跨境電信詐騙犯罪的打擊難點及對策

李妍 *

摘要：近年來，公安機關雖然在打擊跨境電信網絡詐騙犯罪的過程中取得了一定成果，但由於跨境電信網絡詐騙犯罪的複雜性和犯罪嫌疑人的隱蔽性，目前跨境電信網絡詐騙犯罪仍呈現出高發、多發的態勢。跨境電信詐騙犯罪具有犯罪組織專業化產業化特徵突出、犯罪手段精準化智慧化特徵顯著、犯罪空間虛擬化跨域化特徵明顯的特點，在打擊跨境電信網絡詐騙犯罪過程中存在跨境取證難、犯罪成員打擊難、黑灰產業鏈助推跨境電信網絡詐騙犯罪發展壯大等諸多挑戰，為了有效打擊跨境電信網絡詐騙犯罪，應當深度拓展國際警務合作、利用資訊技術助力精準打擊犯罪、實施全鏈條打擊策略。

關鍵詞：跨境電信詐騙犯罪　打擊難點　對策

Difficulties and Countermeasures in Cracking Down on Cross-Border Telecom Fraud Crimes

Li Yan

Abstract: In recent years, despite some achievements made by public security organs in combating cross-border telecom network fraud crimes, the persistent high frequency of such crimes continues due to their complexity and the concealment of criminal suspects. Cross-border telecom fraud crime is characterized by the professional production and industrialization of criminal organizations, the precision and intelligence of criminal methods, as well as the virtualization and cross-domain nature of criminal activities. The fight against cross-border telecom network fraud faces numerous challenges including difficulties in collecting cross-border evidence, combating criminal members, and countering the growth fueled by black and gray industry chains. To combat this crime effectively, it is crucial to enhance international police cooperation, employ information technology for precise crime-fighting measures, and implement a comprehensive strategy across all stages.

Keywords: Cross-Border Telecom Fraud Crime；Combat Difficulties；Countermeasures

*　李妍，中央司法警官學院講師，碩士研究生，主要研究偵查學。

一、前言

近年來，跨國電信詐騙犯罪已成為危害公民財產安全、社會秩序穩定、國家長治久安的一顆“毒瘤”。跨國電信詐騙犯罪涉案金額大，涉案人數多，犯罪組織專業化、成熟化，雖然我國對其進行了嚴厲打擊，並取得了顯著成果，但在資訊技術快速發展的時代背景下，跨國電信詐騙犯罪仍然呈高發多發的嚴峻態勢，並且衍生出了諸如人口販賣、綁架等上下游犯罪，社會危害嚴重，影響惡劣。與此同時犯罪嫌疑人對抗技術升級化，犯罪手段不斷升級，因此，必須持續保持對跨境電信詐騙犯罪的高壓嚴打態勢，全力擠壓詐騙犯罪生存空間。

二、跨境電信詐騙犯罪的特點

（一）犯罪組織日臻成熟，專業化產業化特徵突出

跨境電信詐騙犯罪集團組織嚴密，分工細緻。隨着跨境電信詐騙犯罪的深度發展，犯罪嫌疑人結合公司運營模式和犯罪環節不斷完善調整組織結構，最終呈現出詐騙環節環環相扣，各個犯罪環節分工明確、高度配合的特徵。犯罪組織參照公司化運營方式，主要分為詐騙犯罪決策層、詐騙犯罪實施層、詐騙所得資金處理層。詐騙犯罪決策層主要為犯罪集團的頭目和骨幹成員，主要進行詐騙目標的制定、犯罪所需硬體設施的準備、制定針對執行層的犯罪嫌疑人的規章制度等詐騙犯罪準備工作和犯罪運作事宜，從宏觀層面把控犯罪集團的運作方式。詐騙實施層的主要工作是根據通過黑灰產業鏈非法購買的公民個人資訊、提前制定好的詐騙劇本，與不特定的多數被害人通過網絡或通信建立起聯繫，從而實施詐騙。由於犯罪嫌疑人的主要目的是侵佔公民或單位的公私財產，因此當詐騙實施成功後犯罪嫌疑人必定要將詐騙所得資金進行處理和轉移，以達到“合法擁有”犯罪所得的目的。因此，在詐騙所得資金處理層，犯罪集團會安排專門取現金的大量車手將詐騙所得資金取出，然後運用協力廠商支付、虛擬貨幣交易平台等多種方式進行洗錢，模糊詐騙所得資金來源和流向，最終達到侵佔詐騙所得資金的目的。此外，隨着犯罪集團的深度發展，逐漸呈現出壟斷化的特徵。從資源整合角度來看，如同運作企業一般，將各類分散的犯罪要素彙聚在一起。同時在控制層面通過對詐騙團夥成員的集中封閉管控，使得犯罪集團內部秩序高度穩定，便於調配各種犯罪資源，形成一條完整且高效的犯罪鏈條。例如，最高人民檢察院、公安部第三批聯合督辦的江蘇江陰“6·16”專案，潘某某等 6 名幕後“金主”在緬北出資建造“五金建材城”，先後招攬 18 個詐騙團夥入駐，實現辦公資源的集中供給，並為詐騙團夥提供辦公場所和食宿，進行封閉式管理，持械看守詐騙團夥人員，形成超大犯罪集團[1]。犯罪集團的壟斷化使得跨境電信詐騙犯罪的危害程度愈演愈烈，嚴重危及人民群眾的生命安全和財產安全，嚴重破壞了社會生態。

