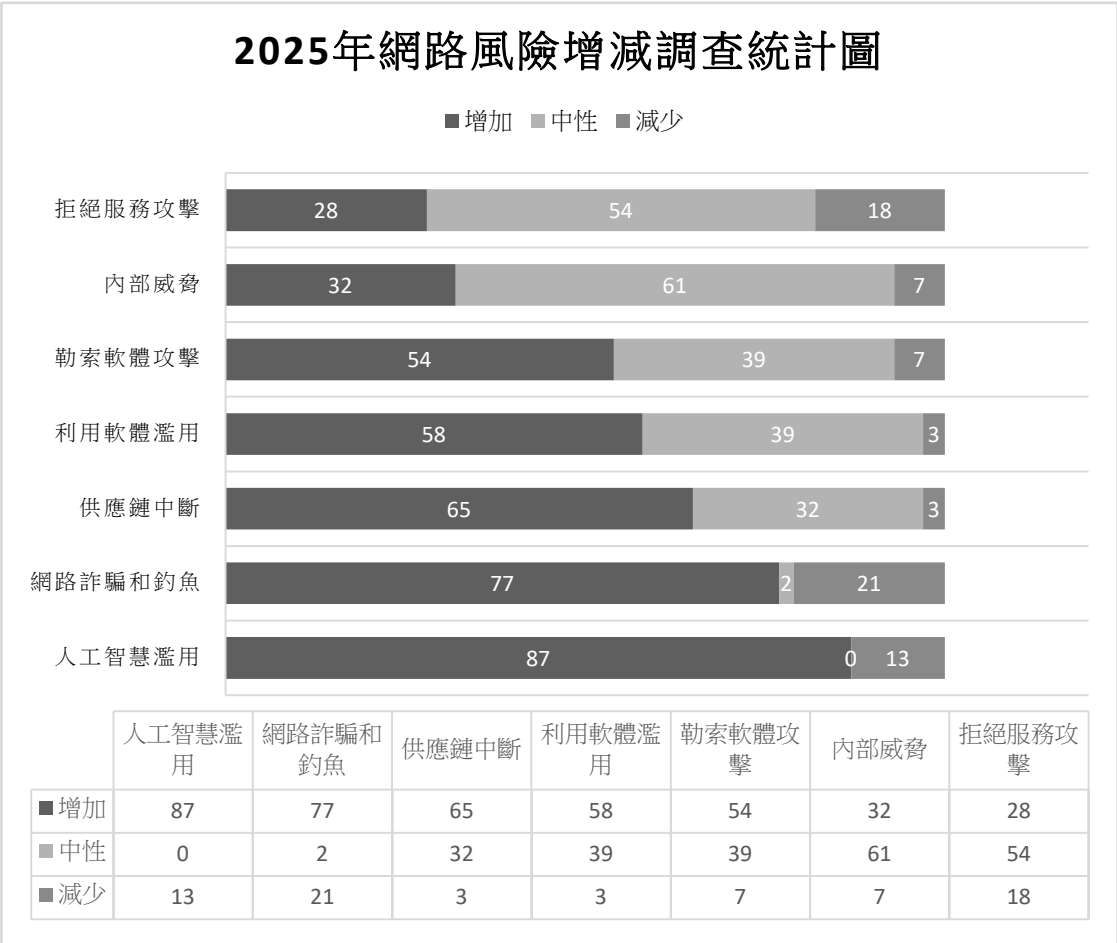
資料來源：聯合國毒品與犯罪署（UNODC）

二、跨國網路詐騙成為灰色產業鏈

事實上，網路詐欺近年快速崛起，全球每年因詐騙產業產生上兆美金，[8]詐騙的機房從原本在台灣與中國大陸，轉戰到東南亞，甚至遠赴非洲、東歐、南美、亞西，最後竟然落腳中南半島經濟特區（SEZ），特別是在柬埔寨、寮國、緬甸和菲律賓。

世界經濟論壇 2026 年 1 月 12 日發布的全球網路安全展望（Global Cybersecurity Outlook）指出，人工智慧正在加劇全球網路詐騙危機，詐騙集團正在利用人工智慧推動快速、個人化的內容創作，使網路詐欺以前所未有的效率擴大詐騙規模，並將詐騙劇本與手段個人化，而當前的網路防禦措施已無法跟上網路攻擊速度和複雜性的快速成長。

[8]https://aqj.org.tw/emerging-fraud-trends-and-supply-chain/



	人工智慧濫用	網路詐騙和釣魚	供應鏈中斷	利用軟體濫用	勒索軟體攻擊	內部威脅	拒絕服務攻擊
增加	87	77	65	58	54	32	28
中性	0	2	32	39	39	61	54
減少	13	21	3	3	7	7	18

圖 3　世界經濟論壇 2026 年發布全球網路安全展望，指出人工智慧正在加劇全球網路詐騙危機。

資料來源：改編自世界經濟論壇 Global Cybersecurity Outlook

三、全球金融犯罪報告紛紛示警 AI 滲透

類似的報導還有總部位於加拿大的反詐騙和反洗錢軟體公司，納斯達克維拉芬（Nasdaq Verafin）發布的 2026 年全球金融犯罪報告，[9]同樣指出 2023 年以來，非法金融活動激增 1.3 兆美元，過去兩年金融犯罪的範圍、規模和演變方式的不斷擴大，從根本上威脅著金融體系的完整性，並助長了人口販運和恐怖主義等破壞穩定的重大犯罪活

