# 压缩网络诈骗的生存空间

加强网络技术风险预判，不断提升对策的科技含量、智慧含量、创新含量，从而让治理技术跑到技术犯罪的前面

“备豫不虞，为国常道”。今天，我们既要打好防范和抵御风险的有准备之战，也要打好化险为夷、转危为机的战略主动战。而互联互通、普惠共享的网络时代，也潜藏着诸如网络诈骗这样的安全隐患，需要防患于未然。

前不久，一份研究报告总结出“2018年十大网络诈骗经典话术”，再次警示人们筑牢网络安全防范意识。这其中，既有网络社交、信贷诈骗等传统“套路”，也不乏利用电商、网游等平台实施诈骗的新手段新表现。除了财产损失，网络诈骗还会给受害人带来难以消弭的心理创伤，甚至酿成生命悲剧。可以说，网络诈骗污损了网络生态，侵蚀了社会诚信土壤，给人们的日常生活带来阴霾。

有鉴于此，近年来，我国对网络诈骗始终保持高压严打态势，着力压实主体责任，努力守护群众的生命财产安全。破获电信诈骗案件31.5万起，成功止付被骗资金300多亿元，赴34个国家和地区开展警务执法合作，捣毁境外诈骗窝点200余个……2018年底，公安部公布了开展专项行动三年来的“成绩单”，全国新一轮打击治理电信网络违法犯罪专项行动也正式启动。重拳出击、重典治乱，以凌厉手段集中整治网络诈骗行为，已成为社会共识。

但也要看到，重点打击之下，网络诈骗仍难以根绝，并日益呈现出新的特点。《2018年网络诈骗趋势研究报告》显示，2018年网络诈骗人均损失创下近5年来新高。与此同时，“00后”正成为网络诈骗的新目标，网龄较短的青少年受害者数量迅速增加。无论是从经济损失数额，还是从受害群体范围来看，网络诈骗潜滋暗长的态势，都值得警惕。

新技术是一把双刃剑。近年来花样不断翻新的网络诈骗手段，有不少是钻了技术的空子。移动支付创造了高效便捷的付款方式，

也成为网络金融风险的“重灾区”；短视频占领移动传播新风口，也为网络诈骗提供了新平台；大数据描摹用户画像，也导致基于公民个人信息的精准诈骗问题日益突出。现实中，恶意应用攻击手机系统、聊天机器人批量操作、互动H5链接骗取用户数据……瞄准移动互联网新业态新技术，新型网络诈骗“技术含量”显著增加，甚至呈现出精准化、智能化、场景化趋势，诈骗方式更趋隐蔽，令治理难度不断攀升。技术之刃一旦被违法者掌握，极易伤害公众利益。

这也启示人们，占领技术高地、让前沿科技为我所用，才能为治理网络诈骗提供强大武器。例如，深圳警方利用“AI+新侦查”模式排查线索，极大提升了破案效率，成功破获特大网络交友诈骗案；腾讯采用人工智能“麒麟”系统，精准打击伪基站；三大电信运营商借助技术手段，有效监控拦截诈骗短信和电话；第三方支付平台运用刷脸支付、指纹认证，不断提升支付安全性能，等等。值得思考的是，政府或企业的技术解决方案不应限于见招拆招，更须加强网络技术风险预判，不断提升对策的科技含量、智慧含量、创新含量，从而让治理跑到技术犯罪的前面。

再高明的网络诈骗技术，也是利用了人性弱点。作为治理网络诈骗的关键，网民不仅需要“技术防护”，更需要“思想防护”。增强网络防骗意识与能力，筑牢思想认识“防护线”，堵住信息“决堤口”，才能最大限度压缩网络诈骗的生存空间。