Dispute Settlement 争议解决, 2025, 11(5), 22-26
Published Online May 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.115162

Hans汉斯

新型网络诈骗犯罪的侦查困境与应对路径

张文杰

湖北大学法学院，湖北 武汉

收稿日期：2025年3月28日；录用日期：2025年4月30日；发布日期：2025年5月12日

摘 要

网络已经融入公民正常生活，网络犯罪已经成为当下主要的犯罪形态和类型，网络诈骗犯罪是其中突出的一类犯罪，网络诈骗对社会诚信和公民生活造成严重影响，成为新的社会治理难题。本文从提出问题、基本态势、新型网络诈骗犯罪侦查的困境、侦查困境的应对路径进行论文的展开。根据新型网络诈骗犯罪虚拟性、智能化、产业化等特征，发现新型网络诈骗犯罪侦查取证困难、管辖权争议等一系列问题，并针对相关问题提出侦查区域协同联动、侦查公私合作机制等相关完善路径。

关键词

网络诈骗，虚拟性，管辖争议，协同联动

The Investigation Dilemmas and Coping Approaches of New-Type Cyber Fraud Crimes

Wenjie Zhang

School of Law, Hubei University, Wuhan Hubei

Received: Mar. 28th, 2025; accepted: Apr. 30th, 2025; published: May 12th, 2025

Abstract

The Internet has been closely related to our daily lives. Cybercrimes have become the most prominent form and type of crime at present. Cyber fraud crimes are a particularly prominent category among them. Cyber fraud has a serious impact on social integrity and citizens' lives, and has become a new challenge in social governance. This paper unfolds by raising questions, analyzing the basic situation, exploring the investigation dilemmas of new-type cyber fraud crimes, and proposing coping approaches to these dilemmas. Based on the characteristics of new-type cyber fraud crimes, such

文章引用: 张文杰. 新型网络诈骗犯罪的侦查困境与应对路径[J]. 争议解决, 2025, 11(5): 22-26.
DOI: 10.12677/ds.2025.115162

as virtuality, intelligence, and industrialization, a series of problems are identified, including difficulties in investigation and evidence collection, and disputes over jurisdiction. In response to these related issues, relevant improvement paths are proposed, such as the coordinated and joint actions among investigation regions and the establishment of a public-private cooperation mechanism in investigation.

Keywords

Cyber Fraud, Virtuality, Jurisdiction Disputes, Coordinated and Joint Actions

1. 问题的提出

伴随着云计算、大数据、人工智能等信息技术的逐步推广，网络诈骗犯罪已经成为近几年案件数量上升最快的刑事犯罪。网络诈骗立案数量逐年增长，由 2019 年的 82 万件增加到 2021 年的 96 万件，2021 年追缴赃款并返还人民群众被骗资金高达 120 亿元[1]。网络诈骗犯罪是在网络虚拟空间进行的，其诈骗对象具有广泛性和非特定性，并且犯罪手段迭代更新，增加侦查机关打击犯罪的难度，该类犯罪行为在数量上呈现出井喷式发展趋势，涉案金额巨大，造成了恶劣的社会影响，严重影响人民群众安全感和社会和谐稳定[2]。

新型网络诈骗犯罪是在高新技术支持下实施的一系列犯罪行为，其出现、发展到盛行，有其深层的原因和时代背景特点。揭示其深层次的产生原因，并探究更加有效的解决路径，是对网络诈骗犯罪相关理论和机制的完善。本文以网络诈骗为对象，研究新型网络诈骗的基本态势，针对现有的问题提出相应的解决机制。国家和地方立法机关应当针对网络诈骗犯罪发案的特点和表现形式，制定出有效抑制网络诈骗犯罪的政策，最终促进法律、法规的同步更新完善。