[9] https://verafin.com/nasdaq-verafin-global-financial-crime-report/

動。而詐騙損失急劇上升的原因是犯罪網路廣泛使用人工智慧，他們利用科技進步來攻擊金融體系的漏洞，這種新型威脅迅速滲透市場。

詐騙不僅僅依靠這些科技軟硬體的發展，還加上地緣政治、供應鏈、法規、AI 與資安技術缺口的交互影響，使得網路詐欺威脅態勢日益複雜，因此，儘管各國打擊行動擾亂了現有犯罪活動，但這些窩點卻不斷在專為網路犯罪活動設立的園區（SEZ）死灰復燃。詐騙利用各國治理漏洞，扭曲和腐蝕政策制定過程，貪腐的過程甚至危害國家主權，這些園區具備永續發展和擴張所需的一切條件，導致詐欺產業變成一個相互關聯永續發展的生態系統，犯罪網絡在治理最薄弱的地區拓展，吸引更多新的參與者，推動了國家等級的腐敗，使非法產業得以繼續擴大規模和鞏固，最終形成了成千上百個工業等級規模的詐騙中心。

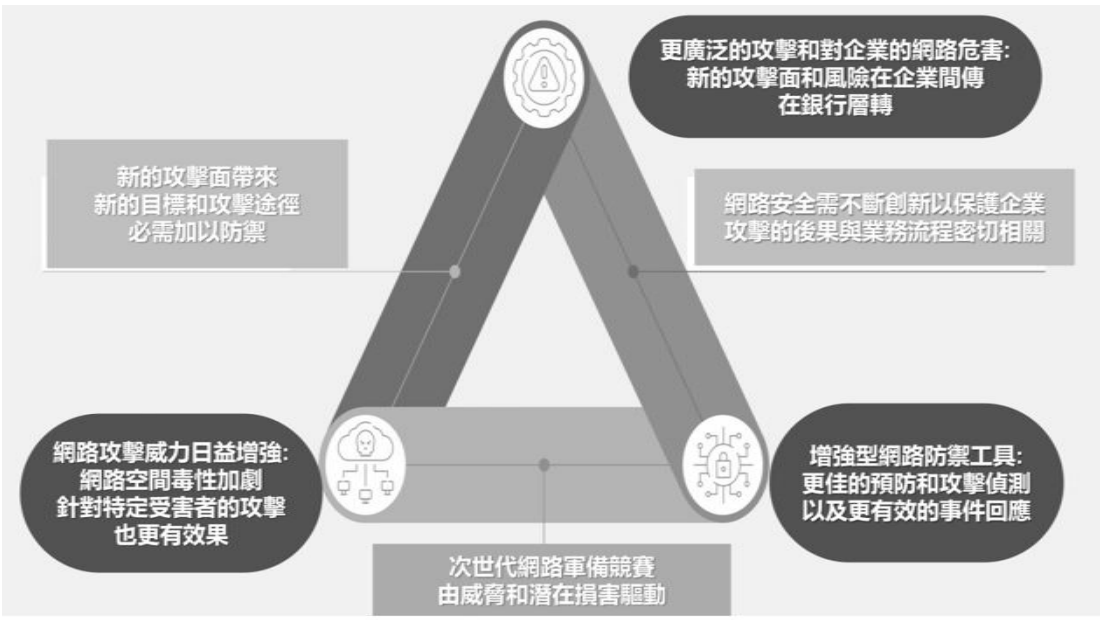


圖 4　人工智慧對網路安全的影響

資料來源：轉譯自世界經濟論壇 Global Cybersecurity Outlook

四、INTERPOL 警告 AI 增強詐騙利潤 4.5 倍

國際刑警組織（INTERPOL）也指出，人工智慧增強型詐騙的利潤是傳統方法的 4.5 倍，人工智慧系統能夠自主規劃和執行完整的詐騙活動－從偵察到勒索贖金。

網路詐騙犯罪除了得力於網路科技的 AI 演算法、社群媒體的匿名性外，更重要的還有新世代金脈－加密貨幣和地下金融洗錢。網路詐騙集團累積了巨額所得，並滲透到全

球銀行系統中，在全球市場中成為洗錢和地下金融的領導者，其影響波及全球。由於發展迅速，資金充沛，網路犯罪從基礎設施、園區保護監管到利益保障一應俱全，但卻缺乏「員工」，於是招募許多不知情或一知半解的人口，限制行動強迫進行詐騙，發展成新型態的人口販運，產業高度組織化，已成為全球性問題。[10]

2026 年國際刑警組織《全球金融詐騙威脅評估》警告稱，隨著全球犯罪合作日益密切，詐騙不再是邊緣的威脅，而是多種犯罪活動的核心，與組織犯罪、人口販運和網路犯罪相互交織。

曾經僅限於特定區域的詐騙中心，如今已遍布全球，涉及數十萬人，其中許多人是人口販運的受害者，被迫從事網路詐騙活動。自 2024 年以來，與詐騙相關的國際刑警組織通緝令和通報數量增加了 54%。同期，國際刑警組織協助成員國處理了 1,500 多起跨國詐騙案件，追回的資產損失高達 11 億美元。

我們必須正視金融犯罪的詐欺，不僅僅只是非暴力的金錢犯罪，這已涉及人們的畢生積蓄、尊嚴，最壞的情況下更有可能涉及生命。

圖 5　BEC 商業犯罪的三瓶毒藥

資料來源：國際刑警組織（INTERPOL）

[10] https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

肆、詐騙心理操縱

當前的詐騙機房，已經遍布全世界，這些詐騙機房，外文稱之為鍋爐室（Boiler room）指的是一種利用電話或電郵等手段，向他人極力推銷有問題產品的詐騙手法，一方面由於這些騙局最初都是在國外租用低廉、空氣悶熱的地方進行，也因為施詐的集團，見被害人上鉤後，通常以各種壓力對被害人強迫施壓，因此被名為「鍋爐室騙局」。

