“养龙虾”火热背后：
智能体大规模落地如何过好安全关

■中国城市报记者 孙雪霏

“你‘养龙虾’了吗？”这句科技圈的流行问话，正折射出AI技术从“能说会道”向“动手干活”的跨越。

近日，开源AI智能体OpenClaw（因图标酷似龙虾被网友称为“龙虾”，曾用名Clawdbot、Moltbot）迅速走红。从广东省深圳市腾讯大厦门口的安装长队，到线上平台火热的部署服务，再到深圳市福田区“政务龙虾”上岗，智能体应用迎来爆发式增长。

在智能体加速融入生产生活的同时，国家互联网应急中心、工业和信息化部网络安全威胁和漏洞信息共享平台均发布安全提示，直指其潜藏安全隐患。

如何平衡创新发展与安全底线，成为智能经济高质量发展的核心命题。

“龙虾”走红：智能体引发广泛关注

3月6日，深圳市腾讯大厦门口上演“千人排队”戏码。数百名开发者、AI爱好者齐聚于此，在工程师协助下完成OpenClaw云端部署。这些人群的年龄跨度为20岁到60岁，既有带着明确办公需求而来的从业者，也有紧跟技术潮流、不愿掉队的普通用户。

据了解，相较于传统对话式AI仅能提供信息参考，OpenClaw可依据自然语言指令直接操控计算机，自主完成文件整理、跨软件数据处理、邮件收发等实操任务，真正实现从“对话模型”到“行动高手”的进化，精准契合个人事务便利化与企业降本增效的核心需求。而这也是OpenClaw快速“破圈”的关键所在。

技术门槛催生了完整的部署服务产业链，让“养龙虾”从技术圈走向大众市场。在闲鱼、小红书等平台，“OpenClaw上门安装”成为热门关键词，远程部署报价为50—100元，上门服务定价为每次500—800元。有从业者短期内靠相关部署服务营收颇丰，大学生兼职接单、专业机构社群派单等模式层出不穷。

与此同时，阿里云、腾讯云、中国电信天翼云、京东云等国内主流云厂商快速跟进，相继推出一键部署服务与配套安全指南，打通个人应用到企业场景的落地通道，进一步推动OpenClaw普及，使其迅速跻身GitHub平台高星标开源项目行列。

政策端的密集加持，为智能体产业发展注入强劲动力。国家层面，《国务院关于深入实施“人工智能+”行动的意见》划定清晰目标，到2027年，新一代智能终端、智能体等应用普及率超70%，到2030年超90%。

2026年《政府工作报告》提出：“打造智能经济新形态。深化拓展‘人工智能+’，促进新一代智能终端和智能体加快推广，推动重点行业领域人工智能商业化规模化应用，培育智能原生新业态新模式。”

地方层面，多地出台专项举措助力智能体发展。近期，深圳市龙岗区人工智能（机器人）署发布《深圳市龙岗区支持OpenClaw&OPC发展的若干措施（征求意见稿）》，推出“龙虾十条”，覆盖部署开发、算力人才、资金扶持等全链条，给予优质项目最高200万元补贴、种子期项目最高1000万元股权投资；江苏省无锡市高新区发布12条专项措施，单项支持最高达500万元；安徽省合肥市高新区推出“龙虾15条”，提供高额算力、语料、模型补贴。此外，江苏省南京市栖霞区、江宁区，江苏省苏州市常熟市，浙江省杭州市萧山区等地也纷纷发力，围绕场景开放、人才安居等方面，构建智能体产业发展良好生态。

全国人大代表、中国工程院院士、鹏城实验室主任高文向中国城市报记者直言，“养龙虾”的火爆超出行业预期，智能体正从技术概念加速落地为产业实践。

北京邮电大学网络空间安全学院副教授李朝卓则表示，OpenClaw的走红是AI技术演进的必然结果。智能体具备自主决策、系统调用的核心能力，打破了传统AI的应用局限，当前已呈现“个人—企业—政务”三级扩散的发展态势，产业生态加速成型，成为激活新质生产力的重要抓手。

政务赋能：智能体拓宽民生服务场景

在深圳市福田区，本土自研的“政务龙虾”已正式上岗，率先在政务外网完成本地化部署，聚焦民生诉求分析、公共场所卫生许可办理两大核心场景，实现智能技术与政务服务的深度融合。

以往，人工处理海量民生诉求工单耗时费力，易出现重点遗漏、效率低下等问题。如今，“政务龙虾”可快速归集、分析海量数据，生成民生热点画像与风险预判报告，推动政务服务从“事后处置”向“事前预防”转型，切实做到“民有所呼，我有所应”。

中国城市报记者从福田区政务服务和数据管理局获悉，在公共场所卫生许可办理场景，“政务龙虾”的落地应用实现了政务服务效能的大幅跃升，将原本1天的预审流程压缩至数分钟，审批效率提升96%，群众办事材料递交次数减少53%，政务服务满意度攀升至98.7%。该智能体依托本土自研架构，仅3000余行核心代码即可实现传统系统数十万行代码的功能，适配国产芯片，全程安全可控。

