“养龙虾”爆火：

智能体概念走向大众 科技巨头抢滩布局

开源AI智能体OpenClaw近日爆火，围绕“让AI动手干活”的产业变革加速到来。与只停留在对话框里的大模型不同，智能体被赋予了“手和脚”，能操作电脑、调用软件、阅读文件，将任务落地实施，被视为人工智能迈向“数字员工”的关键一跃。几乎同时，对智能体“幻觉”、权限过大、数据泄露的担忧随之而来。行业人士普遍认为，在“数字员工”真正上岗前，需要通过软硬件设置，在智能体周围筑起安全围墙。

● 本报记者 王婧涵

视觉中国图片

百度举办“龙虾”集市，现场人员排队等待免费安装OpenClaw。 本报记者 王婧涵 摄

企业竞逐智能体新赛道

OpenClaw的火爆，为用户进行了一次高强度的智能体科普，国内科技企业也以罕见的协同姿态，纷纷宣布将智能体纳入自身生态版图。

3月9日，腾讯正式上线全场景AI智能体WorkBuddy，产品完全兼容OpenClaw的技能体系，从下载安装到连接企业微信，最快1分钟即可实现通过手机遥控电脑干活。目前，WorkBuddy最新版本已支持微信一键直连功能。

百度则依托其智能云生态，发布零部署AI服务DuClaw，用户无需关注镜像选择、服务器配置或API密钥申请，即可实现“即开即用”。百度表示，这一服务集成了百度搜索、百科及学术搜索等核心能力，支持多款主流大模型选配，旨在将复杂的AI集成转化为低门槛的云端体验。

阿里云也已在云市场提供OpenClaw相关部署服务，并面向国际市场推出企业级Agentic AI开发平台百炼专属版。

MiniMax、小米、火山引擎等也相继宣布推出相关产品。小米推出移动端Agent产品“Xiaomi miclaw”，基于自研MiMo大模型构建，能便捷调用小米生态设备及系统级应用，降低了非专业用户的使用门槛。MiniMax和火山引擎则分别上线了网页版MaxClaw和云上SaaS版ArkClaw，用户打开网页即可体验智能体功能。

市场对此反应热烈。3月以来，港股MiniMax股价涨超30%，3月11日最高触及1320港元/股。

3月7日，深圳龙岗就发布了《深圳市龙岗区支持OpenClaw&OPC发展的若干措施（征求意见稿）》，提出抢抓人形机器人量产元年及具身智能爆发机遇，聚焦“一人公司”（OPC）这一最具活力的创新单元，以OpenClaw智能体为技术抓手，充分发挥龙岗区人工智能全域全时应用示范区及完整的智能硬件产业链优势。

多地还以“市集”“沙龙”等形式组织免费安装活动，鼓励市民体验前沿技术，让“养龙虾”从技术圈小范围活跃快速走向大众普及。

权限失控与AI幻觉催生安全焦虑

几乎同时，智能体带来的安全隐患也暴露在人们面前。多位行业专家向记者表示，与传统的软件不同，智能体之所以能“干活”，核心在于它被赋予了极高的系统权限——它可以读取文件、发送邮件，甚至执行代码。

“要让它写日报就要允许他看邮件和文档，让他点外卖就需要给他银行卡密码。这和把查看隐私的权限和银行卡密码给另一个人类一样，给了就会有风险。”有“龙虾集市”上的资深爱好者向记者表示。

另一种风险则来自AI本身的幻觉。某百度工程师在接受采访时表示，智能体依然基于模型进行思考，因此仍有产生幻觉的概率，需要用户在操作中持续纠正。

360漏洞云AI安全及技术发展资深专家宁宇飞介绍，目前智能体风险还存在于使用中的多个环节，黑客可以通过提示词注入攻击，通过诱导智能体访问恶意网站，让其在不知不觉中执行非预期指令；还可能通过插件供应链投毒，大量开源的“技能包”可能被植入恶意代码，而用户在下载安装时往往缺乏审查能力。

此外，智能体的运行机制本身就放大了消耗与风险。传统的大模型问答以Token计费，而智能体完成一个复杂任务可能需要尝试几十种方案、进行数百步推理，Token消耗量是前者的数十倍、上百倍。奇安信董事长齐向东在采访时表示，AI正在向“超人化”演进，具有超级权限、超级能力，一旦被攻破，可能造成核心数据泄露、业务系统瘫痪等链式危机。