騙徒透過頻繁且密集的不同人設，聯繫被害人進行冷推銷（cold calling），[11]自稱是投資顧問，以誤導性的言語游說該人投資高風險公司的股份。上釣的受害人把錢存入騙徒指定的銀行帳戶後，才發現被騙，亦難以追回損失。

騙局成功核心元素之一是先用詐術贏得被害人的「信任」（Confidence），讓對方自願交出金錢、資訊或其他有價值的資源；另一個核心要素就是「成為群體的一部分」（Being Part of the Community），這一點與騙子的社交操縱能力密切相關。騙子經常透過融入社群，建立「自己人」的形象，讓被害人更容易相信他們，當代騙子能夠「成為社群的一部分」，是透過使用智慧科技隨時跨越物理界限，只要它們聽起來有道理、有成功實例，就能贏得受害者的「信任」。而其常見的詐騙常見套路則是快速發財套路（Get-Rich-Quick Schemes），以及假冒官署套路（Authority Imposter Schemes）。[12]

據內政部警政署受理民眾報案資料顯示，投資類詐騙受害者半數在 30 天內發覺自己受害，近 9 成 5 受害者在 6 個月內發覺遭詐。相較而言，非投資類詐騙中假檢警詐騙案件 30%會在 3 日內報案，60%在半個月內報案。網路購物詐騙案件 44%在 3 日內報案，近 60%會在 1 週內報案。從而可知，民眾從遭詐到報案間存在時間差，7 成以上非投資類詐騙受害者會在 1 個月內報案，但大部分投資類詐騙受害者要 6 個月時間才知道遭詐。

此外相關調查研究顯示，投資詐騙 6 成潛在被害人不報案，其中 4 成「知詐但不報」，有 2 成更是堅決不認為遭詐，拒絕警方協助。進一步分析不報案的 3 種狀況，分別是真的被騙，但不願被認為「傻」、「貪心」，不承認被騙、不願報案；另外因假投資摻雜網路曖昧，可能不好意思坦承；最後被騙得團團轉，仍始終不認為被騙的一群人。[13]

---

[11] 「cold calling」一種由諸如經紀商人撥打不相識、潛質顧客電話從而進行直接行銷的手法。

[12] 王曉明，美國打詐策略與法制，警政與警察法相關圓桌論壇(第 86 場)，中華警政研究學會，2025 年 3 月 27 日。

[13] 胡欣男，投資詐欺 6 成潛在被害人不報案，中時新聞網，2023 年 12 月 4 日。

一、從眾效應（Bandwagon Effect）

詐騙集團從來都不只是用一個角色，來遂行詐騙，從金光黨時期就知道採用「眾口鑠金」的多角色包圍，一個「大智若愚」的傻子，一個鬼靈精但是缺乏資金的「一起來賺錢」慫恿者，還有一個配合贊成的附合者，描述成功的未來，除了這說唱俱佳的三個主要角色外，「Sakura」更是詐騙重要的心理學，「Sakura」源為日語「櫻（さくら，）」的音譯，但除了意指櫻花，在台灣或日本文化中，該詞也常被引申為「臨時演員」或「僱傭的假客人（寫手/暗樁）」，專門在店家或展場炒熱氣氛、營造人潮湧動的假象，這種暗樁會讓原本已經有所動搖的人在看到許多人已經成功投入，機會越來越少，於是在現場氣氛與眾口鑠金的效應下再不加入可能就來不及的時間壓力與氛圍中，奮力投入成為被害人，從眾效應有時又稱「羊群效應」或「樂隊花車效應」，是指個體在群體壓力下，放棄自己的意見，盲目跟隨大多數人想法或行為的心理現象。

二、認知需求閉合（Need for Cognitive Closure）

在政府、金融機構以及媒體的努力宣導下，多數民眾大多已經知道當前金融詐騙嚴重，但是許多人以為會被詐騙的人不是貪就是笨，甚至基於台灣俚語「痟貪瞜雞籠」的影響，認為自己不是那個既貪又笨的人，所以無需去關注這些詐騙的社會事件，殊不知詐騙已經進化到「沒有做不到、只有你沒想到」的境界，這是因為人類傾向於在混亂或不確定的狀態中（例如懷疑他人或事件），快速尋找一個明確的答案，以消除不安的感覺。當大腦會認定資訊已足夠，就會終止進一步的思考，結果自己真的遇上時，毫無詐騙的抵抗力，因為缺乏足夠的「媒體素養」，AI 時代的來臨，已經讓我們更難查證，須謹記「盡信網路，不如沒有網路」。

三、名人錨定效應（Celebrity Anchoring Effect）

名人通常象徵著成功、美貌或權威，大眾的「暈輪效應」會導致對名人的崇拜延伸到其所代言的一切，無論該資訊是否準確。名人錨定效應也是一種認知偏差，指出人們在決策時，過度依賴接收到的第一條資訊（即「錨」）。當名人、專家或網紅作為「錨」來推薦產品、宣佈價格或設定觀點時，大眾容易受到其身分影響，將後續的評估基於該明星的價值觀，產生先入為主的「尊貴」或「專業」錯覺。

例如過去的投資詐騙特別喜歡使用「假謝金河」、「假吳淡如」、「假胡睿涵」等名義來吸引被害人加入群組，就是詐騙集團利用名人錨定效應的核心機制與行銷應用，讓人們決策時因其高知名度與專業形象，能將產品的「潛在價值」拉高「這一定很成功」的

