CAICT 中国信通院

信息通信行业防范打击通讯信息诈骗白皮书

（2018 年）

中国信息通信研究院

安全研究所

2018年5月

版权声明

前　言

近年来，我国通讯信息诈骗犯罪活动猖獗，严重侵害人民生命财产安全，严重影响社会生产生活秩序，已成为当前影响人民群众安全感和幸福感的一大社会公害。党中央、国务院对防范打击通讯信息诈骗工作高度重视，建立了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制度，组织部署公安部、工业和信息化部、中国人民银行、中国银行业监督管理委员会、最高人民法院、最高人民检察院等 23 个部门和单位从侦查打击、重点整治、防范治理等方面多管齐下，深入开展全国防范打击通讯信息诈骗专项行动。

通讯联络作为通讯信息诈骗实施的关键环节，也是治理工作的重点内容，信息通信行业承担着行业源头治理和配合打击诈骗犯罪活动的重要使命。在工业和信息化部的统筹督导下，相关企业严格落实主体责任，研究机构、社会组织和人民群众广泛参与，形成了协同联动、开放共治的治理格局。在全行业的共同努力下，治理工作取得阶段性明显成效，初步实现了“涉案号码通报数量明显下降”和“用户投诉举报数据明显下降”的“两降”目标。

然而，通讯信息诈骗治理工作始终处于一个动态博弈的过程，具有长期性和复杂性。当前形势依然严峻，呈现出由电话、短信诈骗向网络诈骗演进、技术对抗强度不断上升、诈骗实施日益精准化专业化、目标人群向境外公民转移的新趋势。与此同时，在工作中法律制度、工作机制、管理措施和技术能力等也有待进一步巩固完善，治理工作仍面临艰巨而复杂的挑战。

中国信息通信研究院以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大精神，牢固树立以人民为中心的发展理念，按照中央经济工作会议、2018 年全国网络安全和信息化工作会议精神及《政府工作报告》相关部署，围绕院“国家高端专业智库、产业创新发展平台”的定位，系统总结国际国内治理经验做法，深入分析当前治理工作的趋势走向和问题短板，研究提出了相关政策建议，希望能与业界同仁一起推动通讯信息诈骗治理工作持续引向深入，构筑起全社会共同治理、保障安全的钢铁长城，为行业长远健康发展营造良好环境，全力支撑好网络强国建设，不断增强人民群众的获得感、幸福感、安全感。

目 录

一、通讯信息诈骗概述

（一）通讯信息诈骗的概念

相对于“通讯信息诈骗”的称谓，可能更多人习惯叫“电信诈骗”、“网络诈骗”或是“电信网络诈骗”，实际上这几种叫法都不够准确，易使民众产生“电信运营商诈骗”或“中国电信诈骗”的错误认识。通讯信息诈骗实际上主要是指诈骗分子以非法占有为目的，利用电信、互联网等信息通信技术和工具，通过发送短信、拨打电话、网络聊天等联络手段，诱骗、盗取被害人资金汇存入其控制的银行账户，实施违法犯罪的行为。为更准确阐述此类犯罪行为，本文以“通讯信息诈骗”的称呼定义。

通讯信息诈骗从出现至今，经过不断演变发展，总体可分为四个阶段:

第一阶段（起始阶段）：从上世纪末开始，通讯信息诈骗首先在我国台湾地区出现，诈骗分子利用刮刮乐、六合彩等形式，并借助通讯网络实施诈骗。之后借助通讯网络实施诈骗的形式越发多样，逐步演化为一种新型的犯罪类型[1]。与当前诈骗形式相比，这一阶段的诈骗手段仍较为简单，作案区域也相对狭窄，主要集中在台湾本地，但诈骗导致的巨大经济损失已初现端倪，以台湾刮刮乐诈骗“祖师爷”级人物李溪泉为首的诈骗集团，从上世纪末开始，通过经营刮刮乐、六合彩明牌等诈骗手段在台湾地区诈骗金额超过 10 亿元[2]。

[1] 摘自秦帅，陈刚《近年来电信诈骗案件研究综述》
[2] 摘自于 2015 年 10 月中国新闻网《台湾刮刮乐诈骗集团 “祖师爷”潜逃 7 年后被拘捕》

第二阶段（扩散阶段）：从 2003 年开始，受台湾地区政府部门的高压打击影响，该类源自台湾的诈骗活动通过我国福建省转入内地，并在全国范围内迅速蔓延。一些受雇于台湾籍诈骗团伙的内地犯罪分子在学习了诈骗方法之后，开始以地缘、亲缘为纽带，纠集亲属、老乡独立干起诈骗的勾当。在我国逐步形成了河北丰宁县、湖北红安县、大悟县、湖南双峰县、广东电白县、福建安溪县和海南儋州市等从事通讯信息诈骗犯罪的重灾区，有的村庄甚至家家户户都有人参与作案[3]。

第三阶段（上升阶段）：从 2008 年开始，我国通讯信息诈骗案件进入持续高发阶段，立案案件数量以每年 20%-30%的速度快速增长，诈骗损失金额持续扩大。诈骗分子在原有作案手法上不断翻新，不仅冒充政府部门、基础电信运营商等社会公信力较高的单位工作人员，还广泛使用网络改号软件等技术手段增强诈骗活动的迷惑性。2012 年 10 月，诈骗分子冒充法院工作人员，骗取四川五名群众 700 余万元。同年 11 月，北京一名群众被同样的犯罪手法骗取 1000 多万元。此外，这一阶段通讯信息诈骗犯罪已呈现跨区域、跨国化趋势，作案范围已经扩大至印尼、越南、马来西亚、泰国等国家。

第四阶段（转折阶段）：从 2015 年开始，我国通讯信息诈骗呈现发案数量急剧增加、发案地域遍布全国、诈骗数额屡攀新高、诈骗手段频繁变换等态势，严重危害人民群众生命和财产安全，扰乱

[3] 摘自繆琛 2010 年《电信诈骗发犯罪治理问题研究》

社会正常秩序，影响社会和谐稳定。2016 年接连发生河南周口男子因遭诈骗在银行门口自杀、清华教授被诈骗分子骗走 1760 万元、山东临沂高考学生徐玉玉因被骗学费 9900 元而猝死等系列影响极其恶劣的诈骗案件，通讯信息诈骗成为最受瞩目的社会热点问题[4]。对此，党中央、国务院高度重视，中央领导同志作出重要指示批示，要求坚决打击通讯信息诈骗，切实保障人民财产安全，相关行业在全国范围联合开展防范打击通讯信息诈骗专项行动。

（二）通讯信息诈骗的分类

当前，通讯信息诈骗形式多种多样，诈骗手法不断升级，按照通讯联络方式、诈骗场景类型、犯罪实施地域等因素条件的不同，可以分为以下几类:

1. 按照诈骗实施通讯联络途径，通讯信息诈骗可分为电话诈骗、短信诈骗和网络诈骗[5]。

（1）电话诈骗。诈骗分子通过拨打受害人固定和移动电话实施诈骗，如利用网络改号软件，将诈骗电话号码修改为政府执法部门或电信运营商客服的专用号码，在电话联络过程中再以办案需要、电话欠费等为借口进行诈骗。

（2）短信诈骗。诈骗分子通过向受害人发送包含诈骗信息的手机短信实施诈骗，如通过购买大量非实名或者假实名登记的电话卡，利用短信群发器发送诈骗短信；或是利用“伪基站”发送诈骗短信。

[4] 参见法制日报 2017 年 9 月 3 日《去年以来公安部先后押回 200 余名台湾籍电诈嫌犯》，新华社 2016 年 9 月 13 日《如何扼住电信诈骗犯罪的“咽喉”》

[5] 参见腾讯发布的《2017 年第二季度反电信网络诈骗大数据报告》

（3）网络诈骗。相较于电话和短信诈骗，网络诈骗形式更加复杂多样，诈骗分子往往通过论坛、QQ、邮箱等网络工具，向受害人发送伪造的购物、银行、博彩中奖等信息，诱导受害人回复这些信息或者点击其中含有木马病毒的网址链接，进而实施诈骗。

上述类型不是严格区隔的，诈骗分子往往会组合利用电话、短信、网络等来实施诈骗活动。

2. 按照受害人心理状态，通讯信息诈骗可分为利诱型、避害型、恐吓型、招摇撞骗型和守株待兔型五类[6]。

（1）利诱型诈骗。诈骗分子主要利用受害人投机致富的侥幸心理实施诈骗。包括虚假中奖信息诈骗、网络购物诈骗、共享单车退押金诈骗、股票诈骗、虚构招聘广告诈骗、虚假团购、微信红包、特价机票和火车票诈骗等。

（2）避害型诈骗。诈骗分子主要利用受害人遇事后的焦急慌乱心理实施诈骗。比较常见的诈骗手法是以“车祸或摔伤住院”为名的诈骗，诈骗分子预先了解受害人以及子女相关资料，利用受害人子女上课或上班时手机关机，冒充医务人员或学校辅导员，联络受害人谎称其子女出车祸或上体育课摔伤，以住院为由要求支付医疗费为由实施诈骗。

（3）恐吓型诈骗。诈骗分子主要利用受害人遇事后的紧张害怕心理实施诈骗。比较常见的是以虚构绑架事实或人际矛盾为名的诈

[6] 摘自四川在线《警惕电信诈骗有五大类型》

骗。由于不少受害者在接到电话后，希望尽快息事宁人，往往使得此类诈骗手法屡试不爽。

（4）招摇撞骗型诈骗。诈骗分子主要利用受害人对他人的信任心理实施诈骗。主要包括冒充上级领导、知名企业客服人员、国家政府部门工作人员等进行诈骗。鉴于诈骗分子冒充的人员都具有一定权威性或特定信任关系，因此受害人往往不能及时辨别真伪，直到被骗后方知上当。

（5）守株待兔型诈骗。诈骗分子主要利用受害人机遇巧合下放松警惕的心理实施诈骗。诈骗分子通过海量发送“你好，请汇款到某某银行账号，谢谢!”之类的短信，让受害人误以为是商业伙伴或债权人，从而实施诈骗。

3. 按照诈骗活动实施地域，通讯信息诈骗可分为境外通讯信息诈骗和境内通讯信息诈骗。

（1）境外通讯信息诈骗。主要是指诈骗分子通过在东南亚、太平洋岛国、非洲、欧洲等境外地区设立诈骗窝点，通过拨打网络改号电话等方式，冒充司法机关实施诈骗。根据公安部统计，此类案件约占全部通讯信息诈骗案件的 20%，但经济损失占全部案件损失金额约 60%[7]。

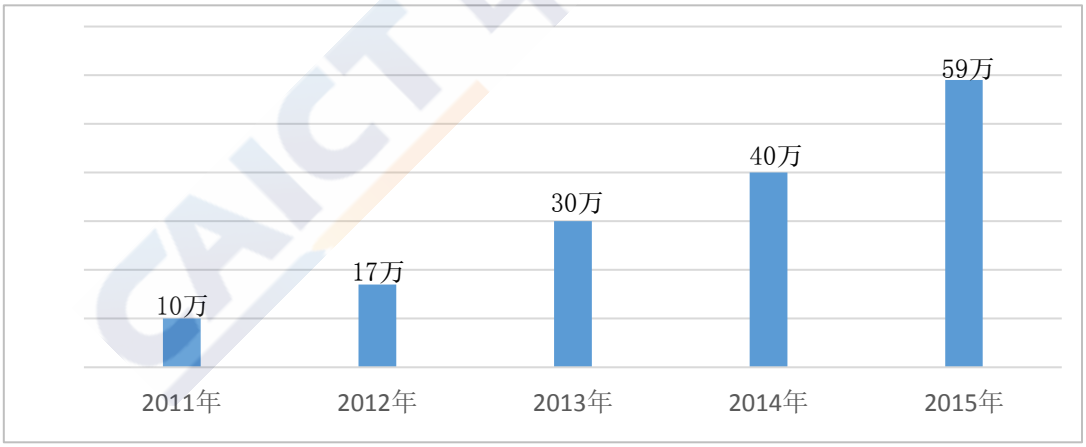
（2）境内通讯信息诈骗。主要是指诈骗分子在境内实施诈骗，并呈现明显的地域集中特点。例如福建龙岩网络购物诈骗、广东茂名冒充熟人和领导诈骗、海南机票改签诈骗以及补卡诈骗等。根据

公安部统计，此类案件约占全部通讯信息诈骗的 80%，经济损失占全部案件损失金额约 40%[8]。

此外，还有部分学者和研究机构按照通讯信息诈骗活动的实施手段类型、法律惩处程度等方面对进行分类，例如根据法律惩处程度分为诈骗罪、非法利用信息网络罪、帮助信息网络犯罪活动罪等，在此不再一一列举。

