AI智能体“龙虾”为何引发广泛警惕

□新华社记者 冯玉婧

今年年初以来，一款俗称“龙虾”的人工智能（AI）智能体工具“开放之爪”（OpenClaw）凭借其自主执行复杂任务、可扩展技能包等强大能力，在开源社区迅速崛起。但爆火之后，“开放之爪”接连被曝出存在多重安全隐患。

目前，多国监管机构和科技企业已陆续发布针对“开放之爪”的使用指南和规范。4月1日，中国国家知识产权局发布风险提示说，“开放之爪”等智能体工具被曝光默认安全配置脆弱，易引发严重安全风险。与此同时，使用此类智能体撰写专利申请文件，也可能诱发多重风险。

新闻分析

安全漏洞频发

“开放之爪”由奥地利软件工程师彼得·施泰因贝格尔开发，是一款开源AI智能体软件。该智能体采用层级化架构，将社交即时通讯软件与自动化智能体深度耦合，同时借助插件系统扩展各种工具能力。这种分层架构虽赋予了“开放之爪”灵活性与可扩展性，但也带来了多维度的安全风险。

1月下旬，开源平台GitHub上发布的一项安全审计报告显示，“开放之爪”存在512项安全漏洞，其中有8项被归类为“严重”，涵盖了身份验证、机密管理等领域。

2月下旬，国际网络安全机构“绿洲安全”研究人员发布报告说，“开放之爪”核心系统中存在一个名为“ClawJacked”的重大安全漏洞，攻击者可能通过恶意网页接管该智能体，从而获取设备权限和访问系统数据。“开放之爪”团队将漏洞定级为“高度危险”，并在24小时内发布了修复版本。

3月30日，中国360数字安全集团在官方微信公众号上发文说，在“开放之爪”平台中发现一处高危漏洞，影响范围覆盖全球50多个国家和地区。

广泛的攻击风险

美国微软公司安全团队发布的风险报告显示，使用“开放之爪”可能面临两类攻击风险：恶意技能插件和间接提示词注入。

“开放之爪”的执行能力依赖于社区平台提供的技能插件。绿盟科技公司近期发布的安全报告指出，如果缺乏严格的代码审计和签名校验，攻击者可通过发布包含恶意提示词和代码的恶意技能插件实现“代码投毒”。用户可能只因一次点击就加载了此类插件，攻击者可在受害者系统中获得持久驻留能力。而攻击者上传自定义技能插件的门槛非常低，只需要注册一个非实名的GitHub账号即可。

据美国派拓网络公司2月发布的数据，研究人员已在相关平台上发现超过800个针对“开放之爪”的恶意技能插件。

提示词注入是一种针对大语言模型的攻击技术，分为直接注入（攻击者直接输入恶意指令）和间接注入（通过网页、文档等外部数据源实现攻击）两种方式。

美国“众击”网络安全服务公司近期在官网发文说，提示词注入的首要威胁是敏感数据泄露，考虑到“开放之爪”对敏感文件与系统的高访问权限，这一风险尤为严重。间接注入则会进一步放大风险，因为攻击者无需直接与“开放之爪”交互，只需污染其读取的数据，恶意指令即可悄悄进入软件决策流程。

多国机构及企业发布使用规范

对于“开放之爪”是否适合在企业中部署应用，“众击”公司的文章指出，若员工在企业设备上部署“开放之爪”或将其接入企业系统，且配置不当、缺乏安全保护，它就可能成为系统“后门”，执行攻击者的指令。

业内人士建议，个人或企业用户不要在常规办公与涉密设备上运行“开放之爪”，如需部署须采取权限治理、沙箱机制、持续监控与全周期安全防护等严格管控措施。

据媒体报道，出于风险管控的考虑，美国元宇宙平台公司、韩国多音通讯公司等多国科技企业已禁止员工在办公设备上使用“开放之爪”。与此同时，多国监管机构也发布了关于使用“开放之爪”的安全指南。

荷兰数据保护局2月发布公报，建议用户和组织不要在存有敏感或机密数据（如访问码、财务行政资料、员工数据、私人文档或身份证明文件）的系统上使用“开放之爪”及类似AI智能体；建议谨慎对待外部插件，实施严格的访问控制，在存在泄露风险时及时更新登录信息。该监管机构还呼吁将“开放之爪”等AI智能体纳入欧盟《人工智能法》的管辖范围。

3月22日，中国国家互联网应急中心等发布了“开放之爪”安全使用实践指南。此前，工业和信息化部网络安全威胁和漏洞信息共享平台组织相关机构研提了“六要六不要”建议，以防范“开放之爪”开源智能体安全风险。（新华社北京4月1日电）

