2026年3月18日 星期三
责任编辑：王勇 编辑：封荣娟 版式：杜琼
十堰晚报

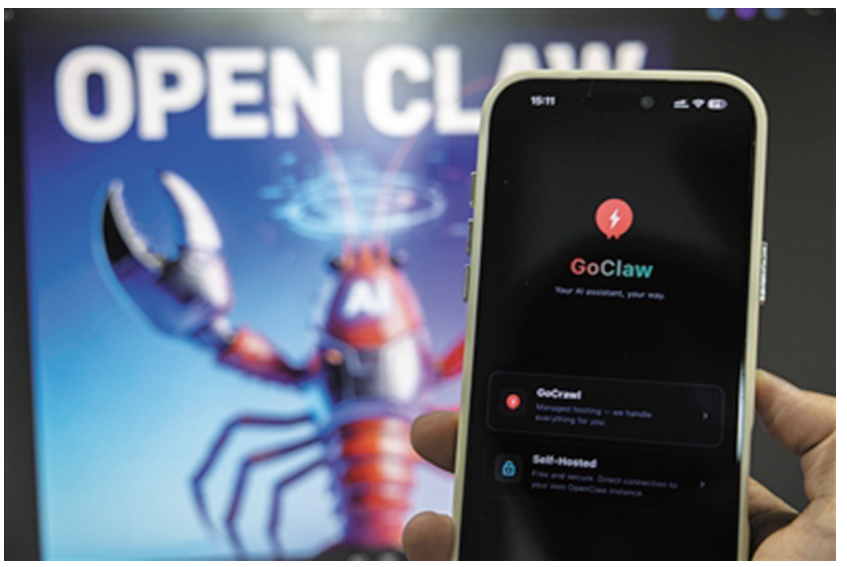
风口之上：“养龙虾”的热闹与隐忧

专家呼吁热潮中需规范引导、重塑业态

■据《经济参考报》

开年以来，人工智能领域刮起了一场破壁跨圈的“养龙虾”热潮。开源智能体OpenClaw，因能协助用户处理文件管理等复杂任务而迅速走红。不过很快，其又暴露出安全边界模糊等致命短板。

受访学者认为，OpenClaw类智能体出现有标志意义，但仍需从严把控安全风险，未雨绸缪引导科技发展向上、向善。



这是开源AI智能体“龙虾”手机端页面。（新华社发）

迅速走红 市场热捧

与单一人工智能产品不同，OpenClaw更像是人工智能产品的综合调度平台，通过整合调用通信软件和大语言模型，在用户本地电脑自主执行文件管理、邮件收发、数据处理等复杂任务。它打破了“能说会道”的对话框，走向“能干善为”的实务层面。

OpenClaw爆红速度令人咋舌。“微信指数”显示，2026年1月29日其关键词指数热度为0，1月30日为253万，3月10日飙升至1.656亿。抖音、小红书、微博等社交平台，关于OpenClaw的话题更是层出不穷。

这股热潮还从网络空间走入现实生活。无论是互联网头部企业门口，排队等待部署OpenClaw的人群，还是今年全国两会首次将“打造智能经济新形态”写入政府工作报告，代表委员热议“养龙虾热”，都透露出社会对新质生产力的好奇与热忱。

广东深圳龙岗区、江苏无锡高新区、安徽合肥高新区等地，还相继出台文件支持人工智能开源项目落地深耕，致力打造“AI+超级个体/一人公司”等新业态。

吉林大学计算机科学与技术学院教授徐昊认为，以OpenClaw为代表的智能体AI，核心突破是实现隐性知识的显性化萃取，通过统一交互入口和长期记忆，实现将此前分散在不同工具平台中的认知、方法和经验，转化为数字化、可复用的“技能”，并可以快速迭代和持续进化。