（三）通讯信息诈骗的危害

在我国全面启动重拳整治通讯信息诈骗专项行动以前，通讯信息诈骗犯罪活动持续高发。从 2011 年至 2015 年期间，公安机关立案数量逐年递增。根据公安部统计，2015 年全国共立通讯信息诈骗案件 59 万起，同比上升 32.5%；2016 年全国共立通讯信息诈骗案件 63 万起，同比上升 5.5%。



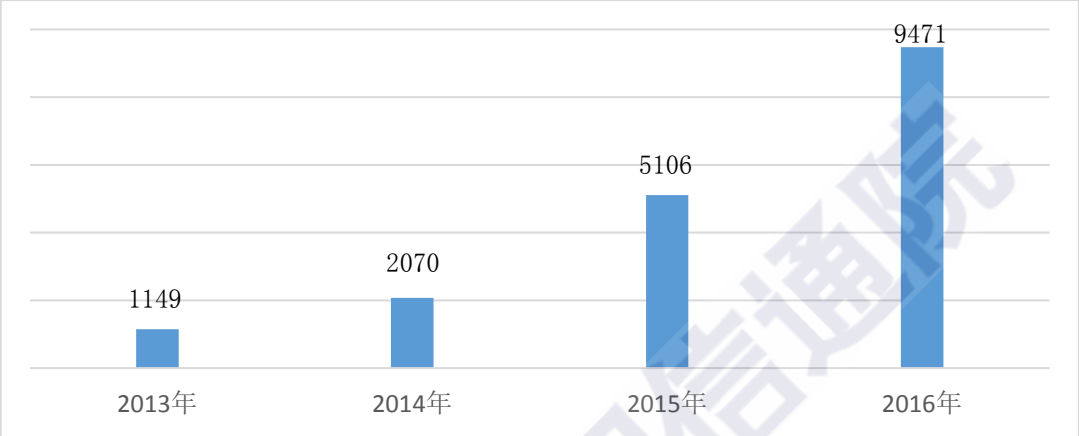
数据来源：公安部公开发布的数据

图 1　全国通讯信息诈骗案发数量（单位：起）

通讯信息诈骗危害人民财产安全。2015 年全国因通讯信息诈骗案件造成的经济损失达 222 亿元，贵州省都匀市发生了单笔 1.17 亿

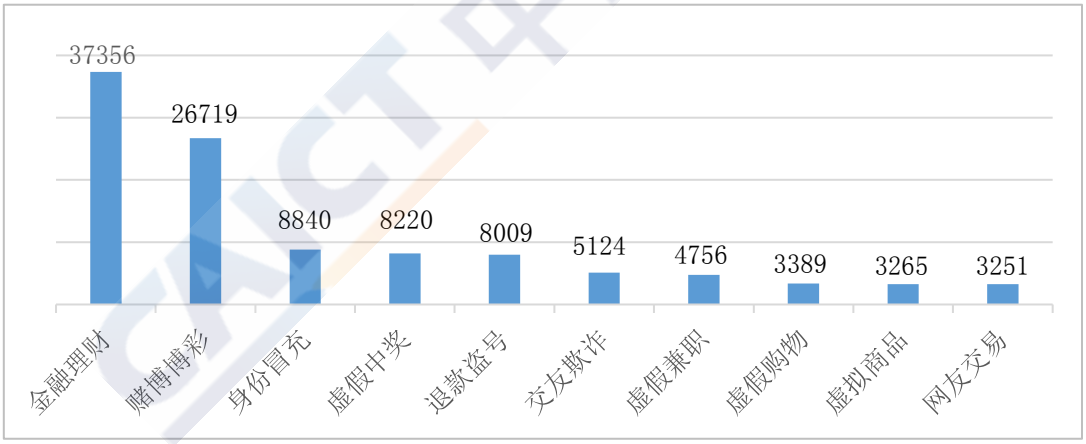
[7、8] 数据来源：2016 年平安中国系列网络访谈第 16 期

元的特大诈骗案件。2016 年上半年，全国通讯信息诈骗案件造成经济损失 80.4 亿元，人均损失超过 9000 元，其中 10 起案件单案被骗超过 1 千万元（注：部分没有达到立案条件的诈骗经济损失尚未统计在内）。



数据来源：360 猎网平台发布的《2016 年网络诈骗趋势研究报告》

图 2 通讯信息诈骗人均损失（单位：元）



数据来源：360 猎网平台发布的《2016 年网络诈骗趋势研究报告》

图 3 2016 年主要通讯信息诈骗类型人均损失（单位：元）

通讯信息诈骗危害人民生命安全。在通讯信息诈骗受害群众中，很大部分是老年人和青少年学生。这些老人和学生的“养老钱”、“救命钱”被骗后，受害人倾家荡产，甚至家破人亡的情况时有发生。2016 年 1 月 5 日，河南周口村民被诈骗分子以银行卡扣年费名

义骗走 8000 元后上吊自杀；同年 8 月，山东、广东连续发生三起学生被通讯信息诈骗后自杀或死亡的案件。其中，18 岁山东省女孩徐玉玉因被骗走了大学学费 9900 元而猝死事件，引发了社会各界高度关注，影响极其恶劣。

通讯信息诈骗危害社会正常秩序。通讯信息诈骗活动日益猖獗，导致人民群众人人自危，甚至出现矫枉过正、以邻为壑的情况,很多陌生电话都不敢接,甚至影响了人们正常的工作生活。以快递行业为例，很多快递员的电话一度出现被拒接的现象，尤其是被新闻媒体称为“诈骗专用号段”的 170、171 号段电话，拒接率高达三成以上。通讯信息诈骗已成为影响群众安全感和幸福感、降低老百姓对政府管理信任度、扰乱社会诚信秩序的一大公害。

通讯信息诈骗危害我国国际形象。一方面，国内持续高发的通讯信息诈骗活动，凸显出我国社会治理体系和治理能力的不完善。据调查报道，美国通讯信息诈骗发案率要远低于我国，诈骗案件数量仅为我国二成左右。另一方面，我国诈骗分子同时也对国外居民实施诈骗。据国外媒体报道，不少华裔、华侨都遭遇过买车被骗、解决移民身份被骗等事件。通讯信息诈骗已成为我国国际形象的一张“黑名片”。

二、通讯信息诈骗特点与原因分析

（一）通讯信息诈骗实施的关键环节

从诈骗分子实施通讯信息诈骗的环节来看，通讯信息诈骗活动可以归结为精准信息获取、诈骗脚本设计、通讯联络、支付转款四个关键环节。

在精准信息获取环节，诈骗分子主要通过非法窃取或购买社会上各行各业泄漏的个人信息，包括身份证信息、电话号码、家庭地址，以及网络账号和密码、银行账号和密码、购物记录、出行记录等。个别企业内部员工为了谋取利益，甚至与诈骗分子内外勾结，窃取和贩卖企业内部用户信息。

在诈骗脚本设计环节，诈骗分子模拟真实的经济社会活动场景，精心设计各种诈骗脚本，更有甚者聘请心理学专业人士利用“社会工程学”等有关心理学理论来撰写诈骗脚本，冒充司法机关、亲戚朋友，假造中奖、退税补贴、机票改签等花样繁多的诈骗脚本。例如，诈骗分子利用改号软件冒充公安机关向受害人拨打电话，称有人以受害人的名义在招商银行开了账户，里面有 XX 万元存款，涉嫌洗黑钱，为确保资金安全，要求受害人把钱转到法院的“安全账户”上。受害人信以为真，把银行卡内存款转入了“安全账户”，进而受骗。

在通讯联络环节，诈骗分子通过单一采用或组合采用电话、短信、互联网等通讯渠道联络受害人，利用之前设计的诈骗脚本与获取的受害人个人信息，骗取受害人信任进而实施诈骗。例如，诈骗

分子通过虚假改号软件将诈骗电话改成国内司法机关对外服务号码，在通话中伪装成司法机关人员诱导人民群众上当受骗。

在支付转款环节，诈骗分子引导受害人通过银行转账、网上支付等方式向其指定账户转款，再经由预先设计的诈骗分赃销赃渠道快速从指定账户中转移受害人资金。在诈骗分子的精心伪装设计下，绝大部分人甚至未意识到自己在进行转账汇款，以为在输入数字或验证码，待发现异常时，账户资金已全部被转走。

（二）我国通讯信息诈骗的现状特点

当前，我国通讯信息诈骗呈现手法变化复杂多样、组织形式分工细化、犯罪窝点地域性集中、实施行为空间跨度大等特点。

1.诈骗实施手段多样化、精准化

随着我国打击通讯信息诈骗力度不断加大，通讯信息诈骗实施手段不断翻新，方式更加隐蔽、花样不断翻新，逐渐从传统的广撒网、诱导式“撞骗”向“连环设局、精准下套”的精准诈骗转变。

一是精心设计人们日常生活场景的诈骗脚本。诈骗分子利用日常生活中可能发生在我们每个人身上的事件，精心设计各种诈骗脚本。仅公安部统计公开的常见通讯信息诈骗案件类型就高达 48 种，包括假冒领导、亲戚、朋友谎称“出车祸”、“被绑架”，假冒企事业单位谎称“欠费”、“邮寄包裹”，冒充执法机关人员谎称“涉嫌洗钱”、“银行卡透支”对受害人进行威胁恐吓等。

二是结合社会热点和诈骗对象编写特定诈骗脚本。诈骗分子紧跟社会热点，针对不同群体量体裁衣、步步设套，具有极强的欺骗

性和迷惑性。例如结合向受灾地区爱心援助的社会热点，诈骗分子利用广大人民群众对灾区同胞的关心，冒充“救援中心”骗取钱财；结合国家出台贫困大学生助学贷款等新政策的时机，诈骗分子冒充学校以发放助学贷款或奖学金为由向大学新生实施诈骗。此外，还有针对春节过后返城务工、学校开学等系列重大社会活动节点的诈骗活动。

三是充分运用各类通讯联络和支付转款手段。随着信息通信技术的发展，通讯联络和支付转款方式日益丰富多样，诈骗犯罪实施方式也随之变化。一方面诈骗分子从最初的打电话、发短信等方式发展到通过网络改号电话、QQ、微信号等联络受害人，例如诈骗分子通过微信“附近的人”加受害人为好友，以优惠券、返利、降价为诱饵，发送带有木马病毒的链接或二维码，受害人一旦点击安装，就会导致手机短信、账户资料等重要信息被盗取，最终导致与手机绑定的银行卡内存款被转走；另一方面诈骗分子利用境内雇佣人员通过线下提取赃款、网上转账、跨境消费、境外提现等方式转移受害人资金，比如诈骗分子通过网上银行转走受害人账号内资金后，立即将这些资金分成若干份转入其它账户,通过反复重复上述操作，最终实现境外消费或提现。

2.诈骗犯罪主体地域化、职业化

近年来，同一地域诈骗分子结伙形成的地域性职业犯罪团伙日益成为通讯信息诈骗犯罪活动的突出特点，目前看可以分为两大类:

一是以台湾人为头目和骨干的“台湾系”诈骗集团。其在全球各地流窜设立诈骗窝点，向我国境内实施诈骗。例如，在肯尼亚、马来西亚、柬埔寨、亚美尼亚等国家设立诈骗窝点的台湾人就高达200 余人；2016 年由“台湾系”诈骗集团实施的诈骗金额达千万元以上的案件就有 11 起[9]。

二是以大陆省份人员为主的通讯信息诈骗团伙。其通过立足本地设置集中性的诈骗窝点对全国范围实施诈骗，如河北丰宁县冒充黑社会诈骗、福建龙岩网络购物诈骗、江西余干县重金求子诈骗、广东茂名冒充熟人和领导诈骗、广西宾阳假冒 QQ 好友、海南机票改签诈骗以及补卡诈骗。据不完全统计，我国境内的通讯信息诈骗案件中，90%是此类重点地区地域性职业犯罪群体所为[10]。

3. 诈骗组织构成专业化、产业化

通讯信息诈骗呈产业化发展，分工越来越细，专业化程度越来越高，环节越来越多，总体呈现出一个盘根错节的利益化链条或者网络。

一是诈骗团伙内部形成环节严密、分工精细的工作链条。典型的诈骗犯罪集团通常按照工作职责分工对人员进行细致划分：有负责总体统筹整个诈骗过程的管理人员、提供技术系统维护的技术人员、诈骗剧本设计的写作人员、专职拨打诈骗电话的通讯联络人员、赃款转账的操作人员以及赃款取现的收款人员。

[9] 参见新华网 2016 年 12 月 27 日《公安部：前 11 月破获 9.3 万起电信诈骗案 避免群众损失 48.7 亿》
[10] 参见中国青年报 2015 年 7 月《2010 年至今电信诈骗涉案金额屡攀新高》

二是诈骗活动外部形成协作化、专业化的灰色产业群。随着诈骗案件数量和损失金额持续攀升，在经济利益驱动下，逐渐形成了为通讯信息诈骗活动提供协助支持的服务群体，包括买卖公民个人信息、开办贩卖银行卡、第三方支付平台洗钱、POS 机套现、为诈骗分子提供通讯线路、开发网络改号平台、虚假交易软件、制作手机木马程序等一系列相对独立、互不相识、时分时合的高度专业化犯罪活动产业群。