2. 新型网络诈骗犯罪的基本态势

2.1. 新型网络诈骗犯罪虚拟性升格

新型网络诈骗犯罪与其他类型触及虚拟空间的传统犯罪相比较，其更广泛、更深刻、更多样、更复杂地触及虚拟空间[3]。目前犯罪分子主要利用新型诈骗工具 GOIP 实施网络诈骗犯罪活动。GOIP 是一种虚拟的拨号硬件设备，其功能是将传统电话信号转化为网络信号，一台设备可以将数百个电话信号同时转化为网络信号[4]。当前为网络诈骗犯罪提供通讯传输技术支持也主要是通过 GOIP 设备实现的。新型网络诈骗虚拟性升格主要是来源于高科技和“黑科技”的结合，虚拟定位、拨号、IP 地址等各种虚拟的手段被广泛应用，加密算法和虚拟货币也增加了查清资金流向的难度[5]。新型网络诈骗的虚拟性促进犯罪分子的诈骗手段日益升级，从以往的利用银行卡中转账取现，发展至今通过比特币、第三方支付以及其他渠道进行洗钱，诈骗后所取得的赃款的转移，全程不需要在线下与被害人有接触。

2.2. 新型网络诈骗犯罪智能化迭代

网络技术的发展对新型网络诈骗犯罪有着极大地推动作用，诈骗团伙往往通常聘请高科技人才开发和维护非法平台，大量的黑科技运用到网络诈骗犯罪过程中，致使网络诈骗智能化加强。伴随公安机关对网络诈骗侦查技术的改进与加强，犯罪分子便想利用加密通信、网络和货币等手段去逃避公安机关的

侦查措施。犯罪分子往往采用 PGP 加密技术和 Telegram 的端到端加密通讯加密技术对相互之间的通信进行加密[6]。犯罪分子在诈骗过程中还利用高新技术进行数据收集、数据分析，并利用人工智能等手段以提高诈骗成功率，促使利益最大化。现代通信技术的进步，导致网络诈骗犯罪越来越智能化，给公安机关的侦查工作带来巨大的挑战。

2.3. 新型网络诈骗犯罪产业化升级

新型网络诈骗犯罪是一种以多个环节、多个参与主体为核心的犯罪活动，呈现出较强的产业化。网络诈骗犯罪分子采用产业化的作案方式，提高了犯罪效率。他们组成犯罪团伙，分工明确，分别负责不同的任务，按照流水线的方式进行诈骗。有些诈骗集团为了掩人耳目，甚至成立公司进行组织和协调。团伙成员从事的具体行为包括获取个人信息，谋划作案计划，拓展线下渠道和办理银行卡以及提取赃款等。犯罪团伙内部各司其职，形成一条完整的犯罪产业链。诈骗犯罪团伙会根据犯罪成员的特点将其予以具体划分，其目的就是使诈骗行为能够顺利实施。

3. 新型网络诈骗犯罪侦查的困境与成因

3.1. 犯罪行为地域跨越性引发侦查管辖权争议

刑事案件管辖是刑事案件的起点，公安、司法机关统计指定管辖的适用率时发现网络诈骗犯罪适用率明显高于传统犯罪[7]。新型网络诈骗犯罪往往具有多犯罪地、多层级、跨地域等特征，犯罪人实行诈骗犯罪行为较为灵活，会出现多个犯罪行为地，导致法定地域管辖更具复杂性。公安机关的侦查管辖权因地域与级别的不同而产生边界。地理上的管辖权分割，表现为侦查管辖权的属地化、条块化与排斥化特征[8]。网络空间无法划定明确的管辖区域，而网络空间的犯罪行为及其造成的危害结果，需要与某个特定的地理位置关联，并由该地理位置所在地的公安机关管辖。而网络诈骗犯罪行为的具有跨地域性，导致网络空间与地理空间的连接不容易界定，若按传统行为规范执行，可能会出现争抢或者推脱现象。

