Advances in Social Sciences 社会科学前沿, 2023, 12(5), 2463-2469
Published Online May 2023 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2023.125333

Hans汉斯

跨境电信网络诈骗犯罪预防机制的构建

——以情境预防为视角

朱荣赫，许梓蓼

北京师范大学法学院，北京

收稿日期：2023年4月7日；录用日期：2023年5月18日；发布日期：2023年5月25日

摘　要

面对常态化的高压打击，电信网络诈骗分子越来越将境外作为主阵地，跨境电信网络诈骗防控形式异常严峻。跨境电信网络诈骗犯罪呈现出的犯罪行为跨境化、技术手段多样化、犯罪组织集团化和犯罪分工专业化的特征，这使得传统的社会预防和刑罚预防展现出了疲态。而情境预防理论在跨境电信网络诈骗的治理中具针对性、全面性、可行性和高性价比的优势。从情境预防理论的五大类技术手段出发，归纳跨境电信网络诈骗犯罪情境预防的可能路径，全面提升我国数字时代电诈犯罪的综合治理能力。

关键词

跨境电信网络诈骗，情境预防，犯罪预防，犯罪治理

Construction of Cross-Border Telecom Network Fraud Crime Prevention Mechanism

—From the Perspective of Situation Prevention Theory

Ronghe Zhu, Zilu Xu

School of Law, Beijing Normal University, Beijing

Received: Apr. 7th, 2023; accepted: May 18th, 2023; published: May 25th, 2023

Abstract

Faced with the normal high pressure crackdown, telecom network fraudsters increasingly take overseas as the main position, and the prevention and control forms of cross-border telecom net-

文章引用: 朱荣赫, 许梓蓼. 跨境电信网络诈骗犯罪预防机制的构建[J]. 社会科学前沿, 2023, 12(5): 2463-2469.
DOI: 10.12677/ass.2023.125333

work fraud are extremely severe. The cross-border telecom network fraud crime presents the characteristics of cross-border criminal behavior, the diversification of technical means, the collectivization of criminal organizations and the specialization of criminal division of labor, which makes the traditional social prevention and penalty prevention show weakness. The situational prevention theory has the advantages of pertinence, comprehensiveness, feasibility and high cost performance in the management of cross-border telecom network fraud. Starting from the five types of technical means of situational prevention theory, this paper summarizes the possible paths of situational prevention of cross-border telecom network fraud crime, and comprehensively improves the comprehensive management ability of electric fraud crime in the digital era.

Keywords

Cross-Border Telecom Network Fraud, Situation Prevention Theory, Crime Prevention, Crime Management

1. 引言

电信网络产业的快速迭代和高速发展将人们带入移动互联网时代，使大众的生活空间逐渐从“现实”转入“虚拟”。移动互联网在为我们带来便利的同时也为违法犯罪创造了新的场域。伴随着无线通信技术、网络社交平台、电子支付工具的全面铺开，电信网络诈骗迅速蔓延至全国，已成为发案最多、上升最快、涉及面最广、人民群众反映最强烈的犯罪类型。我国司法机关高度重视，持续开展“云剑”“拔钉”“断流”“断卡”等专项行动，在国内对电信网络诈骗犯罪形成了常态化高压打击态势。据统计，截至 2022 年 11 月底，全国共破获电信网络诈骗案件 39.1 万起，破案、犯罪嫌疑人抓捕数量同比上升 5.7%和 64.4%，立案、造成财产损失数量同比下降 17.3%和 1.3% [1]。电信网络诈骗犯罪集团鉴机识变纷纷转战海外，最高人民法院公布的数据显示，我国当前电信网络诈骗犯罪境外作案占比已达 80% [2]。

“消未起之患、治未病之疾，医之于无事之前。”2022 年 12 月 1 日施行的《反电信网络诈骗法》强调了源头治理和前端预防，将预防同遏制、惩治并列作为犯罪治理的重要手段。情境预防理论旨在通过改变或控制日常生活情境，防止因此诱发犯罪动机或利于实施犯罪行为[3]。本文拟通过分析跨境电信网络诈骗犯罪的一般规律，探讨其庞大的犯罪基数和跨境因素叠加的治理难题的应对之策。