（二）犯罪手段多元複合、精準化、智慧化特徵顯著

在經濟利益和科技的雙層因素的催動下，跨境電信詐騙犯罪逐漸由粗放式向精細化方向演變，愈加專業化。首先是詐騙手段由原來的單一型逐步發展為多元複合型。一方面是由於犯罪集團日趨壟斷化，使得犯罪鏈條進一步加長，更多的犯罪行為加入其中；另一方面是犯罪嫌疑人將不同的詐騙模式相結合，步步滲透、層層攻破，使詐騙更具欺騙性和迷惑性。如殺豬盤詐騙犯罪就是將情感詐騙加虛假投資相結合的詐騙方式，犯罪嫌疑人先以情感交友為手段騙取被害人的信任，然後再引誘被害人進行虛假投資，從而騙取被害人的財產。其次，犯罪嫌疑人為了增加犯罪成功率，將資訊技術成果運用到犯罪當中，以增加犯罪的迷惑性。如犯罪嫌疑人除了非法購買公民個人資訊之外，還利用 AI 換臉、AI 語音合成等技術騙取被害人的信任，面對真實的個人資訊和智慧技術的加持，被害人往往深信不疑，從而落入犯罪嫌疑人的圈套。與此同時，犯罪嫌疑人還專門研究人類的心理規律及其弱點，並根據購買來的被害人的住址、電話、工作等詳細真實資訊，進行有預謀的精準化詐騙。被害人心理的把握、被害人個人資訊的獲取、智慧技術的支撐，三者有機結合，使得詐騙更為精準和高效。

[1] 中華人民共和國最高人民檢察院：〈檢察機關打擊治理電信網絡詐騙及其關聯犯罪工作情況（2023 年）〉，https://www.spp.gov.cn/xwfbh/wsfbt/202311/t20231130_635181.shtml#1，到訪日期：2024 年 3 月 2 日。

（三）犯罪空間雙層交錯，虛擬化、隱匿化特徵凸顯

隨着互聯網基礎設施和技術的快速發展，使人們在全世界的範圍內通過網絡技術實現互聯互通。而犯罪嫌疑人也緊跟時代腳步，犯罪方式借助網絡實現了由接觸式犯罪到非接觸式犯罪的轉變，使得犯罪突破了物理空間和地理位置的限制，犯罪空間呈現出實體空間和虛擬空間交錯的狀態，在全球快速蔓延的跨境電信詐騙犯罪正是典型的代表。犯罪嫌疑人通過網絡技術在境外隱匿在網絡平台後面，對境內不特定的多數被害人實施詐騙，導致犯罪嫌疑人身份虛擬化，難以追蹤。此外，為了逃避公安機關的打擊並順利地實施犯罪，犯罪嫌疑人將犯罪窩點轉往境外，利用網絡空間的無國界性，以電信網絡為紐帶，一邊隱匿在境外對境內的被害人實施持續詐騙，另一邊指揮境內的犯罪分子為其招募犯罪成員、實施詐騙、轉移贓款，發展相關的灰黑產業，使得犯罪集團網絡盤根錯節，密切聯繫[2]。例如，在陳某某、黎開強等詐騙犯罪案中[3]，陳鵬（另案處理）邀請被告陳某某招募人員偷渡到緬甸猛波金牛湖從事電信詐騙，招募一人給 5,000 元，參與詐騙的人有提成，招募人可從詐騙金額中獲取相應提成，陳某某表示同意，並將這一信息告知被告人黃平、王旭揚、黎開強和楊軍（另案處理），他們為境外詐騙犯罪組織招募數名人員並偷渡緬甸，成功加入犯罪集團。通過互聯網使位於不同地域、國家的犯罪嫌疑人實現犯罪環節間的互相配合，實現了異地詐騙、遙控指揮和異地支付的高效統一[4]。

