

## 电信网络诈骗犯罪的独特属性与治理路径

王 洁

(北京市社会科学院, 北京 100101)

**【摘要】** 电信网络诈骗犯罪简称电诈犯罪,是网络技术和传统诈骗相结合的新型犯罪,它内在的立体式、操控式、应和式特质,使得其社会危害性与传统的诈骗犯罪不可相提并论,对其采用传统的末端司法管控的治理模式难以达到良好的治理效果。治理电诈犯罪应充分考虑其态势与特性,从被害预防角度引入新的管控理念,以期实现被害主体不应和、单方面脱离诈骗锁链等目标,有效维护社会安全与公民权益。

**【关键词】** 电诈犯罪; 立体式犯罪; 操控式犯罪; 应和式犯罪

**【中图分类号】** D917.7

**【文献标志码】** A

**【文章编号】** 2096-3165 (2019) 04-0001-10

电信网络诈骗犯罪(以下简称电诈犯罪),是指行为人以非法占有为目的,利用通信信息技术和手段实施诈骗的违法犯罪行为。<sup>①</sup>2016年《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》要求“人民法院、人民检察院、公安机关要针对电信网络诈骗等犯罪的特点,坚持全链条全方位打击,坚持依法从严从快惩处,坚持最大限度追赃挽损”。从这些措辞可以看出,政府将刑罚作为主导的控制电诈犯罪的手段,高度重视对电诈犯罪的打击和治理。在公检法各部门的精

心部署和严打整治,以及从政府到社会各界多部门联动下,对电诈犯罪的打击取得了一定效果,如最高人民法院《司法大数据专题报告之电信网络诈骗(2016.1-2017.12)》显示,2017年在电诈案件审理数量上,福建、广东两地的案件量同比降幅显著。但是,2016年至2017年,全国电诈案件量呈上升趋势,2017年全国已结一审电诈案件量较2016年上升70.34%。2018年底,国务院打击治理电信网络新型违法犯罪工作部际联席会议决定“从2018年12月起至2019年底,在全国范围内组织开展为期一年的新一轮打击治理电信

**【基金项目】** 2019年北京市社会科学院重点课题“北京市涉众型经济犯罪治理研究”(2018A5284)的阶段性研究成果。

**【作者简介】** 王洁(1975-)男,北京市社会科学院法学所副研究员,博士。作者感谢美国科罗拉多州立大学 Olivia Yu 教授,中国政法大学皮艺军教授,中国人民公安大学陈洪彝教授,中国应用法学研究所周维明博士,南昌市人民警察学校陈利老师以及柳波、孙利、段伟、朱洪范等同门师友在本文写作过程中所提的修改建议。特别感谢接受课题组进行深度访谈的受访人,但为保护受访人及其单位隐私,在此只能匿名。

<sup>①</sup> 国际电联对“电信”的定义是:使用有线电、无线电、光或其他电磁系统的通信。按照该定义,采用符号、文字、声音、图像以及由这些形式组合而成的各种可视、可听或可用的信号,向一个或多个确定的接收者发送信息的过程,都称为电信。而电诈主要是指嫌疑人利用电信、互联网等技术和工具,通过发送短信、拨打电话、植入木马等手段,骗取或窃取被害人资金转入嫌疑人控制的银行账户,实施诈骗的违法犯罪行为。参见南京邮电大学信息产业发展战略研究院. 中国反电信网络诈骗蓝皮书(2016) [M]. 北京:人民邮电出版社,2017:1-6.

网络违法犯罪专项行动。”<sup>[1]</sup>这些都说明,在重拳打击下,全国范围内的电诈犯罪并未偃旗息鼓,而是在不断变换手法、升级模式、扩散区域<sup>[2]</sup>。在互联网犯罪手段不断升级更新的背景下,公检法机关管控电诈犯罪的治本效果是有限的,而司法机关介入时犯罪已是既成事实,只能在末端补救正义。当前需要适应信息时代趋势,在充分考虑电诈犯罪独特属性的基础上,创新治理手段,充分激发潜在被骗人的被害预防理念,才能从根本上管控电诈犯罪的蔓延。

## 一、电诈犯罪的独特属性

电诈犯罪是网络技术和传统诈骗相结合的新型犯罪,诸多既有研究较为强调信息技术对传统诈骗犯罪的“赋能”,关注电诈犯罪的非接触性特质<sup>[3]</sup>,说明犯罪隐蔽性强、智能化高<sup>[4]</sup>,以及由此导致的取证难、抓捕难、定性难、追赃难等等<sup>[5]</sup>。可以看出,既有研究主要是从犯罪控制角度研究电诈犯罪,强调通过控制、打击犯罪人进而减少犯罪。换言之,对于电诈犯罪而言,少有论文从被害人权利保护角度研究如何减少电诈被害。电诈犯罪与传统诈骗犯罪有重大差异,通过刑罚惩罚电诈犯罪,只能在事后发挥刑事责任的追究功能,而无法实现被害的事前预防。电诈犯罪内在的立体式、操控式、应和式特质,使得其社会危害性与传统的诈骗犯罪不可相提并论,传统的犯罪治理模式并不适应此种新型犯罪行为。<sup>①</sup>

### (一) 电诈犯罪是一种立体式犯罪

传统诈骗犯罪多是一种线性犯罪,犯罪人通常要直接和被害人进行面对面互动才能获取被害人财产;但是,科技发展使得电诈犯罪成为一种非线性犯罪,犯罪人不与被害人进行面对面接触,犯罪人借助电话、网络设计骗局,使被害人置身于虚假信息的全方位、立体式包围中,形成一种

“逼真”环境,并通过隔空操纵,让被害人“自愿”地交付财产。作为一种立体式犯罪,犯罪人通过全方位、多链条地设置骗局,对被害人进行心理钳制,向被害人发送犯罪指令,不断裹挟被害人配合实施犯罪行为,危害性凸显:

