

热点解读

今年3月,我国国家安全部发文,揭露境外间谍大肆捏造虚假言论、伪造公务人员不当视频、炮制虚假政策画面等违法犯罪行为。

这则新闻的背后,指向人工智能时代背景下——一项高速发展的技术——深度伪造技术。

在去年热映的电影《捕风追影》中,由演员梁家辉

等饰演的反派“影子”团伙,正是利用深度伪造技术伪造监控影像,误导警方“天眼”系统,完成高科技犯罪。

这让人们不禁思考,当深度伪造技术“以假乱真”,当一段伪造视频足以扰乱人们的思想认知时,我们该如何面对? 又该如何防范其带来的危害? 请看本期关注。

深度伪造技术正在给人工智能时代带来新的挑战——

警惕“数智易容术”

■钟晓东



深度伪造技术检测系统对人脸、语音等进行综合分析示意图。

一张假脸背后的技术链条

深度伪造,英文为 Deepfake,由“深度学习”(Deep Learning)和“伪造”(Fake)这两个词合成而来。顾名思义,它是利用深度学习等算法框架,对图像、视频、音频和文本等内容进行高度逼真伪造的技术。

通俗地说,深度伪造技术就像“数智易容术”——它能让张三的脸出现在李四身上,也能让一个人说出他从未说过的话,甚至可以凭空捏造出一个现实中并不存在的“人”。

那么,这种“易容术”是怎样炼成的? 从本质上讲,深度伪造技术是人工智能通过自我对抗实现“以假乱真”的训练过程。其关键技术引擎,是一种名为“生成对抗网络”的神经网络架构。这种网络架构包含生成器与鉴别器两大组件。

其中,生成器负责生成逼真的伪造内容,鉴别器则致力于准确识别内容的真实性。二者在同步训练中持续博弈——生成器不断优化生成策略以迷惑鉴别器,鉴别器亦持续提升鉴别能力以识破生成器的新手段。在这往复对抗的过程中,两者实现共同进化。经过反复迭代,当鉴别器也无法分辨生成器生成的内容时,深度伪造技术便成功生成了人眼与算法都难以识别的产品。

根据伪造对象不同,深度伪造技术主要分为以下几类。

人脸伪造。这无疑是目前最成熟且应用最广的伪造形式。它包括换脸、表情操控以及人脸生成。目前,人脸伪造技术已发展到连专业人士也难以凭肉眼识破的程度。

语音伪造。基于语音克隆技术,深度伪造技术仅需采集目标人物数秒的语音样本,便能习得目标人物的音色、语调、语速乃至口头禅,进而合成一段足以乱真的“本人语音”。更令人瞠目的是,一些开源工具已将此过程简化:只需上传一段录音、输入一段文字,即可一键生成伪造语音。

视频伪造。这种伪造形式融合了人脸伪造与语音伪造,并结合了全身动作迁移与口型同步等技术。在一段伪造视频中,伪造人物能做出与语音内容高度吻合的口型动作与肢体语言,使整段视频看上去流畅自然、真假难辨。

当人脸、语音与视频伪造技术叠加使用,不法分子便能捏造出一个完整的虚拟人物——“他”拥有面容、声音、表情与动作,甚至可以在视频会议中与真人实时互动。

值得人们警惕的是,目前深度伪造技术的门槛正在降低。以往,制作一段逼真的换脸视频需要专业团队、海量数据与高性能计算设备提供支撑;如今,随着开源工具的普及与算力成本的降低,即便是普通用户,仅需一部智能手机、一张照片和一款免费软件,便能在几分钟内生成一段换脸视频。有记者调查发现,各大电商平台上的AI换脸软件安装包售价低至9.9元,服务涵盖从“活体认证”到“实时换脸”的全套流程。这意味着,深度伪造技术的威胁来源,已不再局限于国家层级的精密策划,还可能是任何一个掌握基本技术的个体。

动摇了“眼见为实”的信任准则

深度伪造技术一旦被恶意使用,其产生的危害或将迅速扩散至军事安全、政治稳定等诸多领域。

战场之上,一段假冒“己方指挥官”发布的紧急下令撤退音频通过通信网络传播,音频中人物的声音、语气乃至口头禅都与真实指挥官毫无二致。士兵在精神高度紧张的情况下很难去及时核实信息,一旦执行虚假指令,这将至少带来两重隐患。

其一,引发指挥混乱与决策失误。在高度信息化的战场上,指令传递日益依赖数智通信手段,这恰恰为深度伪造技术提供了可乘之机。通过伪造指挥员的音视频下达虚假命令,这极易引发战场指挥混乱与决策失误。

其二,威胁作战决策链条。战场上,如果不法分子借助深度伪造技术伪造卫星侦察图像、战场态势图或敌方调动信息,就会严重干扰指挥员对情报的分析与作战决策。未来战场上,准确的情报是制胜的关键。一旦情报源被深度伪造技术污染,整个作战决策链条都将面临风险。