三、跨境電信詐騙犯罪的打擊難點

（一）跨境取證難度大

目前在取證過程中，公安機關加強了技術手段的應用，總的來看，取證渠道進一步拓寬，取證效果較之前有顯著改善。通過資訊技術手段對電信詐騙犯罪進行追蹤和偵破，利用大數據分析、網絡追蹤等技術手段，獲取了很多證據，也成功偵破多起案件。但是，在進一步打擊跨境電信詐騙犯罪的過程中，取證方面仍然凸顯出一些亟需解決的問題。

首先，由於跨境電信詐騙犯罪的虛擬性所導致的犯罪嫌疑人在實施詐騙犯罪的過程中自然形成了人員流、資訊流、資金流、網絡流、通訊流[5]等不同類別的涉案電子數據，而這些多樣化、多形式的電子數據給公安機關取證造成諸多困難。以洗錢環節為例，由於犯罪嫌疑人最關心如何將犯罪所得收益“安全合法”地裝入自己的口袋，為了逃避公安機關的打擊，犯罪嫌疑人往往不直接取現，會使用協力廠商支付平台、虛擬貨幣交易平台、地下錢莊等多種方式實現資金多次流轉，以模糊資金流向。而在實際的偵查中，這些平台提供的證據往往無法說明贓款去向，沒有證明力度。涉案資金在短時間內跨域跨國的多次轉移，會形成成千上萬條資金轉帳記錄，導致對證據追蹤偵查困難重重，難以在短時間內釐清資金流向。

其次，各國證據制度不同，導致取證障礙。國界為犯罪嫌疑人提供了天然庇護，致使偵查人員在跨境取證的過程中面臨諸多挑戰。一方面，在沒有法律特定授權的情況下，我國公安機關原則上無權在境外收集和提取證據，需要通過國際警務合作來進行有關證據的收集[6]。在國際法框架內，基於國際公約中的司法協助條款取證、基於國家間簽署的司法協助協議取證、基於互惠原則取證、基於司法協助函取證、基於雙多邊警務合作是五種典型的跨境數據調取形式[7]，但在合作的過程中雙方均出現手續繁多、耗時較長，導致效率低下的狀況。如以美國協助取證為例，倘若他國偵查機關通過刑事司法協助程序獲取谷歌公司存儲於美國境內的電子數據，通常需耗費 10 個月甚至更長時間[8]。與此同時，國內公安機關也需根據規定層層上報，