4. 诈骗实施行为跨境化、跨区化

随着我国经济全球化和区域一体化进程的不断推进，交通通讯工具日益便捷，人员国际往来日趋便利，区域间物流支付日益发达，通讯信息诈骗活动跨境、跨区域成为常态。

一是诈骗分子持续将诈骗窝点向境外转移。诈骗分子为规避我国相关政府部门的直接打击，纷纷向东南亚和非洲转移。台湾诈骗分子充分利用多个国家和地区免签的便利，不仅在东南亚和非洲设立犯罪窝点，而且向东亚的韩国、日本以及欧洲、大洋洲、南美洲的国家转移，甚至有在近 30 个国家的 300 余个诈骗窝点对我国境内实施诈骗的迹象。

二是诈骗分子诈骗实施环节横跨多个地区。由于通讯信息诈骗具有非接触性特点，诈骗分子为提升诈骗活动的隐蔽性，往往将诈骗实施环节进一步打散，以期加大相关政府部门的侦查打击难度。

如徐玉玉案件中，诈骗窝点、取款地、银行账户开户人、银行卡归属地、电话卡归属地、个人信息泄露源头分属 6 个不同省份[11]。

（三）通讯信息诈骗活动的主要成因

当前，我国全面建成小康社会进入决胜阶段，实现中华民族伟大复兴进入关键阶段，但经济社会发展不平衡不充分的深层次问题日益突出，各方面风险不断积累和逐步显露。互联网与经济社会各领域融合渗透持续深化，使得网络空间日益成为映射现实社会问题的窗口。通讯信息诈骗作为传统诈骗犯罪在信息时代所衍生的一种特有犯罪形态，其形成原因十分复杂。

1. 直接原因

（1）个人信息泄露是诈骗活动成功实施的关键因素。通讯信息诈骗案件持续高发、经济损失不断扩大，关键在于诈骗分子掌握了受害人的真实信息，进而实施了精准诈骗，大大提高了成功概率。当前，我国个人信息在网络黑市上贩卖猖獗，不仅涉及身份信息、电话号码、家庭住址、工作单位，甚至还包含消费记录、家庭财产收入、购物记录、出行记录等信息。诈骗分子在精准掌握用户个人信息的情况下，很容易编造出迷惑性极高的诈骗场景。据中国互联网协会调研统计，2015 年下半年至 2016 年上半年，我国网民因为个人信息泄露、垃圾信息、诈骗信息等遭受的经济损失为人均 133 元，总经济损失约 915 亿元[12]。

[11] 参见南宁晚报 2017 年 6 月 28 日《“徐玉玉被电信诈骗案”开庭审理 案件将择期宣判》
[12] 数据来源：中国互联网协会发布的《中国网民权益保护调查报告 2016》

（2）信息通信技术发展为诈骗活动提供了便捷渠道。以搜索引擎、电子商务、即时通信为代表的互联网技术飞速发展，在为人们生产生活带来便利的同时，也为诈骗分子获取各类诈骗活动所需信息和工具提供了条件。诈骗分子在互联网上通过搜索引擎可以方便地搜索到所需的改号软件、虚假交易软件等非法工具；通过淘宝等互联网电商平台可以迅速找到商家贩卖的个人信息；通过 QQ、微信、旺旺等社交软件建立通讯群组可以隐蔽地交流诈骗活动经验，或是雇人发送伪基站信息、拨打电话、转账取款、洗钱等。

（3）相关企业安全责任意识淡薄为诈骗活动提供了可乘之机。部分企业安全发展的理念不牢固，存在重发展轻安全、重效益轻责任等思想，在执行政策法规要求上存在不规范、不严格、不到位等问题。如移动转售企业安全管理松散，不实名登记、违规开卡等问题突出，170、171 号段一度成为诈骗分子的首选。部分农村信用社、地方银行违规办理的大量非实名银行卡被诈骗分子用来层层转账，快速提取赃款。贵州破获的全国单笔最大电信诈骗案件中，1.17 亿元资金被诈骗分子通过 9000 余张银行卡在 2 天内取走[13]。

（4）防范意识不强、贪图小利是诈骗活动成功实施的重要原因。相比于信息通信技术的快速发展，我国网络安全知识的普及教育相对滞后，民众安全防范意识和能力不均衡，这不仅体现在经济发达省份与欠发达省份的民众之间，也体现在一般人群与老人、青少年、农民工等特殊群体之间。这种不均衡的状态客观上为诈骗活动的成

[13] 参见贵州商报 2016 年 4 月 24 日《贵州侦破全国单笔最大电信诈骗案 主管被骗 1.17 亿》

功实施提供了可乘之机。同时，受害者喜欢贪图小恩小惠、幻想天上会掉馅饼的心理也是导致诈骗活动成功实施的重要原因。犯罪分子充分利用受害者这种心理，借助各种手法进行诱导，消除受害者疑虑，最终实施诈骗。例如 2014 年 12 月，湖南一市民收到一条中奖短信，内容为该事主被某热门真人秀栏目组抽取为幸运观众，要求事主向指定账户转入风险保证金，事主转账 5000 元后，对方又要求事主缴纳个人所得税 9800 元，事主发觉异常后才意识到被骗。

2. 深层次原因

（1）通讯信息诈骗活动兴起与我国正处于社会发展转型阶段有密切的关系。某一违法犯罪活动的兴起多是由经济社会发展和犯罪活动规律所决定的。当前，中国正处在经济社会转型期，社会贫富不均、城乡差异大、道德观念下滑等诱发违法犯罪的各种消极因素大量存在。同时，我国是人口大国，大量的剩余劳动力以隐性失业的形式散布在农村，就业形势压力巨大、收入不稳定，生活难以维持。这部分群体文化教育程度相对较低，加之法律意识淡薄，在生活压力下往往选择不择手段获取财富。这为通讯信息诈骗犯罪活动的滋生蔓延提供了土壤。公安部在防范打击通讯信息诈骗工作中实施挂牌整治的河北丰宁、湖南双峰等重点地区大都是国家级重点贫困县，丰宁当地农村人口人均纯收入不足千元，双峰县贫困人口也高达 12 万，占全县人口的十分之一。

（2）我国现有社会治理体系与治理能力尚不适应通讯信息诈骗活动特点。与信息通信技术快速发展相比，我国社会管理和行业安

全防范工作相对滞后。通讯信息诈骗作为一种远程非接触的新型犯罪活动，时空跨度大、技术含量高，传统社会治理手段难以适应，相关部门和企业防范打击经验明显不足。再加之，通讯信息诈骗活动涉及人员流、信息流、资金流的综合跟踪、分析和查处等工作，紧靠单一地区单一部门单一主体难以实现有效治理。即使发现诈骗行为，由于涉及案件主体众多，对直接实施诈骗的犯罪分子取证和量刑比较困难，对间接为诈骗活动提供便利条件的灰色产业（如贩卖个人信息、开办贩卖银行卡和电话卡、制售改号软件等）缺乏评判标准，这都给通讯信息诈骗犯罪活动提供可乘之机。

三、主要国家和地区通讯信息诈骗治理的经验做法

从国际上看，通讯信息诈骗犯罪活动同样普遍存在。为治理通讯信息诈骗，主要国家和地区政府部门纷纷加强法律法规建设和组织体系保障，对用户要求电话实名登记，同步配套相应技术手段，积极强化信用管理制度和用户举报等社会监督机制，有效遏制通讯信息诈骗活动的泛滥蔓延。

（一）注重立法先行，强化诈骗治理的法制基础

法律是社会良知和秩序的底线，治理通讯信息诈骗离不开法律的制度保障，主要国家和地区均将完善相关法律制度作为规范社会行为的优先工作领域。

一是制定专门性法律法规。在诈骗前置环节治理方面，个人信息保护专项立法已成为国际惯例，目前全球已有近 90 个国家和地区制定了专门针对个人信息保护的法律。欧盟已发布全球最严格的个人数据保护法规《通用数据保护条例》，适用于所有为欧盟居民提供商品服务的境外数据处理商。美国 2012 年颁布的《消费者隐私权利法案》，集中体现了美国政府应对大数据时代隐私保护问题的做法。在诈骗信息传播管控方面，美国在《电话消费者保护法》及《控制非自愿色情和推销侵扰法》两部法律中明确规定，不得向消费者发送与商业营销、产品推广、服务广告有关的垃圾短信、诈骗短信。在打击网络犯罪方面，国际上普遍强化针对性法律制定。美国早在 1984 年即制定了《计算机欺诈与滥用法》，为打击通讯信息诈骗等网络犯罪行为奠定制度基础。欧盟于 2001 年 11 月通过了

《网络犯罪公约》，成为世界上第一部针对网络犯罪行为制订的国际公约。

二是通过立法明确企业处置义务和权力。在美国，除通过法律保护用户外，还分别赋予银行和通信运营商主动封锁账户、拦截电话等权利。韩国则在《电信事业法》修正案强制要求运营商采取相应的技术措施，拦截虚假主叫电话，否则将被处以罚款。巴基斯坦通过相关立法要求运营商加强在非法营销电话、诈骗电话传输源头的识别和拦截能力。日本《反垃圾邮件法》也规定从事通信传送业务的运营商在出现违法发送特定电子邮件时，应尽可能向用户提供发信人的相关信息，以规避潜在的网络诈骗风险。

三是加强支付转账环节安全管理。俄罗斯电信法修正案要求手机用户必须建立独立账户支付附加内容服务费，其核心目的就是防止手机用户银行主账户可能因关联而遭受的诈骗损失。日本《假冒账户存入受害者救济法》授权银行可以对可疑账户进行冻结，并对受害人的债务减记、受骗金额返回等做出规定。

四是加大违法行为惩处力度。美国联邦法规定，对不法分子的电信诈骗行为可处以超过 10 万美元、监禁多年的处罚，对电话营销企业或个人可处以每次 1.6 万美元的罚款。台湾修正了“组织犯罪防制条例”部分条文，将电信诈骗犯罪纳入组织犯罪的范畴，原先定刑为 1 年以上 7 年以下有期徒刑，并处新台币 100 万元以下罚金，改为对主谋处 3 年以上 10 年以下有期徒刑，并处新台币 1 亿元以下

罚金，对欺诈参与者处 6 月以上 5 年以下有期徒刑，并处新台币 1000 万元以下罚金。

（二）加强组织保障，强化治理工作的统筹协调

从主要国家和地区实践看，建立强有力的组织领导是保障通讯信息诈骗治理工作有力有序推进的基础。

一是设立负责通讯信息诈骗治理的专门机构。俄罗斯内务部设立了专门负责防范打击通讯信息诈骗的局级单位，通过网站主页、媒体等宣传渠道向民众介绍诈骗案例，提供实用的防范措施；日本警视厅则设立副部长级别的防范“汇款诈骗”本部，并在各区县设有独立的搜查班和技术班。

二是建立跨部门协调机制。台湾设立“反诈骗联防会议”、“电信技术咨询小组会议”等联席会议制度，协调“法务部”、“交通部”、“财政部”、“农委会”、“金管会”、“行政院金融监督委员会”、“金融联合信息中心”，各电信运营商及“行政局”等科技、研发、通讯、监察、司法领域单位，构建一体化防范打击诈骗犯罪网络，通过建立“电信联合服务平台”实施“警示账户联防机制”。韩国警察厅、放送通信委员会、金融监督院等部门，联合建立跨部门协调工作机制，强化通讯信息诈骗研判与打击力度。

（三）强化实名管理，大力提升实名登记准确率

电话实名制作为对诈骗等违法犯罪活动进行跟踪溯源的重要手段，已成为全球普遍做法，各国通过多种方式确保实名登记准确率。

一是强化移动电话办理用户真实身份登记。在美国，手机账户需要与个人社会安全号捆绑，如果用户不能提供社会安全号，必须出示护照、信用卡、学生证等能证明身份的文件。运营商也可通过技术手段来“强制”用户提供身份证明文件，即当用户没有提供社会安全号时，运营商会对手机设置开启“网页卫士”功能，阻止用户进入一些网站。德国《2004 年电信法》要求服务提供者在提供商业性电信服务时，必须在服务生效前收集和保存电信用户个人信息。

二是明确责任主体用户身份认证管理要求。新加坡信息通信发展局要求所有移动业务零售店和业务经营者都配备“身份扫描识别系统”，新用户必须提交身份证到系统进行扫描和登记后才能开通服务。在德国有两种途径可获得手机号码，一种是与移动通信运营商签订至少两年的使用合同，另一种是购买预付费手机卡。德国电信法规定，运营商必须监督用户进行实名登记。

