

“互联网+”背景下电信网络诈骗犯罪防控机制探讨

◆ 廖凌宇

(福建警察学院, 福建 福州 350007)

【摘要】互联网及相关计算机技术的高速发展,在给人们带来生活便利的同时,也为电信网络诈骗犯罪提供了犯罪空间。在此背景下,电信网络诈骗犯罪表现出犯罪团伙产业化、犯罪对象精确化、跨区域特征明显等特点,对防控工作提出了新的要求。可以从健全相关法律规制、创新精准宣传形式、深化各行业合作、培养专业队伍、建立多维打击协作机制入手,构建“互联网+”背景下的电信网络诈骗犯罪防控机制。

【关键词】“互联网+”;电信网络诈骗;防控机制

随着互联网技术的飞速发展,网络正在逐渐改变人们传统的生产生活方式和社会经济形态。但网络在为人们提供工作生活便利的同时,也给违法犯罪行为带来了更广的犯罪土壤。“互联网+”背景下,电信网络诈骗犯罪数量快速上升,不仅破坏了社会的和谐稳定,也严重阻碍了社会经济的发展。现在,如何防控电信网络诈骗已经成为了一个高度关注的问题。

一、“互联网+”背景下电信网络诈骗犯罪的特点

(一)电信网络诈骗犯罪的概念

电信网络诈骗犯罪是近年来新兴的一种犯罪形式,是指犯罪分子以非法占有他人财物为目的,利用电话、短信、互联网等电信网络技术手段,虚构事实,设置骗局,实施远程、非接触式诈骗,骗取公私财物的行为。

(二)电信网络诈骗犯罪的常见手段

当前流行的电信网络诈骗犯罪手段名目繁多。常见的类型有网络贷款诈骗、刷单返利诈骗、“杀猪盘”诈骗、冒充熟人诈骗、冒充“公检法”诈骗、投资理财诈骗等。

随着时代的发展,电信网络诈骗犯罪更新换代极快,不论是犯罪手段、犯罪目标、犯罪工具无时无刻都在发生着新变化,并结合高新科技、热点时事呈现出全新的特点。这些电信网络诈骗犯罪隐蔽性更强,影响范围更广,社会危害性极大。犯罪分子不仅懂得充分利用互联网特点和社会热点,随时为诈骗行为披上新的外衣,并且会针对不同人群进行不同的诈骗犯罪,诈骗手段方式多变、内容具有极强的针对性,让大众很难防范。

二、“互联网+”背景下电信网络诈骗犯罪的特点

(一)犯罪团伙产业化

当下,越来越多的电信网络诈骗犯罪表现出组织化的特点,仅单人或两三人很难完成诈骗,逐渐发展出了多人协作、分工明确、集体作案的团伙诈骗模式。其主要表现形式为:组织结构严密,团伙内部成员有明确的分工,彼此之

间协调配合,每个人均有自己扮演的角色和所要承担的任务。典型的电信网络诈骗集团呈金字塔式分布,即由团伙投资人进行控制,下端进行多级分层,由专人负责不同的职能,有专人进行搭建和维护硬件技术平台、接听电话和实施诈骗、开展银行流转业务等多种诈骗环节,并且采取逐级负责制,然后按照工作业绩进行分赃活动。整个过程由犯罪分子头目进行单向联系指挥,每个阶段成员只负责自己负责的工作,互相之间并不熟悉,即使被抓,也无法提供关于诈骗团伙的完整信息。同时,与电信网络诈骗有关的上下游产业也高速发展,上游职业黑客负责提供技术保障,核心诈骗团伙进行电信网络诈骗,而买卖账户、取钱、收卡、贩卖身份证等,则由各类下游组织负责,逐步形成各种组织严密分工精密的灰色产业。这些上下游组织通过为电信网络诈骗犯罪提供服务牟利,并形成了相对固定的合作关系,严重侵害大众利益。

(二)犯罪对象精确化

与以往电信网络诈骗“广撒网”的方式相比,如今的电信网络诈骗犯罪最大特点在于受害群体选择明确。犯罪团伙非法获取大量个人信息,并通过计算机技术对这些个人数据进行分类、整理,之后选择恰当人群,有针对性地编造合适的剧本进行诈骗,实现精确诈骗。如针对待业青年、主妇进行刷单返利诈骗,对于办理信用卡的人员进行网络贷款诈骗等。

(三)跨区域特征明显

电信网络诈骗从东南沿海侵入,蔓延至我国境内。我国相关部门对电信网络诈骗犯罪采取了高压打击态势,同时经济全球化,犯罪分子也没有了空间上的约束,逐渐向境外转移,更倾向于跨地域犯罪活动。目前,我国西南边境一带国家及东南亚地区是很多电信网络诈骗集团盘踞的窝点。为了逃避国内相关部门打击,犯罪集团一般在境外,租用境外服务器,通过网络技术对国内受害者进行诈骗。这种跨