[2] 王智：〈跨境電信網絡詐騙犯罪治理研究〉，《雲南財經大學碩士學位論文》，2023 年，第 18 頁。

[3] 參見陳某某、黎開強等詐騙犯罪案，湖南省新化縣人民法院 (2021) 湘 1322 刑初 589 號刑事判決書。

[4] 馬小琴：〈跨境電信詐騙犯罪偵查研究〉，《中南財經政法大學碩士學位論文》，2021 年，第 12 頁。

[5] 李雙其、褚紅雲、陳雁：〈電信網絡詐騙犯罪偵查特性論〉，《公安研究》，2023 年，第 7 期，第 21 頁。

[6] 劉道前：〈打擊跨境電信詐騙國際警務合作的問題與對策〉，《犯罪研究》，2019 年，第 6 期，第 53 頁。

[7] 洪延青：〈“法律戰”旋渦中的執法跨境調取數據：以美國、歐盟和中國為例〉，《環球法律評論》，2021 年，第 1 期，第 39 頁。

[8] 梁坤：〈基於數據主權的國家刑事取證管轄模式〉，《法學研究》，2019 年，第 2 期，第 191 頁。

需要耗費一定的週期。鑑於電子證據易銷毀、篡改的特點，在取證的時間差中，犯罪嫌疑人很有可能已將相關證據毀滅。此外，在刑事司法協助程序中，請求國司法機關在取證階段很難對協助國司法機關的取證過程進行監督與規範，而且無權行使管轄權[9]。一旦協助國司法機關在取證過程中存在操作不規範等問題，相應證據可能會面臨被排除的風險[10]。另一方面，目前各國的取證標準各異，並未統一，證據的固定、提取往往受制於各國的取證技術與取證規則，證據異國轉換及證據規格差異問題無疑增加了取證的難度，這將極大影響到跨境電信詐騙犯罪證據的調取與轉化。以搜查的規定為例，有的國家需要法官授權才可進行搜查，只有在緊急情況下偵查機關不立即採取搜查措施可能延誤偵查的情況下才可以由警察進行搜查，並且沒有無證搜查的規定[11]。根據我國的規定，搜查並不需要法官授權。

（二）犯罪成員隱匿難尋，犯罪集團摧毀受阻

跨境電信詐騙犯罪的顯著特徵就是犯罪行為突破地域的限制，許多案件的伺服器在國外，犯罪嫌疑人分佈在不同的地域和國家，僅僅通過電信網絡、銀行網絡等高科技載體，就實現了坐收境內漁利[12]。鑑於公安機關在境外無執法權，跨境、跨區域致使公安機關不能像在國內一樣鎖定嫌疑人大致落腳點範圍後迅速開展進一步的抓捕和偵查行動，雖然目前我國陸續與犯罪集團常隱藏的東南亞國家進行國際警務合作，但由於各國政治體制、法律制度、司法解釋等方面與我國存在差異，深度合作仍存在障礙，目前由於跨境電信詐騙犯罪的跨國特徵而導致的諸如境外無執法權等一系列問題仍是境外抓捕犯罪嫌疑人的痛點。與此同時，被害人與犯罪嫌疑人全程無接觸性、網絡身份的虛擬化都增強了犯罪嫌疑人的隱蔽性。犯罪嫌疑人通過生活、工作機隔絕，通過黑灰產業鏈非法購買他人名下的支付帳號、社交帳號、通訊帳號等手段，使資金流、通訊流裡面的註冊者個人信息無法關聯到真實的犯罪嫌疑人[13]，導致犯罪嫌疑人蹤跡難以尋覓。此外，犯罪嫌疑人利用互聯網技術，運用虛擬 IP 位址、浮動 IP 等方式隱匿自身真實信息，導致偵查人員很難確定犯罪嫌疑人的真實作案地點；而且基於電子資料易於篡改、銷毀的特徵，待犯罪完成後犯罪嫌疑人可輕鬆清除犯罪痕跡。

此外，犯罪團夥組織結構層次化、內部分工的系統化以及公司化的運營結構使各個犯罪環節的犯罪嫌疑人互不認識，犯罪嫌疑人之間單線聯繫，主要犯罪成員更是隱匿幕後，身份難以確定。即使抓住一些犯罪嫌疑人，由於他們是非骨幹成員，掌握犯罪線索較少，不能幫助偵查人員有力拓展偵查線索和關聯其他犯罪嫌疑人。再者，犯罪嫌疑人“物化”屬性明顯，可替代性較強，尤其是犯罪結構最底層犯罪嫌疑人的缺失並不影響犯罪集團的正常運轉。如從事撥詐騙電話、發送詐騙信息、取現等技術含量較低的犯罪團夥成員，其自願加入或被迫受控於犯罪組織後，只需要按照既定腳本，扮演給定角色，執行設定動作，完成一定任務即可[14]。當位於犯罪鏈底層的犯罪嫌疑人被抓後，在招攬成員後很快可以重建恢復運營，繼續犯罪。是以在未抓獲犯罪頭目和骨幹成員的情況下，公安機關無法一舉摧毀犯罪集團。

（三）黑灰產全鏈賦能犯罪，犯罪打擊難度升級

隨着資訊技術的發展，黑灰產業鏈不斷反覆運算升級，逐漸形成完整成熟的產業鏈條。網絡黑灰產業鏈線上線下、境內境外圍繞着宣傳推廣、犯罪所需物料供應、技術支撐、資金結算這四部分持續為跨境電信詐騙犯罪“輸血供糧”，與跨境電信詐騙犯罪集團相伴相生，共同形成了複雜冗長的跨境電信詐騙犯罪鏈條[15]。具體而言，目前的黑灰產業鏈總體可分為四個方面：人員、信息、技術、資金四部分。其中，人員模組主要組織運送他人通過偷越國（邊）境或其他方式赴境外從事電信網絡詐騙犯罪；信息模組主要為犯罪集團提供精準公民個人信息、電腦信息系統數據等，以設計詐騙話術實施精準詐騙；技術模組涉及提供平台、軟體、工具等

