关注网络安全之一：

吃“技术饭”？别成了“技术犯”！

新华社记者 宋立崑 熊琦 唐文豪

对普通人来说，哪些网络犯罪就藏在我们身边？面对网上形形色色的诱惑，怎样避免卷入网络犯罪？

近日，记者采访多地公安机关和法院，为你起底破坏网络安全的新手法、新动向，帮你擦亮双眼，安全上网。

砸了“金饭碗”，收获冰冷的手铐

“挂暗链，特定网站每条100美元，普通网站每条50美元……”今年初，在广东有稳定工作的吕某，与境外犯罪团伙勾结，用黑客技术非法入侵某系统后台，植入涉黄链接进行引流，不到一个月时间，他就“赚”了6000多美元。

不久，吕某又将黑手伸向武汉一家公司开发的社交平台小程序。他利用黑客工具扫描漏洞，上传木马程序夺取后台控制权，在其中植入涉黄网页链接。正是这条“暗链”，触发湖北武汉网警的风险预警快速反应机制。

3月18日，武汉网警前往广东，对吕某实施抓捕。落网时，吕某电脑还登录着云服务器，运行着各类黑客惯用的木马等工具。

经查，自今年2月以来，吕某总共入侵全国多地80余个网络系统后台，非法植入涉黄链接。这些非法链接还涉嫌服务下游电诈分子的犯罪活动，帮助境外犯罪团伙获取用户手机权限和个人信息，有针对性地设计“剧本”、实施诈骗。

案件侦破后，武汉网警迅速向全国80余家相关单位发出安全预警，并督促涉事平台修复漏洞。目前，犯罪嫌疑人吕某因涉嫌非法控制计算机信息系统罪，被武汉公安机关采取刑事强制措施。

“我的技术就像菜刀，凭啥追究我？”

4月11日，武汉网警接到上海某科技公司报案称，两个月前，公司旗下社交平台突然涌现1.7万余个“僵尸”账号，大量推送涉黄、涉赌等引流广告。

网警循着软件信息链，迅速锁定一款技术软件及其开发者袁某。经查，为挣快钱，计算机科班出身、凭技术“吃饭”的袁某于2024年底开发出一款技术软件，能绕过平台的登录验证机制，无需手机号实名绑定即可自动批量登录海量账号，进行评论、点赞、群发私信等操作。

“基础版月费3000元”“高级版4090元”袁某将软件服务明码标价，用户交的月费越多，解锁的功能越多。他还能针对不同社交平台防火墙的更新换代，及时开发新版本跟进破解。

“我的技术就像菜刀，人家买回去可以切菜也可以伤人。凭啥客户犯罪，要来追究我？”4月16日，武汉网警将袁某抓获归案，审讯室内，袁某为自己开脱辩解。

“你的‘生意’，本质上是提供侵入、非法控制计算机信息系统的程序和工具。”民警向袁某展示了相关证据链，指出其行为的违法本质和社会危害。在事实和法律面前，袁某最终无法抵赖。

技术尖子，更要穿上“法律铠甲”

近年来，网络信息技术犯罪主体年轻化趋势明显。湖北省公安厅数据显示，在2025年以来打击查处的网络信息技术犯罪嫌疑人中，40岁以下占比近78%。其中，掌握一定网络技术的无业人员和刚步入社会的年轻人，占比较为突出。

网络技术犯罪还逐步呈现团伙化、专业化特点。据警方介绍，整个犯罪过程被拆解为多个环节，由境内外不同犯罪团伙分工完成。值得注意的是，每个环节的犯罪分子都会针对性研究相关领域的最新技术、软件工具，在社会上广泛招募“兼职人员”，以此转移警方的注意力和规避相关法律风险。

“抢票、批量注册、破解验证码是常见的非法开发目的。”武汉市公安局网安支队办案负责人表示，一些年轻的技术狂热者，渴望在圈内证明自己，反而被不法分子利用。

2023年12月，出于好奇和炫技心理，自学成才的四川“00后”青年刘某某，侵入某游戏公司服务器，删除、修改了该游戏公司在用户社区播放的两个游戏角色宣传视频，还利用公司的服务器非法搭建网盘，免费分享给网友用以上传、存储文件，给公司造成损失。

经估算，刘某某给游戏公司造成直接经济损失超10万元，后已全部退赔。5月27日，成都市青羊区人民法院以破坏计算机信息系统罪判处刘某某有期徒刑二年六个月，缓刑三年。

网络并非法外之地，无知也不是违法犯罪的借口。真正的技术高手，是用技术保卫网络安全，而不是破坏它。越是手握高精尖的技术，越是要主动学习法律和网络安全知识，为自己穿上“法律铠甲”，方能大展身手、实现个人价值。 新华社电

“一秒生成制服照”？AI岂能如此换装

新华社“新华视点”记者 刘宇轩

用户只需上传一张生活照，便可一键生成个人军装照、警察照……“新华视点”记者调查发现，一些AI工具推出“换装”功能，引发不少军警迷的追捧。但是，有不法分子利用“AI换装”功能，伪造军警身份招摇撞骗，亟待引起警惕。

AI生成制服照被滥用

记者以“AI换军装”为关键词，在部分短视频平台搜索到多款相关应用。这些应用以“穿电子军装过把瘾”“AI圆了我儿时梦”等为亮点吸引用户。有网民称，只需上传一张生活照，即可“秒变军人”，配上战车、阅兵场等背景，感觉圆了自己的“从军梦”。