3.2. 犯罪过程信息技术融合性导致侦查取证难题

新型网络诈骗犯罪行为主要依靠信息网络空间进行，犯罪行为人进行诈骗活动的全过程主要运用人工智能、大数据等技术进行的，因此证据的数据化程度较高。互联网高速发展，随时产生海量的电子数据信息，给侦查机关在海量的电子数据信息中搜索犯罪信息证据增添了技术难题[9]。并且相对于传统物证而言，电子证据具有易篡改性、可删除性、可分离性、易复制性、易破坏的特性[10]。在网络诈骗中，犯罪人获取个人信息都是以电子数据的形式进行存储的，从案发到侦破案件这个过程时间很长，犯罪人有足够多的时间去销毁或者转移数据，增加公安机关收集完整有效证据的难度，由于部分侦查机关侦查技术的限制，增加侦查机关恢复、固定、分析证据的难度，侦查机关对于电子证据的收集将遭遇较大困难。

3.3. 犯罪组织链条扩散性阻碍侦查追赃实效

网络诈骗犯罪已经形成一条完整的犯罪链，并且该链条容纳相关的网络灰黑产业犯罪。电信网络诈骗犯罪共有三个犯罪节点，包括犯罪链条的上中下游犯罪节点。处于上游的犯罪人的主要任务是通过人工智能或者黑客技术从各软件平台获取公民个人信息。处于犯罪链条中游的犯罪人利用上游犯罪人提供的公民个人信息进行针对性的诈骗，对受害人来说往往具有较强的真实性，受害人最终遭受财产的损失[11]。下游犯罪人的主要任务是将诈骗的财物使用“地下钱庄”、支付加密等方式，通过比特币、第三方支付以及其他渠道进行洗钱。新型网络诈骗犯罪不光形成犯罪链条，并且在犯罪节点上扩散出产业性的犯罪组织。例如在犯罪下游提供结算业务的帮助犯，有许多帮助犯都是为了谋取非法利益的社会闲散人员，这些帮助犯已经远离犯罪的核心节点和组织者，公安机关即使抓获这些帮助犯，也只会增加追赃的

难度，浪费司法资源。

4. 新型网络诈骗犯罪侦查困境的应对路径

4.1. 加强侦查管辖区域协同联动

侦查协作就是指在侦查犯罪过程中，侦查部门之间或者与其他机关之间的协同配合。随着新型网络诈骗犯罪分子流动性的增强，跨区域的犯罪行为时常发生，应深入推进侦查区域协同联动，尽快形成全国“一盘棋”的打击格局[12]。面对各地公安机关与政府只对其管辖范围内的犯罪进行打击与治理的问题，应当由中央司法机关或者中央人民政府进行协调，确保公安机关内部达成治理网络诈骗犯罪的一致意见，避免公安机关对案件的相互推诿，并在各地公安机关之间达成信息的互通。网络诈骗犯罪具有跨区域性，准确、高效的信息情报对于犯罪人所在地的公安机关侦查工作的开展具有重要的支撑作用。在追缴诈骗犯罪违法所得过程中也需要侦查区域协同联动，诈骗犯罪分子为了逃避打击，通常诈骗所得异地转移，犯罪所得转移渠道较为隐蔽，当地公安机关不仅采取措施控制违法所得外流，最重要的是及时地向外流地的公安机关通报案情，争取得到外地公安机关的协助。

4.2. 构建信息技术融合侦查公私合作机制

公安机关作为国家行政机关，其任务就是维护社会治安与打击违法犯罪。但是面对新型网络诈骗犯罪所产生的数据的海量性与复杂性，单纯地以公安机关为治理主体的治理结构还需要进一步扩展。现在新型网络诈骗犯罪的犯罪分子在进行诈骗活动时必定会留下犯罪痕迹，也就是数据痕迹。而对于这些网络平台数据的占有和分析，互联网巨头相对于公安机关来说具有得天独厚的技术优势。将腾讯、阿里巴巴、百度等企业纳入协同治理中有其必要性。腾讯公司研发的一款用于识别分析诈骗信息与潜在受害人的软件“鹰眼盒子”，“鹰眼盒子”的启动需要具备相应的条件[13]。腾讯要在信息保护与数据分析方面有较强的能力与丰富经验，其次还需要电信运营商为腾讯提供电话数据和硬件设备。当“鹰眼盒子”启动时，它会识别出潜在的受害人正在接听犯罪分子的诈骗电话，然后“鹰眼盒子”会从运营商提供的电话数据中将受害人的号码提取出来，并且通过短信提示等方式阻止诈骗行为的进行。