感受，直接錨定在名人品牌上，雖然刑事警察局與數發部合作製作「白名單」讓假名人無法出現，但是各種利用名人照片或假公司商標、假董事長甚至假穿制服的超商店員案件仍層出不窮，例如日本首位在國際太空站（ISS）停留的民間人士、知名富豪前澤友作以「允許未經同意使用姓名與肖像刊登廣告」為由，向美國與日本 Meta 的提告請求賠償「1 日圓」，澳洲礦業大亨佛瑞斯特（Andrew Forrest）也出面指控臉書（Facebook）未能預防加密貨幣廣告而從中獲利。

四、確認偏誤（Confirmation Bias）

刑事警察局偵查第一大隊，曾透過大數據分析 165 反詐騙系統平台資料，勾勒出假出金詐欺集團的犯罪手法，詐騙集團以假投資網站招攬被害人投資，等被害人遭誆騙投資小額款項後，再指派「出金手」透過臨櫃匯款或其他方式，由「出金」匯入其等指定帳戶，被害人誤認投資可以獲利假象，重複一兩次出金後，被害人往往就會不假思索開始投入大量資金。

因為人們通常只會致力於確認最初的懷疑，而不是試圖證明自己的假設是錯誤的。所以當人們查證兩次以上，就會確認已經成功的觀點及證據，而非尋找反證，於是原本的確認，成為確認偏誤，因為一開始有查證過，從此不再查證，殊不知這是「詐騙算計了你的算計，預判了你的預判」，於是初始賺到一些小獲利，最後反而賠上自己的大額本金。

五、焦慮型依附（Anxious Attachment）

殺豬盤是當前橫行於全球，被公認造成最多財損的類型，這與台灣投資詐欺佔所有的詐騙中，造成最多財損的情形類似，這種投資詐欺利用心理學尋找有「焦慮型依附人格」的被害人，從安全感的建立與適度的信任下手，在建立親密關係或曖昧關係中，重複的確認來培養情緒價值，不斷回應被害人的聯繫，來緩解被害人的焦慮、建立安全感的過程，最後當雙方互動呈現一致的溫和與信任（查證結果一致），大腦會將對方視為「安全信號」，進而放下防備。

例如投資群組的小助理，經常反覆確認對方是否早餐午餐與晚餐，完成被害人極度渴望陪伴，略有不回應就懷疑對方不再在乎你，建立緊密聯繫，讓被害人害怕分離，甚至無時無刻想知道對方的行蹤，又不自覺地想掌控對方，這種現象在心理學中被稱為「焦慮型依附人格」。

網路詐騙已經 AI 化，真假越來越難辨，犯罪集團利用這些被騙的心理效應，營造被害情緒價值的培養，使得網路詐騙成為持續得逞的溫床。我們必須面對「只要疏於防護，就有可能犯錯」，而不能抱持被騙的人不是因為「貪」就是因為「笨」，否則，一旦認為自己不貪也不笨，就容易掉入詐騙的陷阱，現代的電信網路詐欺是「歹徒精心設計的劇本」，只有你想不到，沒有詐騙做不到，如果你還沒被騙，那是因為還沒遇到適合你的詐騙劇本；多一分查證、少一分被騙，萬一被騙，更應在第一時間報案，與警方及金融機構合作，而不是妄想單靠一己之力扳倒詐團，我們必須理解，詐騙集團早已千錘百鍊，騙過成千上萬的人，取得成千上億的財產，詐騙已經企業化、科技化、國際化。

網路詐騙已經 AI 化，真假越來越難辨，萬一被騙不要先自責，真正的壞人是詐團，而不是被害人；親友也應是給予適切關懷支持，而非指責。惟有停止責怪，開始傾聽，給予心理支持與扶助，才能讓被害人有勇氣說出自己的經歷，社會才能累積防詐經驗，進一步形成集體免疫力。

伍、結語

在一場行政院打擊詐欺的會議上，兆豐金控董瑞斌董事長曾經說「金融業是防詐第一線，也是阻詐最後一哩路」，這句話讓與會的公私部門都深深感動，其實近年各金融機構承受重重壓力，我們不斷看到櫃檯前因為勸阻客戶，產生的衝突與客訴，奈何被騙的客戶早在來銀行前就被洗腦，「銀行都在賺利差」、「銀行怕客戶提款」、「銀行都是吸血鬼」，因此取款時務必編織藉口，銀行不接受提領錢就在櫃檯大鬧，威脅向金管會申訴，甚至曾發現客戶轉帳現金一千三百萬，卻攔阻失敗，原因是詐欺集團提供客戶一份偽造的購買工具機合約文件，也有客戶拿出購買黃金的估價單，結果仍然是詐騙集團提供資料。

近期，由「台版 Jisoo」擔任主嫌的最大假出金「美樂」詐騙集團，在一審被判刑 24 年後，新北市刑警大隊溯源追查，掌握幕後金主，發現該集團共架設 2230 個假投資網站，詐騙 158 億多元，造成 5,082 人受害，另台中豐原王姓一家五口遇投資詐騙，因無能力再承受而走上絕路。被害人遭到詐騙後，往往身心遭受到極大打擊，又缺乏資金進行訴訟與求償，心力交瘁孤單無助，遲遲等不到賠償金亦無被害補償金。