三问太原高层建筑火灾

□新华社记者 马晓媛 王皓

3月28日晚，位于山西省太原市中心城区的一栋高层建筑发生火灾，目前已致3人遇难，23人受伤，其中9人重伤。这起火灾因地处闹市、火势较大，引发关注。

建筑因何起火？为何蔓延迅速？暴露出哪些消防隐患？“新华视点”记者进行了采访。

商业综合体为何暗藏隐患？

记者了解到，起火建筑是一座功能用途较多的商业综合楼，主楼为地上16层、地下2层，主楼北侧配建裙楼，共4层，主楼与裙楼相连通。楼内8层以上为卡萨精品酒店，其他楼层有月子会所、医疗美容机构、律师事务所、KTV、网咖等，裙楼底商则以餐饮商户为主。

在事发现场，记者看到，起火建筑东侧地面底商过火严重，主营烧烤、炒菜的两家餐饮商铺门脸、招牌已烧毁，楼体东侧从底商到16层楼顶被大面积熏黑，外立面装饰材料几乎全部脱落，露出内部墙体。

有消防人士指出，这样的综合楼业态多样、人员密集，且餐饮场所明火多、用电负荷大，存在较大隐患。

特殊的建筑结构又额外增加了风险。记者注意到，裙楼的主体与主楼相连，在东侧延伸出约7米的宽度，形成了一个由主楼东侧墙面、裙楼南侧墙面构成的夹角；在这个狭小的空间内，主楼底商小餐馆向外搭建出一小块门脸，门脸上方则是多家餐饮商户的外置烟道，再往上则是高层墙面，这些都为火势迅速蔓延提供了条件。

有消防人士表示，着火区域正好是主楼和裙楼连接处，最初起火的主楼底商小餐馆面积较小。如果是正常的商业综合体，按规定必须有双疏散通道；如果没有双疏散通道，一旦大门被火封住，人员难以及时逃出。需要关注楼的功能是否发生改变、是否符合消防要求。

记者多方了解到，遇难与受伤人员主要来自主楼东侧底商小餐馆。

相关人士建议，加大对商业综合体、高层建筑等人员密集场所的消防隐患排查力度，对建筑功能改变、消防设施缺失、消防通道堵塞、违章搭建等行为依法严处。

油烟管道为何成为易忽视的风险？

“最先发现着火的地方是那家大龙烧烤炒菜的上方，那儿有几家饭店的油烟管道。”距离起火点几十米外的某小区居民说，他看到火苗从主楼东侧底商餐馆房顶窜出，“没几分钟，火就窜到了高层，速度快得吓人。”多位现场目击者和现场视频也印证了这一细节。

相关人士表示，此次事故也暴露出当前餐饮商户油烟管道存在消防隐患。

一位消防救援人士告诉记者，餐饮商户使用的油烟管道需要定期清洗。如果没有及时清洗，烟道内壁会积存大量油垢；一旦遇到明火，如厨师炒菜时的火苗被卷入，就容易引发火情，且燃烧初期不易被发现，等肉眼可见明火时，火势往往已充满整个烟道，易错过最佳灭火时机。

记者梳理发现，近年来餐饮场所烟道火灾频频发生。2025年4月，浙江温岭市松门镇一美食城发生火灾，起火部位为沿街商铺厨房油烟管道；2025年3月8日，吉林长春二道区亚泰新动力商城一餐馆后厨烟道起火；2024年10月，云南昆明一家烧烤店因油锅起火，火苗被吸入排烟管道引燃管内油脂，引发火灾；2024年2月，北京市朝阳区一饭店后厨烟道起火，两名员工被行拘10日。

与此同时，烟道监管方面缺乏硬约束。多位消防从业人士表示，目前对餐饮场所的日常消防检查主要聚焦于喷淋系统、灭火器、应急照明等消防设施和消防通道畅通情况。对烟道的监管，仅是要求经营者登记清理记录。“烟道清理行为本身，并未纳入现行消防法的强制监管范畴，没有明确的处罚依据。日常检查中，我们只能对经营者进行风险提示，这就容易形成监管盲区。”

记者了解到，按照人员密集场所消防安全管理规定，餐饮场所油烟管道应至少每季度清洗一次，一些地方消防条例和餐饮单位安全生产规定也对餐饮经营单位油烟管道清洗作出规定，但这些要求很多餐饮商户并未严格落实。有餐饮从业者透露，一些中小餐饮商户为压缩经营成本，油烟管道往往长期不清理，部分商户甚至开业数年从未彻底清洗过烟道。