其一,犯罪外卷。犯罪外卷主要是指为了实现特定目的,犯罪行为不断延伸翻卷,不仅让更多的人加入犯罪圈成为犯罪人,而且使犯罪行为精细化,犯罪破坏力提升。首先,从犯罪行为要素的角度来看,实施电诈犯罪,通常需要搜集公民个人信息,然后利用电信网络实施诈骗,最后达到通过银行取款提现目的。完成这些犯罪行为需要众多犯罪人的分工、协作,实际上也就是通过众多犯罪人对被害人进行全方位、立体式围猎。根据刑法基本理论,在各行为人明知犯罪目的时,构成诈骗罪的共同犯罪;在不明知时,则可能分别构成侵犯公民个人信息罪、诈骗罪或掩饰、隐瞒犯罪所得罪等。概言之,电诈犯罪行为呈弥散性扩散趋势,导致更多的人成为犯罪人。<sup>②</sup>其次,从犯罪专业化角度来看,众多犯罪人的逐利加入和生存竞争,会进一步提升犯罪技术水平,推动犯罪行为向更加专业化、精细化的方向发展。立体式犯罪通常可归类于《刑法》第26条规定的集团犯罪,<sup>③</sup>这些犯罪集团采用高度公司化管理机制,分工协作水平较高。在高度分工情况下,犯罪人仅仅是犯罪链条中的一个环节,犯罪人之间松散的联系也可能让犯罪人感觉不到其是在实施电诈犯罪行为,无需担心被追责。犯罪集团利用此种机制不断扩大犯罪规模,使得犯罪能量增大,犯罪破坏力增强。

其二,被害内卷。被害内卷是指被害人自身在一定时间内处于持续被骗过程中,并且被害程度不断加深的现象。首先,从被害时长来看,传统诈骗犯罪多是在较短时间迅速完成或者一次完成。这是因为:在熟人社会活动区域中,很少有

<sup>①</sup> 有研究指出,我国的惩治犯罪的刑事对策主要是以传统犯罪为基准设置的,故应对传统犯罪较为有效;而沿袭传统犯罪的对策应对网络犯罪,没有充分考虑网络犯罪自身的特点,导致刑事对策在一定程度上失灵。“从一定意义上讲,网络犯罪是‘现代’的,而应对网络犯罪的对策却还是传统的,所形成的局面可能是‘人在天上飞,我在地下追’。”参见喻海松:《网络犯罪二十讲》[M],北京:法律出版社,2018:5-6。

<sup>②</sup> 为了实现精准诈骗,部分犯罪人会采用代码病毒去搜集潜在被害人相关信息,而此时,犯罪人需要找人写码,产生写码人(码农);随着分工发展,随之产生售码人;最后就到用码人(骗子)手里,而这些为电诈“服务”的“开发者”都可能会被认定为犯罪人,他们的行为可能构成诈骗罪,也可能构成《刑法》287条之二的帮助信息网络犯罪活动罪。

<sup>③</sup> 最高人民法院公布的《司法大数据专题报告之电信网络诈骗(2016.1-2017.12)》显示,2017年全国已结一审电诈案件中共同犯罪率为44.78%。

机会对被害人进行持续不断的诈骗,因此被害人较少,被害程度相对有限。但是,依靠心理学技术和网络技术相结合的精准信息诈骗,不仅能找到“合适”的犯罪对象,还能对犯罪对象的心理特征及财产信息进行研判,由此不仅让很多民众上当受骗,还让被骗人在一段时间内持续地、“主动地”将所有财产“让与”犯罪人,被害程度逐步加重。其次,从被害严重性来看,立体式犯罪使得犯罪人对被害人“服务更全面”,不仅骗取现金等流动资产,还要求被害人通过抵押、质押等方式变现固定资产,类似假民间借贷外衣行诈骗之实的“套路贷”<sup>[6]</sup>,被害程度比传统诈骗犯罪严重很多。

综上所述,犯罪外卷使犯罪圈扩大,被害内卷使犯罪危害加深。立体式犯罪更可能形成一种犯罪产业,犯罪链条不断延伸,推动更多的犯罪产业发展。犯罪产业化水平提高,不仅会使犯罪分工加强、犯罪链条加长、反侦查能力提升,更会使相应的被害人数倍增,被害程度加深。

## (二) 电诈犯罪是一种操控式犯罪

电诈犯罪的专业化和精细化,使得作案方式类似于流水线生产,当事方只要在特定阶段完成特定角色即可,并不需要发挥当事方的主观能动性。从某种意义上说,部分电诈犯罪人、被害人等逐步呈现物化特性,他们被电诈集团当作犯罪工具或者“棋子”,受制于电诈集团主犯,被精细设计的诈骗剧本和程序操控,电诈犯罪的社会危害性被逐步推高。

其一,心理操控。为了使诈骗更具有欺骗性,犯罪人会“精心研发”诈骗技术,针对被害人心理进行预判,并预设相应的机制去全方位“帮助”被害人,由此将被害人套入骗局且深信不疑。心理操控可以分为两种类型:一种是恫吓型操控,嫌疑人冒充司法机关、冒充黑社会等对当事人进

行恫吓,逼迫被害人进行转账;另一种是利诱型操控,嫌疑人利用中奖、送手机、积分兑换、网络贷款等利益形式,向当事人抛出利益,诱使被害人将资金转账进入他们控制的账户。利诱型操控可以进一步划分为物质性利诱和精神性利诱。<sup>①</sup>无论哪种类型操控,嫌疑人基本都是按照预先研发的骗术对被害人进行心理操控,让被害人比较容易形成代入感,诱使被害人陷入环环相扣的链条之中,无暇去验证信息真伪,深陷骗局而不能自拔。