热潮之下，有人尝到了“龙虾”的鲜美。“我2月初在一台新电脑上，根据网上教程部署了OpenClaw。整体用下来，感觉不错。”山东大学电气工程学院教授杨明说，自己每天都会与OpenClaw进行交互，跟踪最新科研进展、搜集整理实验数据、细化项目产品规划，并将成果共享给学术团队。

“OpenClaw的走红，会让‘数字员工’越来越多、越来越聪明，也拓展出新的业务范畴。”山东济南泉峰信息技术有限公司创始人康建峰说。这家“一人公司”2月底入驻科大讯飞济南产业加速中心，主业聚焦AI智能体技术应用实训平台等产品。

安全存忧 警示不断

不过，记者注意到，在复杂的网络环境中，许多尝鲜者不仅未能体验新技术的奇妙之处，反而暴露在隐私泄露、资产受损等风险中。

3月13日，国家网络与信息安全信息通报中心发布OpenClaw安全风险预警，点出OpenClaw在架构设计、默认配置、漏洞管理、插件生态、行为管控等方面存在较大安全风险，建议从谨慎安装第三方插件等方面防范风险。

3月12日，针对“OpenClaw”典型应用场景下的安全风险，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）组织智能体提供商等发布“六要六不要”建议，包括防范社会工程学攻击和浏览器劫持等具体措施。

3月10日，国家互联网应急中心的专项风险提示，点明OpenClaw智能体软件为实现“自主执行任务”的能力，被授予较高的系统权限，由于其默认的安全配置极为脆弱，攻击者一旦发现突破口，便能轻易获取系统的完全控制权。

国内一些安全团队对OpenClaw基于完整运行轨迹的系统性安全评估显示，其整体安全通过率不足六成。记者梳理发现，一些试用OpenClaw的用户称遭遇密钥被盗用、隐私数据被暴露于公网、重要资料被误删等损失。

“OpenClaw的不当行为，可能令使用者面临法律风险。”北京中银律师事务所高级合伙人刘晓亮说，比如将其无限制接入公司内网、服务器，误删生产数据库或核心代码，使用者可能因间接故意涉嫌破坏生产经营罪、故意毁坏财物罪。

“不法分子可能对‘OpenClaw’‘AI智能体’等概念移花接木进行诈骗。”吉林大学天和劳动关系研究院研究员尹希文说，相关骗局或宣称投资AI智能体可通过“自动炒股”等方式产生高额稳定回报，或以“符合地方扶持政策”为噱头，销售虚假产品。

规范引导 重塑业态

多名受访专家认为，接踵而至的风险警示，为“养龙虾热”及时踩了刹车，有助于人工智能产业发展避暗礁、过险滩。

——OpenClaw魅力犹在。国家网络与信息安全信息通报中心3月13日发布的监测数据显示，目前全球活跃的OpenClaw互联网资产已超20万个，其中境内活跃的OpenClaw互联网资产约2.3万个，主要集中在北京、上海、广东等互联网资源密集区域。

日前，由江苏南京鼓楼高新区主办的南京首场OpenClaw集中安装与体验活动举行。联通（山东）产业互联网有限公司上线OpenClaw安全服务一站式解决方案。

——智能体发展方兴未艾。“去年学校举办的首届人工智能创新应用大赛，吸引1700多人参赛。AI编程创新工坊活动，则有100余名不同专业背景的本科生、研究生深度参与。”山东大学数智化支撑研究院副院长于磊磊说，智能体被师生们“玩出了花儿”。

“现阶段OpenClaw的技术门槛和部署过程，有着专业人士的‘手搓感’。规模化应用，必须要实现标准化和规范化。”山东讯中大数据有限公司执行总经理曹毅认为，不断涌现的“OPC”将推动智能体探索更精细的生产场景。

——社会生产方式面临革新。东南大学网络空间安全学院研究员霍赋硕说，社会不再满足于“能聊天的大模型”，更渴望“能干活的大模型”。从注意力经济向行动力经济的转移，是生产力变革的核心特征。