境化的犯罪模式不但将指挥本部设在境外，还可能将其它有关犯罪环节，如话务、转账、洗钱等以承包的形式，分包给不同国家的犯罪下家，也进一步加大了我国相关部门对电信网络诈骗犯罪的打击难度，给公安机关的打击治理工作造成较大的麻烦。

三、防控难点

(一) 相关法律规制不健全

目前在我国，电信网络诈骗犯罪还是以诈骗罪论处，规定的刑期为无期徒刑或者10年以上的有期徒刑。对于一些系列性严重性的诈骗案件来说，这个处罚力度威慑力远远不够，这也导致了犯罪分子在实施犯罪时肆无忌惮，目前的刑事法律已经难以满足司法实务中的需求。同时，与电信网络诈骗犯罪相关的行业法律也存在漏洞，如公民个人信息保护的相关法律还不够完善，电信行业、金融行业管理的相关法规还严重滞后，这些都是导致公民的个人信息大量泄露，电信通信流与银行资金流链条上存在诸多漏洞的原因，使得电信网络诈骗分子有机可乘。

(二) 相关行业监管存在漏洞

“两卡”是目前大数据时代中开展电信网络诈骗犯罪的必需品。切断“两卡”与公民个人信息的流通，就能有效遏制电信网络诈骗犯罪的蔓延。与之相关的通讯运营商、银行、网络运营商等有关部门，存在着或自身责任感缺失或监管缺位，并未采取有效的运营机制，违规经营、管理松懈的现象依然存在。例如：实名制落实情况差强人意，新开户人员信息随意审核等。同时，面对相关侦查协作时未及时配合，也使有些电信网络诈骗犯罪案件侦查错过了最佳时机。

(三) 大众防骗意识较弱

随着时代和科技的发展，电信网络诈骗的手段越来越高明。从最初的广撒网，到如今犯罪分子根据非法获得的个人信息而精确的“定制型”诈骗，普通人往往难以辨别真假。在如今的电信网络诈骗中，利用时事热点内容和冷门专业知识都是常见的诈骗手段。犯罪分子不断推陈出新，冒充公检法、二维码诈骗等方式层出不穷，令人防不胜防。特别是近年来火热的区块链、5G、虚拟币等概念，更是电信网络诈骗的重灾区。趋利避害、心存侥幸的心理也是诈骗分子常利用的点，在电信网络诈骗犯罪案例中，骗子利用一些诱导策略，建立信任，造成假象，利用高额回报作诱饵，很容易使一些防骗意识差的人上当。

(四) 打击侦查工作困难

电信网络诈骗具备很强的流动性，作案地点不固定，甚至跨境犯罪。由于目前国际间协作机制尚不完善，且各国司法体制各异，协作侦查跨境电信网络诈骗案件还存在困难。犯罪分子在国外架设服务器，使用黑灰产业购买的无

实名的电话卡，锁定犯罪分子具体位置的难度加大。作案成功后，资金很快就通过层层分解进入了多级下级账户，下级账户也将继续分割所收到的资金，资金去向难以追踪。在电信网络诈骗犯罪团伙中，各成员之间基本都是单线联系，互不认识，这样即使有人落网，也很难交代出其它的情况。此外，电信网络诈骗的主要证据均为电子证据，提取难度大，且很容易被损毁，这就导致了公安机关取证难度很大。

四、构建“互联网+”背景下电信网络诈骗犯罪防控机制

(一) 健全相关法律规制

健全严明的法律法规，才能严厉打击电信网络诈骗犯罪行为，惩处和威慑电信网络诈骗犯罪。在刑法规制上，很多专家学者提出应当将电信网络诈骗罪名独立出来，并制定更加合理、全面的刑法罪名和量刑。同时，加紧完善与之有关的银行业、通信业、网络环境等相关的法律或规章，规范行业市场准入条件，优化行业经营者的经营准则和服务规范，明确其监管职责以及失职所应承担的法律责任等，从法律层面规范相关行业的经营行为。

(二) 创新精准宣传形式

增强大众的安全防范意识，从源头减少大众被骗概率，是有效防范电信网络诈骗的方式。第一，要加强精准宣传，突出在特定时段对特定人群开展反诈宣传。如对易受骗的老年人、青少年等防骗意识较弱的群体要经常下社区宣传，对各单位和企业的财务人员要定期普及诈骗的新手段。第二，创新情境式宣传。在日常进行电信网络诈骗宣传防范时，要特别注意结合当前的时事热点，针对热点事件梳理风险易发点，进行有针对性的宣传教育。同时，提高大众主动参与防骗宣传的积极性，营造全民参与打击电信网络诈骗犯罪活动的社会氛围。可由公安机关主导成立反诈宣传小组，运用情景剧等方式，进入企业、社区、学校等场所开展反诈宣传，发挥社会力量各自的优势，提高大众对宣传活动的认可度，从而提升宣传教育效果。第三，可对诈骗犯罪高发的区域进行普法宣传教育，增强该区域大众的法制意识，促使亲友规劝犯案人员弃恶向善，并拒绝盲从犯罪，从而减少犯罪。

