

電信網絡詐騙犯罪的演變分析與防控措施

牛驚雷、王豔紅^{*}

摘要：打擊防範電信網絡詐騙犯罪是一項長期工作，電信網絡詐騙活動不會隨着緬北電詐園區的瓦解而收斂，反而詐騙行為會借助新的技術手段形成新的演化。建立有效的防控體系，推動社會共治對於保障人民安居樂業，增強人民群眾獲得感、幸福感、安全感極為重要。電信網絡詐騙犯罪防控體系的建設要以電信網絡詐騙犯罪行為的底層邏輯為目標，根據電信網絡詐騙犯罪信息不對稱的運行機理，從信息不對稱產生的環節入手，全面揭示信息不對稱產生根源，由此構建有針對性的防控措施，才能有效提高反詐成效。

關鍵詞：電信網絡詐騙犯罪 防控 信息不對稱 演變

Analysis of the Evolution of Telecom Network Fraud Crimes and Prevention and Control Measures

Niu Jinglei; Wang Yanhong

Abstract: Combating and preventing telecom network fraud crimes is a long-term task. Telecom network fraud activities do not diminish with the collapse of the telecom fraud park in northern Myanmar; instead, fraud activities evolve through the adoption of new technological means. Establishing an effective prevention and control system and promoting social co-governance are crucial for ensuring people's well-being and enhancing their sense of gain, happiness, and security. The construction of a prevention and control system for telecom network fraud crimes should target the underlying logic of these crimes. Through the operational mechanism of information asymmetry in telecom network fraud crimes and identifying their root causes from the links where information asymmetry arises, targeted prevention and control measures can be developed to significantly improve anti-fraud effectiveness.

Keywords: Telecom Network Fraud Crimes; Prevention and Control; Information Asymmetry; Evolution

* 牛驚雷，中國人民警察大學偵查學院副教授、中國人民警察大學新型犯罪防控研究中心研究員，博士。研究方向：公共管理與社會治理。
* 王豔紅，中國人民警察大學偵查學院副教授、中國人民警察大學新型犯罪防控研究中心研究員，碩士。研究方向：經濟犯罪偵查。

一、前言

面對日益氾濫的電信網絡詐騙，我國公安部會同最高法、最高檢、工信部、人民銀行和三大運營商持續開展“斷卡”、“雲劍”、“長城”等專項行動，對電信網絡詐騙犯罪始終保持依法嚴打嚴懲的高壓態勢，極大地震懾犯罪，電信網絡詐騙立案數已從 2021 年至 2023 年連續同比下降。同時，隨着中國、緬甸和泰國聯合打擊跨國電信網絡詐騙犯罪，盤踞在緬北地區的明家、白家和劉家等各類詐騙集團被一舉搗毀，一大批重大犯罪嫌疑人被押解回國，境外詐騙團夥的生存空間受到有力擠壓，電信網絡詐騙犯罪上升勢頭得到遏制。緬北電詐園區的瓦解並不意味着世間不再有“電詐”，電信網絡詐騙依舊會存在，而且會不斷演化新的詐騙手段繼續施詐，電信網絡詐騙犯罪的打擊防範工作是持久戰。

二、電信網絡詐騙的演化分析

目前，眾多電信網絡詐騙團夥都窩藏在境外，國際合作又受到不同國家社會制度和不同法域等因素制約，使得打擊跨國有組織犯罪難以有效及時實施。在嚴厲打擊電信網絡詐騙犯罪的同時，做好廣大群眾的防範工作，提高防詐意識愈發重要。為此，全面分析電信網絡詐騙的演化過程，揭示其本質則是做好群眾防控措施的基本前提。

(一) 電信網絡詐騙犯罪本質

《中華人民共和國刑法》第 266 條規定：詐騙罪是指以非法佔有為目的，用虛構事實或者隱瞞真相的方法，騙取數額較大的公私財物的行為。電信網絡詐騙犯罪目前並沒有獨立的罪名，在司法實踐中被廣泛運用，其具體的定義主要是突出了犯罪的技術手段和犯罪行為特徵，即《反電信網絡詐騙法》第 2 條規定：以非法佔有為目的，利用電信網絡技術手段，通過遠端、非接觸等方式，詐騙公私財物的行為。所以說，電信網絡詐騙犯罪本質依舊是詐騙。無論是傳統詐騙還是電信網絡詐騙，詐騙的實質沒變，都是通過傳遞虛假信息，獲取受害人的信任，使用欺詐方法騙取數額較大的公私財物，變化的是犯罪行為特點。