新技术不断涌现的当下，更要保持谨慎理性。山东社会科学院智库研究中心副主任李剑认为，OpenClaw的效率红利与安全风险均源于自身强大的技术能力，既不能放任自流，忽视“龙虾热”的潜在危害，也不能因噎废食，否定技术进步的价值。必须同步构建与之匹配的安全框架、法律规范和伦理准则，将技术红利引导到可持续、可信赖的发展轨道上。

北京中银律师事务所张苏楠律师认为，当前应充分调动现行法律法规体系，如《网络安全法》等，积极应对新技术应用带来的潜在系统性法律漏洞。同时严格审查评估相关智能体安全性，履行算法备案和变更、注销备案手续。

名词解释

“养龙虾”是科技圈对部署与调教开源AI智能体框架OpenClaw的戏称。OpenClaw是2025年底发布的本地优先的AI智能体（Agent）框架，其最早的图标是一只小龙虾，因此被广大爱好者称为“养龙虾”。核心是给大语言模型装上“手脚”，能直接操控电脑完成任务。因其能让AI“动手做事”而非仅仅“动嘴聊天”而爆火。

今明两年或成历史最热年份

■据《光明日报》

近日，“今明两年或成历史最热年份”“地球或将迎超级厄尔尼诺现象”等相关话题冲上网络热搜。针对社会关切，3月16日，科技日报记者采访了国家气候中心气候预测室首席专家陈丽娟和国家气候中心气候预测室主任刘芸芸，就厄尔尼诺发展趋势及其影响进行权威解读。

据多家媒体报道，全球多个科研机构预测，今年晚些时候可能出现强厄尔尼诺现象，进而扰动全球气候，不仅可能引发极端高温、洪水、干旱等灾害，还可能进一步推高全球气温，导致今年和明年夏季气温攀升至历史新高。

对此，陈丽娟解释说，厄尔尼诺-南方涛动（ENSO）是发生在热带太平洋、具有3—7年周期的海气耦合振荡现象，属于气候系统的自然变率。一般利用热带中东太平洋固定区域海表温度异常值（即偏离气候平均态的程度）持续的时间和强度来表示ENSO的位相。如果3个月滑动平均海表温度值持续5个月大于0.5°C，则为暖位相，称为厄尔尼诺；如果持续5个月小于-0.5°C，则为冷位相，称为拉尼娜；如果在-0.5°C至0.5°C之间变化，称为中性状态。

国家气候中心基于最新监测数据和国内外多家气候模式的预测结果分析，近期拉尼娜状态趋于结束，后续将进入中性状态。未来热带中东太平洋海温将持续回升，今年春季后期可能进入厄尔尼诺状态。

刘芸芸表示，从历史统计看，拉尼娜事件结束后，当年进入厄尔尼诺状态的概率约为三分之一。国际上多个模式预测进入厄尔尼诺的具体时间存在差异——欧洲中期天气预报中心预测为4月，澳大利亚预测为5月，日本气象厅预测为6月，美国专家投票预测为7—9月。也就是说，最早可能出现在今年4月，最晚可能在夏末秋初。

“总体来看，今年下半年赤道中东太平洋处于厄尔尼诺状态的可能性较大，但目前尚无法准确预测其具体形成时间和总体强度。”刘芸芸指出，目前国际上多个气候预测模型的结果还存在较大分歧，尚未达成共识，因此现在就断定今年会出现“超级厄尔尼诺”还为时过早。

针对“最热年”的预测，陈丽娟提示，厄尔尼诺事件往往伴随全球平均气温升高。但具体升温幅度和极端天气表现，还需根据厄尔尼诺的强度、类型及区域气候响应进一步监测研判。

陈丽娟表示，天气和气候变化与百姓生活和经济社会发展息息相关，正因如此，天气和气候领域的信息资讯更容易受到百姓高度关注。当前社交媒体上关于“最热年”“极端天气”等话题讨论热烈，部分信息可能存在夸大或断章取义。