(三) 深化各行业合作

网络安全问题不能仅仅依靠相关部门，更需要社会上各行各业联手合作。因此通信、金融、互联网各部门必须尽职尽责，加强合作，同时相关部门也应强化对通信、金融、互联网行业的监管，规范相关企业或个人的经营行为，进一步压缩电信网络诈骗犯罪分子的活动空间。首先，在通信行业，工信部门和运营商应该联手加强对于通信流的管理。工信部门对改号软件、伪基站等设备应开展专项整治行动，严惩违反相关规定的行为，有效遏制犯罪分子肆意利用网络

通信工具的势头；电信运营商和相关服务提供商应积极研发识别诈骗电话、短信的技术，采用技术措施阻断诈骗信息的传播渠道；电信运营商应严格执行手机号码实名制，并对一证多卡用户进行清理，防范电话卡被冒用或非法买卖。其次，在金融行业，央行和银行业监督管理机构应加强对商业银行等金融机构，办理银行账户及银行卡业务的执法监督检查，要求金融机构依法履行身份信息核验职责，防止出现使用虚假或冒用他人身份证明骗领银行卡的情况；金融机构在涉案资金环节，可以在及时查询可疑资金流向、紧急终止可疑资金交易、快速冻结可疑账户等方面进一步完善，实现以快制快，提高涉案资金的查控效率。互联网企业可以发挥自身的技术优势，通过大数据运算技术等方式发掘侦查线索，提供内部数据记录作为证据，如第三方支付平台微信、支付宝等协助发现、识别、阻止可疑资金流动协助侦查办案部门。

（四）培养专业人才队伍

目前，公安机关在打击电信网络诈骗方面的专项人才缺失严重，专业技术人才的缺失给案件侦破造成很大困难。电信网络诈骗案件往往会应用到高科技手段，需要侦查人员具有电子取证、计算机网络、经济犯罪侦查、法律知识等诸多专业领域的素质，而大多数的侦查人员在这方面的业务素质还比较缺乏。首先，可以通过整合刑侦、经侦、网安等多警种的专业人才，形成专业化电信网络诈骗犯罪侦查队伍，使电信网络诈骗犯罪侦查队伍的人员整体专业技能提高。其次，加强与网络安全、电子通信以及金融业务方面的专家、技术人员合作，能够熟练运用各自专业领域的特长与犯罪分子斗智斗勇，有效遏制、打击电信网络诈骗犯罪。最后，可以通过组织相关培训，培养一支有理想、有本领、有担当，“懂科技、熟业务、善指导、会研判”的专业人才队伍，为全面打击防控电信网络诈骗犯罪提供强大的人力和智力支撑。

（五）建立多维打击协作机制

电信网络诈骗犯罪的打击不仅需要公安系统各部门内部加强协作，还需要加强与电信部门、金融部门等其他部门的协作。根据电信网络诈骗犯罪的特点，打击协作方式可以

从两点入手：一是充分挖掘电信网络诈骗中的“信息流”与“资金流”。根据电信网络诈骗犯罪行为依赖于电信信息流和银行资金流的特点，公安机关要加强与电信、银行等多部门的合作，可以从犯罪手段上对其实施有效打击，截断其犯罪途径，并顺藤摸瓜找到犯罪窝点进行根源性铲除。通过提高可疑账户信息查询、资金冻结、网络IP溯源、移动终端定位的时效性等有效手段，为人们的财产安全提供最大保障。二是打破空间壁垒，进行区域间的信息共享。要加强区域之间的警务合作，同时充分利用大数据技术，对网上海量的信息进行整合，从中挖掘出有价值的情报线索。同时也要加强各类新技术新平台的整合应用，将公安等部门的防范电信网络诈骗大平台与大数据、人工智能、物联网、云计算等应用平台进行整合，充分利用互联网平台进行网上协查、信息共享等行为，加强信息的流动性，优化侦查协作机制。

五、结束语

电信网络诈骗犯罪已成为近年来增长最快的犯罪形式，造成的社会危害极大，是目前社会重点关注的问题之一，互联网等技术的普及和发展也对其起到了推波助澜的作用。近年来，为打击电信网络新型违法犯罪活动，多个部门针对不同地区、不同类型的电信网络诈骗犯罪行为与其有关的灰色产业链，开展各式各样的专项打击行动、出台专项规定，并取得了一定成效。

参考文献：

- [1] 张扬, 邓志源. 电信网络诈骗犯罪态势分析与体系化应对[J]. 湖北警官学院学报, 2021, 34(06): 80-88.
- [2] 程桦, 王翔雯. 基于“互联网+”贸易背景下的网络犯罪治理研究[J]. 老字号品牌营销, 2019(11): 24-26.
- [3] 陈睿毅, 刘双阳. “互联网+”背景下电信诈骗犯罪防控机制研究[J]. 犯罪研究, 2019(03): 51-58.

作者简介：

廖凌宇(1989—), 女, 汉族, 福建泉州人, 硕士, 助教, 研究方向: 侦查学。