其二,技术操控。在当事人不知情或者未授权情况下,嫌疑人通过远程控制技术手段,对被害人的财产处置等关键信息进行相关操作,骗取或者窃取被害人财物。典型例子如,嫌疑人基于概率,随机向当事人的手机、电脑等发送隐藏木马病毒的链接,一旦当事人点击链接,木马病毒就会自动窃取与被害人手机、电脑绑定的银行卡信息。然后通过控制被害人电脑操作网银,把被害人的网银资金直接转入嫌疑人控制的账户。

无论是故意杀人、故意伤害、强奸、抢劫等自然犯罪,还是非法经营、非法吸收公众存款等法定犯罪,抑或是传统的诈骗犯罪本身,其中的犯罪人与被害人多数都有面对面的互动和接触,否则犯罪就不能完成。而互动过程中必有可能留下相关痕迹,便于司法机关采集证据后进行追责。但是,电诈犯罪人通过电话、信息、网络等方式进行遥控操纵,回避和当事人面对面的接触,不仅使犯罪现场证据极大地减少甚至没有证据,增加司法机关追责的难度,而且还使得当事人报案缺少有效证据,使司法机关介入匮乏依据,从而让犯罪人较轻易地逃避司法机关的打击。

## (三) 电诈犯罪是一种应和式犯罪

电诈犯罪通常有三个基本阶段,即搜寻被害人信息、实施骗术、转账提款。这三个阶段又不

<sup>①</sup> 2018年由最高人民法院、中央电视台联合评选为“2017年度推动法治进程十大案件”的“徐玉玉被电信诈骗案”是物质性利诱的典型案。该案由2016年《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》颁布的主要动因之一,影响甚大。“徐玉玉被电信诈骗案”主要案情如下:2016年8月19日,已接到大学录取通知书的徐玉玉,在临沂市公安局罗庄分局报案,其9900元学费通过自助取款机转账被骗。在离开公安局回家的路上,徐心力衰竭,被立即送医院,21号经医院抢救无效死亡,时年19岁。此案发生之后,当地公安机关22号立案,23号成立专案组,26号就有犯罪嫌疑人被抓获,至28日首要分子陈文辉投案之日,此案主要犯罪嫌疑人都被抓获。也就是说,各地公安机关协同银行、电信等相关部门,仅仅用了9天时间就破案。2017年7月19日,临沂市中级人民法院一审分别判处7名被告人无期徒刑和3年到15年不等的有期徒刑。部分被告不服,提起上诉。9月15日,山东省高级人民法院做出二审刑事裁定书,裁定驳回被告人上诉,维持一审判决。参见王祎,2017年推动法治进程十大案件评选揭晓[EB/OL].[2019-05-23].<https://www.chinacourt.org/article/detail/2018/02/id/3196549.shtml>.

断细分成不同层级、不同环节,环环相扣才能诈骗成功。尽管电诈犯罪结构复杂,但被害人的应和是诈骗完成的关键环节,可以说,“无应和,无电诈”。犯罪人通过被害人的回应和双方的互动,一方面过滤掉那些不太可能被骗的人,比如那些听到中奖信息的人因为不相信“天上掉馅饼”就立即挂电话的,或者对司法程序较熟悉因而不相信电话讯问、安全账户的等等,从而提高犯罪效率;另一方面,更全面地掌握与被害人财产相关的信息,实施精准诈骗,“诈干”被害人所有财产,提高犯罪收益;并且,通过立体式操控,使被害人自己“同意处分”甚至“帮助处分”财产,还会使被害人基于自责、羞愧等心理不敢报案,司法机关无法介入,由此进一步降低犯罪风险。

其一,主动应和。这主要是指潜在被害人轻信嫌疑人的骗术,“积极参与”诈骗进程,从而使诈骗犯罪顺利完成。由于涉及通话、转账、取款等手续,电诈犯罪往往要经过一定的时间跨度才可能既遂。在被害过程中,部分被害人仅凭直觉就相信来电或者信息的真实性;即便有所怀疑,或者在别人提醒下有所怀疑,也多数会反复暗示自己,“这应该不是骗子电话”“他们应该不会是骗子”等等,被害人通过这种心理暗示机制,不自觉地去“营造”一种被骗环境,将自身陷入骗局而不能自拔,从而使骗术得逞。实践中被害人不顾银行、公安机关劝阻执意要给诈骗分子转账的报道时见报端。<sup>①</sup>“在许多骗局中,对于说谎者的破绽,受害者总是故意不去面对,一厢情愿地往好的方面设想,害怕谎言一旦拆穿,可怕的后果将难以收拾,于是成了骗局得以持续下去的帮凶。”<sup>[7]</sup>传统诈骗犯罪比如以假钞或者假金饰的

方法施行诈骗,主要是面对面即时完成,当发觉被骗之后,被害人虽然也可能说“他们不会是骗子”这类话语,但此时只不过是犯罪既遂之后被害人寻求的一种心理安慰而已。

其二,被动应和。主要是指潜在被害人基于畏惧、怕事、厌讼等心理,消极地“配合”犯罪人完成诈骗行为。“冒充公检法诈骗”作为诈骗高端形态之一,就在于犯罪集团充分掌握被害心理,并根据被害心理“研发”骗术,让潜在被害人深陷诈骗圈套之中,成为犯罪人侵害自己财产的工具。被动应和则多存在于恫吓型诈骗中。如调研发现,有一位被害人居然每天都和诈骗人保持联系,并按照诈骗人指示,早晨、中午、晚上分阶段“报平安”,<sup>②</sup>在近30天的时间里,被害人一直置身于犯罪人编织的“诈骗锁链”中,竟然没有“挣脱”,不断转账400多万人民币进入犯罪人账户。被骗人说“女儿这段时间比较忙,不能经常回来,即便回来,也是简单说几句,不敢将转钱的事情告诉女儿”;“天天都睡不着觉,让孩子损失这么多,对不起孩子!”<sup>③</sup>