[9] 王玫黎、楊逸瓊：〈刑事司法協助所獲“境外證據”如何適用〉，《檢察日報》，2021 年 4 月 6 日，第 3 版。

[10] 姚浩亮：〈論跨境電信網絡詐騙犯罪的電子取證〉，《湖南警察學院學報》，2023 年，第 4 期，第 80 頁。

[11] 同註 6，第 54 頁。

[12] 秦帥、陳剛：〈近年來電信詐騙案件偵查研究綜述〉，《公安學刊（浙江警察學院學報）》，2015 年，第 3 期，第 39 頁。

[13] 王曉偉、趙照：〈電信網絡詐騙犯罪人員流的構成與偵查方法研究〉，《中國人民公安大學學報（社會科學版）》，2022 年，第 4 期，第 55 頁。

[14] 羅威麗：〈電信網絡詐騙犯罪成因分析及關鍵要素識別〉，《河南警察學院學報》，2024 年，第 1 期，第 35 頁。

[15] 王曉偉：〈海峽兩岸合作打擊跨境電信詐騙犯罪研究〉，《中國人民公安大學學報（社會科學版）》，2021 年，第 2 期，第 74 頁。

技術支援，如非法提供用於犯罪活動的“貓池”、GOIP 設備、多卡寶等硬體設備，加大了反制攔截和信號溯源的難度，提高詐騙行為的隱蔽性和欺騙性；資金模組主要為犯罪集團提供詐騙所得資金結算和清洗服務，包括支付渠道、跑分平台、地下錢莊、虛擬貨幣交易平台等，為詐騙犯罪所得提供“洗白”渠道，以逃避金融監管和偵查調查[16]。黑灰產業鏈為跨境電信詐騙犯罪集團提供了一條龍式的全覆蓋服務，從犯罪準備階段的各種物料資源，到犯罪實施階段的以開發定制犯罪工具為代表的技術支援，再到犯罪完成後的犯罪收益洗白變現，參與到了跨境電信詐騙犯罪的各個環節，為其不斷更新犯罪工具、輸送豐富的犯罪資源，對跨境電信詐騙犯罪的迅速蔓延起到了重要支撐作用。此外，隨着公安機關的嚴厲打擊，黑灰產業鏈針對公安機關的打擊措施不斷衍生出新的犯罪工具和手段，為跨境電信詐騙犯罪手段翻新升級提供了有力支撐，目前已經發展為利用個人信息和人工智能技術的精準化詐騙。如犯罪嫌疑人通過黑灰產業鏈事先獲取被害人的面部特徵和身份信息，然後利用 AI 換臉技術冒充被害人騙取被害人親人或朋友的信任，進而實施詐騙行為。

四、打擊跨境電信詐騙犯罪的有效路徑

（一）深度拓展國際警務合作

國際警務合作已成為有效打擊跨國電信詐騙犯罪的共識，各國之間的合作越來越緊密。為了有效提高打擊跨國電信詐騙犯罪的效率，應當進一步加深國際警務合作，打通國際警務合作的銜接關口，提升合作效能。