高层外墙为何成火势蔓延的“高速路”？

多位现场目击者反映，现场火势蔓延“特别迅速”，且不断有大片燃烧物从主楼东侧外立面掉落。住在附近的居民刘先生说：“我出去看的时候，火已经裹着整个楼的东侧往上窜，外墙的材料一片一片带着火往下掉，根本不敢靠近。”

一位消防救援专家表示，高层建筑的外立面如果使用的是易燃、可燃材料，一旦发生火情，火势就会沿外墙迅速向上蔓延，“相当于给火势铺了一条高速路”。

有消防业内人士分析，建筑外立面材料如果未达到国家规范要求的阻燃标准，燃烧时就会伴随材料脱落加速火势扩散。“与室内独立单元火灾相比，外墙火灾因保温材料连续分布易形成‘烟囱效应’，火势蔓延速度更快，且燃烧产物（如烟雾）会迅速充满楼道，使人员疏散时间大幅压缩。”

根据2021年8月1日起施行的《高层民用建筑消防安全管理规定》，禁止使用易燃、可燃材料作为高层民用建筑外墙外保温材料。国家标准《建筑防火通用规范》（GB55037-2022）也对建筑外墙保温材料的燃烧性能作出详细规定，明确人员密集场所的外墙外保温材料的燃烧性能应为A级（不燃材料）。

卡萨精品酒店订房页面显示，该酒店于2008年11月开业，2018年2月进行装修。附近一名商户回忆，2018年应该是酒店内部装修，不涉及外立面，现有外立面的施工时间可能更早。

有业内人士表示，建筑外墙防火相关规范历经多轮修改完善，事故所涉建筑主体建设和后续装修改造过程中，是否严格执行彼时相关消防安全规范，还需要进行深入核查。

受访者建议，针对建筑外墙材料监管，进一步明确设计、施工、监理、日常运维等全流程的责任主体，厘清住建、消防等部门的监管职责，防止出现“标准明确、验收缺位”问题。对新建、改建、扩建的人员密集场所建筑，严格执行阻燃保温材料的强制标准；对既有高层建筑开展安全排查，尤其要聚焦核心商圈高密度老旧建筑，消除存量安全隐患。

（新华社太原3月31日电）

中东战事如何影响俄乌“棋局”

□新华社记者 黄河

持续蔓延的中东战火，正给俄乌局势带来外溢影响。近期，俄罗斯和乌克兰分别与伊朗、海湾国家等中东地区国家频繁互动。俄罗斯暗中“布局”，而乌克兰高调“刷存在”。

分析人士认为，美以伊战事与俄乌局势正呈现深度交织、相互牵制的态势，前者或使后者向着长期化、复杂化的方向演变。

国际观察

俄罗斯双线“布局”

美以伊战事爆发以来，俄罗斯在中东地区采取“巩固俄伊关系、平衡海湾关系”的双线策略，在明确支持伊朗的同时，也与海湾国家展开协调。

外交层面，俄罗斯多次声援伊朗。战事爆发以来，俄总统普京称俄是“伊朗忠实可靠的伙伴”，并两次与伊朗总统佩泽希齐扬通话。俄外交部3月以来就伊朗局势已发表5次声明，谴责美以袭击伊朗，呼吁各方立即停火。此外，俄方还向伊朗提供大量药品等人道主义援助。

军事层面，俄外长拉夫罗夫近日表示，俄伊已签署军事技术合作协议，俄方向伊朗提供“某些类型的军事装备”。有媒体报道说，俄在战事开始前后向伊朗提供了攻击直升机、便携式防空导弹等武器装备，但这些消息未得到俄官方证实。

针对被战火波及的海湾国家，俄罗斯也积极展开协调，表态支持其维护自身安全利益。3月以来，拉夫罗夫同阿联酋、沙特阿拉伯、卡塔尔、阿曼等国官员沟通，表示支持海湾国家主权和安全关切，谴责美国将其海湾盟友置于险境。

有分析指出，美以伊战事牵制了美国在俄乌问题上的战略精力，压缩其相关资源投入，而俄罗斯对伊朗的支持，也有助于缓解来自美方的压力。对海湾国家，俄罗斯也需维护与它们在经贸、能源等领域的合作关系，并强化在地区事务和能源议题上的影响力。

乌克兰寻求“破局”