4.3. 提高侦查犯罪组织链条扩散性科技赋智水平

侦查机关需要加强对网络的巡查执法，利用人工智能技术发现违法犯罪的线索。相较于传统案件的侦查工作，新型网络诈骗犯罪的侦查活动的对象更多的是数据信息，因此需要有掌握计算机与网络安全技术的侦查人员进行侦查活动，确保侦查人员准确合法的搜集诈骗犯罪数据信息，并对数据信息进行分析与保存[14]。通过人工智能技术，可以更好地分析海量数据，保障数据的有效性和信息的完整性，同时也可以提高网络数据的安全性和可靠性。人工智能技术能够协助网络安全分析，并以适当方式储存数据信息，提升数据存储效率，为后期数据分析奠定良好的基础。为了防止网络诈骗犯罪，需要利用人工智能、云计算、物联网和区块链等技术的优势，建立完善的数据库，以便对网络赌博平台、涉嫌诈骗的链接和资金进行有效拦截，从而有效防止网络诈骗犯罪的发生。

5. 结语

我国迈入人工智能时代，互联网和通信技术的高速发展推动了社会进步，但是当前网络诈骗犯罪形势严峻，严重危害了我国社会稳定和人民财产安全。做好应对网络诈骗犯罪的治理工作，需要公安机关提升侦查技术，以技术作为侦破案件的重要保障，同时加强与互联网企业、银行等相关部门的合作，形成打击合力，并由相关机关完善侦查管辖区域联动机制，才能打赢遏制网络诈骗犯罪的攻坚战。

参考文献

[1] 高宏美竹, 王鑫. 电信网络诈骗犯罪的现状及对策分析[J]. 现代商贸工业, 2023, 44(12): 201-203.

[2] 曾磊, 王争辉. “电信网络诈骗”刑法概念的厘清与独立构罪的逻辑证成[J]. 政法学刊, 2023, 40(4): 5-15.

[3] 李双其, 褚红云, 陈雁. 电信网络诈骗犯罪侦查特性论[J]. 公安研究, 2023(7): 19-26.

[4] 尹一扬. 犯罪预防视域下涉 GOIP 电信网络诈骗犯罪的预防与打击[J]. 网络安全技术与应用, 2023(7): 150-152.

[5] 李雪峰, 王铼. 电信网络诈骗的特征与治理路径[J]. 人民论坛, 2023(20): 65-67.

[6] 文硕, 吴琪, 郑锦莹. 大数据智能化时代非接触性犯罪的侦查模式[J]. 政法学刊, 2022, 39(2): 12-17.

[7] 孙潇琳. 我国网络犯罪管辖问题研究[J]. 法学评论, 2018, 36(4): 186-186.

[8] 陈如超. 电信网络诈骗犯罪侦查管辖制度的反思与调整[J]. 浙江工商大学学报, 2022(5): 60-71.

[9] 郝小辉. 网络诈骗犯罪案件侦查取证研究[J]. 辽宁警察学院学报, 2023, 25(1): 33-38.

[10] 李萌, 刘文奇, 米允龙. 基于区块链的公共数据电子证据系统及关联性分析[J]. 智能系统学报, 2019, 14(6): 1127-1137.

[11] 秦雨田. 电信网络诈骗以诈骗罪为核心罪名的逻辑展开与犯罪控制[J]. 太原学院学报, 2024, 25(4): 95-104.

[12] 王晓伟. 如何提高电信网络诈骗侦破打击能力[J]. 人民论坛, 2019(35): 108-109.

[13] 孙少石. 电信网络诈骗协同治理的制度逻辑[J]. 治理研究, 2020, 36(1): 100-113.

[14] 吉宁, 张裕杰. 公安机关打击治理电信网络诈骗困境与对策研究[J]. 网络安全技术与应用, 2022(3): 151-154.