1. 完善跨境電子數據取證機制，提高取證效率

基於跨境電信詐騙犯罪的虛擬性特徵，其證據形式主要是電子數據。為解決跨國電信詐騙犯罪取證的諸多難題，建議進一步完善跨境電信詐騙犯罪電子取證機制以暢通協作渠道，解決取證困境。首先，各國應通過溝通協商，精簡取證流程，提高取證效率。在司法實踐中，證據收集和審查雙方需要根據本國不同的法律規定進行合作，往往需要由法院、檢察院、公安部、外交部等多部門層層審報和審批，最後才可以進行取證。鑑於電子數據易毀滅的特徵、實物證據也易被犯罪嫌疑人銷毀的實際情況，取證程序繁瑣、流轉時間過長可能會導致犯罪窩點的轉移、相關證據的滅失，我國應與犯罪地所在國家積極溝通，堅持互惠原則，暢通取證渠道。如在取證過程中，經評估不涉及國家安全和外交風險的涉案數據信息，建議直接由相關執法部門提取使用，鼓勵數據依法自由流轉[17]，從而使取證更加高效化。其次，各國應加強溝通，就取證原則、方法、制度等方面形成合意，統一標準。各國取證原則、制度的差異是導致跨境取證的重要障礙之一，統一標準可減少因取證制度不同而產生的爭議，而且可以簡化取證流程，極大的提高取證效率。最後，建立聯合取證機制，提高證據的轉化利用率。由於各國法律和外交制度上的差異，導致在跨境取證的過程會出現很多問題：如請求國委託被請求國主管機關代為提取證據的過程中，由於取證技術、取證程序的不同很有可能導致後續證據存在瑕疵或被認定為不合法，而地域的遠距離、證據的易滅失、跨境取證程序繁瑣決定了公安機關很難進行二次取證，因此，建議請求國人員和被請求國人員聯合取證，請求國人員參與調查取證便於證據的提取固定，儘可能減少由於取證制度、程序不同而導致的涉案電子數據的棄用率，增加了證據的有效利用度。

2. 妥善解決刑事管轄衝突，有力打擊犯罪成員

對於跨境電信詐騙犯罪嫌疑人抓捕難、收網難所造成的管轄權爭議問題，各國應秉持平等互惠原則，通過深度溝通尋求合理的解決方法。在不違反國家主權原則，並保證不侵害他國主權的前提下，合理擴大警務合作的範圍，以更好地解決犯罪嫌疑人抓捕、運送回國內的難題。如，基於引渡條件比較嚴格複雜，可以通過雙方合作積極尋求引渡的替代性措施。在不損害主權的前提下，通過協商探討，作出一定程度的變通、讓步、妥協和承諾，協商通過遣返非法移民、驅逐出境等方式實現對犯罪嫌疑人的境外抓捕或羈押，剝奪其在該國的居留權，為將其順利遣返創造可能性和必要的條件[18]。此外，也可通過簡易引渡的方式，簡

[16] 同註 1。

[17] 張傑：〈中國與東南亞合作應對電信網絡詐騙犯罪策略優化：結構性錯位與現代化融合〉，《東南亞縱橫》，2024 年，第 1 期，第 53 頁。

[18] 夏凱：〈論打擊跨境電信詐騙犯罪的國際刑事司法合作——以“9.27”跨境電信詐騙案為例〉，《華中師範大學碩士學位論文》，2017 年，第 31 頁。

化引渡程序，縮短將犯罪嫌疑人移交回國的時間，提高引渡合作效率，以破解因各國地域和法律制度不同而造成的犯罪嫌疑人抓捕障礙，實現對境外犯罪嫌疑人的有力打擊。

（二）利用信息技術助力精準打擊犯罪

針對跨境電信詐騙犯罪因智能化、虛擬化特徵突出而產生的取證難度大、犯罪嫌疑人追蹤難等打擊困境，公安機關必須堅持科技強警，提升信息技術在偵查中的融入度，以更好地遏制犯罪。