为严防智能体越权操作、数据泄露等问题，福田区严格落实《福田区政务辅助智能机器人管理暂行办法》，为每一台“政务龙虾”配备在编公务员担任“监护人”，全程把控操作规范、审核执行结果，筑牢政务数据安全防线。这一“技术+制度”的双控模式，为智能体政务场景落地提供了可复制、可推广的范本。

截至目前，福田区已搭建智能政务“场景超市”，累计发布超千个智能政务场景需求，吸引数十家科技企业入驻，推动智能体在基层治理、城市管理、民生服务等多领域落地见效。“政务龙虾”实现24小时不间断运行，无需休整轮岗，已累计节约政务人力超3000小时，有效缓解基层政务人员工作压力，让公职人员聚焦更精准、更优质的服务工作，释放政务服务新效能。

《政府工作报告》起草组成员、国务院研究室副主任陈昌盛解读称，完善人工智能治理，核心是推动AI朝着安全、有益、公平的方向发展。政务场景的智能体应用，正是这一治理理念的生动实践。

全国政协委员、中国科学院计算技术研究所研究员张云泉向中国城市报记者表示，政务领域的智能体落地，既提升了公共服务质效，也探索出安全可控的应用路径，为行业规范发展提供了实践参考，有助于推动智能体在更多合规场景中释放价值，真正做到科技赋能民生、服务发展大局。

安全护航：筑牢智能体发展的底线

在智能体产业蓬勃发展的同时，安全风险不容忽视。近日，国家互联网应急中心、工业和信息化部网络安全威胁和漏洞信息共享平台均发布安全提示，双重预警直指OpenClaw安全隐患。

据了解，该智能体为实现自主执行任务的能力，被赋予访问本地文件、调用外部API（应用程序编程接口）等高权限，但默认安全配置薄弱，缺乏严格的权限管控与防护机制，极易被不法分子利用，引发各类安全问题。

国家互联网应急中心明确，OpenClaw主要存在四大核心安全风险：一是提示词注入风险，攻击者通过隐藏恶意指令诱导智能体，可窃取系统密钥；二是误操作风险，智能体误解指令易删除核心数据、重要文件；三是插件投毒风险，恶意插件可窃取信息、部署木马，导致设备沦为“肉鸡”；四是高中危漏洞风险，漏洞被利用后，易造成数据泄露、系统被控，威胁个人与行业安全。相较于传统AI，智能体自主运行、系统调用的特性，让其安全风险成倍放大，一旦失控，威胁将从数字世界延伸至物理世界，必须高度警惕、严加防范。

面对安全隐患，政企研多方联动发力，构建全方位安全防控体系。在企业端，奇安信等网络安全企业针对性研发智能体安全检测与加固工具，可自动扫描风险、修复配置漏洞，为上百家部署智能体企业提供加固服务，通过关闭公网暴露端口、完善身份认证、隔离运行环境、严控智能体权限等措施，筑牢安全防线；阿里云、腾讯云、中国电信天翼云等云厂商同步发布安全部署指南，开展实例安全检测，提供风险预警与一键加固服务，引导用户规范部署、禁用非可信插件，守牢应用安全关口。

在制度层面，新修改的《中华人民共和国网络安全法》明确要求，加强人工智能风险监测评估和安全监管，完善伦理规范，为智能体安全治理提供法律遵循。

在地方层面，深圳市福田区依托政务云防护体系，建立全流程操作日志审计机制，日志留存时长超180天，实现智能体操作全程可追溯、可监管。多地网信、通信管理部门发布安全科普提示，引导用户规避明文存储密钥、随意开放权限等违规操作，提升全民安全防范意识。

中国科学院自动化研究所研究员曾毅表示，智能体安全治理需坚持预防为主、防治结合，通过技术、标准、合规协同发力，从源头防范风险。

中国政法大学法治政府研究院院长、教授赵鹏也对中国城市报记者说，要强化法律法规落地执行，厘清智能体研发、部署、使用各方责任，完善与《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》的衔接，形成安全防护与治理合力。

全国政协委员、360集团创始人周鸿祎认为，2026年是智能体规模化落地关键之年，企业需摒弃“重功能、轻安全”的理念，将安全设计融入研发全流程，坚持“以技防险、以智治安”，让智能体在安全轨道上健康发展。

工业和信息化部网络安全产业发展中心方面表示，将持续完善智能体安全标准与监管体系，强化风险监测预警，推动产业安全规范发展。

3月11日，北京首场“龙虾”市集活动在百度科技园举行。图为活动现场，参与者排队为笔记本电脑安装开源AI助手OpenClaw（“龙虾”）。 人民视觉