【治理偷窥黑产之三】

四部门5月以来严打摄像头偷窥黑产 已处置平台账号4000余个

治理进入后半程 问题平台应尽快整改

网信办等四部门此次对于摄像头偷窥黑产的集中治理，是从今年5月份开始的，持续到8月底结束，为期四个月。集中治理的工作重点主要分为三个方面：非法利用摄像头偷窥个人隐私画面、交易隐私视频、传授偷窥偷拍技术，而这三个方面也正是公众反映最为强烈的侵害公民个人隐私行为。中央网信办有关负责人表示，此次集中治理工作已进入后半程，存在问题的企业、平台要尽快整改，不留死角。下一步，中央网信办将会同有关部门继续加强治理，坚决遏制摄像头偷窥等黑产生存空间，切实保护公民个人隐私安全。

重点打击三方面违法行为

打击利用摄像头偷窥隐私

对于第一大工作重点，打击非法利用摄像头偷窥个人隐私画面，近年来各种案例可谓层出不穷。根据公安机关公开发布的案例，包括酒店、民宿、商场试衣间、公共洗手间、电动扶梯、公交车、地铁等地方是高危区域，部分犯罪分子甚至将黑手伸向了家用摄像头。不仅严重侵犯了公民个人隐私，更可能带来敲诈、勒索、损害网络安全等一系列更大的危害。

打击隐私视频交易行为

犯罪分子非法获取他人隐私画面，究竟用来干什么？警方表示，有的纯粹是为了满足自己的偷窥欲，而更多的则是以此牟利。这也就是此次四部门严打摄像头偷窥黑产的第二大工作重点：打击隐私视频交易行为。有案例显示，不法分子将针孔摄像头暗藏在酒店客房内，再分享App邀请码，使他人获得观看权，这是要付费的。针孔摄像头安装者以每个150元到200元的价格，将邀请码销售给下线代理，代理再加价分销，最终一个邀请码可卖五六百元，而每个摄像头可生成100个邀请码，供百人同时在线观看。

打击传授偷窥偷拍技术

此次四部门严打的第三大工作重点是严厉打击传授偷窥偷拍技术，最大程度杜绝摄像头偷窥这一违法行为进一步泛滥。网上充斥着所谓的家用摄像头破解教程，破解方法也是五花八门，比如通过扫描器破解摄像头的IP地址、端口、设备的出厂账号等。

业内专家称，家用摄像头的信息安全涉及多个方面，既有设备本身的终端安全，也有云平台的安全，以及移动应用与数据传输的安全。任何一台信息设备只要连入了公共信息网络，它就至少要开一个信息端口，这就有可能带来信息安全隐患。

已收缴窃听窃照器材1500余套

据8月9日中央网信办公布的消息，在推进治理摄像头偷窥等黑产工作中，各地网信办督促各类平台清理相关违规有害信息2.2万余条，处置平台账号4000余个、群组132个，下架违规产品1600余件。

网信部门还对存在隐私视频信息泄露隐患的14家视频监控APP厂商进行了约谈。

据悉，5月以来，中央网信办会同工信部、公安部、市场监管总局推进摄像头偷窥等黑产集中治理工作，对非法利用摄像头偷窥个人隐私画面、交易隐私视频、传授偷窥偷拍技术等侵害公民个人隐私行为进行集中治理。

工信部组织对18家具有行业代表性的视频监控云平台开展检查，发现处置越权操作等一批高危漏洞；全面排查联网摄像头存在的安全隐患，发现4万多个弱口令、未授权访问、远程命令执行等摄像头漏洞，取证并处置500余个。

公安部组织全国公安机关依法严打提供摄像头破解软件工具、对摄像头设备实施攻击控制、制售窃听窃照器材等违法犯罪活动，共抓获犯罪嫌疑人59名，查获非法控制的网络摄像头使用权限2.5万余个，收缴窃听窃照器材1500余套。

市场监管总局组织召开互联网平台企业行政指导会，要求强化对平台内假冒伪劣摄像头等商品的治理，并要求限期一个月完成全面整改。

中央网信办有关负责人表示，此次集中治理工作已进入后半程，存在问题的企业、平台要尽快整改，不留死角。下一步，中央网信办将会同有关部门继续加强治理，坚决遏制摄像头偷窥等黑产生存空间，切实保护公民个人隐私安全。

现象分析

责任主体缺位 为黑产提供生存空间

近年来，诸多不法分子或利用黑客技术破解并控制家用及公共场所摄像头，或将智能手机、运动手环等改装成偷拍设备，又或出售破解软件、传授偷拍技术以供客户“偷窥”隐私画面并借此牟利，已形成黑产链条。这与社交软件、网站、论坛等互联网平台没有严格履行信息发布审核主体责任、摄像头生产企业没有严格履行网络安全主体责任、电商平台没有及时清理下架假冒伪劣摄像头有着直接关系。