1. 綜合運用技術反制措施提高取證效質

目前偵查實踐中為了打擊跨境電信詐騙犯罪已經實施了一些技術反制措施，並在及時制止犯罪、預防被騙取得了顯著成果。如反詐平台的前期研判功能、對涉詐資金的攔截功能在犯罪預警和制止正在發生的跨境電信詐騙犯罪方面具有突出的貢獻，但是對於已發案件的偵查取證方面仍存在明顯短板。鑑於此，公安機關應進一步綜合運用多種技術反制手段，通過科技賦能提高取證品質。首先，基於跨境電信詐騙犯罪虛擬性而產生的人員流、資訊流、資金流、通訊流具有顯著特徵的分類涉案資料，可構建基於多類證據融合的詐騙犯罪行為的證據鏈條，先利用不同技術方法分別收集人員流、資訊流、資金流、通訊流四類涉案數據，如可通過資金追蹤法、軌跡碰撞法、設備關聯法、網絡滲透法等來收集人員流數據[19]。然後對收集來的人員流、資訊流、資金流、通訊流四類涉案數據進行進一步分類整理，釐清證據之間的關聯和在證實犯罪事實中的邏輯關係，結合跨境電信詐騙犯罪引流推廣、與被害人建立聯繫、引誘被害人進行虛假投資、處理犯罪所得等犯罪流程，多方面、綜合證明犯罪嫌疑人的犯罪行為。其次，充分利用大數據偵查手段，一方面大量收集涉案數據信息，並利用大數據技術自動篩選出有效信息，減輕偵查人員的工作負擔；另一方面，根據前期篩選出的犯罪嫌疑人的行蹤記錄、出入境軌跡、聊天記錄等涉案數據信息，同時通過總結跨境電信詐騙犯罪的案件特點搭建數據信息關聯模型，綜合運用數據比對、數據碰撞、數據研判等手段，關聯案件信息，挖掘犯罪線索，夯實證據基礎，完善證據鏈條。最後，基於跨境電信詐騙犯罪借助科技力量而形成的犯罪手段智能化、精準化的特徵，公安機關應當改變事後偵查的被動局面，一方面，與時俱進，加強對當下多種新興技術的深入學習，深化這些技術在打擊電信詐騙方面的應用，提升打擊犯罪能力。如除了大數據技術之外，研究學習聲紋識別技術、自然語言處理技術等新技術，提升偵查人員的知識與技術儲備，以在未來更好、更有效地應對不斷轉型升級的跨境電信詐騙犯罪。另一方面，加強對新技術的前瞻性預防，盡可能消除技術用於犯罪的風險。針對當下出現的新技術，應及時對新技術進行應用評估，根據新技術的特點、應用場景等科學研判其應用於犯罪中的風險，並根據風險特徵制定完善的約束措施和應對方案，切實降低新技術被犯罪分子利用的可能性[20]。

2. 利用技術手段鎖定犯罪嫌疑人真實身份

跨境電信詐騙犯罪嫌疑人利用先進的互聯網技術實施犯罪，全程與被害人無接觸，導致犯罪嫌疑人難以追蹤。公安機關可充分利用大數據偵查技術手段確認犯罪嫌疑真實身份。首先偵查人員可以通過 IP 信息分析法、交易數據關聯法、設備信息關聯法等方法來確認犯罪嫌疑人身份。如由於網絡登入日誌記錄一般是帳號使用人的真實信息，這是確認犯罪嫌疑人當時位置的一個數據參照，可通過對涉案帳戶的 IP 信息進行溯源和研判，進而發現犯罪嫌疑人的具體和身份。與此同時，通過相同 IP 信息下的其他資訊的碰撞分析[21]，可進一步搜集更多的犯罪線索。此外，通過對電話即時定位、網絡即時追蹤，解決因任意顯號而無法追蹤真實來源的難題，快速鎖定犯罪嫌疑人身份。再者，犯罪嫌疑人不可能脫離社會環境而存在，公安機關可以通過數據獲取、數據碰撞數據比對等多種手段關聯、挖掘犯罪嫌疑人日常生活的涉網資訊，從而獲取犯罪嫌疑人的真實身份，如犯罪嫌疑人的網購信息、外賣信息、出行信息、社交信息等等。例如，可從社交信息入手刺破犯罪嫌疑人的偽裝面紗，在犯罪過程中，犯罪嫌疑人通常以 QQ、微信等社交工具作為聯繫

[19] 同註 13，第 62 頁。

[20] 賈國偉、崔紀鵬、王順兵等：〈科技助力反電信網絡詐騙對策研究〉，《山東警察學院學報》，2022 年，第 2 期，第 130 頁。

[21] 王曉偉：〈電信網絡詐騙犯罪信息流偵查方法探析〉，《人民論壇·學術前沿》，2022 年，第 15 期，第 95 頁。

被害人的重要媒介，出於隱匿身份的目的，這些社交工具的註冊信息往往是虛假的，但根據心理學規律，社交工具的頭像、昵稱、個人簽名等信息往往能反映出使用者真實的個人偏好和性格特徵，並且具有一定的穩定性。換句話說，犯罪嫌疑人很有可能在日常個人社交工具中使用相同的頭像、昵稱、個人簽名。偵查人員可利用這些個人信息去篩查出犯罪嫌疑人日常社交所用的 QQ、微信號，從而識別犯罪嫌疑人的真實身份。

（三）實施全鏈條打擊策略

跨境電信詐騙犯罪的發展壯大不僅源於犯罪集團的專業化、產業化、日趨壟斷化，更得益於圍繞在詐騙犯罪集團周圍的黑灰產業鏈源源不斷地為其輸送犯罪資源。因此，必須實施全鏈條打擊策略，徹底剷除犯罪滋生土壤。