相較於台灣 114 年被騙 893 億元，[14]美國 2025 年遭詐欺總金額為 159 億美元，又較上年的 125 億美元增加 34 億美元，[15]惟美國聯邦貿易委員會（FTC）日前在美國國會經濟委員會，進行反詐欺執法與消費者保護報告答詢時，指出 FTC 協助消費者提起 40 件訴訟，並為消費者追回超過 18 億美元的賠償金。針對發布虛假收益承諾和虛假退款保證、推銷虛假人工智慧商業支援服務等，依據違反《聯邦貿易委員會法》、《電話行銷銷售規則》和《商業機會規則》等，要求被告支付賠償金，並永久禁止被告銷售或推廣任何商業機會，嚴禁在電話行銷或商品及服務銷售中做出虛假聲明或收益承諾。

FTC 與美國聯邦調查局（FBI）的網路犯罪投訴中心資產追回小組（IC3 RAT）合作，將涉及高額損失且符合 FBI 標準的消費者報告，在消費者同意的情況下轉交給 FBI，啟動名為「金融詐欺殺傷鏈」（FFKC）的流程，通知銀行合作夥伴，嘗試凍結已匯給詐騙者的資金，從而追回損失。2024 年，IC3 RAT 針對 2,651 起事件啟動了 FFKC，並在銀行合作夥伴的協助下，凍結了 6.515 億美元報告損失中的 4.69 億美元。

一、服務快不能再是目標

近期新聞報導某大銀行發生銀行員在執行異常客戶清查與攔阻後，情緒失控，砸桌並試圖跳樓，所幸被同事及時拉住，避免悲劇發生，再次凸顯金融業為了阻詐防止客戶被騙，不但投入更多的人力、物力甚至財力，但是看起來不斷增加的是壓力與阻力。畢竟全球金融秩序已經因為金融犯罪而大幅震盪，我們雖瞭解，銀行透過模型分析出異常帳戶，並不是就能認定客戶是犯罪人口，而是發現客戶可能有被利用的高風險，所以暫停客戶的電子交易，只是希望客戶臨櫃釐清金流與帳號密碼有無外洩遭他人控制的情形。畢竟金融業正面臨轉型，從過去「服務快就是好」的基礎轉型為「能守護客戶才是好銀行」的關鍵時刻。

二、建立詐欺情報互惠交換（FIRE）計畫

雖然重新釐清異常帳戶會造成客戶一時的不便，但是確認客戶沒有被騙、沒有被利用是很重要的一環，因為過去的資料顯示，「客訴少的銀行，警示帳戶就多」、「客訴多的銀行，警示帳戶就少」，英國銀行目前合作打擊詐騙使用的詐欺情報互惠交換（Fraud

[14] 詳見打詐儀錶板全年度資料累計。

[15] Consumer Protection Office of Congressional Relations Bureau of Consumer Protection Consumer Sentinel Network deceptive/misleading conduct/FTC Testimony - Joint Economic Committee Hearing on the Rising Scam Economy /Date March 25, 2026

Intelligence Reciprocal Exchange, FIRE）計畫，是一項針對金融機構威脅的情報共享計畫，英國放寬銀行可以分享反詐欺情報，以共同打擊詐欺，在該計畫初期階段，已經對詐騙者相關的數千個帳戶採取行動，並根據共享資料刪除大約 20,000 個帳戶，並將繼續接納更多銀行一起加強詐欺偵測能力，為英國和全球的客戶創造一個更安全的數位環境。

不只銀行業強調情報分享，Meta 也加入這項金融情報合作計畫，對詐騙者運營的數千個社交媒體帳戶採取管制行動，說明銀行和社交平台共同努力解決這一社會問題的重要性。Meta 的反詐欺主管表示，只有共同努力並分享這些相關的訊息，才能擊敗詐欺犯罪，金融機構可以與 Meta 分享去識別化的訊息，利用這些訊息訓練系統，以便在全球範圍內採取更多打擊詐騙的行動。

英國的試辦計畫成功摧毀一個試圖針對英國和美國民眾的大型音樂會門票詐騙網絡，從共享的 185 個 URL 中刪除詐騙者運作的 20,000 餘帳戶，以減少被害者損失，任何一個曾經匯款給這些帳戶都可能是被害人，必須暫停他們的電子交易，並通知他們可能被害了。FIRE 計畫在英國受到歡迎，被認為是打擊詐騙的關鍵一步，我們也必須加快腳步，迎頭趕上守護客戶的資產，銀行與銀行員及警員在這些阻詐的過程中，必須確認自己的目標是守護客戶，運用同理心說服客戶，同時也要建立更強壯的心理素質，否則自己也會成為詐欺案件的間接被害人。

三、分析與預測警示帳戶

打擊詐欺作戰必須彙整資金流、資訊流與電信流，然而當前詐欺集團不斷拋擲重金，建構人頭帳戶、假社交媒體帳號，以貓池（Modem Pool）發射假簡訊，以節費器發送假電話號碼，造成民眾鉅額損害。在數位經濟時代，中央必須設計一個風險可控管的監理沙盒（Regulatory Sandbox），解決現行法規與新興科技的落差，提供給各新興科技與新創業者測試、服務以及可以協助進行風險辨識的資料庫模式。

鑒於過去偵查與預防電信網路詐欺，多偏向台北富邦的「AI 鷹眼模型」，期能先一步辨識出「可疑警示帳戶」，然而，警示帳戶卻不斷膨脹增長，從 2015 年的 17,521 戶成長至 2024 年已達 149,274 戶。