2. 跨境电信网络诈骗犯罪的特征

2.1. 犯罪行为跨境化

电话、短信、网络社交平台、电子支付工具等网络基础设施的普及创造的虚拟场域使得诈骗犯罪有了可以突破空间限制的条件。随着国内电信网络诈骗打击治理水平的加强和全民反诈意识的提高，犯罪分子在境内实施电信网络诈骗的犯罪成本和风险不断增大。于是电信网络诈骗集团纷纷转战经济发展低迷、社会管理水平欠佳、法制不健全的境外国家尤其是东南亚国家。他们在境外建立犯罪窝点，雇佣甚至诱骗国内人员实施犯罪，也将诈骗经验与方法传授给当地民众[4]。并且利用境外服务器进行作案，所骗取的被害人财物也通过黑灰产业转移至境外。从 2021 年到 2022 年，我国电信网络诈骗犯罪境外作案占比从六成提高到八成，电信网络诈骗犯罪呈现出明显的跨境化特征。

2.2. 技术手段多样化

在境外，实施诈骗的犯罪分子可以轻易地利用新技术更新自己的犯罪工具。虚拟拨号器、计算机病毒、区块链、虚拟货币、远程操控、数据爬取、人工智能等设备和技术工具被诈骗分子用以监控内部人员、接入网络、获取隐私信息、扩大诈骗范围、转移资金和逃避调查抓捕等用途。电信网络诈骗犯罪更加智能化、隐蔽化，社会危害性激增、打击治理难度加大。同时，虽然远在境外，但诈骗分子也时刻紧跟国内的社会经济发展状况，并在总结诈骗经验的基础之上不断翻新迭代诈骗手段。冒充司法人员、刷单返利、色情赌博、保健养老、恋爱交友、贷款理财等模式层出不穷，甚至元宇宙、区块链、NFT 等新概念也被用于诈骗剧本和话术之中。诈骗分子的诈骗手段套路繁多且不断更新升级，新的诈骗模式对被害人更具针对性和迷惑性。

2.3. 犯罪组织集团化

在社会管理和法治水平欠佳的境外，诈骗犯罪组织在缺乏“天敌”的环境中得以做大做强。从人数上看，近些年公布的跨境电信网络诈骗案中许多犯罪组织的人数达数十人甚至上百人，组织规模和体量显著增大。从外观形式上，犯罪组织穿上了公司的“马甲”，经常以科技公司、博彩公司、网络公司为“外衣”掩护其犯罪组织的性质。在组织上也更加严密，犯罪组织开始实行公司化管理，制定完善的组织章程、绩效方案、考核标准、工作守则、奖惩细则等一系列现代公司规章制度。在分工上也更加细化和完善，在组织者、领导者、参与者之间形成了自上而下的金主、代理商、管理团队纵向分工。又根据实施诈骗犯罪的不同流程设立人力资源、后勤保障、技术服务、业务管理、财务管理、安全保卫等业务部门，形成了完整的横向业务分工。犯罪组织规模扩大、组织严密、分工明确、协作高效，具有显著的集团化特征[5]。

2.4. 犯罪分工专业化

为了高效地实施诈骗和逃避法律制裁，境外诈骗分子之间形成了更专业的分工。在犯罪实施阶段，实施诈骗的“话务员”之间有着专业的角色分工，角色之间相互配合。在犯罪集团内部，从人员招募、实施诈骗、转移资金的各个流程也分工明确。同时，电信网络诈骗犯罪还形成了上下游黑灰产业链的分工。包括提供银行卡、电话号码、各类网站和平台账号、专业诈骗设备的作案工具提供商，非法获取和交易公民个人信息、组织偷渡、提供包网服务、从事洗钱等业务的服务商。每个环节的人员都具有较高的专业技能，从而提高了犯罪的效率和成功率。整个跨境电信诈骗网络分工明确、相互协作，形成了一个社会危害性大、打击难度高的“毒瘤”生态链。

3. 情境预防理论引入跨境电信网络诈骗犯罪防控的必要性

3.1. 跨境电信网络诈骗犯罪防控现状

预防始终是应对犯罪的最佳手段，然而面对跨境电信网络诈骗犯罪严峻的形势和特征，传统的社会预防和刑罚预防展现出了疲态。

3.1.1. 刑罚预防的阙如

刑罚预防强调通过立法和司法防止犯罪的发生，对于预防跨境电信网络诈骗犯罪起到了必不可少的兜底作用。然而，跨境电信网络诈骗犯罪是在社会、心理、情境等多种因素的作用下滋生的，刑罚本身“治标不治本”，发挥作用的空间有限。同时，犯罪的跨境化、专业化和集团化给司法机关开展侦查取证、追回赃款和罪犯抓捕工作带来了极大的困难[6]。

