『魔改』陷阱 谨防深度伪造

生成式人工智能技术的突破性进展，正推动AI视频制作加速普及，在提升创作效率、活化历史记忆等方面展现出巨大潜能，成为数字时代的内容生产利器。但技术若被恶意用于金融欺诈、政治渗透、谣言制造、间谍窃密等非法活动，将侵害公民合法权益，甚至扰乱社会秩序、危害国家安全。

伪造权威，动摇公信力

境外间谍情报机关、各种敌对势力可能利用深度伪造技术，捏造虚假言论、伪造公务人员不当视频、炮制虚假政策画面，以此制造社会恐慌、撕裂舆论、抹黑国家形象，冲击政治安全与制度安全。

精准诈骗，侵害公私财产

不法分子可能利用深度伪造克隆亲友、客服等声音和面容，实施冒充转账、虚假投资、仿冒官方渠道诈骗等非法活动。更有甚者，企图通过伪造企业公告、专家言论，引发市场波动。

信息泄露，危害数据安全

不法分子可能利用深度伪造人脸、声纹等生物特征，突破身份认证、权限校验等核心数据防护机制，造成账号被盗、后台入侵、敏感数据批量泄漏，甚至引发关键信息基础设施安全系统失控等重大安全事件，对数据安全造成危害。

国家安全机关提示

《互联网信息服务深度合成管理规定》明确，任何组织和个人不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等活动。具有舆论属性、社会动员能力的深度合成服务，必须依法备案、内容审核、实名管理、合成标识，禁止删除篡改标识；严禁未经授权使用人脸、人声等生物识别信息进行恶意编辑。

技术本身并没有善恶之分，关键在于如何使用。面对深伪技术，每一位公民都应自觉增强安全意识、提升辨别能力、遵守法律法规，以实际行动维护国家安全和网络清朗。

提高辨别能力。

理性看待网络信息，不盲目轻信不合常理的音视频、图片内容，遇到可疑信息要优先通过官方渠道核实真伪。

自觉遵守法律。

合理合法使用各类AI生成、图像编辑、音视频处理工具，不参与、不支持制作、传播有害虚假信息。

维护网络文明。

每一位公民应自觉维护清朗的环境，抵制互联网上各类有害内容，不随意转发未经证实的信息，如发现AI视频平台或作品存在可能危害国家安全的问题线索，可通过12339国家安全机关举报受理电话、网络举报受理平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

那些悄悄“上位”的链接

我们每天都在使用搜索引擎查找信息、获取资源，它早已是数字生活的必备工具。正规搜索引擎持续优化升级，以强大算法与安全能力拦截成千上万的恶意攻击，全方位保障用户的使用安全。但仍有不法分子不遗余力地钻空子，一步一步诱导用户走入他们设下的陷阱。国家安全机关工作发现，有不法分子通过给搜索结果添加恶意模块等方式，大肆开展站点权限获取、敏感文件资料窃取等非法活动，威胁国家安全。

手段揭秘：投毒“黑招”

所谓搜索“投毒”，就是不法分子利用黑帽SEO技术，通过违规手段恶意操纵搜索引擎排名，把虚假信息、木马链接、诈骗页面、有害内容推到搜索结果靠前位置，让普通网民在不知情的情况下点击有害网站，从而实现引流、诈骗、窃密、传播不良信息等目的。他们的作案流程，就好比“地下流水线”。第一步，找“被忽视的网站”。一些单位的网站，如长期不更新、未及时修补漏洞、密码设置简单，就可能成为攻击目标。第二步，入侵并植入“伪装页面”。攻击者不会更改首页显眼位置，而是在后台悄悄添加一些隐藏页面，这些页面看似是普通资讯，实际塞满了虚假关键词、诱导链接，专门欺骗用户。第三步，用技术手段把假页面“抬上排名”。通过批量堆砌关键词、做假外链、刷流量等方式，让搜索引擎把这些恶意页面当成“相关内容”，推到搜索结果的前列，甚至出现在官方信息旁边。第四步，用户一点击，就可能“中招”。网民搜索相关内容时，看到域名像“官方网站”就容易产生信任，一旦点击进去就可能跳转至诈骗页面、木马下载页，甚至被诱导泄露个人信息。攻击者会反复循环这个流程，不断切换网站、更替关键词，致使危害持续扩散。

