文|北京市海淀区人民检察院 张志婧 李鹏 郭树正

当下电信网络诈骗犯罪呈现出技术性强、骗术变化快、波及产业链广、被害人众多、涉案钱款巨大等特点。行为人通过非接触方式作案，背后的基础工具是银行卡、电话卡等，基础技术是通知类短信技术、跨境数据通信技术、短网址服务技术、网络社交软件技术等。国内的基础工具与技术被非法利用且存在监管缺漏，是跨境电信网络诈骗犯罪断而不绝的重要原因之一。

2019 年至 2022 年 7 月，北京市海淀区人民检察院（以下简称“海淀院”）办理帮助信息网络犯罪活动案共计 342 件 649 人，通过汇集孤立个案形成大数据剖析发现，案件背后的深层问题集中于通信渠道、推广渠道、资金渠道方面。因此，在打击犯罪的同时，亟须对隐藏在跨境网络犯罪背后深层、根源性问题，开展针对大数据的深层法律监督以及全链条、多元化的源头治理。

一、跨境网络犯罪利用境内服务器、网络线路实现“非接触”通信，通信渠道监管存在漏洞

网络的境内外连通需要通信线路、服务器等技术支持。在通信线路方面，跨境网络连通需要租用电信运营商提供的国际专线，而国内存在大量专门从事跨境数据通信业务转租赁服务的公司。根据《工业和信息化部关于清理规范互联网网络接入服务市场的通知》《中国跨境数据通信产业自律公约》等规定，公司办理合法租用的跨境通信业务的只能自用不得非法转租，而在现实中，这些公司将合法租用的国际专线非法转租牟利，违法打通境内外网络通信，为跨境电信网络诈骗提供了技术支持，而相关监管部门对于国际专线被非法转租的问题监管措施执行力度有限，导致治理跨境网络犯罪无法实现釜底抽薪式的源头治理。

基于海淀院的案件数据发现，每一起电信网络诈骗及其关联犯罪中均存在通信渠道的问题，境内的被害人能够直接通过点击域名访问境外虚假网站进而被骗，但是依照《互联网域名管理办法》第五十一条，未在境内备案的境外域名不得在境内实现域名解析。海淀院针对电信网络诈骗案件的通信渠道进行大数据归集，发现涉嫌诈骗平台的服务器主要位于境外，但部分内容分发网络（CDN）加速服务器、跨境数据通信业务等通信、技术服务存在由境内云服务提供商、电信网络运营商提供的现象，导致境内的被害人能够直接访问境外在境内未经备案的非法域名导致被骗。如赵建宁帮助信息网络犯罪活动案中，海淀院通过串联各个孤立案件，形成案件大数据后发现，在同一时间段内存在 13 名被害人因下载、使用“无量”App 投资而遭遇电信网络诈骗，集中反映出电信网络诈骗分子引导被害人通过网络链接或二维码下载“无量”App 投资平台

，继而对被害人实施诈骗，而该涉诈平台能够在境内直接访问的技术原因，系电诈分子使用了境内的某公司云服务器与某电信运营商的通信线路。再如打击跨国电信网络诈骗犯罪的“长城行动”中，海淀院发现电诈分子非法使用跨境专线，使境内的被害人可以直接访问架设在境外、未在境内备案的涉诈网站域名导致被骗。此外，在姜某等人帮助信息网络犯罪活动案中，姜某等人自 2019 年起运营多家公司，在明知多个客户租用其服务器推广、运行赌博网站的情况下，仍为上述人员提供互联网接入和服务器维护、租赁、托管、技术支持等服务，致使违法犯罪信息在境内传播，非法获利人民币 7000 余万元。

二、违法信息通过“106”通知类短信、短网址、社交平台等进行“全渗透”，推广渠道审核问题突出

电信网络诈骗集团利用多种渠道发布信息诱导群众，推广渠道主要反映在通知类信息号段、短网址服务、网络社交媒体等方面，由于运营相关服务的企业审核缺陷与行政主管部门掌握相关线索情况不充分，导致了乱象的出现。