3.1.2. 社会预防的不足

社会预防号召全社会共同参与消除和削弱引起犯罪现象发生的各种社会因素。然而，社会预防效果的实现需要一个长期性的过程，“远水难解近渴”。同时，社会预防的措施往往较为理想化，实践中会受有很多复杂的社会因素影响，并且往往需要长期付出较高的社会成本，难以真正地落实见效[7]。

3.2. 情境预防理论的优势

所谓情境预防指的是通过确认、管理、设计、调整等方式，持久、有机地改变情境，影响行为人的理性选择，减少犯罪的机会情境因素和促成情境因素，从而达到预防犯罪的目的。简言之就是立足情境与潜在犯罪人的互动关系，从日常生活的细节之处出发采取措施，改变情境因素，防止犯罪动机的诱发和犯罪行为的实施。其并不追求“放诸四海而皆准”的犯罪防控方法，而是针对具体情境采取措施。而对于具体措施的概括和总结，以克拉克在 2003 年提出的“情境预防技术表”最为典型。其中囊括了增加犯罪难度、提升犯罪风险、减少犯罪收益、减少犯罪刺激、排除犯罪借口五大类 25 小类的具体措施[3]。

在跨境电信网络诈骗犯罪的防控中，情境预防既有其不同于刑罚预防、社会预防的独特优势，又符合有效抵制电诈犯罪的客观要求。跨境电信网络犯罪本质上是传统诈骗犯罪在新的技术条件和社会环境下所衍生出的新形式、新变种。其依然继承了传统诈骗类犯罪高度依赖犯罪人与被害人高互动性的特点。而情境预防理论一方面注重从减少合适被害人的因素入手防控犯罪，另一方面也注重从具体的互动环境切入防控犯罪的实施。此外，跨境电诈犯罪跨境化、多样化、集团化和专业化的特征在提高了诈骗效率和侦查抓捕难度的同时也使得犯罪的网络链条更加复杂、互动情境增多，这为情境预防提供了更多发挥作用的空间。最后，情境预防的有关措施立足具体情境，手段更加便宜和可行，相比其他预防手段所需要的社会资源和成本更低。因此，情境预防理论在防控跨境电诈犯罪中具有针对性、全面性、可行性和高性价比的优势。

4. 跨境电信网络诈骗情境预防的具体措施

通过前文对跨境电信网络诈骗犯罪特定情境因素的分析，结合情境预防理论，笔者尝试从多角度构建一套跨境电信网络诈骗犯罪情境预防机制。

4.1. 增大犯罪难度

增大犯罪难度主要是通过让犯罪人远离犯罪目标和犯罪工具等方式来实现的。具体到跨境电信网络诈骗犯罪领域，随着当今时代科学技术的迅猛发展，此类犯罪已呈现出跨区域、隐蔽性、近乎全产业链等区别于传统犯罪的新型共犯形式[8]。基于此，可以通过对犯罪分子可能实施犯罪或企图利用的目标物进行强化，增加其实施电信网络诈骗的难度，从被害人角度实现事前的积极预防[9]。

4.1.1. 控制犯罪工具

针对高技术型跨境电信网络诈骗犯罪，在充分保障个人隐私的基础上，电信运营机构应当加大实质审核力度，建立重点号码预防机制，及时关停可能涉嫌诈骗的电话号码，查封各类伪基站，并对虚拟号码设置自动拦截系统，进一步查清其来源[10]。例如，公安机关要重点关注互联网平台上销售恶意软件的相关群聊或讨论帖，使诈骗分子难以获取作案工具。同时，可以尝试借助人工智能辅助系统，增加诈骗犯罪的困难度。

4.1.2. 侦查转向

由于当前跨境网络诈骗犯罪上下游产业链存在较为严重的“黑吃黑”问题，尤其是在洗钱环节，洗钱团伙通过“黑吃黑”的形式将诈骗犯罪所得据为己有的案例屡见不鲜。因此，为解决洗钱环节的“黑

吃黑”问题，大多数洗钱团伙与诈骗犯罪集团都有相应的担保或抵押关系[5]。这在某种程度上似乎也为情境预防提供了一种新的思路，笔者建议在侦查环节可以尝试通过犯罪分子建立的这些防止黑吃黑的环节发现相关人员之间的联系，确定人员身份和组织结构，有效提高破案率，进而增大犯罪分子的犯罪难度。