三是实施移动电话与相关业务捆绑。墨西哥将移动电话与固定电话进行捆绑，《联邦电信法》要求用户必须提供两部其亲戚或朋友家中的固定电话，以便工作人员查证该手机用户信息的真实性，待实名登记手续和个人资料真实性验证完成后，手机才会被激活。德国实施移动电话与银行账号捆绑，后付费手机卡用户签合同时必须同时提供身份证明、居住登记证明原件和银行账号，通信费用必须由运营商按月通过银行账号自动扣款，不得由个人自行交款。

四是强化号码过户、预付费业务等特定环节实名制管理。德国相关法律要求用户在办理过户手续时必须提供相应的身份证明，否

则新持卡人用该手机卡从事违法行为，原持卡人将会负法律责任。新加坡信息通信发展局要求所有现存的预付费 SIM 卡用户都需要在 6 个月内到移动运营商的零售店重新注册个人信息，否则其业务将不能继续使用。

五是实名制的应用范围扩展到其他与手机相关的业务。日本移动业务是手机、SIM 卡一体模式，《移动话音通信业者确认用户身份及防止移动话音通信服务不当利用法》规定，实名制适用环节不仅包括移动运营商手机办理业务，也包括各种手机登记主体和使用主体相分离的业务（例如手机租赁业务、手机转让业务等）。

（四）建立信用平台，强化信用警示与约束效应

建立健全社会信用管理是整顿和规范市场秩序的重要举措，也是增强社会诚信的有效手段。部分国家通过引入社会信用监督和奖惩机制，为防范打击通讯信息诈骗提供重要助力。

一是强制签订信用合同。德国建立起一套完备的信用网络，所有德国个人和公司在德国信贷风险保护协会（Schufa）都有信用档案和评分。用户在银行开户，签订手机、网络等服务合同时，必须进行实名登记，接受严格的身份检验，并签订“信用合同”。银行、电信、网络、租房等公司会定期将用户的个人信用信息向 Schufa 报告。一旦发生通讯信息诈骗，银行可以通过 Schufa 的系统查出相关信息，为用户追回钱款，系统将自动扣除被查出涉嫌通讯信息诈骗的个人和公司的信用分。

二是依托信用体系增大诈骗犯罪成本。美国电信技术发展较早较快，但通讯信息诈骗却得到有效遏制，关键原因之一在于其社会信用体系较为健全。在美国，主要由完全市场化运作的私人征信服务公司负责个人信用记录收集整理，据不完全统计，相关征信服务公司已掌握了全美 1.6 亿成年人的信用资料。信用记录有显著瑕疵（如通讯信息诈骗犯罪行为）的个人和企业，其生活和发展会受到明显的负面影响，在法律规定的时限内，失信记录会被保存和传播。失信者会受到惩罚，而守信者则会获得种种便利和好处。美国完善的信用管理体系极大增加了社会主体实施通讯信息诈骗等失信行为的违法成本，成为诈骗治理体系中的重要一环。此外，英国也采取了类似的信用体系，英国征信机构采集来自私人部门和法院判决的信用信息，具有严重不良信用记录（如通讯信息诈骗犯罪相关判决）的个人，在就业、贷款、生活等方面将会受到严格限制。

（五）建立专门机制，提升诈骗治理工作主动性

为有效保护用户合法权益和防范企业违规营销行为，发达国家普遍建立“拒绝来电”登记制度，对骚扰电话、诈骗电话进行事前防范，治理效果明显。

一是通过立法明确建立“拒绝来电”机制。美国联邦贸易委员会根据《电话消费者保护法》推出“拒绝电话推销名单”免费登记平台，全美任何座机和手机用户都可在专门网站上免费注册，选择是否接受电话推销的来电，一旦被用户列入“拒绝来电名单”，除了慈善机构、政治团体等公益性质的机构外，任何人向该电话推销

都属于违法行为。截止 2014 年，美国每 100 个家庭中有 180 个号码通过“拒绝来电”用户登记平台完成了注册。新加坡《个人资料保护法》规定了“拒绝来电”登记制度，电信用户可以申请其电话号码加入或退出登记簿，商家在拨打营销电话前，都要确认“拒绝来电”登记处没有该名消费者的号码，否则不能拨打用户电话。

二是限制违规责任主体电信资源使用。印度要求基础电信企业一旦发现未通过“谢绝来电”注册的企业或个人拨打营销骚扰和诈骗电话，必须立刻切断其所有电信资源并列入黑名单，要求基础企业在收到由“谢绝来电”平台提供的黑名单后 24 小时内切断名单上电话营销者的电信资源。

三是在治理过程中注重疏堵结合。美国、英国、澳大利亚要求对营销类电话建立详细的电话营销行为准则，加拿大要求对全部合法的电话营销者主叫号码进行登记。

（六）强化技术手段，加强电话诈骗拦截与提醒

政府监管部门建立相应技术手段，对提升行政监管效率有着明显作用，往往能在与犯罪分子的较量时占得先机、赢得主动。发达国家为有效压缩通讯信息诈骗的传播渠道，均将建立针对性的技术手段作为工作的重中之重。

一是发达国家普遍建设诈骗电话拦截屏蔽技术手段。韩国电信企业被强制要求采取相应的技术措施，拦截虚假主叫的电话，否则将被处以罚款。美国联邦通信委员会（FCC）敦促主要的美国电话公司采取措施免费为消费者提供自动呼叫电话的拦截技术，AT&T、苹

果、谷歌、Verizon 等美国通信领域巨头，联手组成“反自动呼叫电话打击行动组”，开发主叫号码 ID 识别技术，屏蔽虚假号码拨出的电话。日本部分银行在 ATM 机上安装了手机信号干扰器，用户在取钱或汇款时不能使用手机，以防止诈骗分子用手机指挥用户操作取钱。

二是部分国家积极开发面向用户终端的安全防范技术。日本富士通公司和名古屋大学合作开发出一种“手机会话分析软件”，将诈骗汇款内容中包含的所有关键词设定为危险词语，如交通事故、汇款等。同时，该软件可基于关键词和通话语调变化等，综合判断用户是否可能正被诈骗。软件一旦发现用户处于被欺骗状态，手机会马上发出警报声，并在手机屏幕上显示提示语：这可能是诈骗电话，请注意！美国迈克菲（McAfee）公司针对安卓、苹果智能手机推出安全软件，可以过滤垃圾邮件、垃圾短信和骚扰诈骗电话，扫描应用程序、安全数据卡（SD 卡）和文件中是否存在恶意代码，实时主动检查网页安全，阻止短信、电子邮件、社交网站和二维码中潜在的网络钓鱼站点、浏览器漏洞和恶意链接。俄罗斯卡巴斯基公司推出安卓手机安全软件，具有拦截恶意软件和危险链接、过滤骚扰电话和短信等功能，可以有效提升用户终端侧通讯信息诈骗安全防范能力。

（七）加强社会监督，构建协同治理的工作合力

从世界各国治理实践看，民众既是深受通讯信息诈骗侵害的主要对象，更是参与通讯信息诈骗治理的重要主体，各国均将发挥民众监督作用和提升用户安全防范能力作为治理工作的关键一招。

一是在社会监督方面，各国均将畅通社会举报渠道作为吸引社会民众参与治理的重要途径。美国、德国组建了专门机构，负责集中受理用户举报和问题调查。法国组织电信运营企业建立了名为“33700”跨运营商联合举报平台，统一负责接收用户举报。英国设立了名为“投诉”的专门网站，接收来自用户的举报，并定期按照危害程度进行列表，提醒人们不要上当受骗。澳大利亚则在设立电信诈骗举报官方网站（http://www.fraud.org）的基础上，进一步将举报信息在超过 90 个执法部门之间进行信息共享，对诈骗分子形成强大的震慑作用。

二是在提升民众防范能力方面，各国均将宣传教育作为治理工作的优先方向。法国内政部、澳大利亚竞争和消费委员会（ACCC）均在其网站专门发布近期常见通讯信息诈骗手法，并为用户提供了相应的信息核查验证渠道。美国联邦通信委员会（FCC）通过面向民众举办“录音电话解决方案挑战赛”，吸引民众参与到通讯信息诈骗治理工作，其中一名参与比赛的独立工程师设计开发的解决方案得到广泛应用，截至 2015 年其已为美国电信用户拦截骚扰、诈骗等电话超过 3000 万次。日本则将电信诈骗统一更名为“汇款诈骗”，

由警察部门定期在大众媒体上分析典型案例，公布最新作案手法，指导民众学会应对策略。

综合看，主要国家和地区的通讯信息诈骗治理工作呈现以下基本特征：**在治理模式上，**注重依法治理、政府联动，不仅通过明确各环节各主体的责任义务，还通过设置政府机构来统领整个治理工作。**在治理举措上，**注重标本兼治、技管结合，既大力建设技术防范管控手段持续提升防范打击能力，又采用实名制、信用管理、“拒绝来电”机制等管理措施巩固治理成效。**在治理机制上，**注重专群结合、群防群治，积极构建政府、电信运营商、科技公司（如苹果、谷歌、富士通）、安全厂商（如迈克菲、卡巴斯基）、高校（如名古屋大学）、社会组织（如澳大利亚竞争和消费委员会）、用户等各类主体共同参与的多元治理格局。

四、信息通信行业防范打击通讯信息诈骗主要举措

（一）我国防范打击通讯信息诈骗工作总体情况

通讯信息诈骗违法犯罪日益猖獗，严重侵害人民群众财产安全和合法权益，严重影响社会稳定和群众安全感。能否有效遏制此类犯罪高发势头，及时铲除犯罪活动滋生土壤，是对国家治理能力和治理水平的重要考验。党中央、国务院对此高度重视，从顶层设计到具体落实进行了周密部署，各有关部门全面尽职履责，持续强化对通讯信息诈骗的防范打击。

一是全面加强顶层统筹，构建综合治理体系。2015 年 6 月 4 日，国务院正式批复建立“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制度”[14]，统筹协调全国防范打击通讯信息诈骗工作。联席会议由公安部牵头，工业和信息化部（以下简称工信部）、中国人民银行、中国银行业监督管理委员会（以下简称银监会）、最高人民法院、最高人民检察院等 23 个部门和单位参加。部际联席会议要求各级党委政府要把防范打击工作纳入社会治安防控体系建设范畴，切实加强组织领导，做好统筹规划，积极构建党委政府统一领导、联席会议制度组织协调、有关部门齐抓共管、社会各方面积极参与的打击治理电信网络新型犯罪工作格局，努力形成打击治理的强大合力。

二是明确治理工作目标，持续强化组织部署。2015 年 10 月 9 日，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召开

[14] 参见新华网 2015 年 10 月 10 日《23 部门联手打击治理电信网络新型违法犯罪》

第一次会议，宣布在全国范围内开展打击治理电信网络新型违法犯罪专项行动，坚持以打开路、坚持齐抓共管，坚持综合施策，侦察打击、重点整治、防范治理三位一体，掀起“集中侦破一批案件、打掉一批犯罪活动、尽快整治一批重点地区”的工作高潮，坚决把犯罪分子的嚣张气焰打下去。针对境外诈骗分子对境内实施诈骗金额巨大的突出问题，会议明确了深化国际合作，切实加强打击境外犯罪嫌疑人和追赃追逃工作的要求。同时，会议还提出了治理工作不仅要注重关口前移，强化源头治理，进一步规范银行、电信、网络公司、软件开发企业的经营行为，还要充分发动群众、紧紧依靠群众。

2016 年 2 月 25 日，国务院召开打击治理电信网络新型违法犯罪工作部际联席会议第二次会议暨专项行动推进电视电话会议，部际联席会议 23 个成员单位分管负责同志和联络员参加了本次会议。会议通报了专项行动开展以来的进展情况，深入分析了打击治理电信网络新型违法犯罪面临的新形势新问题，提出了补齐短板和改进打击治理工作的具体措施。同时，部际联席会议决定，将打击治理电信网络新型违法犯罪专项行动延长至 2016 年底，力争实现“查处违法犯罪嫌疑人数量明显上升、破案数明显上升、发案数量明显下降、人民群众财产损失明显下降”的“两升两降”目标。

2016 年 9 月 23 日，国务院召开打击治理电信网络新型违法犯罪工作部际联席会议第三次会议暨深入推进专项行动电视电话会议，就进一步深化打击治理电信网络新型违法犯罪专项行动进行再部署、

再推进、再落实，并聚焦侦查打击和源头治理两大环节，强化重点整治和宣传教育，不断推进打击治理电信网络新型违法犯罪专项行动向纵深发展，坚决把犯罪分子的嚣张气焰打下去，坚决遏制此类犯罪高发势头，切实维护人民群众合法权益。

三是积极构建协同治理合力，深化各项工作落实。为贯彻落实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第一次会议精神，协同推进防范打击电信网络新型违法犯罪，有效遏制此类违法犯罪活动的发展蔓延势头，2015 年 10 月 30 日，联席会议办公室召开电视电话会议，部署开展为期半年的打击治理专项行动。同年 11 月 4 日，国务院部际联席会议印发《打击治理电信网络新型违法犯罪专项行动工作方案》，明确了 12 类需重点打击治理的违法犯罪人员，7 类需重点规范治理的违规行为，规定了开展铲除境内地域性诈骗犯罪源头、参与捣毁境外诈骗犯罪窝点、切断违法犯罪产业链、打掉转取款犯罪窝点、强化打击处理、集中治理电信、银行领域的突出问题等相关工作，切实维护人民群众切身利益，创造持续安全稳定的社会治安环境。