电诈犯罪的立体式、操控式特性,使得卷入犯罪的嫌疑人数增多,相应的被害人数增多且财产损失增大,司法机关对犯罪人处罚过程中就可能存在打击范围界定模糊、刑罚裁量轻缓不当、法律实施不公平等问题,其不仅会导致被害人损失无法追回,同时会让部分犯罪人侥幸逃脱法网。电诈犯罪的应和式特性,使得被害人在发现财产受损后,为了面子问题,通常不太愿意报案,由此使得部分犯罪人得以逃避法律追究。电诈犯罪的独特属性,使得电诈犯罪人获利极高而遭受惩罚的可能性却极低。此种“低风险高利润”犯罪

① 也正是基于自陷性犯罪,被害人信条学主张对于那些信任明显拙劣、虚假骗术的被害人不予刑法保护。

② “报平安”意思是没有被受骗人以外的人发现。通过“报平安”,诈骗人控制犯罪进程。

③ 被骗人:Z女,原铁道部退休人员;住址:北京市丰台区;调研时间:2018年2月3日。电诈犯罪是新型犯罪,基于电诈案件特性,很多被害人被骗后不向公安机关报案,被害后也不愿意接受访谈;而诈骗犯罪人或者被拘禁,或者潜藏在社会之中,更是不易接触,课题组很难获取科研需要用到的数据。故此,采用量化研究,其数据结果可能不易剖析电诈犯罪多发的原因,尤其不能揭示司法机制管控电诈犯罪的效果。作者主持的“北京市涉众型经济犯罪治理研究”根据课题实际需要,采用质性研究方法,直接针对在司法机构中工作的刑事司法人员和电诈案件的被害人、犯罪人进行深度访谈,以及对公安机关的办案卷宗进行文本分析,以此来判断司法机制管控电诈犯罪的作用和效果。目前,通过非概率抽样,课题组已经对14位在刑事司法机构中的专业人士和5位被害人进行了深度访谈。为保护受访人及其单位隐私,课题组对相关受访人员进行编码,并采取匿名保护措施。论文中凡是引用受访人的话语都用引号予以突出,并以脚注形式予以说明。本文所用数据除特别注明外,均为作者调研所得。

行为对犯罪人有很大的吸引力。<sup>①</sup>正如反诈骗电影《巨额来电》中女主角说的,“放着弯腰就能捡钱的生意,谁还会老老实实地做买卖啊”。

## 二、司法管控电诈犯罪的有限性

各省公安机关成立反电诈犯罪中心或者打击平台,依靠公安机关和银行、电信等部门联合办案,合成作战,对被害人被骗财物进行拦截、止付、冻结,并根据电诈犯罪特点,有针对性地进行类似于手机卡实名制、ATM 转款 24 小时到账等相关制度建设,有效地控制了电诈犯罪高发态势。但是,电诈与传统诈骗不同,《司法大数据专题报告之电信网络诈骗(2016.1-2017.12)》显示 2016 年至 2017 年,全国电诈案件中排名前五的诈骗方式是电话、短信、木马病毒、钓鱼网站、QQ,其通常没有物理空间意义上的犯罪现场,且是通过远程通讯方式实施犯罪,这就导致物证痕迹较少,加之,电诈范围往往跨区跨境,调查取证困难等等,使得电诈犯罪收益高而犯罪风险极低。当前,全球化、数据化和自动化为电诈犯罪空间拓展提供了机会,而司法管控的技术仍然不能紧跟犯罪者的步伐,某种意义上,也是为电诈犯罪提供了发展的“契机”。根据 Cyber ROAD 项目在欧洲国家所作的调查,只有 8% 的网络犯罪被成功起诉<sup>[8]</sup>。中国的情况而言,有消息说国内电诈案件的破案率不超过 3%<sup>[9]</sup>。鉴于电诈犯罪的独特成因、内在属性、社会环境等因素影响,刑事司法机关采取的“末端治理”行为,虽有亡羊补牢之效果,却很难成为治理电诈犯罪的长效机制。

### (一) 电诈犯罪的成因阐释

随着互联网的高速发展,物理空间与网络空间界限的模糊,线上线下的无缝对接导致了社会生活的在线化,同时也导致犯罪向在线方式发展。日常活动理论(routine activities theory)在解释犯罪行为中,把微观情景模型(个人的决定和行为)结合到宏观情景模型中(如人们社会活动的时空

范围模式)。对微观情景,该理论认为,犯罪行为的发生需要有三要素的同时存在,包括:(1)有犯罪动机的人的存在;(2)有适合犯罪的靶子;(3)缺乏有控制力的监管。在宏观情景变化时,个人的行为会随之改变<sup>[10]</sup>。日常活动理论能较好解释中国当前高发的电诈现象:(1)中国人口总量世界第一,网民规模有 8.29 亿,<sup>②</sup>互联网使人与人的联系更为便利;当前经济下行压力增大,下岗失业人口增加,由此导致有犯罪动机的人大量存在。(2)人口基数大,人口素质差异大,网络加速了人与人之间的联通,犯罪人通过网络能联系到更多的潜在被害人;同时,诈骗技术也不断更新迭代,网络技术的发展加深了知识的隔阂,使得多数潜在被害人更容易上当受骗。(3)电诈犯罪人以电信网络为犯罪工具,而政府对网络的监管一方面是技术较低,另一方面是监管缺位。三方面因素综合影响,使得当前电诈犯罪情势严重。

犯罪饱和理论主张一定的环境与犯罪数量之间的比例是相对稳定的,对犯罪的打击行为不会减少犯罪,只会使犯罪转移到其他地区,或者其他行业,以另一种犯罪形式继续存在<sup>[11]</sup>。当下司法部门采取的针对高危地区进行挂牌督办治理行为,可能在短期内促使当地政府加大治理力度,遏制诈骗行为产生的总量;但是,如果不能同时对诈骗“亚文化”进行校偏,司法机关打击力度降低之后,该犯罪仍然会再次发生,或者是更新形式继续发生。课题组在江西省某县调研时,当问到当地是否有人继续诈骗,受访人低声说,“其他人仍然在悄悄地做”,<sup>③</sup>这说明该地区打击效果仍然有限。