圖 6　警示帳戶的數量十年來不斷飆升

資料來源：聯合報

以當前警示帳戶成長趨勢，目前由各銀行自行進行風控之機制顯然不足，復以投資詐騙約有 60%潛在被害人不報案，其中 40%「知道被騙但不報案」，另有 20%成更是堅決不認為遭詐，拒絕警方協助。進一步分析不報案的 3 種狀況，分別是真的被騙，但不願被認為「傻」、「貪心」，不承認被騙、不願報案；另外因假投資摻雜網路曖昧，不好意思向家人坦承；還有始終不認為被騙的一群人，最後才是被騙得團團轉。[16]

四、最後的惡魔？最後的天使！

許多詐騙的實際情節都匪夷所思，當我們苦口婆心勸阻可能被騙的民眾時，自以為是民眾心中的天使，阻擋惡魔詐欺集團，但是現實情況最常出現的剛好相反，因為民眾早已被犯罪集團洗腦，不但來取款時，早已設定好不給錢就要大鬧，更受到詐欺集團的強心針，這筆成功後，就要共創人生，享受美好生活，我們的攔阻，正是敲碎詐欺集團向被害人編織的美夢的人，也是被害者最不願面對的事實，此時我們是被害人新的惡魔，

[16] 胡欣男，投資詐欺 6 成潛在被害人不報案，中時新聞網。112 年 12 月 4 日。

被害人的天使就在網路上等他(她)，因此白白挨罵是常有的事，但是金融業幾乎已經是攔阻被害人資金被洗走的最後一道防線，這道防線要承受得住嚴重的炮火攻擊，因為我們擋下的不是一個人，而是一個家庭的未來。因此被尚未清醒的客戶罵不是恥辱，而是行善積德的承擔與奉獻，我們仍應自反而不縮，雖千萬人吾往矣！

五、建立 AI 代理人與地端 LLM

面對海量的詐欺案件，僅由銀行行員與警方的攔阻詐騙，顯然難以力挽詐欺狂瀾，當前資訊科技已經進展到 AI 代理人，但是企業若要導入 AI 代理，最重要的是要先有準確的資料庫與模型，否則 AI 模型無法精準使用，仰賴雲端開放資料的結果是，詐欺集團豢養的網站動輒 2,000 至 3,000 個假網站，上萬的假帳號機器人，因此若要導入有效的 AI 代理系統，建議要先建立地端的大型語言資料庫（LLM）。

因此，我們必須建立執法機構與金融機構聯防預警平台資料庫，透過監理沙盒提供各金融相關行業與壽險業者一同進行風險管控，本研究整合相關資訊，提出建立聯防平台資料庫架構，分別建置以下資料庫。

(一) 紅名單：經各警察局曾經攔阻成功之帳戶持有人，以及各銀行依據刑事局建議判定之高風險潛在被害人（例如 50 歲以上女性，低金額流動帳戶），以及近三年曾遭攔阻提款或轉帳（含虛擬貨幣）資料，供各銀行分享列為高風險易被害族群紅名單。

(二) 灰名單：銀行局針對有被多數人設定為收款帳戶之可疑帳戶，該帳戶可能為詐團之第一層水房，惟需要進一步比對與 STR 帳戶往來情形始能判斷。

(三) 黑名單：遭警方通報警示帳戶之名單。

(四) 白名單：銀行或警方業經落實客戶盡職調查認證的帳戶或公益團體帳戶或政府機關帳戶資料。

(五) 粉紅名單：各銀行偵測為高風險但尚無法確定之客戶或 STR 名單

(六) 於刑事警察局建立聯防預警關聯資料分析平台，相關內容說明如下：

1. 他單位資料蒐集：涉詐電信門號所有人資料、電子支付交易平台資料、第三方支付交易資料。

2. 各銀行發現已遭警示之帳戶仍有嘗試匯入失敗之反向查詢，即可能為潛在被害人資料。

3. 法務部依據洗錢防制法第 15 條之 2 受告誡處分帳戶資料、地政機關通報資料、STR 資料。

4. 中信 ATM 智能防詐車手交易通報系統資料。

5. 富邦鷹眼聯盟預警資料。

6. 各銀行 ATM 分析詐欺提領熱點。

7. 各警察局查緝車手所取得資料（含工作牌姓名、照水姓名、取款收據、假公司章資料、預計收款人資料、使用交通工具與電信手機 LINE ID 等）。

(七) 被害報案 AI 相關輔助語言模型：採購報案資料 OCR 自動辨識回溯過去五年報案筆錄、回溯 165 語音存檔資料，進行自動語音辨識 ASR 轉換為文字，另購置 NVIDIA 及 AI 系統，輔助歸納整理成報案及語音諮詢 165 案件資料庫，成為詐欺被害量刑語言模型，以利將來用於購置 NVIDIA 晶片 AI 主機進行最新詐欺趨勢分析。

(八) 165 系統中可規劃 8 個欄位供各地方警察局攔阻詐欺成功之際即時填輸，以利反向追蹤，拼湊詐欺車手間關聯性。特別是查獲車手或照水之預計收款帳號，收款收據大小章名稱、聯繫方式、line 帳號、車牌、電話號碼等，以及工作牌名稱與公司名稱，除可建立各縣市攔阻資料庫進行分析，查明詐欺軌跡。透過上述輔助系統分析取得警示帳戶、被害人帳戶、加密貨幣錢包及各銀行財損金額。