1. 進一步加強對頭目、骨幹成員的打擊

鑑於跨境電信詐騙犯罪集團組織化程度高，已形成較為成熟的公司化運營的犯罪模式，位於犯罪集團中底層的犯罪嫌疑人物化特徵、可替代特徵明顯，對其打擊並不能起到重創犯罪集團的效果，而跨境電信詐騙犯罪中的頭目和骨幹成員對於犯罪集團的形成和發展起着重要的統帥作用，因此，若想摧毀跨境電信詐騙犯罪集團，必須重點打擊頭目和骨幹成員。一方面，可通過專項行動實現對頭目和骨幹成員有力打擊。之前公安部開展的“斷流”行動在打擊電信詐騙頭目和骨幹成員方面取得了一定成效，對於跨境電信詐騙犯罪具有一定的遏制作用，但已經抓獲的電信詐騙分子只是冰山一角，仍有大量頭目和骨幹成員逍遙法外。鑑於此，必須繼續深入開展專項行動，全面梳理潛逃境外的頭目和骨幹成員，利用軌跡碰撞、數據關聯等多種偵查手段，落實頭目和骨幹成員的位置，組織開展專項緝捕行動，全力擠壓犯罪團夥的生存空間。另一方面，通過加強國際警務合作破除頭目、骨幹成員在國外逍遙法外的難題。一些跨境電信詐騙犯罪集團的頭目、骨幹成員利用國界的天然庇護和各國制度不同的優勢，龜縮在國外，難以實現對其的抓捕和懲治。通過深化犯罪成員引渡、遣送等方面的合作，暢通將犯罪集團頭目、骨幹成員運送回國的渠道，使其接受法律的審判，承擔相應的刑事處罰，從而實現對跨境電信詐騙犯罪集團的有效瓦解。

2. 斬斷涉詐黑灰產業鏈條

跨境電信詐騙犯罪中，犯罪集團往往依託黑灰產業鏈為其提供必要的作案工具、技術支援等犯罪資源，因此若想實現對跨境電信詐騙犯罪的有效打擊，必須斬斷對犯罪起着重要支撐作用的黑灰產業鏈，可通過事前預防、事中偵查反制、事後聯合治理對黑灰產業鏈實施全鏈條打擊。首先，可通過事前預防手段遏制黑灰產業鏈形成。針對黑灰產業鏈中對跨境電信詐騙犯罪形成發展有重要影響，諸如組織運送他人通過偷越國（邊）境、非法獲取公民個人信息等行為，利用技術研判此類行為，並設置疑似行為預警，通過及時預警將其遏制在萌芽階段，從源頭堵住黑灰產業鏈的犯罪資源獲取渠道。其次，可綜合運用各種技術反制手段強力打擊黑灰產業鏈。黑灰產業鏈中的技術支援為跨境電信詐騙犯罪的精準化、犯罪嫌疑人身份的隱匿化提供了重要支撐，因此，公安機關應將科技最新成果用於技術反制能力提升，不斷研究與犯罪相對應的對抗技術和反制手段。例如，針對非法獲取公民個人信息甚至是人臉、聲紋等敏感信息的行為，可運用多種個人隱私保護技術手段提升公民個人信息保護程度，儘可能降低個人隱私用於犯罪的可能性。此外，在非法獲取公民個人信息基礎上的利用 AI 等前沿技術偽造人臉、聲紋的詐騙行為，應深化大數據、人工智能等新技術在打擊跨境電信詐騙犯罪中的運用，加強對深度偽造音視頻的識別與防範研究，以增強對詐騙手段的識別能力[22]。最後，鑑於黑灰產業鏈中的上、中、下游涉及多部門、多行業，公安機關要協同法院、檢察院、電信、銀行、相關企業等多方協同治理，切實增強打擊實效。如電信網絡供應商應加強監管，擠壓黑灰產業鏈“物料”資訊獲取空間，高新技術企業研發新技術成果的同時應加強對新技術的評估，減少新技術濫用的風險，同時相關管理部門應通過嚴格監管和相關制度制定倒逼涉黑灰產企業、行業合法經營。總之，通過多方聯動，形成對黑灰產業鏈的全鏈條打擊和治理。

[22] 同註 20。