欲望流量驱动 暴利黑产市场

随着智能手机、智能家居等设备的普及，网络摄像头逐渐成为一些用户生活的“标配”。数据显示，2020年第四季度，中国家庭安全监控设备销售额接近6亿美元，出货量为817万台，同比增长24.9%。

然而，隐私保护已成为网络摄像头行业迫切需要回应的关键问题。互联网问题专家高扬坦言，网络摄像头的技术特性可能给犯罪分子以可乘之机，其利用部分产品的技术漏洞破解大量摄像头IP地址，高价售卖破解软件与“偷窥套餐”。有商家未经用户允许远程操纵摄像头“直播”，给公民隐私带来威胁。

大量个人私密信息被以低廉的价格，在网络上随意贩卖传播。一份资源卖给多个下家，隐私不断被售卖。利益链绵延不断，每个环节的违法成本都很低，靠贩卖偷拍视频，轻轻松松就赚上万块，这样的低成本高收益的利益不断驱使这条黑色产业链发展壮大。

犯罪门槛低、处罚轻 打击难度大

偷窥问题由来已久却屡禁不止，犯罪成本低、监管难度大或是其中的重要原因。

公安部“净网2019”专项行动发布会上，浙江警方曾表示，针孔摄像头成本较低，不到百元，黑市获利空间可观，而且制作门槛低，加工简单，此前收缴的针孔摄像头有相当部分其实就出自手工作坊。

据介绍，类似犯罪的打击难度在增加。比如，越来越多的针孔摄像头销售方式从线下搬到了线上，通过采取注册虚拟账号进行网络销售的方式来躲避监管。

除了技术上监管难度的增加，也有人提出，较低的违法成本很难遏制不法分子违法获利。

河南省新密市人民检察院的一位检察官曾在接受媒体采访时表示，非法使用窃听、窃照专用器材罪受到刑事处罚的案例并不多见，多数按照治安案件进行处理，即“有偷窥、偷拍、窃听、散布他人隐私的行为的，处五日以下拘留或者五百元以下罚款；情节较重的，处五日以上十日以下拘留，可以并处五百元以下罚款”。犯罪成本低、处罚轻，造成此类犯罪进一步滋生。

专家建议

安全漏洞亟待弥补 应出台行业技术标准

泰和泰律师事务所律师廖怀学分析，摄像头产品质量瑕疵、云端安全防护脆弱、应用端使用弱口令等都可能导致网络摄像头泄露隐私。网络摄像头隐私泄露监管的难点主要在于：一是网络摄像头破解技术日趋隐蔽化、专业化；二是网络摄像头隐私泄露犯罪组织逐渐产业化、链条化。“前者是新型网络隐私犯罪的源头，不法分子会利用更新迭代的技术开发破解工具，攻破厂商设置的安全防线，对侦查工作提出挑战。而犯罪行为的产业化和链条化不仅扩大了犯罪主体和地域范围，还扩展了犯罪场景，这也大大提高了监管难度。”廖怀学指出，贩卖公民隐私的行为可通过民事侵权、刑事追责等加以打击。“首先需要精细化相关立法，为各方主体划定行为红线，监管部门应协同配合，提高执法水平。行业组织应倡导企业和行业自律，出台相应的行业技术标准。企业和公民自身的隐私保护意识也不容忽视。”

违法装窃听窃照装置的 对管理者予以行政处罚

2020年全国“两会”期间，全国政协委员、农工党河南省委专职副主委花亚伟指出，“从社会危害程度上来看，偷拍个人裸体甚至性爱场面对个人和社会的危害远超非法买卖公民个人信息，刑法第二百五十三条规定了侵犯公民个人信息罪，最高可处三年以上七年以下有期徒刑并处罚金，但对严重的偷拍、偷窥、偷听行为却没有列入刑法。”他提出，应完善立法，对偷拍等严重侵犯公民个人隐私的行为予以刑事处罚。对于有商家提供改装服务，花亚伟建议，在市场监管层面，要对销售环节实行备案许可制，以便对偷拍事件进行溯源。开展专项整治行动，从源头上制止针孔摄像头泛滥的局面；进一步明确酒店和公厕等公共空间管理者的主体责任，对出现违法设置窃听窃照装置的管理者予以相应行政处罚。

加强监管势在必行 企业应当完善设计

如何让网络摄像头用得更让人心安？北京航空航天大学法学院教授周友军指出，市场监管部门有必要从生产环节强化监管，要求生产厂家在代码防护、身份鉴别、弱口令校验等方面达到国家标准，避免非法破解事件。企业也应当完善设计，不断更新摄像头安全防护程序，指导用户加固安全措施。同时，公民应提高网络安全意识，购买正规厂商生产的摄像头设备，设置高级别防护密码，及时更新摄像头安全防护程序。

本组稿件据《南方都市报》