在通知类信息渠道方面，
境内的电信运营商往往将通知类短信号段出租给一级代理商，由一级代理商提供短信发送业务。按照现行规定，原则上一个一级代理商只能拥有一个短信号段并需在工信部备案，一个号码只能对应一个使用主体单位，用户看到相关号码即可对该短信的主体单位做出判断。然而，实践中一级代理商会往往继续将相关号段进行转租，层层转租后出现层级越低的代理商为了营利放宽对客户进行审核的情况，这导致了不法分子可以租用官方的短信通知号段，冒充官方发布通知类短信进行诈骗，对此类短信用户辨识难度大因而更容易被骗。如北京某科技有限公司帮助信息网络犯罪活动罪案中，该公司系“106”号段的三级代理商，因其审核存在疏漏不法分子得以租用该公司“10692283********”号码冒充山东省某市交管局，向被害人李某发送驾照考试预约的相关信息，骗取李某人民币 3 万余元。

在短网址服务渠道方面，
由于短信存在字数限制，通知类短信一般会将网站的完整域名压缩成短网址后发送。该类服务需求量大、掩饰性强，因为隐藏了真实的网址信息，用户无法直接判断短网址对应的网站性质。免费的短网址服务容易失效，一旦失效即无法通过起获的短网址追踪原始域名。司法实务中发现，企业和个体提供的短网址服务均存在被非法利用的情况，不法分子往往利用这种不稳定的免费服务转换钓鱼网站链接，给司法机关的追踪溯源工作造成了较大困难，而更为重要的是，目前尚无规范性法律文件对提供短网址的行为进行具体规制。例如，在北京某科技有限公司帮助信息网络犯罪活动的罪案中，不法分子利用某科技公司

的短网址服务，转换成钓鱼网站的链接，导致他人被骗。

在网络社交媒体渠道方面，
当前电信网络诈骗犯罪常常使用网络社交软件进行引流，犯罪分子将不特定的潜在被害人从 A 聊天软件中诱导至 B 聊天软件中，添加 B 聊天软件中电诈分子控制的账号，继而对其实施诈骗。司法实务中发现存在人脸识别同身份证照片完全不一致的情况，而运营软件的公司却未对其采取任何监管措施。如陈某某等人帮助信息网络犯罪活动罪一案，陈某某等人购买大量身份证、手机号注册了大量进行了人脸识别的“探探”账号，利用该软件冒充帅哥同不特定女性聊天，并要求不特定女性添加由不法分子实际控制的微信号，为犯罪分子提供了帮助。

三、有组织性收贩卡、虚拟账户层层隐蔽交易，资金渠道衍生新型逃避监管形式

当前电信网络诈骗犯罪已经链条化，不法收卡行为已经发展为有组织性的批量收卡，电诈分子往往可以收到多个下线向其非法提供的银行卡、电话卡，组织收卡者通过互联网跨区域召集他人办卡并收购，后统一邮寄转移至境外，从办卡、到收卡、再到寄卡，各个环节均不同程度存在违规、监管缺失等问题。金融机构基于完成考核任务的考量，往往选择大量发卡并为他人办理，对于后期非本人使用的卡未进行充分审查，更有甚者一些发卡营业网点的员工伙同他人恶意办卡、贩卖牟利。

银行卡中对公账户的日资金限额远高于个人银行账户，且对被害人具有一定的迷惑性，相较于个人银行卡被滥用产生的危害更大，目前大额电信网络诈骗中涉案钱款较多选择利用对公账户接收。对公银行账户的办理先要经由市场监管、工商登记部门审核，目前工商登记倡导线上办理，只需提供身份信息、远程人脸识别便可成功注册公司，不法分子利用上述简便方式注册公司信息后办理用于电诈的对公银行账户用于收款。疫情期间我国经济下行压力较大，商业银行对小微企业创业持鼓励态度、简化了对公账户的办理流程，此点也被犯罪分子趁机利用。同时需要注意的是，许多物流公司在邮寄环节，也未按照《电子商务法》等法律规范尽到必要的审查义务。

在国家加大对“两卡”犯罪打击力度的背景下，犯罪分子开始利用虚拟货币进行洗钱，且跨区域化、跨国化特征明显。该链条上游往往是电信诈骗、网络赌博、金融犯罪等，中游是洗钱组织者，下游是“炒币”、供卡、取现人。犯罪分子利用虚拟货币的技术特点，绕开国家外汇监管等一系列管控措施，将钱款以虚拟货币形式转移至境外。海淀院办理此类案件 8 件 25 人，如郭某某等人

掩饰、隐瞒犯罪所得罪案，被告人受他人雇佣，以炒虚拟货币赚钱为幌子，通过现金低于市场价格从“上线”收购泰达币（USDT），并同步卖出后取现交付“上线”，二人帮助“上线”洗钱共计人民币 580 万余元。再如瞿某、付某非法经营案，二人成为境外某未在境内注册、备案的书籍网站代理人后，帮助该网站在境内出售电子书并收取钱款，在扣除应收款项 14%
的手续费后，将涉案钱款转换成泰达币跨境转移，支付结算金额人民币 140 万余元，非法获利人民币 19 万余元。