2016 年 9 月 18 日，银监会、公安部联合颁布实施《电信网络新型违法犯罪案件冻结资金返还若干规定》，规定包括 17 条条款，着重解决电信网络新型违法犯罪案件冻结资金及时返还的基本原则与实施程序等问题，减少电信网络新型违法犯罪案件被害人的财产损失，确保依法、及时、便捷返还冻结资金,切实维护人民群众的财产权益。

2016 年 9 月 23 日，最高人民法院、最高人民检察院、公安部、工信部、中国人民银行、银监会等六部门根据有关规定联合发布《防范和打击电信网络诈骗犯罪的通告》，首次公开明确将电信网络诈骗案件依法立为刑事案件，并进一步明确了电信企业、金融机构的主体责任，细化了电话实名制、银行卡管理等方面的管理要求，为提升对电信网络诈骗犯罪精准打击、切实保障广大人民群众合法权益奠定了制度基础。

2016 年 12 月，最高人民法院、最高人民检察院、公安部联合发布《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》，针对通讯信息诈骗犯罪的特点，分别规定了依法严惩诈骗犯罪、全面惩处关联犯罪、准确认定共同犯罪与主观故意、依法确定案件管辖、证据的收集和审查判断、涉案财物的处理等内容，进一步明确了法律标准，统一了执法尺度，为各地司法机关更及时、更准确、更严厉地依法惩治通讯信息诈骗犯罪提供了重要规范依据。

四是持续强化重点环节管理，全面清理整顿相关业务。2015 年 11 月，银监会下发《关于银行业打击治理电信网络新型违法犯罪有关工作事项的通知》，要求各银行进一步强化银行卡业务的规范管理，明确规定同一客户在同一商业银行开立的借记卡，原则上不得超过 4 张，坚决遏制违规代开卡、乱开卡、批量开卡等电信网络新型违法犯罪活动。

2016 年 5 月，人民银行等四部门联合发布《关于建立电信网络新型违法犯罪涉案账户紧急止付和快速冻结机制的通知》，要求银

行机构通过接口方式与电信网络新型违法犯罪交易风险事件管理平台连接，实现对涉案账户的紧急止付、快速冻结、信息共享和快速查询功能，最大限度挽回社会公众的财产损失。

2016 年，人民银行发布《关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》，明确要求自 2017 年 1 月 1 日起，只要经设区的市级及以上公安机关认定并纳入电信网络新型违法犯罪交易风险事件管理平台“涉案账户”名单，银行和支付机构将中止该账户所有业务，严厉打击通讯信息诈骗。

2016 年 3 月，公安部制定出台《公安机关侦办电信诈骗案件工作机制(试行)》，进一步规范侦办通讯信息诈骗案件工作程序，明确工作责任，不断提高公安机关的侦查破案能力和执法办案水平。

五是深入推进技术手段建设，提升精准防范打击能力。为适应新形势下打击治理通讯信息诈骗工作的需要，国务院部际联席会议部署各地全面建设反电信诈骗中心，合理配置和利用警力，集中统一案件数据，采集同类样本，加大分析研判。2015 年以来，以信息技术作为桥梁，全国已建成 32 个省级反诈骗中心和 206 个地市级反诈骗中心，形成打击治理通讯信息诈骗“信息共享、合成作战、快速反应、整体联动”的整体架构[15]，在全国构建一张有效应对通讯信息诈骗犯罪的大网，切实提高防范打击能力。

部分地方公关机关在地方反电信诈骗中心建设过程中，主动探索形成了独具特色、成效突出的技术能力。如厦门公安机关与该市

[15] 摘自中国信用 2017 年 5 月 19 日《公安部：反诈骗信息共享 大数据屡破积案》

银行机构合作成立反虚假信息诈骗中心，以“统一受理、快速阻断、综合研判、动态预警、合成打击、有效控制”为特色，由“反诈骗接警平台”、“反虚假信息诈骗指挥平台”、“金融电信（点对点）查控系统”、“防电话诈骗语音提示系统”等四大系统联合组成，共同实现对通讯信息诈骗的接处警、综合研判、动态预警及合成打击工作。

（二）信息通信行业防范打击通讯信息诈骗工作

通讯联络作为通讯信息诈骗实施的关键环节，也是治理工作的重点内容，信息通信行业承担着行业源头治理和配合打击诈骗犯罪活动的重要使命。全行业坚持人民至上、人民利益高于一切，坚持以人民为中心的发展，是信息通信行业的价值所在，行业主管部门全面贯彻党中央、国务院有关决策部署，相关企业单位深入落实责任，社会组织和人民群众广泛参与，形成了协同联动、开放共治的通讯信息诈骗治理格局。

1.加强组织部署和任务落实，行业主管部门深入开展防范打击通讯信息诈骗专项行动

工信部作为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成员单位和信息通信行业主管部门，坚决落实党中央、国务院决策部署，确立了“突出重点、技管结合、落实责任、标本兼治”的总体工作思路，紧紧抓住通讯信息诈骗的通讯联络这一关键环节，深入推进信息通信行业源头治理和配合打击通讯信息诈骗违法犯罪工作。31 省（市、自治区）通信管理局作为信息通信行业属地监管

部门，切实落实工信部有关工作部署，切实履行组织、协调、监督、检查等属地管理职责，全面强化对各项管理要求的督促落实，深入整治违法违规行为，开展属地防范打击通讯信息诈骗专项行动。

一是加强组织领导，强化专项工作统筹。防范打击通讯信息诈骗涉及面广、政策性强，是一项复杂的系统工程，建立强有力的组织领导是保障各项工作有力有序推进的基础。工信部高度重视防范打击通讯信息诈骗工作，部领导多次做出具体指示和部署，并将通讯信息诈骗专项治理工作纳入 2016 年部重点工作。同时，为充分发挥好工信部对专项治理工作的组织协调、督促指导作用，还专门成立了防范打击通讯信息诈骗专项工作领导小组，下设办公室和工作专班，全面负责统筹推动专项工作中的重点任务，督促检查主要任务落实情况，确保专项工作扎实有效推进。

2016 年 1 月 5 日，工信部在北京召开防范打击通讯信息诈骗专项行动工作部署电视电话会议，深入贯彻落实国务院打击治理电信网络新型违法犯罪工作有关要求，对信息通信行业防范打击通讯信息诈骗专项行动进行动员部署，坚决遏制通讯信息诈骗发展蔓延势头。

2016 年 6 月，工信部印发了《综合治理不良网络信息防范打击通讯信息诈骗行动工作方案》，部署通信行业开展为期半年的专项行动，切实规范国际来话主叫号码传送，严厉整顿规范语音专线、“一号通”、“400”等重点电信业务，加快技术防范拦截手段建设。

按照工业和信息部专项治理工作的有关部署要求，31 省（市）通信管理局纷纷加强了属地专项治理工作的组织领导和工作部署，均建立了以局领导为组长的省级防范打击通讯信息诈骗专项工作领导小组，通过专题会议方式，及时向省内各基础电信运营企业与移动通信转售企业传达工信部有关工作部署要求，对属地专项治理工作进行动员和部署。

二是明确工作目标，细化重点任务分工。明确任务细化责任是全面推进防范打击通讯信息诈骗工作的内在要求和重要保证。2015 年 12 月，工信部制定出台《工业和信息化部关于进一步做好防范打击通讯信息诈骗相关工作的通知》（工信部网安函[2015]601 号文），针对重点电信业务中存在的违规出租、违规使用、违规经营、主叫号码传送不规范等问题，明确提出了抓好重点电信业务清理规范、大力加强技术防范管控力度、强化社会监督举报受理、严肃查处违法违规行为、加大工作监督检查与责任考核力度，完善固化相关工作机制等六大方面 22 项工作任务，确立了企业网络与信息安全责任落实到位、重点电信业务经营秩序有效规范、通讯信息诈骗传播渠道有力遏制、违法违规行为得到坚决惩处的工作目标。

2016 年 11 月，工信部制定出台《关于进一步防范和打击通讯信息诈骗工作的实施意见》（工信部网安函[2016]452 号文），在前期六部委《关于防范和打击电信网络诈骗犯罪的通告》和工信部印发的《关于进一步做好防范打击通讯信息诈骗相关工作的通知》（工信部网安函〔2015〕601 号）等文件基础上，全面对标当前行

业存在的突出问题，深入剖析行业监管薄弱环节，从落实电话用户实名制、规范重点电信业务、整治网络改号、提升技术防范和打击能力、加强用户个人信息保护、强化社会监督与宣传教育、强化行业监管与责任追究、防范治理的工作保障等八大方面，进一步明确细化 29 项具体措施，并首次逐项明确提出各项任务的完成时限要求，为打好打赢通讯信息诈骗专项整治这场攻坚战提供更为清晰的路线图和时间表。

三是强化监督检查，加大违规处置力度。有问题不追责，任何制度都是摆设，任何好的措施，一分靠部署，九分靠落实。为落实相关工作要求，工信部建立了总体调度和重点问题督导机制，梳理形成了任务清单、问题清单和责任清单。对照清单要求，紧扣关键时间节点开展组织协调和督促指导，确保整体工作有序推进。为确保各项工作落到实处，工信部还加强对重点工作任务督促督办，建立了专项督导检查、用户举报通报、诈骗电话责任倒查和约谈整改等工作机制。截至 2017 年 11 月，先后 5 次组织全国 20 余个省份重点地区开展了专项督导检查，全面检查电话实名登记、重点业务整治、号码传送规范和改号软件清理、技术手段建设、行业用户个人信息保护、社会监督和宣传引导等工作落实情况。其中，仅针对电话实名登记这一基础性工作，就专门组织开展了 10 余轮次暗访和数据抽测，对超过 3 亿户电话用户登记信息进行了核查，并在行业内严肃通报相关检查结果，先后约谈问题严重企业和主要分管负责人达 10 余次。

为确保通讯信息诈骗治理工作的针对性和有效性，工信部还建立了严格的月度信息通报和责任追究机制。一方面，结合监督检查和用户监督举报，将基础电信企业、移动转售企业等经营问题情况向全行业通报，针对存在问题的省级基础电信企业，按照网络信息安全责任考核要求从严扣分，并由基础电信企业集团公司依据企业内部专项考核规定进行严肃追责；对存在严重违法违规行为的省级基础电信企业，则由省级通信管理局进行行政处罚，并责成相关责任部门和责任人进行责任倒查、层层追责。另一方面，组织基础电信企业、移动转售企业等相关单位定期上报防范打击通讯信息诈骗工作进展、经验做法、存在问题和相关建议情况，不断固化有益经验做法，积极解决突出问题，持续提升电信企业防范打击通讯信息诈骗的能力。

在工信部的统一部署下，31 省通信管理局通过明查暗访、专题约谈等方式督促基础电信企业进一步落实专项行动各项工作任务。针对基础电信企业管理责任落实不到位等突出问题，分别对本省基础电信企业组织开展了多轮次专项检查和违规处罚。其中，仅贵州省通信管理局针对本省企业违反电话用户实名登记要求的行政处罚就达 16 起。

四是健全技术手段，建立联防联动防线。善于把新技术运用到预防打击通讯信息诈骗工作中，是确保与诈骗分子较量时占得先机、赢得主动的关键。为进一步提升诈骗电话发现、预警和处置的联防联控联管能力，在国务院办公厅、中央政法委、中央综治办、发展

改革委等部门全力协调支持下，工信部指导地方通信管理局、国家互联网应急中心等单位，历经 6 个月的紧密协调部署，完成了全国诈骗电话防范系统的建设，初步形成了全国一体、联防联动的多层次、立体化诈骗电话技术防范体系。全国诈骗电话防范系统于 2107 年 3 月底正式建成并投入使用，系统具备诈骗电话实时发现预警、综合分析研判、精准防范处置等功能，实现了对境内外诈骗电话的监测防范处置。自系统上线运行以来，已累计处置涉嫌诈骗电话号码 1184 万个、呼叫近 1 亿次，通过与公安机关联动，及时劝阻受害客户 7000 余人，挽回直接经济损失 6000 余万元，有力维护了人民群众合法权益。

