

“一秒生成制服照”？ AI岂能如此换装



「AI换装」诈骗
新华社发 朱慧卿作

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。

相关专家在观看部分AI换装视频后指出，不少换装的军人形象并不符合《中国人民解放军内务条令》规定的着装规范，有的混淆军种制式，有的使用假勋章，有的拼凑不同国家军服元素。

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察照片、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。

今年7月，江苏常州的唐大妈遭遇一场精心设计的骗局：诈骗分子通过AI视频与受害人接触，视频中，对方身着带有公安标志的制服，以“涉案”为由恐吓老人缴纳高额“保证金”。好在警方及时预警并上门劝阻，避免了老人的财产损失。

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。

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。

新华社南京10月9日电