四、对策建议

（一）强化电信网络诈骗犯罪在内的跨境网络犯罪的全链条打击与源头治理，注重通过法律大数据深挖孤立案件背后的监督线索

检察机关应当注重个案体现的碎片化特点，对于通信渠道、推广渠道等的违法犯罪线索进行挖掘、深化。通过建设智能大数据法律监督模型将审查、调查、侦查融合，通过大数据法律监督手段，挖掘出相关线索，以线索移送、检察建议等方式开展立案监督、侦查监督，同时延伸职能，挖掘行政监管漏洞及企业风控问题，推进多方监管、实现源头治理，引导科技向上向善，实现多效合一。

（二）针对通信、推广、资金渠道等方面的监管问题，发挥能动履职作用，畅通行刑衔接机制，督促履职整改，形成协同治理的合力

检察机关应当与工商、网信、网安等多部门建立信息共享、双向通报机制，定期通报数字经济相关法律及治理问题，形成司法与行政协同治理的合力，打通检察机关向金融机构、电信部门、互联网机构调取证据的便捷渠道，形成网络空间整治合力，从“九龙治水”到大数据贯通衔接、精准监督，推进形成共建共治共享的良好数字生态。

针对电信运营商的违规问题，检察机关可以制发检察建议等方式督促相关职权部门充分履职，要求他们针对短信信息、网络信息、国际专线等业务加强审核，针对违规、违法内容及时封禁，并对相关服务提供商进行行政处罚，同时向司法机关移送线索，多管齐下打击非法利用信息通信技术、为电信网络诈骗犯罪提供基础服务的犯罪行为。

针对电诈短信中普遍存在的短网址，检察机关应当建议国家网信办等部门建立监管制度，如在国家层面设置域名转化白名单（如将政府企事业单位网站、正规门户网站、正规备案企业网站纳入白名单，其内的域名链接可以转化为短网

址，并为其提供跳转服务），在短网址服务提供商层面设置黑名单制度（禁止对非法域名链接、投诉量大的域名链接阻止跳转，并将相关线索、情况上报行政主管部门）。

针对银行账户滥发不加审核的情况，检察机关应当建议中国银行保险监督管理委员会等行政主管部门严肃履职，对于银行肆意发卡的行为进行约束，建立责任落实到人的追究与倒查机制，使银行的客户经理、风控审核部门严肃发卡流程。

针对涉案企业存在严重违法行为、影响社会公共利益的，检察机关应当制发检察建议要求整改，必要时可启动公益诉讼程序进行调查，并决定是否提起诉讼。

（三）适时完善针对跨境数据通信业务的法律法规，明确相关企业运营者的权责划分

电信网络诈骗等跨境网络犯罪不可或缺的技术支撑之一即跨境数据通信业务，但是现有法律规范内难以对恶意非法提供跨境数据通信业务的行为进行刑事规制。跨境专线业务属于电信业务中的增值电信业务，经营该业务应当遵守《电信条例》的相关规定，该业务属于专营或限制经营的业务，使用者不得非法转租、转卖、非法提供他人使用。根据《最高人民法院关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》（2000 年）第一条，违反国家规定，采取租用国际专线、私设转接设备或者其他方法，擅自经营国际电信业务或者涉港澳台电信业务进行营利活动，扰乱电信市场管理秩序，情节严重的，依照刑法第二百二十五条第（四）项的规定，以非法经营罪定罪处罚。

未经行政主管部门许可擅自经营跨境专线牟利的行为，属于私自设置国际通信出入口的类型之一，违反了《电信条例》的相关规定，但是由于前述司法解释出台较早，仅对国际专线业务中的通话、信息业务做了规制，并未涉及国际专线中的跨境网络通信业务，导致司法实践中难以对非法从事该行为的主体进行监管与刑事规制。建议立法机关根据网络犯罪的新形势做出应对，可以适时更新、出台相关法律规范，对不法行为予以规制；司法实务部门对案件中发现的非法提供跨境数据通信业务主体，可采用拒不履行信息网络安全管理义务或非法经营向相关职权部门移送线索、履行法律监督职责，或以相关罪名予以刑事规制。

（本文刊登于《中国信息安全》杂志2022年第10期）