涉及多地!

藏在弱电井里的电诈“黑匣子”

频繁接到显示为办公电话的陌生来电,有人因此被骗走一年收入。警方调查发现,这些涉诈电话竟是从公立医院的固定电话打出。弱电井里偷偷装上的“黑匣子”背后,是一张席卷多地的电信诈骗网络……

一场VOIP(网络电话)电信网络诈骗黑灰产业链全国集群战役就此打响。新华社记者近日采访侦办案件的内蒙古自治区鄂尔多斯市公安局东胜分局,起底一条为境外电信网络诈骗集团提供呼叫服务的黑灰产业链。

医院来电背后的陷阱

“5月5日,我在家中接到显示归属地为鄂尔多斯的固定电话。对方说我在某直播APP开通了直播带货权限,从下月开始每月自动扣取服务费800元。”一位受害人心急如焚地向警方说,“对方说可以帮我取消扣费服务,我同意了。等我反应过来,银行卡里的11万元都被骗走了,这可是我全家一年的收入!”

今年5月,东胜公安分局刑侦大队接到线索,经过对涉诈电话号码核查,三个电话号码竟然是从该市三家公立医院的办公固定电话打出。

难道是医院内部人员参与诈骗?反诈经验丰富的老刑警分析认为,三家医院同时出现“内鬼”的概率极低,侦查重点应该放在医院的电话通信设备上。

案件分析会后,民警立即联系相关医院,联合运营商对医院通信设施开展排查。当通信维修人员从弱电管道井里出来,指着手机照片上的“黑匣子”惊呼:“语音网关(VOIP固话端设备)!安在医院固话交换机上。”

反诈民警立即冲入闷热的管道井,经现场勘验,发现仅一家医院就有16部固定电话被非法接入语音网关。

“这些‘黑匣子’相当于高级的‘号码转换器’,犯罪分子利用这些设备实现互联网与固定电话的联通。境外诈骗集团通过语音网关,将境外来电包装成了本地号码,极大降低了受害者的警惕性。”办案民警贾海军说。

顺藤摸瓜 全国收网

这些“黑匣子”如何进入医院弱电井?从哪里购买?又是谁指使安装?办案人员顺藤摸瓜,从设备安装、收售设备,再到技术支撑、组织管理等环节,逐渐摸清了该团伙的组织构架及运作情况。

今年5月8日,嫌疑人白某在鄂尔多斯市某旗安装语音网关后,准备逃离时被当场抓获。据他交代,今年4月,老乡给他介绍了一个“高工资、高风险”的工作,就是潜入单位、医院、酒店安装语音网关电话线。

根据白某的供述,一个庞大的电诈犯罪团伙浮出水面。民警在辽宁省某市将语音网关收售头目祁某某及其妻子牛某抓获,从其家中查获语音网关24个、网关合格证书340余张。随后,民警在另一城市将该团伙成员孔某抓获,铲除一处违法收售语音网关窝点。

然而,上线团伙仍逍遥法外。祁某某出售语音网关时,均通过境外加密聊天软件与上线单线联系,案件侦办一度陷入困境。“当时,我们初步判断该团伙涉案语音网关1300余台。如果就此结案,意味着千余台语音网关很可能还安装在全国各地,继续被诈骗分子利用。”贾海军说。

从已查获语音网关上的10万余条诈骗电话入手,10名办案民警花费数月时间,将数以万计的碎片信息拼凑出犯罪团伙的完整“拼图”。经查,该团伙涉及全国21个省区市、犯罪嫌疑人80余名。

鉴于案情重大,东胜公安分局申请发起全国集群战役。2025年10月,90余名民警分赴21个省区市开展收网行动,成功抓获包括顶层管理、中层技术支持和底层设备安装在内的犯罪嫌疑人74名,扣押VOIP相关设备300余台,全链条铲除了这一为境外诈骗集团提供技术支撑的黑灰产业链。

“隐蔽角落”的安全警示

记者梳理发现,近年来相关电信网络诈骗新型犯罪案例多发,已导致不少群众被骗。

东胜公安分局刑侦大队副大队长蔺娜说,犯罪分子从弱电井、机房下手,便于其设备接入内部电话线路。犯罪分子多伪装成电工或通信运营商的维修人员,利用节假日或安保松懈时段,混入写字楼、医院、企业等单位,伺机潜入弱电井,在境外诈骗分子的指挥下实施安装。

网络安全等级保护制度是我国网络安全领域的基础制度,其要求网络运营者落实安全管理与技术防护措施;若落实不到位,自身要承担法律责任。

根据网络安全法,民警提醒,各单位应做好对固定电话涉诈风险的排除和防范工作,应联合运营商加强风险隐患排查,重点检查机房、弱电井、办公电话接口等隐蔽位置是否存在异常,如发现异常设备,立即进行拆除;对进入弱电井的人员进行身份核验登记,要求施工人员提供运营商授权文件,无文件者拒绝其进入弱电井;对机房、弱电井等重点场所加装防撬挂锁,有条件的要安装监控设备。

警方提醒,日常生活中,接到自称机关事业单位、企业的电话,应留个心眼,注意与官方公布的热线电话比对核实。

(据新华社呼和浩特12月15日电)