(九) 透過上開資料庫分析，預計達成目標如下：

1. 形成跨銀行部門阻斷，形成一家攔阻，全國警示。

2. 分析個案車手於判決前持續犯案次數，藉此提高檢方聲押成功率。

3. 與 STR 通報資料、黑名單、灰名單相互交叉比對，使情資更具體，以利交查各外勤大隊偵辦。

4. 追蹤有關可疑的加密貨幣錢包，供科技中心查扣錢包關聯性分析。

5. 將銀行提供之灰名單(尚無法確定之高風險客戶)進一步交集分析，取得具體身分資料。

6. 公布涉詐網站及 APP 警示民眾。

7. 未來公布已列紅名單，卻攔阻失敗原因分析。

8. 分析車手、照水之共同聯繫人及車籍、車輛出沒與停留地點等資料。

(十) AI 預警聯防預警平台資料庫藍圖如圖 7。

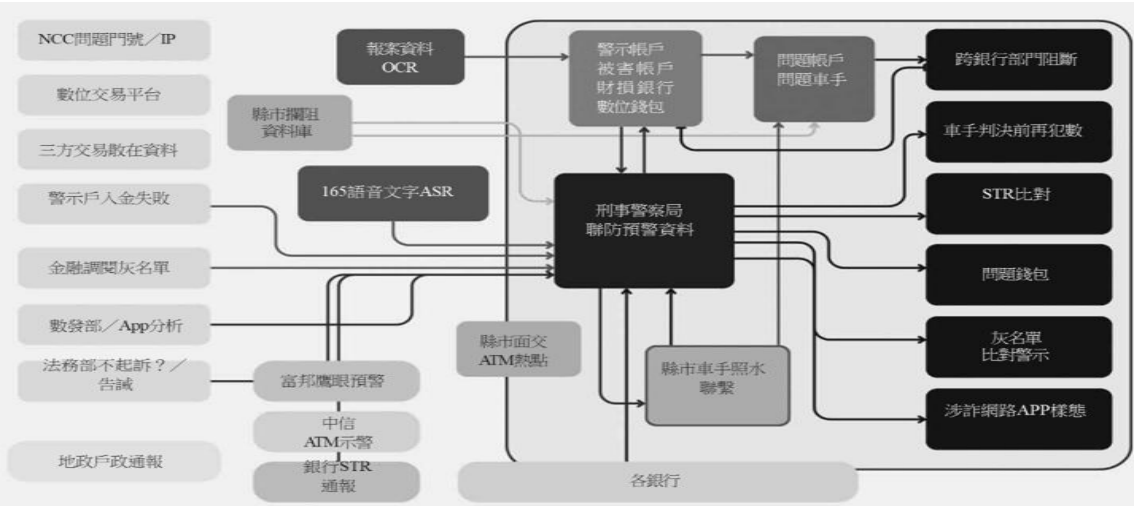


圖 7 AI 預警聯防預警平台資料庫藍圖

資料來源：作者研究自繪

詐欺席捲全球，已經在各國造成嚴重金融風暴，不但傷害國家金融發展甚至造成個人生命的永久損害，近期詐騙更運用 AI 的輔助，每個詐騙集團動輒 2,000 至 3,000 個假網站上萬個假帳號，迷惑人心，即使小心上網求證，仍難逃被詐騙的命運。美國聯邦貿易委員會指出，金融業與刑事執法夥伴的合作在打擊詐騙的工作上至關重要。因此唯有金融業與執法機關的密切合作，建立金融科技的專屬 LLM 資料分析，運用 AI 早期辨識預警被害的潛在客戶，才能更有效率利用 AI 協助攔阻詐欺活動。

參考文獻

一、中文文獻

王曉明，美國打詐策略與法制，警政與警察法相關圓桌論壇(第 86 場)，中華警政研究學會，2025 年 3 月 27 日。

江樂麒，催生「詐欺犯罪危害防制條例」，警光雜誌第 817 期，2024 年 9 月。

李志強，強力打擊詐欺犯行—淺談打詐五法修正重點，清流雙月刊第 47 期，2023 年 9 月。

李奕昕，下架近 5 萬則假投資廣告不斷，聯合報，2024 年 2 月 19 日。

官政哲，建構數位神經網絡之反詐生態系統策略，警光雜誌第 823 期，2025 年 2 月。

林山田，《刑法各罪論（上）》，修訂五版，台北：自版（2005）。

林東茂，〈經濟刑法導論〉，《危險犯與經濟刑法》，初版，台北：五南圖書出版有限公司（1996）。

林書立，電信網路詐欺與警政治理，收錄於鄭善印、許福生主編，警察勤務與智慧警政，五南出版，2025 年 2 月。

林書立，全球防堵 Scamdemic 反詐欺課責與鷹眼識詐，自由時報自由廣場，2023 年 10 月 9 日。

林山姆，最接近真實數據打詐儀表板成公民參與里程碑，自由時報自由廣場，2024 年 9 月 4 日。

林郁平、季志翔，國泰世華與刑事局聯手出擊，鼓勵全民參與反詐倡議行動，中時新聞網，112 年 12 月 6 日。

洪丞奇，打詐新四法法條解析實務應用，2024 年 11 月 26 日，中央警察大學行政警察學系演講簡報檔。

胡欣男，投資詐欺 6 成潛在被害人不報案，中時新聞網，2023 年 12 月 4 日。

許春金，《犯罪學》，修訂五版，台北：三民書局總經銷（2007）。

許福生，刑案統計 e 化介接整合呈現真實治安面，警光雜誌第 819 期，2024 年 10 月。

許福生，「打詐新四法」四箭齊發建構免遭詐騙社會，警光雜誌第 817 期，2024 年 9 月。

許福生，電信網路詐欺犯罪防制政策與法制之回顧與展望，中央警察大學學報第六十二期，2025 年 6 月。

許福生，擴大科技偵查授權斷絕黑幫金源，2025 年 8 月 22 日聯合報民意論壇。

姚惠茹，三方通話即刻通報！玉山銀與警政署合作已阻詐 2 億元，2023 年 8 月 24 日，引自 https://finance.technews.tw/2023/08/24/deceitful/(最後瀏覽日 2025 年 3 月 1 日)。