(二) 傳統詐騙犯罪與電信網絡詐騙犯罪的關聯

1. 犯罪行為實施由線下特定空域轉化為線上虛擬空間

傳統詐騙犯罪一般是線下實施犯罪行為，多表現為街頭詐騙，即發生在街面或商業場所等人員流動空間。所以，傳統詐騙是多對一的詐騙行為，即多個犯罪分子形成團夥，分工明確，直接面對受害者進行點對點的欺騙活動。線下實施詐騙犯罪自然決定了詐騙犯罪呈現流竄作案，犯罪行蹤不定的特點。而電信網絡詐騙犯罪利用電信網絡技術突破了時間、空間限制，在網絡空間實施非接觸性詐騙活動。一方面，非接觸性詐騙無需面對受害者被騙的慘況，不用體會被騙的痛苦，大大削弱了犯罪分子的犯罪畏懼心態；另一方面，為逃避打擊，大批詐騙集團將窩點轉移至境外，形成境內一些上游環節團夥相互勾連的犯罪鏈組織形式。

2. 詐騙犯罪侵害的對象更加精準

傳統詐騙犯罪主要發生在街頭和商業場所，受害人的出現存在一定的偶然性。詐騙分子也需要根據騙術要求對受害人進行初步的篩選，其過程是詐騙分子依據接觸獲取的周邊信息，依靠個人多年詐騙的識人經驗，並造成與受害人“偶遇”場景。電信網絡詐騙犯罪則是精心選擇詐騙對象。一是通過“信號篩選”模式精準鎖定受害人，即詐騙分子利用詐騙“劇本”，採取大面積群發信息，從海量中選擇回應者。因為信息接受者沒有回應，基本上屬於被識破的情形，騙局結束。若有回應，說明回應者屬於可以進一步誘騙，就會產生第二次信息發送，直至回應者逐漸引入騙局成為受害者。^[1] 二是通過非法手段獲取的個人信息，從中精挑細選出滿足詐騙要求的合適對象，進行針對性的騙局腳本設計和話術溝通。例如，“殺豬盤”詐騙根據女性受害者的實際情況和性格，通過精心設計的“劇本”和沉浸式的溝通，誘導女性受害者從好奇和心動逐步發展成網戀關係或是建立起信任關係，一步步陷入騙局。^[2]

[1] 牛驚雷、付立柱：〈基於信任生成機理的電信網絡詐騙防控措施研究〉，《河南警察學院學報》，2023 年，第 6 期，第 37–45 頁。

[2] 牛驚雷、付立柱：〈女性受害者視角下“殺豬盤”詐騙中信任關係的形成分析〉，《中國人民警察大學學報》，2023 年，第 2 期，第 5–10 頁。

3. 犯罪行為內容發生迭代

詐騙犯罪主要是通過虛構的事實或隱瞞真相的欺騙方法，誤導或誘騙受害人生信，產生錯誤決策，“自願地”將財物交給行騙人或行騙人指定的第三人的行為。傳統詐騙主要實施的犯罪活動包括有利用假冒貴重物品兜售行騙、利用非法外匯交易行騙、利用在國際上不能流通的貨幣行騙、利用“拾金平分”行騙等。^[3]在詐騙過程中主要利用受害人的好心、恐懼和貪心，借助假幣、假寶物等道具和行騙者高超障眼技法，編造虛假事實或隱瞞真相，加上其他團夥人員的配合烘托，誘導受害人被騙。例如，易開罐中獎詐騙是由一夥詐騙分子通過做過手腳的易開罐拉環，在某特定場所製造“中大獎”的事實，團夥在旁邊做托相互配合欺騙受害者花錢買下“中獎拉環”。

犯罪行為存在繼承性。電信網絡詐騙犯罪不斷地升級犯罪手法。目前電信網絡詐騙主要根據詐騙對象情況和性格，分別採取“殺豬盤”詐騙、虛假投資理財詐騙、貸款詐騙、刷單詐騙、註銷“校園貸”詐騙、網絡遊戲虛假交易、冒充“公檢法”詐騙、冒充電商物流客服詐騙等詐騙手法。詐騙內容則緊跟社會熱點問題，時刻保持“與時俱進”變化更新。實施詐騙的工具升級為群發軟體，虛假理財軟體、銀行卡、帳戶和GOIP等設備，運用了更為先進的技術，包括區塊鏈、虛擬貨幣、AI智慧等新技術，實現秒撥、VPN、語音、改號呼叫，數位貨幣轉移違法資金，螢幕共用的遠端操控。^[4]例如在“虛假網絡投資理財類詐騙案件”中，詐騙分子通過各種引流方式將受害人拉進各種所謂的投資理財群，群裡其實只有受害人是真正的投資人，其他人包括所謂的理財老師都是詐騙團夥。這種形式的詐騙涉及金融投資方面專業知識，欺騙性更強，不僅損害消費者權益，而且在一定程度上擾亂金融市場秩序。這也意味着電信網絡詐騙犯罪也逐漸向金融詐騙犯罪轉化。