筑牢智能体上岗的安全护栏

面对智能体带来的新型安全挑战，构建与之适配的防护体系已刻不容缓。

宁宇飞表示，普通用户“养龙虾”或使用类似智能体时需遵循五项核心原则：隔离部署、最小权限、凭证轮换、插件准入和异常监测。他建议，高敏主机禁止直接运行AI Agent，实行环境分离，避免潜在风险扩散；对Token、API Key等敏感凭证进行周期性轮换和严格治理；对技能插件的来源、行为模式和更新进行严格审计；实时监控CPU、网络流量及文件访问，对异常进行告警并响应；严格限制AI Agent权限，拒绝默认全盘或全网授权，确保仅能执行必要操作。

“如果是第一次尝试配置相关智能体，最好用一台新电脑或带沙箱的环境运行，以降低安全风险。”宁宇飞表示，“同时，对海量开源的技能包也要保持警惕。”

在企业层面，各大云厂商正将自身的安全能力封装成标准化产品。百度工程师介绍，通过轻量应用服务器为智能体在云端配备“独立电脑”，能有效实现与本地数据的物理隔离，“用户主动地把觉得可以给智能体的文件上传，相当于天然就通过物理环境把文件路径隔离开了。”

标准制定层面，近期中国信通院牵头提出的3项涉及工业智能体系统架构、工业智能体之间互操作要求、智能体与工具之间数据接入接口的国际标准，已正式通过电气与电子工程师协会标准协会审查投票，成功完成立项。中国信通院表示，计划近期再对“工业智能体分类分级”标准进行立项，为智能体在实际应用中的开发、部署、监管和优化提供统一规范。

然而，安全问题并不能一劳永逸。正如360集团创始人周鸿祎所言：“安全问题永远是不能彻底解决的，但不能因为有安全问题就因噎废食。不发展、不进步才是最大的不安全。”

具身智能产业加速落地 专家建议筑牢安全防线

● 本报记者 郑苹颖

“具身智能正处于产业规模化的前夜”“人形机器人已进入场景化竞争的下半场”……从业者谈及具身智能产业发展，纷纷认为今年将是具身智能迈入规模化应用的关键期。具身智能机器人正加速从实验室走向工业制造、商业服务等真实场景，其安全风险也从数字世界蔓延至物理空间。

近日，中国证券报记者采访的多位网络安全专家与具身智能从业者建议，在具身智能技术爆发期同步构建全链条的安全保障体系，让安全成为具身智能规模化落地的基石，同时制定安全规范与测试标准，护航产业发展。

安全问题受关注

在日前举办的2026人形机器人与具身智能标准化年会上，智元机器人联合创始人、总裁兼CTO彭志辉表示，“人形机器人行业已从实验室炫技进入工程化、场景化竞争的下半场。”

2026年以来，具身智能机器人正加速走进工业制造、商业服务等真实场景。比如，亮相2026年春晚的银河通用，已在全国景区、商圈部署超过100个银河太空舱用于零售场景。小米集团董事长雷军表示，小米人形机器人已在汽车工厂“实习”，预计未来5年会有大批量人形机器人进入小米工厂。

同时，具身智能安全问题已被提上日程。“具身智能具有‘智能决策+物理执行’的双重属性。”奇安信科技集团董事长齐向东日前在接受记者采访时说，具身智能面临的安全挑战集中于决策层、执行层、物理层三大层面：决策层易出现数据投毒、模型“幻觉”、框架缺陷等问题，导致具身智能决策中枢紊乱；执行层因软硬件供应链体系复杂，终端漏洞、云平台、API接口易被攻破；物理层则因具身智能物理暴露的特性，易遭到近距离劫持，导致具身智能被非法控制。

安全是具身智能从实验室走向规模化部署的底线。“在数字世界，代码错了可以重启，但在物理世界，机器人面临摩擦、碰撞、形变、老化、噪声等随机约束，一旦失效，便会产生物理成本。”智元机器人合伙人、高级副总裁、具身业务部总裁姚卯青告诉记者，安全不仅是保障商业化落地顺利推进的基础，更影响着大众对具身智能的接受度与信任度，“我们既要跑得快，更要跑得稳，安全标准是产业发展的基石。”

产业链复杂性加剧安全风险

中国信息通信研究院人工智能所安全与具身智能部主任石霖表示，具身智能通过视觉、语音、力觉等多模态感知与物理交互，打破了传统网络安全中“防火墙隔离内外网”的边界防护逻辑。