乌克兰近来在中东地区选择“刷存在、求破局”的外交路径。

一方面，乌克兰将反无人机技术作为与地区国家互动的“筹码”。乌总统泽连斯基3月下旬出访地区多国，向沙特、阿联酋、卡塔尔等国“推销”反无人机技术。乌方还向地区国家派出201名反无人机专家，协助相关国家应对伊朗无人机和导弹威胁。

另一方面，乌方还寻求同海湾国家展开长线安全防务合作。泽连斯基3月底表示，乌方已与沙特、阿联酋和卡塔尔达成安全协议。据媒体披露，相关协议包括推进反导和反无人机技术合作以及联合投资等，部分协议为期10年。

乌克兰在中东“刷存在”遭到伊朗方面指责。伊朗驻乌克兰临时代办沙赫里亚尔·阿穆泽加尔说，乌方“打伊朗牌”是为了获得更多资源。伊朗3月28日称摧毁部署在阿联酋迪拜的乌克兰反无人机系统，但乌方称消息不实。

分析人士认为，美以伊战事爆发后，国际舆论尤其是西方媒体对俄乌局势的关注度显著下降。乌克兰试图通过高层活动以及与海湾国家开展防务合作等方式维持国际舆论的关注，并希望通过探索与中东国家的合作，将战场技术与实战经验转化为经济收益和外交支持。

搅动俄乌“棋局”

分析人士指出，美以伊战事正在军事、经济、外交、战略四个维度深刻影响俄乌局势走向。

军事层面，中东战事的持续将直接影响乌克兰防空能力。美制“爱国者”导弹系统是乌防空体系的关键装备，而美国及其中东盟友为拦截伊朗导弹与无人机，已大量消耗该型防空导弹。随着中东战事持续，势必会有更多“爱国者”导弹被调往中东，乌防空力量或出现明显缺口，防空压力陡增。

经济层面，油价走高给俄罗斯带来“喘息空间”。作为全球重要产油国，俄罗斯受益于高油价带来的石油收入增长；美国为平抑油价还主动放宽部分对俄石油出口制裁，给遭受西方制裁多年的俄罗斯难得的喘息机会。与之相对的是，乌克兰的财政赤字或因能源价格攀升而不断扩大。俄乌在经济财政上的此消彼长或将影响战场态势。

外交层面，中东战事分散了国际社会的关注焦点，俄乌和平进程恐进一步陷入停滞。当前，美欧外交重心已转向中东，原定在阿联酋首都阿布扎比举行的新一轮俄乌美三方会谈被无限期推迟。尽管泽连斯基表示已做好在复活节期间停火的准备，但分析人士认为，随着俄乌局势在国际议程中“遇冷”，加之俄方在战场上占优，俄方在谈判中妥协的意愿进一步降低。

此外，美欧分歧加剧，也为俄罗斯在后续战略博弈中创造了有利条件。当前，美国与欧洲盟友在中东战事上分歧严重，使双方本就因军费、关税、格陵兰岛等问题积累的裂痕进一步加深，或将导致美国对欧洲的安全承诺和对乌援助更具不确定性。专家认为，这一局面正是俄方所乐见。（新华社莫斯科4月1日电）

『健康主播』培训乱象：科普如何更『靠谱』

□新华社记者 李恒 杨淑馨 王楚然

“零基础当‘健康主播’，月入过万不是梦”“三天速成，AI赋能轻松变现”……近期，这类主播培训广告语成为一些机构的“吸睛利器”。

随着人们更加重视健康知识，健康科普类账号备受青睐，“健康主播”培训也日趋火爆。然而，一些速成培训暗藏陷阱，侵害群众利益。治理行业乱象、筑牢公众科学防线，科普如何更“靠谱”？

“一场直播可收入1万”？

“‘健康主播’的黄金十年，普通人改命换运的机会”“只要起号成功，一场直播可收入1万”，在社交平台上，此类诱人口号吸引不少求职者的目光。

记者调查发现，“健康主播”被炒作成“零门槛、高收入”的“金饭碗”，针对“健康主播”的速成培训也成为一些机构精心设计的“围猎”骗局。

一些学员缴纳了高额培训费，培训内容却大幅缩水。

记者调查发现，部分培训机构设置从几百元到数万元不等的培训费，承诺“包教包会、对接资源、流量扶持”，但实际培训内容仅限流量话术、吸粉技巧、带货套路，并无健康知识教学。

湖南长沙的肖女士本想通过学习成为一名“健康主播”，却并未学到专业知识。“交完4563元学费，他们发来几个话术模板，再没下文。”