4. 詐騙犯罪組織模式發生變革

傳統詐騙犯罪是組織結構緊湊的結夥犯罪，內部有着結構緊密的組織分工，犯罪行為鏈始終完整，即由犯罪團夥從頭到尾實施完整的詐騙過程，包括詐騙團夥人員招募、詐騙道具購買製作、詐騙內容設計、詐騙過程安排和實施、詐騙錢財分贓和轉移。電信網絡詐騙犯罪則是發生了犯罪組織變革。詐騙團夥內部實現專業分工，組織結構採用金字塔式架構，具體包括“金主”、代理商、管理團隊、人力資源、後勤保障、技術、業務、財務、保安等部門，呈現出多行業支撐、產業化分佈、集團化運作、精細化分工、跨境式佈局等跨國有組織犯罪特徵，^[5]但詐騙犯罪鏈條逐步分化為三個環節，由不同犯罪團夥承擔，進而提升專業化水平。上游有大量卡商、號商將非法獲取的大量銀行帳戶、電話卡、身份證以及U盾售賣給中游的洗錢團夥或者直接銷售給下游詐騙團夥，而大量的料商包括一些行業的內鬼將盜取公民的個人信息轉售給下游詐騙犯罪團夥；中游有設備商、引流團夥、包網服務商、網絡商、洗錢團夥為詐騙集團提供技術服務和非法資金轉移服務的犯罪團夥；下游則是組織實施具體詐騙的詐騙犯罪團夥。上中下三個專業犯罪團夥構成了整個詐騙犯罪鏈條，並在各個環節形成各自專業的黑灰產業鏈。犯罪環節的分段不僅提高了犯罪的專業水平和犯罪鏈條複雜化，而且每個環節上的犯罪分子只參與詐騙犯罪行為的一部分，導致其悖德感明顯降低，會認為“我就是爬取一下資料而已”，“我只是把銀行卡租借出去”。^[6]同時，這也造成涉及的罪名有詐騙罪、幫信罪，以及掩飾、隱瞞犯罪所得、犯罪所得收益罪等，從而加大了偵查的難度。

三、電信網絡詐騙犯罪行為的底層邏輯分析

電信網絡詐騙犯罪的手法和套路是在不斷升級更新，但犯罪行為的底層邏輯並未改變。無論是傳統

[3] 賈克青：〈街頭詐騙犯罪剖析〉，《北京人民警察學院學報》，1999年，第2期，第4-10頁。

[4] 新浪新聞，〈公安部：電信網絡詐騙已超50種，詐騙手法反覆運算加速！〉，發佈日期：2022年4月14日，網址：<https://news.sina.cn/gn/2022-04-14/detail-imcwipii4246003.d.html>，到訪日期：2024年2月10日。

[5] 人民網，〈公安部：電信網絡詐騙犯罪已成為全球性打擊治理難題〉，發佈日期：2022年7月25日，網址：<http://society.people.com.cn/n1/2022/0725/c1008-32484865.html>，到訪日期：2024年2月10日。

[6] 李佳鵬、孫韶華、張莫等：〈花樣翻新，類型不下50種，防範電信網絡詐騙仍需加力〉，《經濟參考報》，2022年3月28日。

詐騙，還是電信網絡詐騙都是通過一定的技術手段，抓住被害人的心靈或是人性弱點，利用信息不對稱的優勢騙取被害人信任，誘騙被害人陷入騙局，錢財被騙。因此，信息不對稱就是詐騙犯罪得以成功的底層邏輯。

(一) 電信網絡詐騙犯罪的信息不對稱現象

信息不對稱理論闡述了在市場交易中，掌握信息充分的一方擁有比較優勢，出於謀取自身更大的利益，造成信息貧乏的一方處於劣勢，利益會受到損害。從定義上看，由於交易主體掌握信息的差異，反映了信息的分佈及其交易狀況的特性，使得信息不對稱理論成為描述和解釋社會經濟活動的重要工具。^[7] 信息不對稱作為電信網絡詐騙犯罪的行為邏輯，形成一個系統過程。^[8] 要揭示這一犯罪行為的底層邏輯的運行機理，必須構建電信網絡詐騙犯罪信息傳遞鏈，分析信息不對稱的生成過程。

1. 電信網絡詐騙犯罪信息傳遞鏈分析

在非接觸式的電信網絡詐騙犯罪中，騙取被害人信任是非常重要的環節。在網絡虛擬世界裡，信息傳遞是信任構建的主要媒介。根據 Spence 的信號理論，詐騙犯罪中詐騙分子與受害者之間信任的形成是一種信息傳遞過程。從信息傳遞的全鏈條過程切入分析，我們構建的電信網絡詐騙犯罪過程中信息傳遞鏈如下(圖1所示)^[9]：