### (二) 电诈犯罪的社会基础

#### 1. 电诈犯罪是网络黑灰产业链中的一个环节

从整个网络违法犯罪态势的大背景来看,电诈犯罪仅仅是一条长长的网络黑灰产业链中的一个环节。国内黑灰产业链中涉及电诈犯罪的主要包括恶意软件撞库编写、洗库、拖库以及与侵犯

① 已有研究指出,国内电诈犯罪成本低,表现为犯罪条件容易获取,用于实施犯罪的金钱支出少,大量犯罪分子得以逃避刑事处罚和社会谴责;同时犯罪收益高,表现为犯罪分子实现了财富的积累、社会地位的提高和心理的满足。参见陈晓娟. 我国电信网络诈骗犯罪的犯罪学分析[J]. 山东警察学院学报, 2017(5).

② 2019 年 2 月 28 日,中国互联网络信息中心(CNNIC)发布第 43 次《中国互联网络发展状况统计报告》。报告显示,截止 2018 年 12 月,我国网民规模为 8.29 亿,其中手机网民占比达 98.6%,互联网普及率达 59.6%。访问网址: <http://www.cnnic.net.cn>。访问时间:2019 年 4 月 29 日。

③ 受访人:T,男,农民;住址:江西省余干县;调研时间:2018 年 2 月 12 日。

公民个人信息相关的非法倒卖电话卡、身份证、银行卡等违法犯罪活动。目前黑灰产业已经呈现出链条的形式,而整个链条就其上游、中游和下游来讲已经形成了完整的流水化作业。数据显示,目前国内从事黑灰产业的人员已有40万之多,而该群体的年龄平均不到23岁<sup>[12]</sup>。中国互联网协会2016年的调查报告显示,近一年时间,国内6.88亿网民因垃圾短信、诈骗信息、个人信息泄露等造成的经济损失估算高达915亿元<sup>[13]</sup>。几乎每一起网络犯罪的背后都有强大的黑灰产业链的阴影。如何治理日益发展的网络黑灰产业链,营造清朗的网络空间,成为我国网络治理亟待解决的问题。

## 2. 网络黑灰产业链是电诈犯罪屡打不绝的重要因素

由于防控电诈犯罪涉及整条黑灰产业链,往往超出公检法机关的职权范围,结果就造成了“三难”:一是控制赃款难,犯罪分子往往在网络黑灰产业链其他环节的帮助下,很快将赃款通过各种途径迅速转移,给破案追赃带来极大困难;二是抓捕犯罪分子难,电诈犯罪及其关联犯罪往往形成一种黑灰产业链,犯罪分子往往都是链条上的一员,分布在全国各地,甚至窝藏在境外,彼此之间互不相识,随机组合实施犯罪,因此抓捕犯罪分子困难重重;三是工作协调难,公检法机关侦查办案过程中大多需要金融、通信等行业的合作,由其提供挂失支付、信息查询等服务,涉及的部门多、级别高,协调难度极大。

### (三) 司法机制的治理效果

#### 1. 刑事司法资源有限性使得打击范围有限

公安机关采取的拦截、止付等行为是在犯罪人实施犯罪行为过程中实施的,这种警务行为主要针对的是具体的、现实的被害人。受限于警务资源的有限性,其数量必然是有限的;多数被骗者并不能享受到公安机关提供的此种“警务服务”,社会损失仅是在相对范围内有限降低。换句话说,仅有少数被骗者能及时被公安机关提醒并醒悟,进而减少财产损失。

#### 2. 司法末端治理无助于减少诈骗被害数量

一方面,司法行为具有保守本性。电诈犯罪案件进入司法机关处置流程,就表明犯罪行为已经发生或者实施完毕,犯罪已经造成社会危害后果,被害人已经产生。换言之,如果没有证据表

明犯罪已经发生,司法机关通常不能启动司法程序;如果有证据证明犯罪发生,则无论司法机关如何处置犯罪人及其实施的犯罪行为,被害人均已经产生。司法机关的治理举措并不能减少已经发生的电诈案件。另一方面,司法末端治理具有天然弊端。司法机关目前采取的集中治理模式,在一定时间内有助于挽回部分损失,但是随着时间推移和科技进步,犯罪人使用的技术也在不断更新迭代。比如当下公安机关对电话通话实施监听比较容易,但是对于微信语音通话、网络通话则很难监控、很难拦截,同样电诈犯罪的资金流也难以被管控。如果不能及时完善并提升治理电诈的技术,电诈犯罪就可能发生。

#### 3. 网络犯罪证据取证难导致打击力度弱化

传统诈骗犯罪可能留有指纹等具有唯一性的证据,采集到指纹进行比对,有助于快速并且较准确地锁定犯罪嫌疑人;但是,囿于电诈犯罪属于非接触性犯罪,在电诈案件中,没有类似于DNA一样具有高度识别性的证据,特别是电诈案件中很多被害人都是经过一段时间之后才发现自己被骗,而相关电子信息已经被更新或者删除,更是难以采集到高度识别性的证据。尽管目前公安机关在研发类似于声纹比对技术,但目前仍有制度和技術瓶颈约束。

基于以上对电诈犯罪成因、治理效果、社会基础等的分析,以现有模式对电诈犯罪进行管控治理,导致的直接后果有三:其一,对犯罪人打击不力。一方面部分发生的电诈案件因为证据薄弱,只能根据有限的证据对犯罪人进行指控,降低了打击力度;另一方面,多数发生的电诈案件因为证据缺失不能被立案,成为“犯罪黑数”。不立案的直接后果就是不对犯罪人进行刑事追责,诈骗犯罪人依然可以继续行骗,导致诈骗犯罪总量持续上升。其二,对被害人的保护不到位。对被害人的财产损失很难进行补偿。有检察官说,他承办的案件中,诈骗金额的50%以上通常都不能追回,这些赃款被用于犯罪人的消费、投资甚或转移出境,被害人损失无法挽回。有针对司法管控电诈犯罪的实证研究发现,电诈犯罪中被害人80%以上的钱款都无法追回。<sup>①</sup>其三,政府权威下降。尽管电诈案件中的被害人有一定的责任,但是社会上却往往将损失不能挽回之责转嫁给行