偷猎的“空中刺客”,该管管了

夜色如墨,笼罩着赣北连绵的山峦。一阵低沉的嗡鸣声打破宁静,一架搭载热成像摄像头的无人机如幽灵般升起,它的“眼睛”扫过森林。地面上,操纵者紧盯屏幕上闪烁的光点——那是一个活动于林间的温热生命。

“目标锁定。”指令下达后,无人机携带特制的“牙签箭”潜入黑暗。

这是江西省德兴市警方近期侦破的一起利用无人机进行非法狩猎案件的真实场景。类似的“黑飞”狩猎存在安全隐患。

●“黑飞”狩猎隐患重重

今年9月,德兴市万村乡民警凌晨巡逻时,发现洋源村路边停有两辆可疑面包车,车内藏有两头野猪尸体。民警判断附近可能存在盗猎团伙,随即展开搜查,并当场抓获4名犯罪嫌疑人。

万村乡派出所副所长张江介绍,主犯张某为本地种粮大户,平时使用无人机进行农业作业。近期,他在短视频平台接触到无人机狩猎内容后,购买设备并邀卖家洪某现场教学。

在这起案件中,洪某利用无人机热成像功能进行高空侦察,在黑夜中精准定位野猪等动物的位置;随后操控无人机返回自己身边,装上自制的配重箭头;最后操控无人机飞抵目标上空,进行“坠箭”攻击,形成“空对地”狩猎系统。

洪某交代,他自今年7月起销售无人机,原本客户为农户和测绘公司。为拓展销路,他模仿短视频平台内容,以“无人机狩猎”为噱头招揽顾客。“我不知道这是违法的,平台上类似的视频很多。”洪某称。

此类案件在全国多地均有发生。今年年初以来,湖南长沙某养猪场先后丢失20余头猪,场区周边发现多支重约0.5公斤的金属箭头;山西吕梁一名养殖户价值上万元的家养马匹在夜间遭无人机射杀;重庆永川有非法狩猎者利用无人机挂载利箭、钢球等装置,射杀、砸杀果子狸、野兔等野生动物。

“如果不进行有针对性的打击,蔓延会非常快。”德兴警方表示,“黑飞”狩猎已成为具有普遍性的安全隐患,热成像仪在夜间仅能识别目标轮廓,无法准确辨别人与动物,可能误伤村民、护林员等人员。

●灰色产业链暗中滋生

个案背后,一条借助网络平台的灰色产业链正在暗中滋生。

这条产业链的起点,是极具视觉冲击力的境外狩猎内容。一些户外直播人员在缅甸、泰国等地进行实弹狩猎直播。虽然国内平台对相关内容有所限制,但通过使用代号、外语平台或私密社群,这些充满猎奇与刺激的狩猎画面仍能吸引不少受众。

“其实很多人就是猎奇,捕猎野生动物也不是真的为了去交易。”受访民警介绍,与传统的狩猎动机不同,无人机狩猎者多不为贩卖猎物,而是迷恋于新型狩猎技术带来的刺激。

与此同时,一些短视频平台成为非法狩猎教学、工具售卖和引流的温床。

不少商家使用暗语,使交易更加隐蔽。比如,用“牙签”代指狩猎箭头,用“抓佩奇”代指猎杀野猪……这套暗语既规避了平台审核,又成为圈内人的身份识别标志。原本需要特定渠道才能获取的专业狩猎工具,如今在短视频平台上变得触手可及。

部分卖家不仅销售无人机等专业设备,还会“教授理论”,提供从设备操作到狩猎技巧的“一站式”指导。本案中,卖家洪某是德兴隔壁县的,为了售卖无人机,特意来到德兴向买家“教学如何使用无人机狩猎”。这种“售教结合”的模式,极大地降低了技术门槛,让普通人也能快速掌握原本专业的狩猎技能。

●多元共治防范“黑飞”

面对无人机“黑飞”问题,一些地方公安部门在积极探索应对之策。

“我们所里就5个人,巡护的山林面积又比较大。”张江介绍,尽管人手紧张,但派出所依然坚持开展高频次的夜间巡逻,“通常晚上开始,由一名民警带领两名辅警,一直要巡查到深夜。”

与此同时,技术反制手段也在逐步应用。“派出所配备了热成像无人机,也会安排飞行巡查。”张江说,警方正尝试“以科技对抗科技”,弥补人力覆盖的不足。此外,利用物流信息、采购数据等大数据手段进行线索筛查,也成为新的突破口,有效助力提升精准防控能力。

德兴市公安局环食药侦大队大队长王力介绍,根据《无人驾驶航空器飞行管理暂行条例》规定,盗猎者在未经许可的情况下私自使用无人机,属于典型的“黑飞”行为,应予以严厉打击,但是部分盗猎者使用的是未经实名登记的二手无人机,监管起来存在一定难度。建议参考二手车行业或贵金属管理的经验,完善无人机实名登记和全链条管理系统。

针对新型狩猎方式,江西师范大学政法学院教师罗金寿建议,修订野生动物保护法实施细则,将“使用无人机等智能航空器进行追踪、驱赶、骚扰、猎杀野生动物”明确列入“禁止使用的狩猎工具和方法”。

(据新华社南昌12月15日电)