4.2. 增大犯罪风险

增大犯罪风险是指通过强化监视、检查机制等手段及时发现犯罪，该策略的目的是增大犯罪人被发现和逮捕的可能，进而清除其潜在的侥幸心理。

4.2.1. 减少匿名

由于互联网平台相对匿名性的特点，跨境电信网络诈骗犯罪多为“背对背”式的交流过程，被害人与犯罪人并不直接接触，因此，有必要通过减少匿名的方式增大电诈犯罪人的犯罪风险。需要特别说明的是，针对跨境电信网络诈骗犯罪，犯罪人员通常以同乡、宗族等形式出现，其籍贯和活动区域也呈现出地域化、区域化特点[5]。因此，这一预防思路在技术层面也完全具有可行性。例如，可以尝试建立举报登记平台，对诈骗电话和恶意网址进行警告标记，可以相应地暴露诈骗分子的身份，从某种角度看也是减少匿名的技术手段。

4.2.2. 强化监督

完备的监督制度是技术手段发挥作用的前置条件。这里的监督可以包括正式监督和非正式监督两种途径，其中正式监督主要是指警方举报平台的建立。当前我国在国家层面的电信网络诈骗举报平台还不够成熟，虽然公安部网监局等部门已经建立了网络违法犯罪举报网站，然而从实际使用效果看其举报功能还有待进一步深化，特别是大多还停留在“110”直接报警的低效率阶段，难以形成科学严密的防范网络[10]。非正式监督主要体现在利用场所内人员进行随机监督，互联网社交平台的用户群体较多，随着网站内部举报制度的逐步完善，不法分子被举报封号的风险也随之增加。

4.3. 减少犯罪收益

减少犯罪收益可以使犯罪所得的利益减少，有利于清除犯罪人潜在的犯罪动机。对于传统犯罪，该策略主要有隐藏目标、移开目标、标志财产、瓦解黑市、灭除犯罪收益五类技术手段。具体到跨境电信网络诈骗犯罪的实践中，由于此类犯罪的犯罪目标通常以虚拟货币的形式存在，难以对其直接标记，因此笔者着重对其他技术进行分析。

4.3.1. 转移风险目标

相关金融服务机构(含网上银行)在为客户办理相关业务时如果发现异常交易情况，可以启动应急保护预案，在进一步核查相关信息的同时，先行冻结账户并将存款转移至新的安全账户，最大可能地保障公民的财产权益；又如为减少用户点击进入“钓鱼网站”的风险，网络服务商需要定时清理垃圾信息，第三方平台需要及时销毁用户的个人数据信息。

4.3.2. 取缔黑市平台

由于当前被窃取的公民个人信息和其他诈骗犯罪工具大多会在网络黑市平台中集中交易，跨境电信网络诈骗犯罪分子在这些黑市交易论坛中批量购买个人信息数据，并根据诈骗对象的不同身份背景，编制不同情境的诈骗剧本，不断变换身份，提高诈骗成功的可能。基于此，网监部门需要密切监控各类网络交易平台，对其中可能涉及违法犯罪的必须予以坚决打击。此外，尽管当前《反电信网络诈骗法》第四章已经从法律制度的层面就互联网治理问题进行了相关部署，但涉及互联网服务主体的规定大多表现

为较为原则、笼统的宣示性条款，在实践过程中的可操作性较低。因此，笔者建议可以参照《互联网信息服务管理办法》，区分互联网信息服务提供者和互联网接入服务提供者，要求接入服务提供者依照法律、行政法规查验互联网信息服务提供者的合法资质，不得为不具资质的非法网络平台提供网络接入服务，从源头摧毁非法网络平台滋生土壤[11]。

4.4. 减少犯罪刺激

电信网络诈骗犯罪与受害人直接接触的可能性较低，传统犯罪预防策略中涉及此类预防技术的减少挫折感、避免冲突、减少情绪冲突等手段并不适用。与此同时，作为一类情感因素，犯罪刺激的突发性和临时性体现得更为明显，因此在跨境电信网络诈骗犯罪情境预防中，可以通过阻断诈骗犯罪同类模仿的方式实现犯罪预防。数字时代背景下，网络论坛似乎已经取代了传统监狱成为了某些犯罪分子获取犯罪技能的“学校”。一些网民可能出于好奇参与了网络相关话题的讨论，并由此有意识或无意识地学习到诈骗方法、诈骗手段等犯罪技术，转而独立实施电诈犯罪。因此，现阶段警方需要加大实质审查力度，尤其是及时、有效地屏蔽涉及相关敏感信息，尽可能避免网络用户获取相关犯罪技术，减少相应的犯罪刺激[12]。此外，金钱诱惑也是刺激诈骗行为产生的重要因素，通过定期清理互联网中的负面情绪，着力打造风清气正的网络生态环境。