<sup>①</sup> 相关研究可参考:王洁《司法管控电诈犯罪的效果考察》即将刊出。

政、司法机关,使得政府权威下降。当犯罪人假冒公权力机构行骗成功一次,政府在人民群众中的权威也就被侵蚀了一次。

### 三、电诈犯罪治理路径: 被害预防

如上所述,基于电诈犯罪的独特属性,仅仅依靠公检法机关的强力打击,治理效果是有限的。因此,必须另辟蹊径。本文认为,在信息化时代,电诈犯罪治理应该由打击犯罪转向犯罪预防。所谓犯罪预防,是指由国家、社会乃至个人采取各种方略与措施,致力于减少、消除犯罪形成的致罪因素,对于个体犯罪现象以及社会犯罪现象予以预先防范的一系列活动<sup>[14]</sup>。犯罪预防有两个着眼点:一是着眼于犯罪人,从犯罪人的角度去预防犯罪(犯罪人预防);二是着眼于被害人,从被害人角度去预防犯罪(被害预防)。过去的犯罪预防偏重于犯罪人(一般预防与特殊预防)。但是近来的犯罪学研究表明,被害人的行为和个性特征在许多情况下可能成为犯罪人实施犯罪侵害的借口和契机,很多犯罪(尤其是电诈犯罪)是犯罪人与被害人彼此“配合”的结果<sup>[15]</sup>。因此,为了更有效地预防电诈犯罪,就有必要更深刻地理解电诈犯罪行为发生的机制。在这一过程中,仅仅研究和了解犯罪分子是远远不够的。我们还需要研究和了解被害人及其被害可能性,并在此基础上进行被害预防。防治电诈犯罪的实践表明,被害预防是控制电诈犯罪、降低其犯罪率乃至消灭这一犯罪过程中极其重要的一个环节。

#### (一) 对电诈犯罪被害现象的心理学解释

美国著名心理学家丹尼尔·卡尼曼教授在《思考,快与慢》一书中提出的“系统1”和“系统2”概念,用来说明人们总是更容易通过“系统1”去解决问题,因为“系统1是无意识且快速的,不怎么费脑力,没有感觉,完全处于自主控制状态”,比较容易启动。“系统2”是启动质问和怀疑的思考机制,但人们较少通过“系统2”去解决问题,因为“系统2将脑力转移到需要费脑力的大脑活动上来”,而这费时费脑的思考机制通常不是人们处理问题的优先选项。

因此,电诈被害人在接到诈骗电话之后,更倾向于用“系统1”即更多地通过直觉思维机制选择相信犯罪人的话语,并仓促做出决定,甚至形成一种认知错觉,认为骗子说的是真话,其他介

入帮助者说的是假话,由此使得诈骗链条不容易挣脱。“因为系统1不仅好骗,还容易产生偏见,而尽管系统2掌管怀疑和不信任的大权,但是它有时很忙,不忙时也很懒惰,总会擅离职守。的确,已有证据显示,当人们劳累或是精力耗尽时,更容易受那些空洞却有说服力的信息影响。”<sup>[16]</sup>

按照卡尼曼教授的分析,“系统1”包含了对这个世界的认知模式,能立即估测哪些事情是正常的,哪些是出人意料的,它是人们做出快速直觉性判断的依据,且这种判断十有八九是准确的,而人们所有判断活动几乎都是在这一系统的指引下毫无意识地完成的。然而,卡尼曼教授又指出“系统1”也是人们直觉中很多系统性错误的根源。也就是说,日常生活中“十有八九”事情都可以凭借“系统1”的本能反应进行正确处理,类似于日常购买鸡蛋、青菜、逛超市购买家居用品等普通消费都可以依据直觉性判断进行,不会酿成重大错误。可是,“十有八九”也暗示“十有一二”会出错,用俗语说就是“聪明一世,糊涂一时”,这一方面意味着电诈犯罪人有机可乘,同时也说明每个人都有可能成为电诈犯罪的被害人,因为每个人都有可能出现疏忽大意、过于自信等心理状态。不过,如果我们克服惰性,提升理性,在做出重大决定时多启动“系统2”进行审慎思考,我们就有可能避免这些错误,尤其是避免成为电诈犯罪的被害人。在当前防范化解重大风险时期,党和政府更要提醒民众,在通过电信网络处理转账付款的时候,需要尽量减慢速度,谨慎核对相关信息,尽量减少被骗。

#### (二) 治理电诈的根本措施: 被害预防

刑事司法机关的打击并不能有效降低电诈犯罪行为发生。与其他传统暴力犯罪、财产犯罪不同,从减少被害的角度看,电诈犯罪由于其本身运作上的特性,有必要做好被害预防,而预防所需的投入也相对较少。

1. 被害主体不应和: 没有被害人配合,电诈犯罪就不能完成

无论是故意杀人、故意伤害、强奸、抢劫等暴力犯罪行为,还是盗窃、侵占等财产犯罪行为,不管被害人是否配合,凭借犯罪人自身的暴力就可以径直实施;但是,电诈犯罪中,犯罪人往往是通过电话、短信、网络等手段,在不与被害人直接接触情况下,通过隔空对话实施心理影响,进行心理干预,引导被害人自己逐步进入陷阱。