当下一些流行的AI工具提供的AI生图功能，也可以按使用者要求，实现AI变装。然而，“AI换装”被一些人不当或不法使用，可能引发负面效应。

江苏大学管理学院党委书记、教授马国建表示，个别网民用AI将不同国家、军种制式的军服混搭，有的甚至把手持烟酒、勾肩搭背的生活照合成军装或警服照片、视频，与我军警应有的形象不符，是对军人和警察形象的不当消费。

个别网民借AI生成虚假人民警察证、部队任命书。今年3月，安徽黄山市屯溪区网民江某利用AI技术合成身穿军装的照片，并在社交平台发布“经军委同意，任命我为黄山军分区司令员”的虚假信息，意图博取流量。该行为造成不良社会影响，江某被当地公安机关处以治安处罚。

有的不法分子借助“AI换装”技术伪造身份，招摇撞骗。

今年4月，江苏省江阴市人民法院对一起冒充军人招摇撞骗案作出判决。网民路某并非现役军人，却盗用网络上军人训练的照片发布在短视频平台上；收获不少点赞后，他又用AI将自己的头像合成到军装照上，并花钱伪造军官证，摇身变成“少校军官”。在骗取6名女性信任后，他以“车祸”“租车见领导”等借口诈骗3万多元。法院以冒充军人招摇撞骗罪判处其有期徒刑2年。

平台审核缺位 变造制服照“零门槛”

记者在某社交平台上浏览到一些网友发布AI变装视频，通过视频下方小程序链接进入后，按要求上传三张本人面部清晰的照片；系统经过十几分钟的AI合成，便生成了军装变装视频。这期间，平台和小程序并未要求上传身份证明信息，也没有给出不得将合成视频用于违法违规领域的提示。

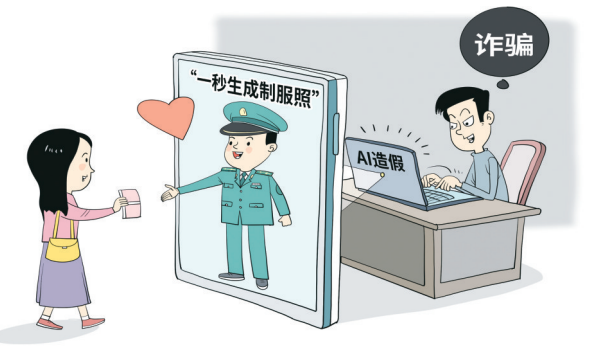
9月1日起施行的《人工智能生成合成内容标识办法》要求AI合成内容必须明确标注，但记者在使用多款AI换装应用后发现，用户合成发布的视频并未标注，容易让人产生混淆。

AI变装技术，降低了伪造身份的技术门槛。在某购物平台上，记者以“AI+军装照”为关键词，搜索到有商家公开出售佩戴军衔的各军种和警察服装模板素材。店家表示，只需要花不到一元钱的价格就可拍下所有这些素材。

记者拍下后，店家很快发来一个网盘链接，内部有数十款供P图的军装模板文件，用户可根据需要的款式和级别，通过PS或AI等方式将自己的头部肖像替换上去。记者尝试将AI生成的军装照和肖像照用于多款社交平台账号，发现并无审核难度，均可正常替换。

北京市炜衡律师事务所律师汪高峰说，一些内容平台和第三方软件疏于审核，纵容虚假内容传播，可能会降低公众对军人、警察职业的信任度和敬畏感。

江苏省政府参事室特约研究员丁宏表示，AI降低了伪造身份的技术门槛，网络上曾出现AI合成的警察抓人视频并配上所谓警情通报，涉嫌传播违法有害信息。这些内容可能误导公众，引发不必要恐慌，扰乱正常社会秩序。



“AI换装”诈骗 新华社发 朱慧卿 作

国家网信办不久前发布了一起执法典型案例：浙江某公司运营的App提供视频换脸、图片换脸、照片舞动配音等图片处理功能，用户可对上传图片、视频中的人物进行换脸，但未按规定落实安全评估要求，相关深度合成内容也未作显著标识，存在较大安全风险，违反《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》等规定。网信部门责令平台对该App予以下架处置。

加强审查审核 防止滥用“AI换装”

《人工智能生成合成内容标识办法》明确，服务提供者提供生成合成内容下载、复制、导出等功能时，应当确保文件中含有满足要求的显式标识；任何组织和个人不得恶意删除、篡改、伪造、隐匿办法规定的生成合成内容标识。

国家网信办等十部门今年印发的《互联网军事信息传播管理办法》规定，互联网军事信息服务提供者和用户使用深度合成、生成式人工智能等新技术新应用，不得损害人民军队形象。

汪高峰等法律人士建议，AI开发者在算法设计中应加强合规性审查，对警察和军队标识等敏感信息内容的使用，应在相关部门指导下，严格把关审核。平台方应该严格落实《人工智能生成合成内容标识办法》，对“AI换装”类产品添加明显标识，并建立审核机制，对违规内容及时下架封禁。

丁宏建议，加快相关立法进程，强化刑事司法衔接。相关部门尽快明确AI涉军涉警等图像的使用边界、责任划分及法律后果，特别是对刻意丑化军人警察形象、借机实施招摇撞骗等行为，要依法依规严肃处理，形成法律震慑；对可能影响国家安全、造成社会危害的行为，追究AI工具开发者和内容平台的连带责任。

马国建呼吁，提高公众对军人、警察等职业形象重要性的认识，普及相关知识，引导公众自觉抵制、检举错误内容、违规应用。加强AI生成合成内容标识方法的宣传推广，降低公众被欺骗、误导的风险。 据新华社

责编：狄媚婷 设计：任宇轩 校对：李彦宏 赵海燕