孫麗菁，重傳三讀通過洗錢利益達一億元處三年以上、十年以下有期徒刑，台灣時報，2024 年 7 月 16 日。

謝福源（1996），《防制洗錢之研究：理論與實務》，台北：金融研訓中心。

蘇文彬，35 家金融業者組聯盟用 AI 模型偵測警示帳戶攔阻詐騙金流，下一步要用聯合學習精進模型，2024 年 8 月 14 日，引自 https://www.ithome. com.tw/news/164486(最後瀏覽日 2025 年 3 月 1 日)。

蘇信雄，電信網路詐欺犯罪機房跨國（境）蔓延之研析，中央警察大學學報第五十九期，2022 年。

嚴浤元，詐欺犯罪現況與策略，當代法律，2023 年 8 月。

行政院，新世代打擊詐欺策略行動綱領 1.5 版(核定本)，2023 年 6 月 19 日。

天下雜誌第 787 期，封面故事報導：「加賴領飆股！」銀行員、工程師變共犯白領詐騙，2023 年 11 月 28 日。

中國信託銀行，金檢聯防再進化，打造詐騙預警偵測機制，2024 年 4 月 18 日，https://www.ctbcbank.com/twrbo/zh_tw/index/ctbc_article/digital_article/blog_digital_ondemand/NB2024041823.html (最後瀏覽日 2025 年 3 月 1 日)。

法務部新聞稿，打詐四法三讀，展開打詐新篇章全面查緝詐欺犯罪，落實罪贓返還，完善被害保護，https://www.ey.gov.tw/File/CF026A7FCF7B5C71？ A=C(最後流覽日:2025 年 4 月 1 日)。

新世代打擊詐欺策略行動綱領 2.0 版，https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/c93637bd-ddc2-4447-8829-246a5ca0befc(最後瀏覽日 2025 年 2 月 20 日)。

ETtoday 新聞雲，從街頭到網路「台灣詐騙調查報告書」20 年詐騙手法歷程與演變，https://www.ettoday.net/news/20230410/2476194.htm(最後瀏覽日 2025 年 3 月 1 日)。

二、英文文獻

Brühl, T. &Rittberger, V. (2001). From international to global governance: Actor, collective decision-making, and the United Nations in the world of the twenty-first century. In V. Rittberger (Ed.). Global Governance and the United Nations System (p. 1). New York: United Nations University Press.

CNN (2025.4.2). Global scam industry evolving at 'unprecedented scale' despite recent crackdown. Retrieved Apr. 2, 2025 from https://edition.cnn.com/2025/04/02/asia/myanmar-scam-center-crackdown-intl-hnkdst/index.html?iid =cnn_buildContentRecirc_end_recirc.

Goldberg, H. G. (2021). The FinCEN AI System: Finding Financial Crimes in a Large Database of Cash Transactions. Springer.

Goswami, S. (2024). Fraud management & cybercrime: Pros and cons of anti-scam rules in UK, Australia, Singapore. BankInfoSecurity. Retrieved May 15, 2025 from https://www.bankinfosecurity.com/blogs/pros-cons-anti-scam-rules-in-singapore-uk-australia-p-3756.

INTERPOL (2024.3.11). Financial Fraud Assessment: A Global Threat Boosted by Technology.

Jacob Sims & Mark B. Taylor (2025.5.2). Inflection Point: What to do when the state is the syndicate？ The Diplomat.

Suparna Goswami (2024.12.5). Pros and Cons of Anti-Scam Rules in UK, Australia, Singapore. https://www.bankinfosecurity.com/blogs/pros-cons-anti-scam-rules-in-singapore-uk-australia-p37-56.

U.S. Attorney's Office (2025.2.25). Three Defendants Arrested on Federal Complaints Alleging They Knowingly Received More Than $13 Million in Scam Victims' Money.

World Economic Forum (2020.1.15). The Global Risk Report 2020 (15th ed.). Retrieved May 15, 2025 from https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

World Economic Forum (2023.1). The Global Risks Report 2023 (18th ed.). Retrieved May 15, 2025 from https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

著作財產權同意書

本同意書人（即著作人）所作刊載於「臺灣銀行季刊」（第　卷第　期）中之＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿一文，著作人享有著作財產權，同意於該文著作財產權存續期間，授與臺灣銀行重製權、散布權及公開傳輸權，享有在任何地點、任何時間以任何方式利用（包括但不限於數位方式出版、登載於臺灣銀行全球資訊網供外界參閱）或再授權他人利用該著作之權利，且臺灣銀行不需因此支付任何費用。

著作人擔保本著作係著作人之原創性著作，僅投稿「臺灣銀行季刊」，且從未出版過。若本著作之內容有使用他人受著作權保護之資料，皆已獲得著作權人（書面）同意，或符合合理使用規定於本著作中註明其來源出處。著作人並擔保本著作未含有誹謗或不法之內容，且未侵害他人之權利。

若本著作為二人以上之共同著作，下列簽署之著作人亦已通知其他共同著作人，本同意書之條款，並經各共同著作人全體同意，且獲得授權代為簽署本同意書。

立同意書人（即著作權人之姓名）：　　（簽章）

身分證統一編號：

戶籍地址：

聯絡電話：

電子郵件信箱：

中華民國　　年　　月　　日