司法实践中,电诈犯罪中被害人与犯罪人的“配合”增加了公安司法机关办案的难度。据某公安局反诈中心警察介绍,在“清华教授被骗1700万”案件中,<sup>①</sup>被骗教授接到诈骗电话之后,警方在很短时间也拦截到相关信息,并且给该教授打电话,提醒她不要被骗,但是该教授不信,也不听警方的劝告;随后,警方联系该教授的家属,让其劝告事主不要上当;之后,警方再追问其家属是否劝告事主,该家属回答说“以后你们别管了”。由此,该教授通过多次、连续被骗、转账,造成至今仍不能挽回的财产损失。实践中也发生过警方、银行工作人员劝阻事主不要被骗、不要转账时反而被事主辱骂的情况。没有被害人及其家属的配合,警方也无法破除被骗者的沉迷。

因此,在整个电诈操作程序中,只要有一个环节中断,或者说,只要被骗人能及时认识到诈骗行为,并不予应和,被骗人就可以免于被害。由此,需要唤醒民众的预防意识,即“不应和”意识,让民众知道通常诈骗犯怎么说话、要怎么应对,在遇到类似情况下,能及时唤醒自身的预防机制进行应对。

## 2. 摆脱锁链: 被害人单方面就可以脱离诈骗锁链

类似于上面提到的故意杀人、故意伤害、强奸、抢劫等犯罪行为,其通常不是共同犯罪,其并不需要进行类似于电诈犯罪这样的分工,其作案手段更没有电诈犯罪如此的复杂。在冲动型杀人犯罪行为中,可能随手捡拾的一块砖头或者木棒就成为命案的凶器,而从犯罪行为实施到犯罪既遂也就在几分钟内完成。生活实践中,被害人对于此种临时起意型犯罪的预防存在极大难度。

但是,电诈犯罪手段相对比较繁琐,需要在不同犯罪人之间进行“链接”,《司法大数据专题报告之电信网络诈骗(2016.1-2017.12)》显示,通过电话方式进行诈骗链接的案件占比高达52.88%,由此却也给被害人挣脱诈骗链条提供了时机。根据当下公安机关办案人员对电诈犯罪的总结分析,均发现犯罪团伙内部有分工,即“一线、二线、三线”等。以实践中发生比例较高的“冒充公检法诈骗”为例,其中“一线”是前台工

作人员,强调事主办理的信用卡有问题或者有人冒用其身份证信息等,让事主赶紧联系“公安部门”;随后,“二线”“公检法人员”登场,以“公检法”公权力机关身份,严肃告诉事主涉及严重犯罪行为,让事主“举证”证明其“无罪”,在此过程中进一步套取事主的信息,同时也是进一步实施心理控制;接着,“三线”登场,建议事主按照他们的指令将资金转移到“安全账户”。这三线之间需要起承转合,并不是无缝连接,也很难在短时间内分分钟迅速完成。在此期间,当事方有足够机会挂断电话、停止聊天、终止转账等等,从而摆脱诈骗锁链。

## 3. “捂紧自己的钱袋子”: 被害预防成本低且较为有效

相对于暴力犯罪,电诈犯罪更具可防性。课题组对10多位在公检法机关工作的人员进行深度访谈,受访人员均强调被害预防的重要性。某刑侦总队的警察在办案实践中,曾成功阻断一个欲通过手机转账400多万人民币的个案,其时当事人正拟告诉犯罪人短信验证码,该警察电话告知当事人说刚才才是骗子,当事人幡然醒悟,及时终止了转账行为,从而有效地避免了巨额财产损失。但当被问及“如果您现在是反电诈中心的主管人员,您现在最想要做什么”时,受访的警察谈到,其最想做的“首先是思路转变,因为打不胜打,容易上当的人更多。”<sup>②</sup>

“转变治理思路”的观点与在一些公开场合的会议发言有显著差异:与会人员通常会强调办案机关在人、财、物方面的资源紧张,要求上级部门增派人手、增加财力、增添物资;而这位从警十多年的警察基于其办案经验,认为要从治理理念角度进行转变,也就是要从偏重打击转变到预防优先。而在检察院工作的受访检察官也同样认为“提高反诈骗意识,关键是‘捂紧自己的钱袋子’。从预防角度看,投入成本最低。”<sup>③</sup>2019年6月7日,中华人民共和国公安部从西班牙成功押解94名“冒充公检法”进行电诈犯罪的嫌疑人回国,参与办理此案的公安部刑侦局电信网络诈骗侦查处负责人在2019年6月接受中央电视台记者采访

<sup>①</sup> 媒体报道被骗金额有1760、1800万等。具体案情参见:清华教授被骗1800万,台警方通报案件细节[EB/OL]. [2019-07-08]. <http://news.cctv.com/2017/02/18/ARTI5JataqhGwHz7iha2gKHw170218.shtml>.

<sup>②</sup> 受访人: B 男,警察,从警11年;住址:北京市丰台区;调研时间:2017年12月26日。

<sup>③</sup> 受访人: C 男,检察官,入职5年;住址:北京市东城区;调研时间:2017年10月10日。



时,明确说治理电诈犯罪“防范还是第一位的”。<sup>①</sup>

需要指出的是,传统犯罪学理论也强调犯罪预防,即通过惩罚、监禁已经实施犯罪的犯罪人,让其不能再犯罪,并由此威慑其他没有实施犯罪的人不敢犯罪。可以看出,此种理论注重从管控犯罪人角度减少犯罪,在特定阶段针对特定时期的犯罪有其合理性。但是,基于电信网络技术实施的新型诈骗犯罪有其特殊性,因此,充分激发、调动电诈被害人的预防意识,对减少电诈犯罪有事半功倍的效果。