真实案例：指尖“陷阱”

点击有问题的搜索结果看似是个人中招，实则可能引发数字供应链安全的系统性风险，一旦关键岗位人员，如信息系统运维人员、财务人员、研发工程师等不慎点击“有毒”链接安装了恶意软件，攻击者即可获得内网立足点，进而实施窃取敏感资料数据、破坏关键信息基础设施等活动，给国家安全带来威胁。国家安全机关工作发现，某企业员工通过搜索引擎搜索某类常用运维软件时，不慎进入了境外黑客组织“精心制作”的虚假页面，下载并运行了带有恶意程序的软件，导致计算机中敏感数据被窃取。经查，该企业承担了多家重要单位信息系统和网站的建设运维工作，境外黑客组织非法获取了网站登录凭证等信息，并尝试非法访问我重要单位信息系统和网站后台，企图窃取我内部敏感资料与数据。所幸，国家安全机关及时发现并消除隐患。

（均转自国家安全部微信公号）

有时候不能“打开天窗说亮话”

一场关乎决策的涉密会议正在室内紧张进行，桌上的文件印着“机密”字样，与会者的发言内容敏感而重要。然而窗外有一双窥探的眼睛，将一切尽收眼底，甚至用长焦镜头拍下了桌上的文件……这并非危言耸听的谍战片情节，而是现实生活中真实存在的失泄密风险——一道没有拉上的窗帘。

拉上窗帘，这个简单的动作究竟是为了防御什么呢？它防的绝不是无心之人的随意一瞥，而是越来越先进的远程无接触窃密技术手段。今天，为大家揭秘几种常见的窃密技术手段与防护方法，希望大家提高警惕，筑牢安全防线。

窃密技术手段知多少

光学成像与远距离摄录。现代光学设备早已突破肉眼可视的局限。高分辨率长焦镜头、红外成像仪甚至智能手机配合AI增强处理，可在数百米外清晰摄录会议幻灯片、纸质文件或白板内容。若未拉窗帘，会场内容极易暴露于外部开阔视野中，形成“天然直播”。

激光侦听与振动还原。若会议室内装有玻璃窗，各类声源的声波会引起玻璃轻微振动。境外间谍情报机关可使用激光侦听设备向窗户发射不可见激光，通过接收反射信号并分析振动模式，完整还原室内语音内容。此类技术无需侵入物理空间，即可实现隔空窃听。

环境反射与信息残留。会议室的白板、屏幕甚至参会者眼镜、手表等均可能成为潜在反射源。窃密者可在附近高楼或相邻建筑上，通过高倍望远镜实时捕捉这些反射画面，结合图像处理技术重构会议内容。尤其在夜间，室内明亮而室外昏暗，窗户更如透明屏幕，极易被远端设备记录。

多角度杜绝失泄密风险

强化物理防护。涉密会议室的选址应当科学合理，优先选择建筑内侧的无外窗或具备遮挡条件的房间。如果必须使用有窗房间，要配备完全遮光的窗帘、防窥膜或智能调光玻璃。涉密会议召开前应按流程检查物理防护设施使用情况，并对会议室周边环境进行定期巡查，排查可疑设备与人员。

加强技术防范。重要涉密会议应在符合国家标准的电磁屏蔽会议室举行，以阻断无线信号传输。同时可在窗户附近安装语音干扰装置防止窃听，必要时使用激光探测器检测室内是否存在激光探测动作。

严格会场管理。建立完善的涉密会议管理制度，会前须开展针对性的保密教育，明确会议密级和保密要求；会中安排专人负责安全巡查，确保各项防护措施落实到位；会后要进行彻底的清场检查，确保涉密文件不遗漏、不外带，并提醒与会人员不得在非保密场所讨论涉密内容。

国家安全机关提示

涉密会场，堪称国家秘密安全防线的前沿阵地，任何细节疏忽都可能导致阵地失守。有关单位和公民应自觉提高防范意识，履行保密安全义务，做好日常防护。如发现涉密会议内容被窃取等可疑线索，可通过12339国家安全机关举报受理电话、网络举报受理平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

责任编辑/王睿卿 E-mail:fzbfyzk@126.com