“攻击者无需突破网络边界，仅通过环境中的视觉欺骗、语音伪造或传感器信号干扰，就能完成攻击。”石霖举例说，在安全竞赛中，白帽黑客通过构造的语音指令，曾直接绕过机器人验证机制，获得系统控制权；在实验室测试中，一张特制贴纸就能让工业机器人将高温焊枪误识别为普通工具，引发安全事故。

除了感知环节，安全风险渗透于具身智能的全产业链。绿盟科技集团副总裁曹嘉告诉记者，从生产制造环节的硬件供应链后门、固件漏洞，到本体硬件层面的物理篡改与传感器欺骗，再到大模型软件层面的提示词注入、训练数据投毒与模型窃取，以及落地部署阶段的权限管理混乱等，安全风险存在于各个环节。

供应链的复杂性放大了风险传导效应。石霖指出，具身智能横跨芯片、传感器、机械制造、算法等多个行业，多级供应商与开源组件依赖使得单一漏洞可能引发级联失效。某品牌人形机器人曾被发现存在高危蓝牙漏洞，但供应链响应滞后，凸显了“重功能迭代、轻安全防护”的行业现状。

曹嘉认为，面对同样复杂的供应链体系，具身智能的安全问题可参考智能驾驶汽车行业。“智能驾驶汽车提供了一套成熟的解决方案叫‘安全左移’，就是在主机厂引入供应商时，要求供应商提供其产品符合安全要求的证明，要求前一个环节做好安全保障工作。”曹嘉说。

产业协同构筑安全防线

面对新型安全挑战，产业界已积极行动。齐向东建议构建具身智能专属安全防护体系。他透露，奇安信已探索搭建“端—网—云—机”一体化防御体系，聚焦攻击入口探测、漏洞验证等核心环节开展渗透测试。同时，他强调要保障数据资产安全，锤炼高水平的网络安全实战能力。

绿盟科技围绕具身智能的安全风险，构建了以AI安全围栏为核心，覆盖发现、评估、防护、审计、运营全链路的解决方案，重点解决具身智能权限滥用、数据泄露、提示词注入、物理行为失控等新型威胁。

企业研发端亦将安全防护内化。姚卯青表示，智元在本体设计阶段融入安全理念，通过系列化关节的高可靠性设计，保障硬件安全。以精灵系列作业机器人为例，其力控臂已实现数百小时无报错运行，从技术底层规避作业过程中的潜在风险。此外，姚卯青认为，真实场景是验证产品可靠性的最有效途径，通过具身智能的规模化部署，收集真实场景运行数据，并持续迭代升级算法，保障运行安全。

今年2月28日，《人形机器人与具身智能标准体系（2026版）》发布，标志着相关产业进入规范化发展新阶段。对于行业发展，姚卯青认为，下一步仍需针对不同应用场景制定更具体的安全规范和测试标准。

石霖则呼吁加快制定产品安全基线、评估标准与事故责任划分规则，并组建产业联盟，建立威胁情报共享与漏洞联合响应机制。

曹嘉表示，当前仍处于具身智能落地部署的初期，行业安全解决方案将随着具身智能的场景探索而进一步细化完善。“要让安全成为具身智能规模化落地的前提，而不是事后打补丁。”他强调，必须推动机器人厂商、模型开发商、安全企业、用户与监管机构多方协同，构建统一的安全架构与合规标准体系。

中复神鹰发布SYT80超高强度碳纤维

● 本报记者 刘丽靓

它比发丝还要细，直径不足头发丝的十分之一；它的密度仅为钢材的四分之一，强度却是普通钢材的十倍。它就是被誉为材料界的“黑色黄金”——SYT80（T1200级）超高强度碳纤维。日前，中国建材集团所属中复神鹰自主研发的SYT80（T1200级）超高强度碳纤维发布。

“这一重大突破，标志着我国在高性能碳纤维领域实现了从技术到装备、从实验室到工程化量产的全链条自主可控，这是以科技创新引领产业创新、向新求质再攀新高的生动实践。”中国建材集团董事长周育先表示，集团将稳步推进连云港板桥3万吨基地全面投产，进一步扩大高性能碳纤维产能规模。