### 结语: 做好被害预防工作最为关键

电诈犯罪是立体式、操控式、应和式犯罪,其犯罪特性决定了预防手段应该与其他传统犯罪有所区别。其一,针对其立体式特性,首先需要提醒民众保护个人信息,减少信息被恶意利用;其次应多宣传揭示骗术,让民众认识到只要不应和,犯罪人就不能得逞;再次,要培养被害人随时摆脱锁链的能力,减少财产损失。其二,针对其操控式特性,要鼓励民众不轻易和陌生人说话,不轻易和嫌疑人合作。在非接触情况下,不应和就根本不会产生类似于抢劫、伤害等暴力犯罪的刑事后果,应该减少当事人担心报复的心理。其三,针对其应和式特性,要着力培养民众自理、自律能力,提升民众理性思考能力,让民众不要陷入诈骗人设计的骗局。由于本文的主题与篇幅限制,具体的被害预防训练措施将另外撰文论述。

需要强调的是,做好被害预防工作不等于让被害人独自防范电诈犯罪。最新的电诈犯罪案例显示,个人信息泄露是电诈犯罪的重要一环。犯罪分子往往利用被泄露的被害人个人信息编写剧本实施精准诈骗,迷惑性极强<sup>[17]</sup>;被害人往往陷入“相信吧,这可能是假的;不相信吧,这可能是真的”困境,有时甚至对公检法机关工作人员产生怀疑和不信任。目前已经有公检法工作人员在办案过程中被误当作电诈犯罪嫌疑人的案例<sup>[18]</sup>。这种矫枉过正、以邻为壑的情况毫无疑问会对被害人挣脱诈骗链条和被害预防产生妨碍。由此看来,被害预防不仅要激发、训练被害人审慎思考

以及随时摆脱锁链的能力,还需要全社会的通力合作,斩断个人信息泄露利益链,堵住个人信息泄露的渠道,从源头上防范电诈犯罪的发生。

### 【参考文献】

- [1] 汤瑜. 2018年全国公安机关打击犯罪大事记[N]. 民主与法制时报 2019-01-06(02).
- [2] 张洋. 打击电信诈骗要治未病[N]. 人民日报 2018-12-07(05).
- [3] 刘启刚, 蒋天蔚. 非接触性犯罪的地缘性特点及应对策略研究[J]. 贵州警官职业学院学报 2018(5): 99-104.
- [4] 王喆骅, 王丽萍. 电信诈骗犯罪之新动向及打防研究——以上海检察机关办理的案为例[J]. 上海公安高等专科学校学报 2016(2): 75-81.
- [5] 黎晴. 当前电信诈骗犯罪的打击难点和对策[J]. 江西警察学院学报 2012(5): 29-33.
- [6] 王瑞山. “小额贷”诈骗之预防[J]. 中国人民公安大学学报(社会科学版) 2017(5): 18-25.
- [7] 【美】保罗·埃克曼. 说谎: 揭穿商业、政治与婚姻中的骗局[M]. 邓伯宸, 译. 北京: 生活·读书·新知三联书店, 2016: 6.
- [8] ARMIN J, THOMPSON B, KIJEWski P. Cybercrime Economic Costs: No Measure No Solution [M]// AKHGAR B BREWSTER B. Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. Basel: Springer International Publishing Switzerland, 2016: 138.
- [9] 张扬. 电信诈骗害死人的背后: 破案率不超过3% [EB/OL]. [2019-04-15]. <http://news.cnhubei.com/xw/sh/201608/t3686711.shtml>.
- [10] COHEN L E, FELSON M. Social Change and Crime Rate Trends: A Routine Activity Approach [J]. American Sociological Review, 1979(44): 588-608.
- [11] 【意】恩里科·菲利. 犯罪社会学[M]. 郭建安, 译. 北京: 中国人民公安大学出版社, 1990: 56.
- [12] 赵军, 张建肖. 网络黑灰产治理须多管齐下[J]. 中国信息安全 2017(12): 73-74.
- [13] 车辉. “黑灰产”网络毒瘤亟待技术利剑铲除[N]. 工人日报 2016-09-23(06).
- [14] 张小虎. 犯罪预防与犯罪控制的基本理念[J]. 河南省政法管理干部学院学报 2008(1): 65-70.
- [15] 陈和华. 被害性与被害预防[J]. 政法论丛 2009(2): 17-22.

<sup>①</sup> 公安部从西班牙成功押解94名“冒充公检法”进行电诈犯罪的嫌疑人回国。中央电视台“面对面”栏目对此跨境打击电诈犯罪行动进行了采访,于2019年6月30日播出。参见中央电视台: 揭秘“长城行动” [EB/OL]. [2019-06-30]. <http://tv.cctv.com/2019/06/30/VIDE2Di1bdJDNUOVjWCLOAOV190630.shtml>.

[16] 【美】丹尼尔·卡尼曼.思考,快与慢[M].胡晓姣,李爱民,何梦莹,译.北京:中信出版社,2012:42-65.

[17] 电信诈骗团伙存21万条个人信息,备380个剧本诈骗[EB/OL]. [2019-04-12]. [http://www.xinhuanet.com/legal/2018-05/16/c\\_129873425.htm](http://www.xinhuanet.com/legal/2018-05/16/c_129873425.htm).

[18] 尹平平.听说,因为电信诈骗,“公检法”最近日子不太好过[EB/OL]. [2019-04-12]. <http://www.haijiangzx.com/2016/0921/1351323.shtml>.

(责任编辑 李记松)

## The Unique Attribute and Governance Path of Telecommunication and Internet Fraud

WANG Jie

(The legal Institute of Beijing Academy of Social Sciences, Beijing 100101, China)

**Abstract:** Telecommunication and Internet Fraud (TIF) is a new type of crime which combines the merit of network technology with traditional fraud. TIF's inherent comprehensive, manipulative and responsive characteristics make its social harmfulness heavier than traditional fraud. It is difficult to achieve good governance effect by adopting the traditional crime control model. The government and the society need to fully consider the situation and characteristics of the TIF, and to introduce a new concept of crime control from the perspective of victim prevention, so as to achieve effective prevention effect. Victims might effectively safeguard its rights and interests by Say NO to criminals and unilaterally break away from the chain of fraud.

**Keywords:** Telecommunication and Internet Fraud, comprehensive crime, manipulative crime, responsive crime