2025年8月,一段伪造政治公众人物的合成视频在社交平台流传。视频中,伪造人物的语气、神态、表情等足以乱真。

这种行为已不仅是博取眼球的闹剧。试想,若某国利用深度伪造技术制

作他国领导人发表激烈挑衅言论的视频,并抢先于辟谣新闻大肆传播,很可能迅速点燃民族情绪,激化地区矛盾。即便事后视频被证伪,裂痕也已造成,外交修复成本远高于造假的代价。自2025年以来,美、俄等国已加速认知战兵器迭代与理论革新,深度伪造技术正被系统性地纳入其认知战工具箱。

还有的画面,可能出现在社会中每个普通人身上。

如今,在社会安全领域,深度伪造技术正致使电信诈骗“升级换代”。传统电信诈骗中,骗子进行冒充时,仅能模仿人物的声音,较易被识破。而深度伪造技术的出现,使不法分子能借助实时人工智能换脸软件进行视频通话。当受害者在屏幕上看到“亲友”或“领导”熟悉的面容时,心理防线往往会在瞬间崩塌。2026年初,我国最高人民法院披露,利用AI换脸软件等实施的智能化诈骗案件呈高发、多发趋势。

深度伪造技术的危害在于,它从根本上动摇了“眼见为实”这一基本信任准则。当视频可伪造、声音可合成、图像可捏造,人们赖以判断真假的感官经验便不再可靠,整个社会的信息信任体系都将将面临重构的严峻挑战。

撕开“数智面具”的多重手段

2025年9月,湖北武汉网警成功破获湖北省首例利用深度伪造技术,非法侵入企业计算机信息系统的案件。

犯罪嫌疑人通过AI换脸,篡改企业

法定代表人信息,进而实施非法活动。不过,该犯罪嫌疑人被技术手段精准锁定,警察一举将其抓获。

该案例表明,深度伪造技术虽给安全防护带来严峻挑战,却并非无懈可击。想破解这类“数智易容术”,需要从技术反制、制度规范、法律保障等多方面协同发力,共同构筑起一道立体的安全防护墙。

技术反制是根本。以技术对技术,是破解深度伪造技术最直接有效的路径。目前,深度伪造检测识别技术正在快速发展。中国移动公司自主研发的AI换脸鉴伪核心技术,可针对伪造图像的局部模糊失真、边缘锐化、通道分布异常等特征进行鉴别,实时鉴伪准确率超95%。在国际上,美国国防部高级研究计划局的“语义取证”计划已实现对AI生成内容的检测、归因与特征分析,相关工具正向军方移交。韩国研发的深度伪造检测模型已在其2026年地方选举中投入使用;下一步,韩国还计划加快推动该模型在军事通信、情报分析、舆情监控等关键场景的部署应用。

制度规范是关键。技术或许能辨别“真假”,却难以界定“责任”。2025年9月,我国《人工智能生成合成内容标识办法》正式实施,办法明确规定,AI生成的内容中必须嵌入隐式标识,传播平台需核验标识并向用户醒目提示。2025年3月,西班牙全面落地《人工智能法案》,要求对深度伪造内容必须进行强制标注。

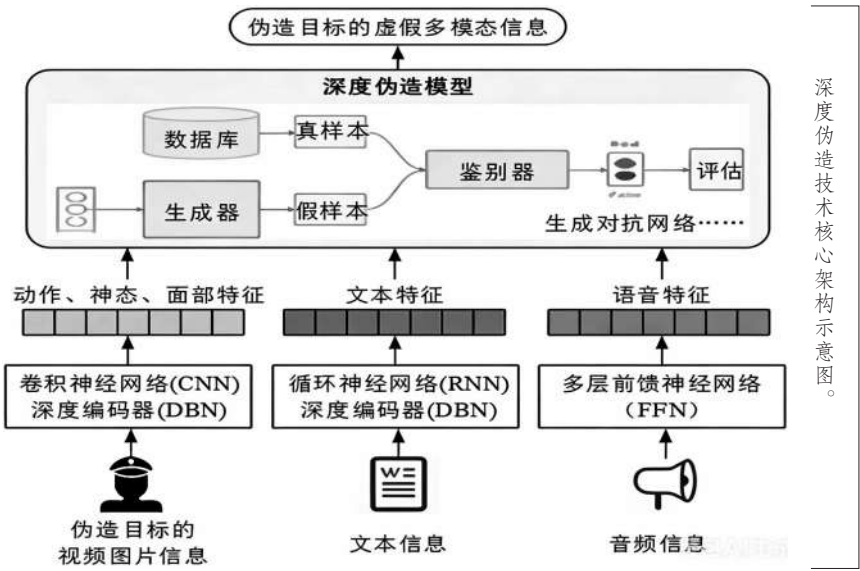
法律保障是底线。恶意制作、传播深度伪造信息,尤其是将伪造内容用于军事欺骗、政治抹黑、金融诈骗等行为的,必须依法予以严厉打击。在我国,依据《刑法》《网络安全法》《个人信息保护法》等多部法律,利用深度伪造技术实施诈骗、诽谤、散布谣言等行为的,将被追究刑事责任。在美国,已有超过20个州通过专门立法,将恶意制作、传播深度伪造内容的行为列为刑事犯罪。