各地通信管理局立足本地实际，建设了各具特色优势的省级防范打击通讯信息诈骗技术平台。上海市通信管理局历时半年建设完成了国内首个反电信网络诈骗中心平台，实现了对诈骗号码、诈骗网址、溯源查询、伪基站监测的快速处置配合，大幅提高了平台对通讯信息诈骗案件的查处效率，有效阻止受害人资金的盗取转移。云南省通信管理局与本省公安厅联合成立了“云南省打击电信网络诈骗中心”，并建设和运行了“云南省诈骗电话监测预警系统”，实现了对不规范主叫的发现与监测、疑似诈骗号码的发现与监测两大功能。江苏省通信管理局建设完成了“诈骗电话智能全网拦截平台”与“防欺诈虚假域名管理平台”，全面实现了诈骗电话的防范拦截与网络诈骗的监测处置。江苏通信管理局组织本省基础电信企业建设“江苏省诈骗电话智能全网拦截系统”，构筑了一道覆盖江

苏省的“智能防火墙”，2017 年上半年已拦截境内外各类诈骗电话 730 余万次，据公安机关统计，江苏省 2017 年上半年利用电话诈骗的案件同比下降 48.9%，案值下降 41.3%。

五是强化宣传引导，提升用户防范意识。通讯信息诈骗是可防范性犯罪，增强广大群众识骗、防骗的意识和能力十分重要。专项行动以来，工信部多次通过中央媒体进行宣传报道，回应社会关切，并通过部官网、微信、微博等累计对外发布新闻稿 400 余篇，持续宣传防范打击通讯信息诈骗政策、工作动态、诈骗案例等信息。同时，工信部还组织三家基础电信企业、中国互联网协会通过短信、彩信、网站、论坛等多种方式向用户进行反诈警示宣传教育。截至目前，三大运营商向用户普发警示类短（彩）信累计超过 45 亿条。此外，工信部还将防范打击通讯信息诈骗纳入 2016 年和 2017 年电信和互联网行业网络安全试点示范工作，引导企业加强相关技术手段创新，积极向全行业推广最佳实践。

各地通信管理局在开展社会宣传教育过程中，也积极创新方式方法。上海市通信管理局建立全国首支电话实名制志愿服务队伍，加强实名制宣传和日常巡检，目前上海市平均每月有约 700 人次志愿者参加此项活动；贵州省通信管理局则在发送防范通讯信息诈骗宣传短信 1.64 亿条的基础上，通过制作电视节目、开设报纸杂志专栏等方式，进一步丰富宣传教育渠道。

2.切实落实责任，信息通信企业深入推进通讯信息诈骗治理各项工作

电信企业作为通讯信息诈骗治理工作的核心责任主体，围绕行业网络与信息安全管理有关工作要求，瞄准“认识到位、执行到位、责任到位、成效到位”的工作目标，积极落实专项行动各项工作任务。

一是在电话用户实名登记方面。三家基础电信企业严格落实行业电话实名登记制度要求，规范营销渠道管理，为近 160 万家实体营销渠道配备二代身份证检验设备，深入开展监督检查，严厉查处违法违规行为，累计组织对 3 亿老用户进行补登记，并依法对拒不配合补登记的 1000 余万老用户停止提供通信服务。经过持续奋战，2016 年底我国全部电话用户实现实名登记。为巩固电话实名登记成果，2017 年 2 月，三大基础电信企业集团公司与工信部签署了《电话用户实名登记责任承诺书》，承诺持续从严做好电话用户实名登记工作，对违反实名登记要求的各级省市公司和公司责任人依法依规从严进行问责。

二是在重点业务整顿方面。三家基础电信企业严格落实工信部关于重点电信业务的清理整顿要求，多次开展自查工作，严格规范语音专线、“400 号码”、商务总机等重点业务的出租与使用。截至 2016 年底，已关停违规语音专线 3.1 万条，关停违规“400 号码”76.4 万个；同时，在全面实施语音专线主叫鉴权的基础上，进一步建立专线业务异常经营行为防范监测手段，严防严控被不法分子利用从事违规经营活动；针对国际诈骗来话高企、社会营销代理违规经营等突出问题，组织完成国际合作运营商的合同修订补签，对国

际通信业务出入口主叫号码传送进行了规范，向用户提供了国际来电提醒，严格执行社会营销渠道代理资质审核制度，切实履行对代理商的管理责任，最大程度防范和化解通讯信息诈骗风险。

三是在技术手段建设方面。三家基础电信企业持续推进行业防范打击通讯信息诈骗专项治理行动，针对“国际、网间、网内”不同源头的诈骗电话，形成一整套治理体系。其中，中国电信各省级公司完成省内网内网间不良号码监测处置系统建设，建设集团-省两级防范通讯信息诈骗体系，该体系可对异常国际来话、网间来话及网内来话进行拦截。自启用以来，集团、省两级异常话务拦截量达 8.5 亿多次。中国移动在洛阳成立了“中国移动（洛阳）信息安全运营中心”，并组建了近 600 人的信息安全集中治理团队，负责骚扰诈骗电话、不良信息的集中发现、集中研判、集中封堵，创新性地实现了从分省治理到集中治理的转变，建立国际诈骗电话集中管控平台，自主研发“天盾”反欺诈系统平台，在全行业率先提出并实践虚拟改号诈骗电话监控拦截系统，针对国际、网间、网内等改号场景，建立虚假改号防控和反欺诈综合体系。截至目前，累计拦截诈骗电话 5.8 亿次，累计劝阻通讯信息诈骗既遂案件 1.3 万件，止付金额达到 3 亿多元，实现了对诈骗电话的精准拦截和受害人群的事中提醒。中国联通则上线了疑似诈骗号码溯源系统，加强用户宣传提醒。

此外，部分省级基础电信企业在通讯信息诈骗防范技术手段建设上也进行了大量有益探索。上海电信基于大数据与智能计算的欺

诈识别，建立了基于账务计费话单的移动欺诈用户识别模型，大大提升了对于诈骗和骚扰电话的覆盖率和命中率，实现对诈骗骚扰电话的精确打击。根据上海市公安反欺诈中心反馈，上海电信涉案号码所占比例从 2016 年的 20%连续下降至 2017 年 7 月的 5%。广东移动则建立了立体化通讯信息诈骗综合防控体系，研发“云管端”联动伪基站短信识别模型，实现准确溯源、精准定位要求。截至 2017 年 7 月，广东移动已配合广东公安破获伪基站案件 304 例，缴获各类伪基站 331 台。湖北联通基于信令数据策略分析运营的语音智能拦截系统，实现对超频、超短、异地漫游等主叫信令的监控，对疑似违规号码进行精准关停处置。自 2017 年 1 月上线以来，据 12321 举报中心的数据显示，湖北联通的“被举报量”、“百万用户被举报率”及“百万用户被举报率环比”均呈明显下降趋势。

四是在管理机制建设方面。三家基础电信企业制定完善任务清单、责任清单，进一步细化明确责任部门、责任人和时间进度表，逐级签订责任书，确保防范打击工作任务到岗、责任到人。此外，三家企业还加大责任追究力度，制定出台本企业防范打击通讯信息诈骗工作问责办法，建立责任倒查机制，对于落实不到位、出现问题的省级公司及集团公司相关部门领导班子、领导干部进行通报、约谈、甚至责令免职等责任追究，形成了不想违规、不能违规、不敢违规的工作局面。

五是在宣传教育及风险预警方面。中国电信与腾讯联合开发运营的“天翼安全中心”APP，对骚扰及诈骗电话进行提醒。中国移动

则在门户网站开设诈骗信息“举报专区”和“预警提示专区”，充分利用传统媒体和新兴媒体加强宣传引导，营造良好的舆论环境，提升用户权益保护意识和安全防护能力。同时，中国移动还在行业内率先上线防欺诈提醒服务，免费覆盖全网手机用户，精准定位疑似被骗用户并进行短信、电话等方式提醒，现已覆盖 31 省约 7800 万用户，周均提醒 1.33 亿次。中国联通上线了防骚扰提醒服务，无需安装客户端即可实现对所有类型手机的免费诈骗电话提醒服务，同时还提供了防欺诈公益服务，摈弃了传统的众标黑名单方式，利用高性能的大数据分析能力识别疑似的诈骗呼叫，2017 年全年累计发送提醒短信 203.5 万条，外呼电话提醒 8.1 万次，转交公安机关线索 1.8 万条，被人民日报评选为“2016 年度互联网+十大优秀案例”，被中央企业安全通报中心评选为“2017 年中央企业网络安全十佳创新解决方案”[16]。

六是在协同联动方面。相关互联网企业在防范打击通讯信息诈骗工作中积极发挥自身技术优势，主动作为、贡献力量。阿里巴巴公司推出了“钱盾反诈公益平台”，利用大数据分析将可疑号码的识别率提升到 92%，同时基于智能手机上线了针对钓鱼链接和二维码的防钓鱼反诈骗钱盾 APP。腾讯公司设立了安全联合实验室，推出了“鹰眼”、“麒麟”等通讯信息诈骗防范技术系统，利用大数据分析技术对向正在受骗的用户提供安全提醒服务。据公安网数据显示，在“麒麟”的帮助下，北京市公安局刑侦总队在 3 周时间内

[16] 参见北京时间 2018 年 1 月 30 日《看完后信心满满！中国联通 2017 年服务质量公告》

侦破 72 起诈骗案件，抓获 107 名犯罪嫌疑人；广东深圳在为期 90 天的打击整治涉“伪基站”专项行动中，共打掉涉“伪基站”犯罪团伙 13 个，缴获“伪基站”59 套，“伪基站”诈骗发案率降低八成。电话邦公司联合行业多家机构成立了“可信号码数据中心”，通过建立官方的、可信的企事业单位基础号码信息数据库，优化号码信息安全相关的服务，增强社会公众对号码信息服务的认知、认同与信任，有效预防通讯信息诈骗。

3.立足自身优势，行业机构积极支撑行业通讯信息诈骗治理工作

为支撑做好信息通信行业防范打击通讯信息诈骗有关工作，中国信息通信研究院（以下简称“中国信通院”）、12321 网络不良与垃圾信息举报受理中心（以下简称“12321 举报中心”）、国家互联网应急中心（以下简称“CNCERT”）等行业组织和研究机构，紧紧围绕“支撑政府 服务行业”的职责定位，全力支撑防范打击通讯信息诈骗相关工作。

一是主动开展通讯信息诈骗治理工作。中国信通院开展了防范打击通讯信息诈骗长效机制、网络数据安全和个人信息保护法规体系等专题研究工作，为进一步完善通讯信息诈骗治理相关制度机制提供科研支撑；制定国际局+86 号码处理、通用号码处理、国际来话实施提醒、违规主叫号码呼叫处理等相关技术方案，推动《通信网络不良语音信息判定技术要求》《互联网新业务安全评估指南》等行业标准出台，为企业主动识别和防范通讯信息诈骗安全风险提

供有力指引；开展通讯信息诈骗防治行动工作量化统计研究，研究形成防范打击通讯信息诈骗专项治理成效评估报告，直观展示治理工作成果。

二是积极支撑行业专项治理工作。中国信通院积极推动行业相关主体建立电话号码核查机制，建设了覆盖工信部、各地通信管理局、省级基础电信企业、移动转售企业、国内大型互联网企业的电话核查系统，实现了核查案例的高效派发流转、核查结果自动汇总分析。2017 年上半年累计完成 6.9 万余个核查案例；支撑制定省级基础电信企业网络与信息安全责任考核方案，结合通讯信息诈骗治理工作任务，分解形成了三大类 20 余项可量化的考核项目和评分标准，及时跟进和汇总电信企业防范打击工作进展和问题；推动部署电话用户实名登记远程在线监督检查系统，并积极组织力量配合开展技术检查和抽样调查，2017 年上半年累计抽查 2.89 亿个电话号码。此外，中国信通院、CNCERT、12321 举报中心深入参与专项工作督查重点工作，抽调精干力量 60 余人次，参与全国 16 省市专项督导检查。

三是充分发挥社会监督作用。12321 举报中心积极发挥行业自律平台作用，建立通讯信息诈骗用户投诉受理处置机制，一年来共受理举报诈骗电话近 16.8 万件次，受理涉嫌欺诈类短信 4 万件次，受理涉嫌个人信息泄露的网址信息达 4.7 件次，督促新浪爱问、百度文库、51 游戏等 26 家网站及时删除泄露个人信息内容近 10 万条，

组织国内重点应用商店和搜索引擎企业联动处置侵犯网民隐私、网络改号类 APP120 余款、网络链接 1000 余个。

四是深入推进行业协同治理。中国信通院深入推进诈骗号码标记信息共享，会同三大基础电信企业和奇虎 360、腾讯、电话邦、泰迪熊等 6 家互联网标记企业建立了涵盖了号码举报、标记、回收等全环节的数据信息共享机制，实现了终端用户和电信企业之间的标记信息联动。12321 举报中心与三家基础电信企业建立了诈骗电话的举报处置机制，将举报的诈骗电话和短信中的相关受益号码提交给基础运营商，由其进行快速关停处置。