68岁的王女士告诉记者，她花费8039元报名多个课程，想通过学习推广健康知识实现再就业，培训老师却频繁更换，最终“突然消失，发信息不回，课程直接停滞”。

被机构推至“台前”的学员，还有可能面临非法行医的风险。

记者梳理发现，一些参加过“健康主播”培训的账号将仅具“辅助调理”作用的成分，夸大宣传为能“根治疾病”，账号还发布虚假食疗、违规养生手法、错误用药指导等。

业内人士表示，“主播”如若判断病情、分析病因、提出治疗方案、指导用药、替代就医决策，就可能越过科普边界，进入诊疗活动范畴。在主播不具有相应资质情况下，可能构成非法行医。

更有甚者，陷入以培训为名、行传销之实的骗局。

江苏的傅女士在求职平台上寻找“健康主播”工作，却不慎“踩坑”。参加招聘方的免费直播培训后，傅女士被邀请至线下“直播基地”学习。

在对方话术洗脑下，她最终交了2.2万元“会员费”购买对方的保健品。“要求我们先自用、再销售，实际就是为了高价卖产品。”傅女士表示，同期学员中，有人甚至被诱导追加十几万元，用于“自建主播基地”，最终钱也打了水漂。

如何步步“围猎”？

记者调查发现，一些机构利用精密的话术与流程，步步“围猎”求职者：

——免费培训“诱捕”，虚造高薪神话。

“实打实扶持”“全程专业培训”“独家AI赋能”，一些机构在社交平台和招聘软件上投放大量招聘“健康主播”的“电子传单”，声称入职即可获得“专属孵化”，从而实现财富自由。

多名受访者表示，入职的免费培训就是线上的集中“洗脑”。一些机构要求在培训前提交一份“培训申请”，以此营造名额紧缺性。“培训过程中，讲师不断展示所谓成功案例，称普通人转行做‘健康主播’，短时间就能涨粉数万、月入数万。”傅女士告诉记者。

——“打卡”保持黏性，诱导发展下线。

为了保证学员黏性，一些机构会建立培训课程聊天群，要求“打卡式”学习，在群内制造“火爆”氛围。“如果没有分享学习内容会被清退，还会设置线上考核。”有学员表示。

记者在参加一场专注“肠胃健康”的主播培训中发现，培训导师要求主播发展下线，数次提到“没有底薪，全靠提成”，想要高收入就要“拉人建立团队”，“有团队管理奖金”。

——线下分别“逼单”，兜售高价产品。

线上免费培训结束后，一些机构则会邀请学员到线下学习或参会，举起收割“镰刀”。

据傅女士介绍，所谓的线下学习，其实是一对一单独沟通“逼单”。“对方会轮番劝说，我所在批次超过60%的人都交了钱购买产品。”

傅女士注意到，对方提供的产品是公司自有品牌保健品，虽为注册品牌，但售价畸高，一小盒需三四百元。

还有受访者告诉记者，一些线下的健康峰会要求其自费体检，查出“小毛病”后，便要求购买该公司产品进行“调理”，让人陷入“高价囤货”的套路。

让科普更“靠谱”

业内人士指出，彻底斩断灰色产业链，需多方协同、系统治理。

武汉大学法学院副院长武亦文教授建议，对以“培训”为名行诈骗、传销之实的机构，要依法严厉打击，并及时向社会公布典型案例，形成有效震慑。针对跨区域作案特点，可探索建立全国统一的投诉举报平台和协查机制，压缩违法机构的生存空间。

医药行业AI创新联盟秘书长张蕊认为，平台需压实主体责任，加强对招聘广告、培训课程的严格审核与风险提示。

在专家看来，需进一步完善关键词拦截机制，及时清理虚假宣传内容，切断“健康主播”培训乱象传播渠道；对于用户投诉集中的机构账号，及时采取下架、封禁等措施，并向监管部门报告。

受访人士认为，要加快完善“健康主播”职业标准与准入机制。中国健康教育中心科普部主任陈国永建议，对于从事健康类直播人员，可探索实行备案管理或能力认证制度，建立严格的市场准入制度，从源头上提升行业专业化水平。

此外，公众也需提高警惕，增强识别能力。

武亦文建议，求职者要树立理性就业观，在选择培训机构时，核实资质、查看条款。

一旦发现上当，要及时收集证据，保存好培训宣传页面、聊天记录、付款凭证、电子合同等相关材料，并向12315平台、市场监管部门投诉，必要时也可向法院提起民事诉讼，维护自身合法权益。

受访专家表示，大健康产业关乎民生福祉。要形成监管合力，铲除乱象滋生土壤，壮大专业主播队伍，更好传递健康知识、服务社会大众。（新华社北京4月1日电）