此外,针对前文提到的战场上可能出现的“深度伪造画面”,军队内部也需要构建一整套完善的涉密信息、指挥指令与宣传内容的生产、审核及发布体系。例如,对于需要通过通信网络传达的关键指令,我们要同时辅以加密认证、双人核验等多重保障手段,从流程层面彻底封堵可能出现的漏洞;对于扑朔迷离的战场信息,我们必须设立应对深度伪造内容的快速响应与辟谣机制,以大幅压缩可能出现的虚假信息的传播窗口期。

深度伪造技术的出现提醒我们,在人工智能技术高速发展的今天,“眼见为实”已未必是可靠的判断准则。而对于军人而言,战场信息的真假之辨,事关战局胜负和官兵生死。认清深度伪造技术的本质与威胁,掌握识别与防范这一技术的有效手段,是未来智能化战场对军人提出的新要求。

不过,技术的迷雾再厚,也遮不住明亮的眼睛;伪造的面具再逼真,也瞒不过有准备的头脑。矛与盾的较量不会停止,但只要我们时刻保持清醒、持续筑牢防线,就能在未来战场上,始终立于不败之地。

本文图片由作者提供



新成果速递

最近,一则新闻引发人们关注:人形机器人有“身份证”啦。

5月22日,我国首个人形机器人全生命周期管理服务平台及配套标准《人形机器人全生命周期管理规范》正式发布。自此,每台人形机器人自“出生”起即配发全球唯一的编码。这串编码由29位字符组成,记录了人形机器人从制造、使用、维护到回收的完整轨迹。

这串编码好比我们使用的身份证,根据机器人身上的编码,我们就能知道它的“底细”:开头的2位是“国家码”,标识机器人的国籍与产地;紧接着的4位“企业码”代表机器人的制造商;中间的6位“产品型号码”记录机器人的功能配置;最后的17位“序列码”实现对机器人个体的精准追踪。

给机器人办“身份证”,源于我国机器人产业爆发式增长带来的问题现状:各厂家对机器人的编码规则不统一,机器人进入公共场合,若发生故障或失控,责任难以界定……如今,有了这套统一规范的编码,一台人形机器人从出厂到退役,每一步都被记录在案。

此外,中国电子技术标准化研究院副院长于秀明强调,编码将强制贯穿机器人研发、生产、准入、销售、使用、维护、报废、回收共8个环节,真正做到人形机器人“不合格不出厂,无编码不流通”。与此同时,人形机器人更换核心部件需经过用户授权并重新绑定编码;远程维修需确保数据全程加密传输。人形机器人退役时,存储在机器人中的隐私数据将被彻底清空,机体被物理销毁,从源头杜绝翻新后的旧机流入市场。

给人形机器人办“身份证”,是为

人形机器人这个快速发展的行业建立一套规范、安全、可信的管理体系。依托这套编码体系,每台人形机器人都

人形机器人有『身份证』啦

■陈菲莹

将拥有一份不可篡改的全生命周期溯源档案,确保其行为可追溯、责任可落实。工信部表示,后续将推进人形机器人进行实景实战演练,让人形机器人“身份证”在真实场景中真正好用、管用。



在北京人形机器人创新中心具身智能机器人数据与训练基地,工作人员对机器人的挂衣服动作采集数据。

新华社发

美军加快推进新一代军用气象卫星计划

■史文丽

他山之石

环境数据是未来战场上指挥员决策时重要的参考依据,而军用气象卫星则是获取环境数据的重要方式。

目前,美军正在加快推进由大空

军主导的新一代军用气象卫星计划,逐步淘汰“国防气象卫星计划”。据悉,新计划放弃“单平台集成多载荷”的复杂设计,转而采用分布架构、军民互补、商用备份的思路,以搭载分布式有效载荷的小型卫星星座为主。新计划重点关注以下几个方面。

一是将“国防气象卫星计划”整合至“后续—微波气象卫星”和“光电/红外气象卫星”这两个项目中。

“后续—微波气象卫星”为太阳同步轨道卫星,用于识别热带风暴和强风,测量积雪和土壤深度以及提供覆盖全球的气象监测服务。据悉,第一颗“后续—微波气象卫星”已于2024年4月发射升空,第二颗计划于

2028年前发射。“光电/红外气象卫星”则搭载光电红外传感器,用以提供云层覆盖图像和天气预报,计划分别于2026年、2028年发射。

二是与美国国家海洋和大气管理局(NOAA)紧密协作,彼此共享、验证和校准气象卫星数据,用以支撑全球气象监测和战场指挥员决策。

三是探索累积商业卫星数据,提升军用气象卫星获取数据的准确性。

目前,美军正在围绕低成本有效载荷、传感器、大气仪器、数据处理系统等升级改造,最终目标是提升未来战场上军用气象卫星获取环境数据的韧性、响应性和准确性,进而辅助指挥员进行科学决策。

据悉,早在2025年10月,美国大空军曾依托小企业创新研究计划与小型卫星制造商Muon Space公司签订了一份价值4460万美元的合同,改造并发射3颗气象卫星,旨在将成熟的商业技术快速应用于军用领域。