4.5. 排除犯罪借口

排除犯罪借口旨在抑制犯罪人的犯罪动机，在传统犯罪领域，该策略主要有制定规则、张贴告示、唤醒良心、帮助守法、毒品和酒精控制五种技术手段。事实上，毒品和酒精控制对跨境电信网络诈骗犯罪预防效果相对有限。因此，在罪刑相适应原则的基础上，可以适当加大对行为人的惩处力度，并通过全社会道德谴责，尽可能消除与实施新型诈骗犯罪相关的犯罪借口，努力唤醒其良知。同时，要注重对跨境电信网络诈骗团伙成员的规劝教育，帮助他们树立守法意识。

5. 结语

现阶段我国电信网络诈骗犯罪问题依然相当严峻，特别是随着国内反诈力度的空前增加，跨境电诈犯罪的发案率持续上升，打击电信网络诈骗仍然是一场“持久战”。与传统犯罪预防体系下的刑罚预防、社会预防相比，情境预防具有简捷经济、立竿见影的突出优势。在社会治安综合治理的背景下，通过梳理此类犯罪的犯罪特征和防控现状，归纳跨境电信网络诈骗犯罪情境预防的可能路径，全面提升数字时代电诈犯罪的综合治理能力，是本文研究的重点所在。需要特别说明的是，由于实践经验和统计数据的相对缺乏，很多思考和分析只能从理论层面展开，今后如果条件允许，还需做深入调研，特别是以跨境电信网络诈骗司法实务案例为基础进行实证研究，补充相关数据资料，进一步完善本文的研究成果。

基金项目

本文系北京师范大学刑事法律科学研究院 2022 年度学术型研究生专项科研基金课题《跨境电信网络诈骗犯罪预防机制构建研究——以情境预防为视角》(编号：2022CCLS030)的研究成果。

参考文献

[1] 中华人民共和国公安部. 公安机关打击治理电信网络诈骗违法犯罪取得显著成效[EB/OL]. https://app.mps.gov.cn/gdnps/pc/content.jsp?id=8812495, 2023-03-05.

[2] 张晨. 全国法院五年一审审结电诈案件超 10 万件[N]. 法治日报, 2022-09-07(003).

[3] 张远煌. 犯罪学[M]. 第四版. 北京: 中国人民大学出版社, 2020: 251-272.

[4] 吴照美. 电信网络诈骗犯罪的境外考察[J]. 武汉公安干部学院学报, 2020, 34(2): 65-67.

[5] 王晓伟, 赵照. 电信网络诈骗犯罪人员流的构成与侦查方法研究[J]. 中国人民公安大学学报(社会科学版), 2022, 38(4): 53-64.

[6] 尹俊翔, 陶杨. 打击跨境电信网络诈骗犯罪的困境与对策[J]. 人民论坛·学术前沿, 2022(16): 109-111.

[7] 孙丽刚. 情境预防理论在电信网络诈骗犯罪治理中的适用[J]. 上海公安学院学报, 2022, 32(2): 23-33.

[8] 卢建平, 王昕宇. 以现代化治理方略应对电信网络诈骗[N]. 检察日报, 2021-04-29(003).

[9] 邹世杰, 王明生. 大数据视角下“杀猪盘”电信诈骗犯罪的被害预防研究[J]. 网络安全技术与应用, 2023(2): 149-151.

[10] 吕美琛. 电信网络诈骗犯罪预防理论研究——以情景犯罪预防理论为视角[J]. 北京警察学院学报, 2020(5): 96-103.

[11] 皮勇, 汪恭政. 大数据背景下网络交易平台诈骗犯罪的治理路径[J]. 刑法论丛, 2018, 54(2): 461-488.

[12] 张明诚. 网络平台诈骗犯罪的情境预防——以 605 份刑事裁判文书为切入点[J]. 福建警察学院学报, 2021, 35(5): 56-66.