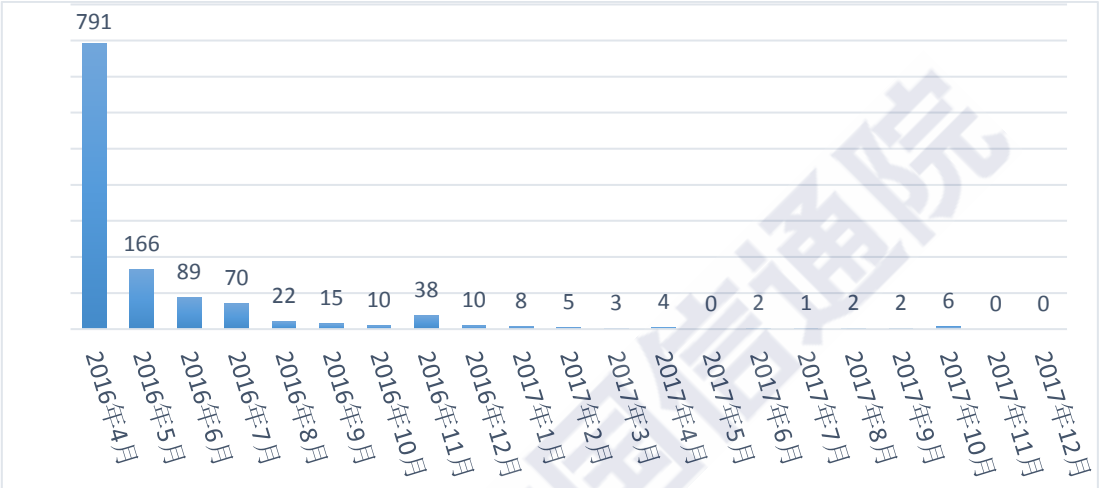
五是持续开展宣传引导工作。中国信通院积极配合行业主管部门开展专项宣传工作，组织制作行业专项工作专题宣传片，展示通信行业防范打击通讯信息诈骗有益经验做法，组织专家团队撰写专题文章，对通讯信息诈骗热点难点问题进行剖析。12321 举报中心定期将网络诈骗趋势和特点整理成典型案例向社会公布，并编写了《防范打击通讯信息诈骗创新实践案例汇编》，通过剖析典型案例的方式，向社会公众普及安全防范知识；同时，还举办以反诈骗为主题的网民节宣传活动，将常见的诈骗手段和“套路”融入到测试题之中，吸引了数十万网民参加。

（三）信息通信行业专项治理工作的阶段性成效

防范打击通讯信息诈骗专项工作历时两年多时间，构建了由政产学研共同参与、群防群治的治理格局。经过全行业共同努力，通

信行业通讯信息诈骗治理取得阶段性明显成效。从各方反馈数据看，基于电话、短信等形式的通讯信息诈骗活动得到初步有效遏制。

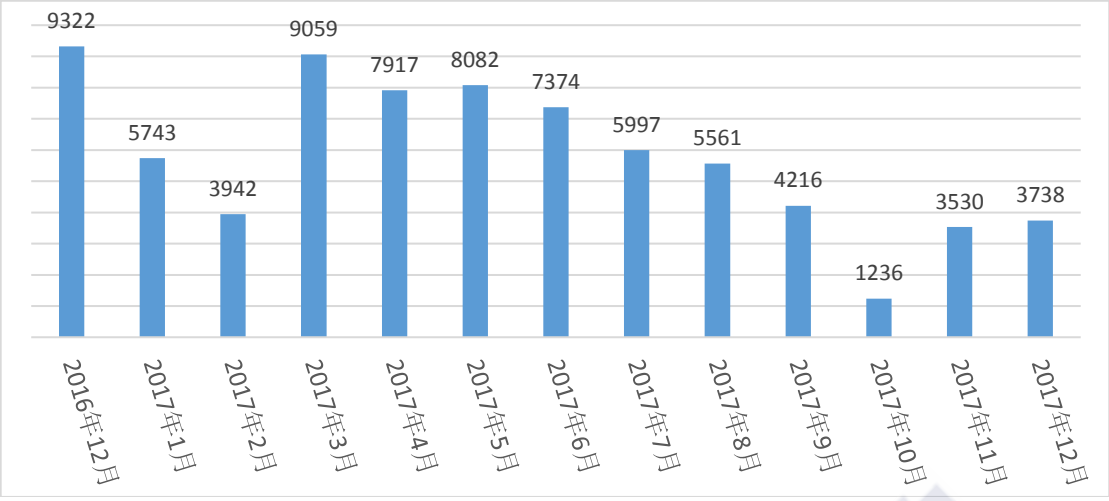
一是从公安部通报情况来看，涉案号码数量逐月大幅下降，以“400”号码举报量为例，已由 2016 年月均 700 多个下降到目前的个位数。



数据来源：工业和信息化部

图 4 公安通报涉案“400”号码数量（单位:个）

二是从 12321 举报受理中心数据看，2016 年 12 月至 2017 年 12 月，诈骗电话用户通报举报数量呈现整体持续下降趋势。2017 年 12 月份用户举报数与去年同期相比下降了 59.9%，数量下降为原来的近三分之一。结合用户举报的类型看，基础电信企业手机号码、固话号码、“400”号码、不规则来电号码被举报件次与去年同期相比全面大幅下降。其中，基础电信企业手机号码 2017 年 12 月份被举报件次与去年同期相比下降 49.3%。



数据来源：中国互联网协会

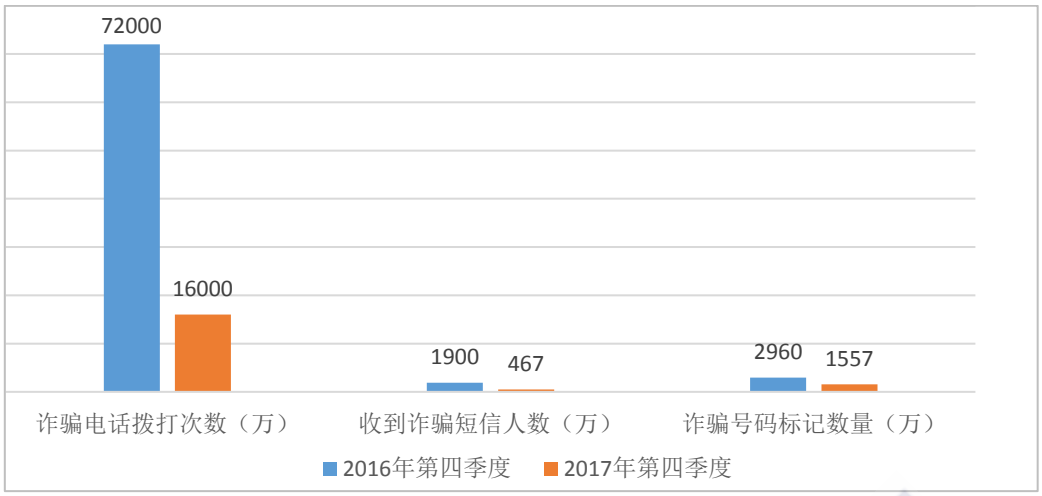
图 5　12321 举报平台接收到电话举报数量(单位:件次)

表 1 2017 年 11 月诈骗电话举报情况统计

诈骗电话号码分类	被举报件次	占比	同比	涉及电话号码个数
基础电信企业移动电话	2481	66.37%	↓49.34%	2411
固定电话	106	2.84%	↓96.94%	106
移动转售企业电话	1090	29.16%	↑263.33%	1025
“400 号码”	5	0.13%	↓93.16%	5
不规则来电	56	1.50%	↓90.49%	53

数据来源：中国互联网协会

三是从互联网企业数据看，腾讯公司的用户标记诈骗电话号码数量也呈现总体下降态势。腾讯手机管家的用户诈骗电话标记数据显示，2017 年第四季度，诈骗电话拨打次数同比下降 78.2%，收到诈骗短信人数同比下降 75.4%。在诈骗号码基数大幅减少、用户反诈骗意识增强的双重因素影响下，诈骗电话号码标记量同比去年同期下降 47.4%。



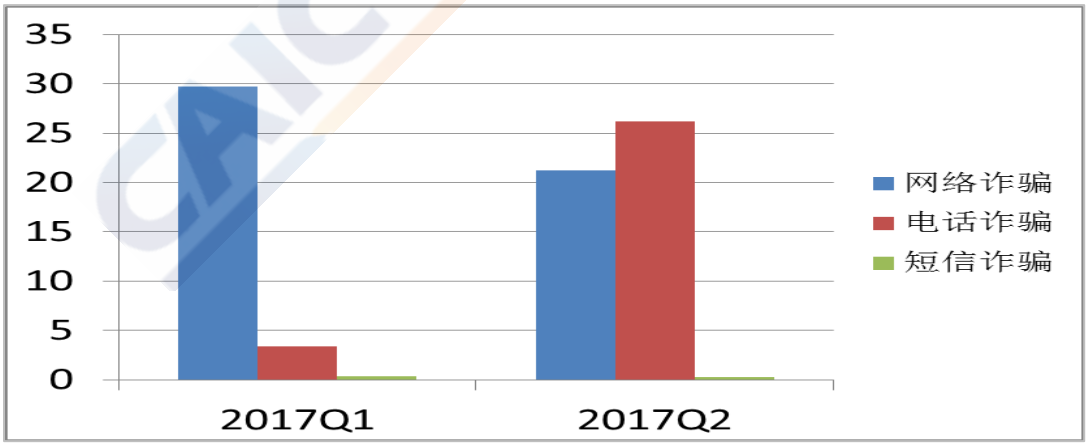
数据来源：腾讯发布的 2017 年第四季度《反电信网络诈骗大数据报告》

图 6　腾讯海量大数据分析诈骗情势

五、我国防范打击通讯信息诈骗工作的形势与挑战

（一）防范打击通讯信息诈骗工作面临的形势

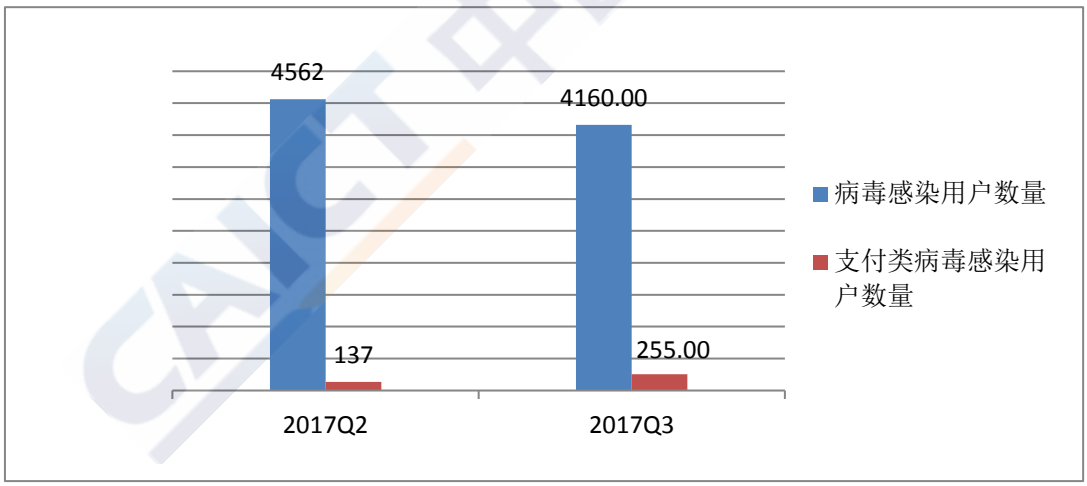
一是通讯信息诈骗从电话短信诈骗向网络诈骗演进。当前，传统基于电信网络的通讯信息诈骗加速向互联网转移，如网络销售伪劣商品诈骗、网络赌博诈骗、网络色情诈骗、网络非法集资诈骗（如 ICO 诈骗）、网络交友诈骗、网络购物诈骗、网络刷单诈骗等，花样繁多、层出不穷，相关案件数量明显上升。据有关报告显示，2016 年全国共发生网络诈骗案件 30 余万起，约占全部通讯信息诈骗案件 50%；2017 年第一季度，该比例提升至 89%。网络诈骗已成为发案最多、增长势头最猛的通讯信息诈骗。加之，网络诈骗具有信息传播链条长、涉及主体多、身份信息易隐藏等特点，为诈骗分子提供了有效规避现有监管手段的途径，加大了政府部门溯源查处难度。



数据来源：腾讯公司

图 9　2017 年第一、第二季度各类电信网络诈骗涉案金额占比情况（单位：亿元）

二是通讯信息诈骗治理对抗强度不断上升。随着诈骗分子诈骗手段和经验的不断提升，其在研发新型骗术时，往往会深入研究现有的网络服务，通过发现的各类业务的管理规则和技术防范漏洞，或利用用户对业务规则不熟悉，不断创新诈骗犯罪实施方式。据有关部门介绍，部分诈骗分子不仅利用传统 QQ、微信等社交软件进行诈骗，还通过视频直播平台、网络云盘、虚假 APP、微信外挂、微信木马、虚假微信红包等新兴技术手段进行诈骗。2017 年发生的“主副卡”诈骗案件中，诈骗分子正是利用了用户对手机“副号”和手机云服务等冷门业务的不熟悉，进而实施诈骗。这些不断推陈出新的诈骗实施方式，大大提高了通讯信息诈骗防范打击的技术难度。