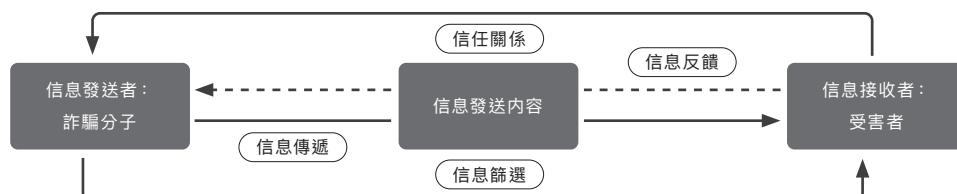


圖1 電信網絡詐騙犯罪信息傳遞鏈

電信網絡詐騙犯罪的整個信息傳遞鏈主要包括三個要素，即信息發送者（詐騙分子）、信息、信息接收者（受害者），構成“信息發送者（詐騙分子）—信息（詐騙劇本）—信息接收者（受害者）—信息反饋（信任）”的信息傳遞鏈邏輯。^[10] 無疑，信息不對稱就是在由詐騙分子發佈詐騙信息，通過電信網絡傳遞信息和受害者接收信息構成的鏈條中生成並運行。

2. 電信網絡詐騙犯罪信息不對稱產生過程分析

信息不對稱主要產生於兩個環節。一是受害人個人信息暴露形成受害人與詐騙分子之間的信息不對稱。作為有預謀的詐騙分子，在實施詐騙之前會做好“功課”，與料商進行黑市資料交易獲取大量的公民個人信息，通過傳遞預先設計的信息，測試、觀察和套取信息接收者的性格特徵，以便篩選出具有容易產生信任性格特徵的信息接受者作為繼續推進詐騙的對象，^[11] 在全面剖析受害者的基礎上，針對不同職業、性格，甚至不同實際需求編造詐騙內容，合理塑造人設，以確保詐騙過程中自己的特長得到最大程度發揮，做到“知己知彼”。這一精心的篩選過程就決定了在詐騙犯罪整個過程中從一開始，受害者就處於信息缺乏的劣勢方。二是詐騙分子在掌握受害者基本情況和相關性格特徵後，作為信息的優勢方，利用專門設置的詐騙內容，完全操控整個詐騙進程。在傳遞詐騙信息的過程中，根據進程設置相應語義情境和虛假內容，加以各種虛假圖片，微小返利等工具配合，利用近似完美的話術引導受害者對其指令生成依賴、緊張、盲從等情況，從而促使受害者陷入錯誤的認知陷阱，做出錯誤決策。

[7] 韓志明：〈跨越信息不對稱的陷阱：國家治理現代化的信息維度〉，《江蘇社會科學》，2024年，第1期，第86–96頁。

[8] 饒贊：〈論詐騙犯罪過程中的信息不對稱〉，《湘潭大學2010年碩士學位論文》，第10頁。

[9] 同註1。

[10] 李輝、王娜：〈警民信任源於何：基於信號傳遞鏈邏輯的解釋〉，《中國人民公安大學學報（社會科學版）》，2020年，第6期，第82–98頁。

[11] 同註1。

反觀受害者由於自身因素，對一些詐騙內容所涉及的情況不了解，例如：不了解網上購物退款客服流程、公安辦理各類案件規定、銀行借貸具體要求等社會行業基本工作標準流程，從而對電信網絡當中的“公安民警”、“檢察官”、“購物平台客服”、“貸款公司高管”等虛構人物的深信不疑。在信息掌握完全不對等的情況下，受害者陷入詐騙是自然的。

(二) 電信網絡詐騙犯罪信息不對稱產生根源分析

1. 公民個人信息洩露和侵犯個人信息是信息不對稱生成的首要原因

公民個人信息的洩露和侵犯一般集中在通信、銀行、保險、房產、酒店、物業、物流等行業領域。這些行業領域管理不善，存在着大量的“內鬼”為了個人利益，售賣公民個人信息。2021年全國公安機關抓獲行業內部人員680餘名，全國檢察機關起訴侵犯公民個人信息的行業“內鬼”500餘名。^[12]2021年侵犯公民個人信息十大典型案例顯示侵犯公民個人信息的手段主要有利用外掛程式、木馬釣魚病毒等技術竊取使用者手機信息、上網標籤、註冊遊戲帳號、快遞信息販賣給詐騙團夥。^[13]