“黑色黄金”攀上新高峰

在材料科学的殿堂里，碳纤维素有“黑色黄金”之称。此次发布的SYT80（T1200级）碳纤维，工程化拉伸强度突破8000兆帕，达到了行业全球顶尖水平。

“这不仅解决了‘有没有’的问题，更是解决了‘好不好’的关键一步。”周育先表示，新材料是全球材料工业发展的先导，是孕育新质生产力的沃土。SYT80的规模化量产，意味着这种顶尖材料将不再是实验室里的奢侈品，而是可以成为服务全球经济发展和民众生活的常用品。

他进一步阐释，这一突破将为航空航天等“大国重器”锻造更轻更强的“翅膀”，让国产大飞机更轻盈安全、航天运载效率更高；也将为氢能储运、低空经济、具身智能等未来产业提供更可靠的“筋骨”，让新能源汽车续航更长、医疗器械更轻便耐用，从根本上夯实服务国家战略与人民美好生活的材料基础。

自主创新链打通“最后一公里”

从实验室样品到百吨级量产，看似简单的跨越，背后是无数科研工作者的日夜坚守与技术攻坚。

“当碳纤维强度迈入8000MPa级别后，材料的性能对微观缺陷极其敏感，哪怕是纳米级、亚纳米级的微小缺陷，都会大幅影响材料的拉伸强度和稳定性。”中复神鹰碳纤维股份有限公司董事、总经理陈秋飞在回顾研发历程时坦言，要实现SYT80的性能突破，必须把全流程的微观缺陷降到极致；而更难的是，实验室小批量制备可以通过精细化控制做出高性能样品，但要放大到百吨级量产，如何在原丝制备、均质预氧化碳化、表面处理等全流程保持工艺的高度稳定性，避免缺陷批量产生，是行业内长期未能解决的难题。

为攻克这一难关，陈秋飞团队依托SYT70超高强度工程化技术积淀，走出了一条精准溯源、工艺革新、反复验证的攻坚之路。“我们整合了SYT70研发生产积累的海量试验数据，建立了碳纤维缺陷数据库，通过微观结构分析，精准定位各环节缺陷的产生机理和影响规律。”陈秋飞介绍，团队迭代第四代干喷湿纺技术，升级装备精度、优化工艺参数、创新分子结构设计，从原丝制备到碳化处理全流程最大限度减少缺陷产生。

如此高效的技术突破，离不开一套科学完善的攻关机制。“SYT80的突破，离不开中国建材集团的战略引领和资源支持，更离不开我们构建的‘战略统筹、资源集聚、闭环管理、激励保障’重大技术攻关管理机制。”中复神鹰首席科学家张国良详解了这套机制的核心内涵。

在集团层面，碳纤维产业被列为新材料板块核心发展方向，将SYT80研发纳入集团重大科技攻关项目，统筹协调研发、装备、材料等各类资源，提供资金与政策重点支持；在公司层面，实行项目负责人制，成立专项项目组，明确各环节责任，建立周例会、月复盘的闭环管理机制；在团队层面，打破内部壁垒集聚合力，实现“研发与生产同频、检测与优化同步”，同时坚持研发人员下一线、生产人员参与研发，加快了实验室技术向工程化量产的转化速度。

“我们充分赋予攻关团队技术研发的自主权，宽容合理失败，充分激发团队创新活力，这也是我们能在一年内实现从实验室到百吨级量产的关键。”张国良说。

四维发力绘蓝图

发布不是终点，而是新赛道的起点。对于这款材料的未来，中国建材集团已绘就清晰的“技术、产能、成本、市场”四维发展蓝图。

在技术研发上，将持续优化SYT80现有工艺，并依托材料基因工程等创新资源，加快M65J级超高模量、高强高模高韧等更高性能碳纤维的研发，探索构建从材料研发到应用落地的全链条技术体系。在产能布局上，将依托西宁、连云港等三大生产基地稳步扩产，保障国家战略需求和市场民用需求。在降低成本上，将通过“规模化量产+工艺优化+全产业链协同”，让高端碳纤维的性价比持续提升。

在最为关键的市场化推广方面，中国建材集团正打造一条让顶尖科技惠及民生的高效路径。“我们将坚持‘国家战略领域+民用消费领域’双轮驱动。”周育先表示，集团将在持续保障航空航天、深海探测等国家战略领域供应的基础上，重点推动碳纤维在新能源、低空经济、具身智能、高端装备、民用交通等领域的规模化应用。

他透露，目前，集团聚焦低空经济、具身智能等新兴民用赛道，提前布局技术验证和产品适配，并与龙头企业签订了战略合作框架协议。