数据来源：腾讯公司

图 10 2017 年第二、三季度手机病毒感染用户数量（单位:万人）

三是通讯信息诈骗实施精准化程度持续提高。在与行业监管部门的博弈对抗过程中，通讯信息诈骗产业链条也愈发成熟，部分诈骗团伙的规模和专业度可媲美中小型企业。同时，诈骗分子利用其

通过不法渠道获得受害人真实、准确信息，对受害人进行“量身定做”诈骗脚本，实施通讯信息诈骗。如不法分子利用在微信朋友圈发起投票的方式，骗取父母录入孩子的身份、姓名、就读的学校甚至照片等信息，并在骗取相关信息后编造重病、车祸等虚假信息，对父母进行诈骗。诈骗团队的专业化、诈骗脚本的精准化大大提高了诈骗脚本的可信度，为通讯信息诈骗的识别和预防增加了难度。

四是通讯信息诈骗目标人群向境外公民转移。在政府部门的高压打击、相关企业和行业机构的协同治理下，我国境内通讯信息诈骗活动空间明显压缩，诈骗分子逐步将目标转向在境外的中国公民。诈骗分子通过在境外实施网络改号等方式假冒中国驻外使领馆工作人员，以谎称有人冒用受害人身份犯罪等虚假案情为由，威胁当事人进行转账汇款。由于诈骗活动实施地点在境外，国内有关部门也很难实现追踪溯源和跨境打击，治理此类通讯信息诈骗仍面临较大难度。目前，仅中国驻洛杉矶总领馆每天接到类似核实情况的电话就超过 20 起，甚至个别中国公民已致电反映其家人被电话诈骗 10 万美元[17]。

（二）防范打击通讯信息诈骗工作面临的挑战

尽管通讯信息诈骗治理工作取得了阶段性明显成效，但与持续变化的诈骗犯罪活动形势相比，防范打击工作仍存在一定的“短板”，法律制度尚不健全、工作机制亟待完善、管理措施和技术能力仍有进一步细化和提升的空间。

[17] 参见中国新闻网 2017 年 12 月 13 日《洛杉矶频发电信诈骗 中领馆提醒公众保持警惕》

一是在法律法规方面，由于通讯信息诈骗不仅具有非接触、时空跨度大、技术含量高等特点，而且涉及主体多、面向广，导致无法可依和有法难依现象突出。例如，个人出卖本人银行卡、手机卡、网上支付账号等行为存在如何定性问题，为诈骗分子提供技术支持、广告推广、支付结算等行为的法律适用问题也有待研究解决；再如，诈骗行为电子证据的收集、固定难度较大，特别是跨境案件，证据容易灭失，执法手续复杂，抓捕难度大。

二是在行业管理方面，现有用户个人信息保护、电话用户实名登记基础性制度已经较为细化和完善,但在具体的企业责任落实方面，特别是对“实人实名”（即电话用户实际信息与实名登记信息一致）等管理要求的监督落实力度仍需加强。物联网卡实名登记管理制度尚不够细化，存在一定的通讯信息诈骗安全隐患。同时，伴随手机全网漫游费取消，在漫游通话成本进一步降低的情况下，利用异地手机号实施诈骗的案件呈现增多趋势，如北京手机号码漫游到其他地区冒充领导、冒充公检法实施诈骗的案件出现较大增长，相应安全管理机制有待完善。此外，信息通信行业执法人员力量相对薄弱，进一步制约了防范打击工作的持续效果。

三是在技术手段方面，针对通讯信息诈骗技术对抗强度不断提升的新形势，已有技术平台和系统在相关技术实施策略上仍需持续优化，在利用大数据、人工智能等新兴技术实现事前有效防范和事中事后精准溯源等方面还需深入探索。

四是在社会共治方面，相关部门与企业、行业组织建立了高效的联动处置机制，但在具体操作流程方面尚有待进一步规范；企业、研究机构等相关治理主体在总结和固化现有技术手段和管理经验的基础上，仍需打破各治理主体各自为政的局面，进一步加大在违规号码标记、用户信用分级、异常行为监测、安全风险预警等方面的信息共享和技术交流，避免各主体之间能力参差不齐，制约行业整体治理效能的持续提升。

六、深化行业防范打击通讯信息诈骗工作的建议

防范打击通讯信息诈骗工作仍处于一个动态博弈的过程，具有长期性和复杂性。诈骗分子始终在不断寻找和利用管理与防控工作漏洞，需要常抓不懈、久久为功，持续完善法律法规，不断提升行业监管效能，进一步充分发挥社会共治作用，将防范打击通讯信息诈骗工作不断引向深入，切实保护人民群众合法权益，促进行业健康可持续发展，维护社会和谐稳定。

（一）法律法规方面

一是在立法层面，应该结合防范打击通讯信息诈骗实际需求，从源头治理、防范打击的角度出发，在法律上细化出卖本人银行卡、手机卡等涉及通讯信息诈骗的违法违规行为，切断违法犯罪途径，使防范打击通讯信息诈骗工作有法可依、有据可循，从而推动防范打击通讯信息诈骗治理工作高效开展。

二是在执法层面，加快制定办理信息通信行业通讯信息诈骗案件（特别是电子证据取证、执法等操作流程）的规范指引，进一步明确政府相关部门与企业、行业组织联动处置的流程规范。探索在省、市层面成立专业的行业执法队伍，进一步充实基层执法监察力量，逐步建立部-省-市三级行政执法队伍体系，强化防范打击通讯信息诈骗监督处罚，督促企业落实安全责任。

（二）行业管理方面

一是强化行业用户个人信息保护工作。研究出台电信和互联网企业网络数据安全保护指导意见，明确企业数据采集、传输、存储、

使用、共享等各环节保障数据安全的范围边界、责任主体和具体要求，强化重点企业网络数据安全监督检查，督促企业健全数据安全管理制度，加强安全防护技术手段建设，对典型案例公开曝光。加强企业数据安全防护能力，强化用户个人信息保护监督管理要求，明确企业在与第三方共享用户个人信息前，严格审查能够反映第三方数据保护能力的相关证明文件，确保其对共享数据的保护水平不低于原有数据保护水平。鼓励相关单位在正规的数据交易机构开展数据交易活动，数据交换或传输在数据交易机构运营的交易系统中完成，交易的用户个人信息应符合《网络安全法》的有关规定。

二是巩固电话实名制工作成效。加强用户登记信息核验，进一步提升登记信息真实性和准确率，实现电话用户“实名实人”；尽快细化物联网卡实名登记管理要求，为相关管理工作提供明确的实施指引；同步加强监督检查，督促电信企业落实行业管理要求，针对行业卡突出问题，加大监督问责力度；进一步加强移动转售业务管理，建立移动转售企业电话实名制工作成效评价制度，完善移动转售业务监管和违规退出机制。

三是重点整治钓鱼网站、“僵木蠕”、移动互联网恶意程序等网络诈骗突出问题。加强对钓鱼网站、木马僵尸网络的监测处置，建立安全事件受理处置和威胁信息共享平台，及时汇总疑似钓鱼网站或木马僵尸网络的模板及特征、基础资源日志等信息，并对相关信息进行验证和处置。重点打击窃取用户信息并发送诈骗短信、恶

意扣费或诱骗付费、通过锁屏或加密文件进行勒索的三类诈骗 APP，督促相关企业及时关停相关服务器域名及 IP 地址等。

四是大力整治通讯信息诈骗信息传播渠道。进一步加强即时通信、社交平台、搜索引擎、电商平台等信息传播渠道管理，加强用户账号管理，落实用户实名认证要求，禁止企业以链接、摘要、快照、联想词、相关搜索、相关推荐、页面展示等形式提供改号软件、非实名电话卡等涉嫌诈骗的违法违规信息，推动企业建立网络诈骗信息巡查处置机制和技术手段，及时清理违法信息，依法关闭违法违规账号。建立通信行业诈骗短信息监测处置机制，对含有诈骗文本、钓鱼网站链接、木马程序链接等短信息进行监测拦截。

五是强化通讯信息诈骗高风险业务安全评估。重点评估二维码、短域名转换、云计算、互联网金融（移动支付、网络理财、ICO）等新技术新业务，即时通信、搜索引擎、手机应用软件商城、电商平台、社交平台等互联网业务平台，以及一卡多号、融合通信、短信营业厅等存在通讯信息诈骗风险的基础电信业务，积极消除安全隐患。

六是强化行业主管部门监督检查和考核问责。加强监督检查与安全考核，强化公安通报、用户举报、行业监管部门监督检查涉及违法违规问题的整改，固化和完善约谈、责令整改、行政处罚、通报、公开曝光等工作机制，督促企业切实落实安全责任。同时，充分发挥信息通信市场信誉管理机制对电信和互联网企业的监督约束作用，对拒不整改或整改不力的企业纳入违法不良记录信息库，对

于情节严重的，列入电信业务经营不良名单或电信业务经营失信名单，并在全行业实现信息共享。

（三）技术手段方面

一是利用大数据技术强化对诈骗信息研判能力。不论是通过何种方式伪造权威部门号码发送短信或拨打电话，诈骗分子的行为轨迹总有异常之处。积极探索基于大数据分析的技术管控能力，及时预警高风险短信与电话。拥有电话通讯记录的电信企业可以利用大数据技术标记出此类高危电话号码。

二是强化诈骗实施技术手段的跟踪应对。及时跟踪诈骗分子利用二维码、短域名转换等互联网新技术新业务实施诈骗的趋势，细致分析典型诈骗案例中技术特征，研究应对思路和技术手段，不断提升技术安全保障能力。

（四）社会共治方面

一是搭建技术能力共享交流平台。以行业研究机构为主导，积极分析总结行业通讯信息诈骗治理的优秀做法和有益经验，定期发布通讯信息诈骗治理最佳实践指南，引导各企业逐步提高技术能力，提升行业整体治理效能。

二是健全完善行业自律规范制度。发挥行业自律组织的作用，组织企业制定出台防范打击通讯信息诈骗相关行业自律公约，特别是针对语音专线、400 等诈骗风险较大的重点电信业务制定专门性的自律公约；积极探索基于违法违规码号、通讯信息诈骗关键词和

网址链接、用户黑名单信息的共享查询机制，实现违法违规主体和相关责任人的“一处违规、处处受限”。

三是建立用户参与通讯信息诈骗治理激励机制。推动政府和企业联合建立健全奖励机制，通过实施有奖举报、组织安全竞赛、评选优秀代表等多种方式激励广大用户参与防范打击通讯信息诈骗工作，形成群策群力、群防群治的生动工作局面。

四是强化用户宣传教育。针对通讯信息诈骗手法不断翻新、花样层出不穷、让人防不胜防的特点，由政府部门组织企业、行业研究机构等主体建立通讯信息诈骗手法快速发布机制，及时向社会公众发布预警防范提示；推动防范诈骗宣传活动进社区、进单位、进学校，针对老年人、青少年等重点群体，有的放矢开展宣传工作；推动基础电信企业和互联网企业主动提供涉嫌网络诈骗的账号、手机号、不良网址、恶意 APP 等相关信息的警示和提醒。

附 录

信息通信行业重点政策文件

1. 《关于防范和打击电信网络诈骗犯罪的通告》（2016 年 9 月 23 日）
2. 《工业和信息化部关于进一步做好防范打击通讯信息诈骗相关工作的通知》（工信部网安函〔2015〕601 号）
3. 《工业和信息化部办公厅关于进一步做好防范打击通讯信息诈骗信息通报工作的通知》(工信厅网安函〔2016〕114 号)
4. 《工业和信息化部办公厅关于印发<基础电信企业防范打击通讯信息诈骗不良号码处置技术能力要求>的通知》(工信厅网安〔2016〕143 号)
5. 《工业和信息化部办公厅关于进一步清理整治网上改号软件的通知》（工信厅信管函〔2016〕753 号）
6. 《关于对举报通报电话呼叫进行快速倒查有关要求的通知》（工网安函〔2016〕1086 号）
7. 《关于开展重点电信业务清理整顿情况专项检查核验的通知》（工信管函〔2017〕65 号）
8. 《关于进一步加强码号资源数据管理的通知》（工信管函〔2017〕374 号）
9. 《工业和信息化部关于进一步加强境外来源诈骗电话防范打击工作的通知》（工信部信管函〔2018〕3 号）

通讯信息诈骗用户举报指引

1. 中国电信客服热线：10000
2. 中国移动客服热线：10086
3. 中国联通客服热线：10010
4. 报警电话：110
5. 工业和信息化部公共服务电话平台：12381
6. 中国互联网协会网络与不良信息举报电话：12321
7. 国家网信办互联网违法和不良信息举报电话：12377

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839

传真：010-62304980

网址：www.caict.ac.cn