2. 傳遞的詐騙內容是信息不對稱生成的關鍵原因

詐騙內容之所以能夠矇騙受害人主要原因，在於詐騙內容是詐騙分子精心打造的有針對性的話術和劇本。有些內容是根據國家社會經濟戰略發展規劃精心創作，緊貼社會生活的熱點問題，例如，“萬眾創業”、“地攤經濟”、“碳中和”、“養老經濟”和“數字貨幣”等，從而具有較強的迷惑性；有些內容具有行業特點，對於受害者來說相對陌生，甚至神秘。例如，不清楚網絡購物退款流程，受害者在無意識狀態下將個人帳戶驗證碼提供給虛假的“平台客服”；在“冒充公檢法詐騙”中，受害者不了解政法部門日常對外業務，加上出於對公共權威的敬畏，對冒充公檢法幹部的詐騙分子所下達的指令深信不疑，毫不懷疑地按照要求，將自己“涉案”帳戶裡的資金轉入所謂的“安全帳戶”進行安全審查和隔離保護。^[14]而且詐騙內容都是來源於生活，有其真實的一面。這也是受害者深信不疑的原因，但關鍵的是這些內容對於受害者來說，由於不熟悉而缺乏正確認識，處於特定場景中，信息不對稱的劣勢促使受害者在短時間內極易做出錯誤決定。

3. 傳遞技術為信息不對稱的生成提供了保障

一是詐騙分子塑造各種符合詐騙內容的虛假身份。有滿足面孔可信度^[15]的“白富美”、“高富帥”；有容易產生信任的具有較高社會地位、能力特質突出“成功人士”、有身穿制服，手持證件的“公檢法人員”。為了進一步佐證詐騙分子虛構身份的真實，詐騙分子還加以各種伎倆提升行為可信度，^[16]推進受害者生成錯誤認知。例如，利用受害者嘗試性地小投資，獲得較高回報來驗證詐騙分子所具有的特質能力：有不一般的社會關係、在大數據處理方面的超人技能，或掌握某些博彩網站的漏洞，從而增加受害者對詐騙分子身份的信任。

二是營造特殊語境擴大受害者性格弱點，加大受害者信息不對稱的劣勢。一方面，在信息傳遞過程中，詐騙分子通常是以敘事性方式講授個人經歷，以拉近與受害者之間的距離，產生共鳴且形成情感建構的效應，^[17]從而加強對詐騙分子的信任。另一方面，製造緊急情境加劇受害者緊張情緒。詐騙分子會安排製造一系列緊急情況，例如告知受害者“帳戶涉嫌洗錢”、“行為違規影響個人誠信”，同時配置虛假網絡頁面、假通緝令等圖片，再通

[12] 靳高風、張雍錦、郭兆軒：〈2021—2022年中國犯罪形勢分析與預測〉，《中國人民公安大學學報（社會科學版）》，2022年，第2期，第1—12頁。

[13] 中華人民共和國最高檢察院，〈檢察機關全鏈條懲治電信網絡詐騙犯罪 2021年起訴 4 萬人〉，發佈日期：2022年3月2日，網址：https://www.spp.gov.cn/spp/xwfbh/wsfbh/202203/t20220302_546333.shtml，到訪日期：2023年2月27日。

[14] 同註1。

[15] 可信度 (trustworthiness) 指被信任方可以被信任或者依賴的程度。可信度作為被信任方自身特質直接影響雙方信任關係的建立。可信度分為面孔可信度和行為可信度兩種類型。

[16] 行為可信度指由被信任方的行為特徵所決定的其自身可以被信賴的程度，如通過信任雙方的直接交往或是通過其他渠道得知的有關個體日常行為中表現出的善良、正直等相關的行為信息。引用 Zucker, L. G. Production of trust: Institutional sources of economic structure, 1840–1920[J]. *Research in Organizational Behavior*, 1986, 8(2):53–111. 參見梅晶：〈面孔可信度對信任行為的預測：一般信任傾向的調節作用〉，《浙江師範大學碩士學位論文》，2017年，第6頁。

[17] 葉洪、段敏：〈“殺豬盤”網絡詐騙行為的個案分析與模擬實驗研究〉，《中國人民公安大學學報（社會科學版）》，2020年，第5期，第10—16頁。

過以急迫的“查案和詢問”加快各環節緊扣的時間和營造緊張氣氛，甚至命令受害者自我設置封閉空間，切斷與外部聯繫，使其陷入緊張無助的困境，喪失心理抵抗力，無形之中放大了受害者劣勢狀態，壓迫其從潛意識裡產生“避免損失”的本能，在慌忙之中陷入偏執性判斷，完全聽從詐騙分子指令。^[18]

四、電信網絡詐騙犯罪防控體系建設

雖然 2021 年全國檢察機關起訴電信網絡詐騙犯罪 4 萬人，同比下降了 20%，^[19] 但電信網絡詐騙犯罪不會削弱，還會利用各種新技術、新的應用場景等因素進行犯罪行為裂變，演化出新的犯罪業態。目前，依舊嚴峻的電信網絡詐騙犯罪形勢也說明了電信網絡詐騙犯罪不是簡單的社會治安問題，而是複雜的社會治理難題，^[20] 其打擊防控工作是長期性的。打擊是威懾的重要手段，在犯罪問題的治理上存在被動性。建立有效的防控體系，對於全面提高電信網絡詐騙犯罪的治理水平會起到事半功倍的效果。

(一) 加強個人信息安全保護，切斷信息不對稱源頭

通過前文分析，電信網絡詐騙犯罪之所以容易成功，與詐騙分子提前精準掌握詐騙對象的大量個人信息有密切關係。公民個人信息的洩露和盜取使得受害人在詐騙過程中完全處於被操縱狀態，實施精準詐騙，而且高額非法收益又衍生出侵犯公民個人信息罪行為。2021 年全國公安機關破獲侵犯公民個人信息案件 9,800 餘起，抓獲犯罪嫌疑人 1.7 萬餘名。^[21] 2021 年全國檢察機關起訴侵犯公民個人信息犯罪嫌疑人 9,800 餘人，同比上升 64%。^[22] 2021 年全國人民法院審結利用各種形式竊取、釣魚欺詐、販賣個人信息犯罪相關案件 4,098 件，同比上升 60.2%。^[23]

目前侵犯公民個人信息犯罪行為主要包括信息盜取、提供和倒賣三大環節，公安機關針對相應環節分別構建了針對性的偵查打擊策略。通過發起打擊駭客犯罪集群戰役，偵破一批利用木馬病毒、釣魚網站、滲透工具、網絡爬蟲等駭客手段竊取公民個人信息案件，全面清理侵犯公民個人信息犯罪的技術交易源頭；針對行業內部洩露問題，協同電信運營商、醫院、保險公司、房地產、物業、快遞等行業，開展個人信息洩露治理專項行動，打擊行業“內鬼”，加強行業職操監管；通過買賣信息線索鎖定那些從事公民個人信息的銷售網絡平台，壓縮資料中間商和物料供應商的生存空間。^[24]

在打擊侵犯公民個人信息罪的同時，必須系統全面加強個人信息保護。2021 年 6 月，全國人大常委會審議通過了《數據安全法》，8 月通過了《個人信息保護法》，不僅在立法上對個人信息安全作出了法律保障，也為全面提高社會安全行業管理和源頭治理，有效打擊侵犯公民個人信息罪提供了法律支援。公安機關在綜合治理的過程中，以問題為導向，在互聯網平台日常執法監督檢查中，聯合網信、工信等部門，加強網絡資料的安全防護和安全責任落實，同時向群眾開展宣傳教育，普及個人信息保護知識和注意事項，切實形成保護公民個人信息和數據安全的工作合力。^[25]

(二) 科學預測詐騙手段變化趨勢，消除信息不對稱運行基礎

1. 根據大數據採擷技術，掌握詐騙內容變化規律，精準預測未來詐騙關鍵詞

詐騙內容是電信網絡詐騙信息傳遞的對象。公安機關提前將其破解，先一步掌握詐騙“劇本”，第一時間發佈權威提示，無疑有助於群眾做好防範措施。^[26] 為此，公安機關要運用大數據採擷技術，根據詐騙內容變

[18] 謝玲：〈論跨境電信網絡詐騙案件的打擊困境及破解對策：以“人員流”證據的收集、運用為視角〉，《中國刑警學院學報》，2021 年，第 1 期，第 75–81 頁。

[19] 同註 1。

[20] 浙江新聞，〈持續遏制電信網絡犯罪高發多發態勢〉，發佈日期：2021 年 9 月 17 日，網址：https://zjnews.zjol.com.cn/zjnews/202109/t20210917_23103156.shtml，到訪日期：2023 年 2 月 2 日。

[21] 中華人民共和國中央人民政府，〈“淨網行動”這一年：偵辦侵犯公民個人信息等網絡犯罪案件 6.2 萬起〉，發佈日期：2022 年 1 月 5 日，網址：https://www.gov.cn/xinwen/2022-01/05/content_5666617.htm，到訪日期：2022 年 2 月 5 日。

[22] 同註 17。

[23] 中華人民共和國司法部，《最高人民法院工作報告》，網址：https://www.moj.gov.cn/pub/sfbgw/zwgkztl/2022zt/2022qglh0222/022qglhbgqyd/2022qglhfybg/202203/t20220315_450733.html，到訪日期：2022 年 3 月 16 日。

[24] 董凡超：〈筑牢維護公民個人信息安全銅牆鐵壁〉，《法治日報》，2023 年 11 月 2 日。

[25] 劉丹、廖澤婧：〈重拳出擊，保護公民個人信息安全〉，《人民公安報》，2023 年 8 月 11 日。

[26] 陸愛紅：〈治理電信詐騙須打擊與防範並重〉，《人民公安報》，2016 年 4 月 14 日。

化規律，通過構建關聯模型不斷學習詐騙內容的敏感欄位，結合社會環境特徵和經濟發展趨勢，實現詐騙新“劇本”精準預測，提高全民防範的針對性。詐騙內容基本都來源社會生活，緊貼熱點問題，不斷變化詐騙手法，更新犯罪技術，使犯罪更加隱蔽，也更具迷惑性。^[27] 諸如，“網絡購物詐騙”、“網絡遊戲詐騙”、“冒充好友詐騙”等詐騙與人們日常社會中網絡應用極高有關。“移動社交、移動視頻、移動購物的活躍滲透率均在90%以上”；^[28]“投資理財詐騙”、“帳戶涉嫌洗錢或涉稅詐騙”等詐騙所涉及的投資、理財、稅收，甚至洗錢都是我國市場經濟不斷深化發展過程中的產物和現象；“養老投資詐騙”、“養生保健詐騙”等詐騙也是詐騙分子利用我國正在探索養老產業市場化發展的相關政策。所以，運用大數據構建模型，學習詐騙劇本語義環境和與關鍵字的相關規律，根據我國未來社會、經濟以及科技發展新態勢，加快計算未來詐騙關於諸如“金融創新”、“區塊鏈”、“虛擬貨幣”、“元宇宙”、“AI智慧”等情境內容，實現精準反詐防範和宣傳。

2. 掌握詐騙犯罪手段變化動態，明確公安打擊方向

當前電信網絡詐騙犯罪組織多以現金網公司、博彩公司、科技公司等形式，採取產業化和企業化對外運行模式，內部組織嚴密、分工明確、管理高效，專業化程度極高，^[29] 不僅具有極強的迷惑性，也加大了公安偵查打擊難度。究其根源在於犯罪組織的產業化和專業化。犯罪組織的產業化和專業化有助於詐騙犯罪手段產生新變化——複合化，以加大迷惑性和反偵查效果。詐騙通過網絡技術實現了詐騙涉眾面廣，要提高詐騙的迷惑性，不僅要推進犯罪手段複合化，更要結合專業化。2021年8月以來，以“兼職刷單”、“戀愛交友”為開端，融合“殺豬盤”、虛假貸款等多種詐騙手段的複合型詐騙案件高發，已成為當前電信網絡詐騙犯罪中變種最多、變化最快的一類。^[30] 金融創新業務明顯符合專業化的要求，電信網絡詐騙犯罪與金融詐騙犯罪交織一起，詐騙手段更加專業，無疑會進一步增加偵查打擊難度。除此之外，還有利用曝光受害者隱私的“裸聊詐騙+敲詐”、“交友聊天+賭詐”結合等新的犯罪手段。為此，做好相關部門信息共用，強化技戰法相互學習，是提高部門協同打擊效能的必要前提。

（三）構建精準的群眾預防宣教體系，改變信息不對稱中劣勢地位

針對詐騙分子的精準詐騙，我們的宣傳也應構建精準的反詐宣傳體系。

1. 根據受害者性格特徵分析，優化反詐宣傳邏輯思路

在電信網絡詐騙中，受害者具有容易生成信任的性格特徵也是被詐騙的關鍵原因之一。這也是詐騙分子前期進行詐騙對象篩選的目的。目前我們不斷加大了反詐宣傳力度，但各種詐騙案件依舊發生，一些受害者依舊陷入老套的騙局，甚至面對勸阻的民警產生極大的不信任。其中問題在於我們的反詐宣傳更多的是種面對大眾的普遍宣傳，是一種大水漫灌式宣傳。其結果是沒有針對性，感覺別人的教訓與己無關，宣傳沒有深入人心。要實現精準反詐，必須優化反詐宣傳邏輯思路。一是運用大數據技術分析，從大量詐騙案例中梳理不同類型詐騙所塑造人設和情景，總結出在詐騙過程中容易產生信任的受害人性格特徵，由此確立潛在受害者的人群範圍，再根據詐騙類型有針對性地開展反詐教育宣傳。二是根據電信網絡詐騙犯罪案件中受害人出現老年人和未成年人被害率較高趨勢，加大反詐宣傳和社會幫扶的協同治理。未成年人多以直播打賞、網絡遊戲、網絡購物等形式被騙，而老年人則多因養老投資、養生保健、情感交流等幌子落入圈套。^[31] 關注未成年人和老年人的身心健康是需要各級政府部門、學校、社區和家庭共同攜手給予關愛服務、心理疏導和家庭教育指導。

2. 公開透明相關行政部門和行業的業務流程，提高群眾的信息優勢

在詐騙中，由於對相關政府和行業業務流程的不了解，成為詐騙分子矇騙群眾的關鍵，也是受害者

[27] 同註5。

[28] 同註6。

[29] 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53–64頁。

[30] 同註6。

[31] 同註12。

在信息不對稱中劣勢產生的原因之一。要提高群眾的信息優勢，必須說明群眾全面了解政府部門和行業對外的業務流程。所以，反詐宣傳應增加涉及群眾切身利益的業務辦理流程的講解。例如，公檢法機關通過公開基本業務流程，消除群眾對公檢法業務的“神秘感”；金融機構通過宣講國家金融政策，各種理財產品特點和存在的可能風險點，提高群眾金融風險意識；知名購物平台要利用多種渠道說明網絡購物各項服務流程，消除服務環節中的“盲點”，通過提高群眾對各種信息的掌握程度，改變群眾在詐騙中信息不對稱的劣勢地位。

(四) 以制度創新增強警民之間的制度信任，築牢反詐治理的社會基礎

制度信任是在法律規範的基礎上生成的，遵循制度約束的理性信任。由於制度能夠在社會運行中通過建立秩序，降低社會的高度複雜性和高度不確定性，增強個體行為人的理性選擇，^[32] 甚至在一定程度上調節了日益充滿張力的人際信任。^[33] 制度信任在現代社會良性運行和協調發展中的重要性越發凸顯，^[34] 同理警民之間的制度信任直接關係基層警察與社區居民的警群關係，影響着公安機關基層社會治理水平和效能。

1. 創新多元基層社會治理模式，改進警民制度信任

基層社會治理（包括治安治理）是多元主體參與治理的活動。依靠群眾、發動群眾和凝聚群眾是公安工作的群眾路線具體內容。僅依靠社會監督和群眾投訴等制度難以建立親密警民關係，反而可能滋生抱怨的負面情緒，自然影響群眾參與社會治理的積極性，從而造成單純以制度信任為基礎所形塑的警民信任關係不斷弱化。^[35] 創新基層社會治理模式必須提高制度建設的科學性。科學性體現在制度經歷實踐檢驗，並在實踐中通過評估和回饋機制得到不斷完善。為此，社會治理要在制度上賦予社會組織、群眾在制度執行過程中科學評價制度有效性的機會，^[36] 促進警民之間形成民警真實充分了解群眾訴求，不斷提升執法水準，群眾不再做“旁觀者”，積極參與治理和績效評估，逐步建立起共建共治共用理念的制度信任。

2. 以問題為導向，解決群眾切身利益，營造提升制度信任的社會環境

要提升警民制度信任水平，社會治理制度必須確保對群眾利益的維護和保障。只有人民獲得更多、更直接、更實在的獲得感、幸福感、安全感，才能保持制度優勢的可持續發展。公安機關在構建反詐防控體系建設中，要通過開展接待日、走訪調研等活動積極公開工作業務流程和政務信息，將公安民警的職責和執法要求向群眾擺明，要以解決群眾最關心、最直接、最現實的利益問題為驅動力，吸引群眾真心加入社會治理行動中，通過營造“公平、公正、公開”的社會環境，提高警民制度信任，實現既能深入了解社會民情，掌握群眾基本訴求，又能接受群眾監督，加強執法公正，築牢反詐治理的社會共治防線。

五、總結

電信網絡詐騙犯罪會長期存在是一個客觀事實。我們必須清楚地認識到打擊防範電信網絡詐騙犯罪是持久戰，同時，也要意識到這是一個複雜的社會治理難題。有效的防範不能單靠公安機關的依法嚴厲打擊，更需要多部門、各行業、眾多社會組織和廣大群眾參與到電信網絡詐騙犯罪防控體系的建設中，通過落實各級政府部門和行業監管主體責任，將管控治理工作納入績效考評，從制度上推進協同共治，通過基層社會治理模式創新，構建全社會參與共治防線，合力擠壓犯罪空間，^[37] 守護好群眾的“錢袋子”。

[32] 戚玉覺、楊東濤、何玉梅：〈組織中的制度信任：概念、結構維度與測量〉，《經濟管理》，2018年，第2期，第192–208頁。

[33] 鄒宇春：〈提升制度信任：確保政府良性運行的重要方向〉，《中國發展觀察》，2014年，第8期，第28–30頁。

[34] 周延東、閻煌：〈“制度——關係”互構視閾下的警民信任研究〉，《中國人民公安大學學報（社會科學版）》，2022年，第1期，第149–156頁。

[35] 同註32。

[36] 同註1。

[37] 中國青年網，〈公安部：打擊電詐犯罪成效顯著成功避免6178萬名群眾受騙〉，發佈日期：2022年4月14日，網址：https://news.youth.cn/gn/202204/t20220414_13611187.htm，到訪日期：2023年2月18日。