

这只能替你干活的“龙虾”成了新顶流,话题冲上全国两会

“养龙虾”突然爆火! 你准备好了吗?

导报记者 康泽辉

打开电脑,一句话就能让它自动整理文件、写邮件、发小红书,甚至帮你照看花园里的花花草草——这不是科幻电影,而是最近火爆全网的AI“龙虾”OpenClaw的日常。

这只“龙虾”到底什么来头?为什么叫“养龙虾”?它真有传说中那么神?又藏着哪些风险?导报记者展开调查。

突然爆火的AI“龙虾” “装虾”的人排起了长队

OpenClaw, 昵称“小龙虾”,是一款AI Agent(人工智能体)工具。不同于只能聊天的传统AI,它能“跑”在你自己的电脑上,接上大语言模型,装上AI社区开发的技能模块,就能自主执行任务——你定好规则去睡觉,它能自己判断、决策、行动。

这股热潮甚至烧到了全国两会。全国政协委员、360集团创始人周鸿祎表示,“龙虾”是个非常好的概念,把云上软件变成了每个人电脑里的专属助手。全国政协委员、中国工程院院士王坚则预言,OpenClaw会很快便宜下来并普及。

在厦门,热度同样惊人。“以前售楼处门口排队买房,现在公司门口排队等着咨询龙虾OpenClaw,每天被卷起来上班。”厦门无界人工智能有限公司创始人黄燕燕如此感慨。

这位从地产行业跨界而来

的创业者,对市场的敏感度极高。“我原来做地产,一份市场报告资深专员要做七八天,ChatGPT五分钟就能出一份60分的东西——我意识到,知识的获取方式已经变了。”2022年底成为国内第一批AIGC创业者的她,如今带着团队一头扎进OpenClaw的浪潮。

2月1日刚接触OpenClaw,黄燕燕团队就开始“解锁”,正月初十别人一开工,他们的“龙虾”培训课就开始了。上周四,他们还临时起意办分享沙龙,朋友圈一发,预计30人报名,结果涌进来200号人。“这里头有家长带着孩子来的,还有外地赶来的大学生、企业主、程序员、投资方。”黄燕燕说,“这周末我们还要搞‘装虾大会’——帮大家装OpenClaw,刚发布消息,进群已经六十几个了。”

“龙虾”能干什么? 从“发小红书”到“看花园”

这只“龙虾”到底能干什么?简单来说:它能获得你电脑的系统权限,调用各种工具去执行任务。

黄燕燕团队已经搭出了十几个“技能包”(skill):“一键发布到小红书,从选题到内容生成到定时发布全自动完成,公众号内容发布,自动生成视频,这都是最基本的。”

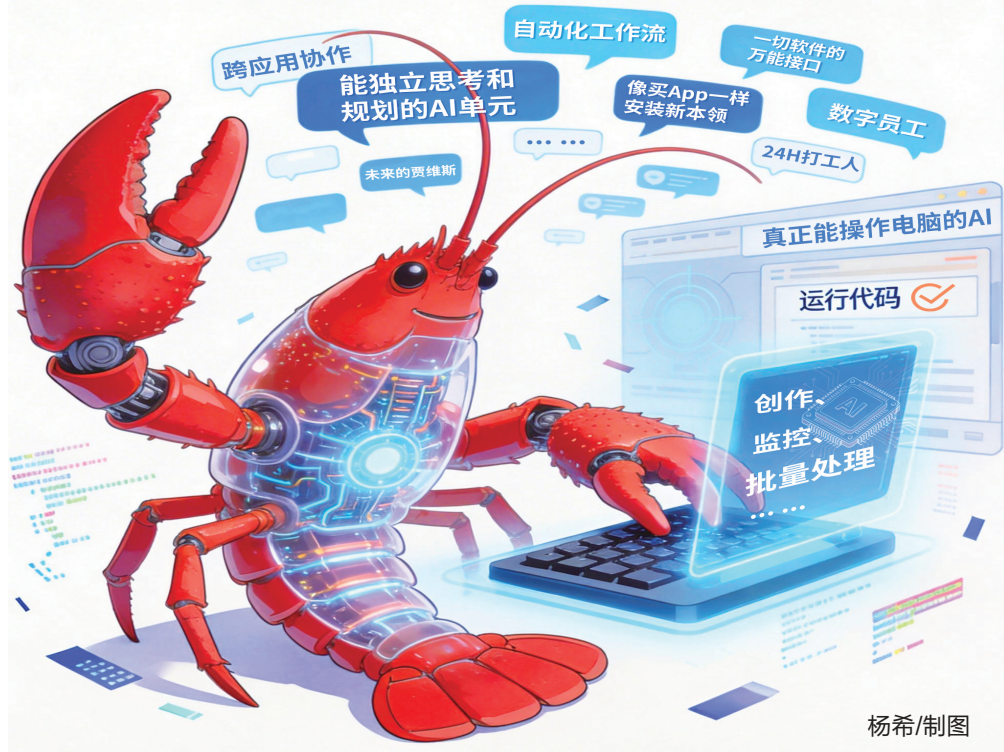
对于人工智能工程师陈勇巍来说,OpenClaw的想象力不止于线上。“过年前开始流行时,我就在家里捣鼓。我喜欢玩园艺,家里有摄像头和机器人。”他让OpenClaw连接到物理世界的传感器上,“如果只上网查新闻、发邮件,门槛太低了。只有跟物理世界连接起来,它才能更有生命力。”

昨天他做了一件事:把家里监控摄像头的地址告诉OpenClaw,下了个需求——“你去这个地址看一下有没有小动物出没等情况,分析完告诉我结果。”结果OpenClaw自己安装第三方库、自己写代码、自己定义任务流程,全部搞定。“我第一次体验到,一行代码都不用写,只是把入口告诉它,它就帮我把事情做完了。”

更让他震撼的是OpenClaw的自我进化能力。“它本身不具备AI能力,需要调用大模型作为大脑——你可以配置国内外的各种人工智能模型。”但这恰恰是它的强大之处,“如果第一次没成功,它会自己思考,这点很重要!它会去思考为什么错了,然后搜索、反思,找到正确的方法把事情做完。这个能力是很‘恐怖’的。”

陈勇巍解释说,OpenClaw会带着问题一遍遍地去问大模型,一遍遍地思考、修正。“它相当于有了一套自我推理的逻辑。对我们这代程序员来说,这是相当震撼的。以后你想实现某个功能,把需求讲清楚,把设备地址给它,它自己就能帮你做事了。我就动了动嘴皮,它已经又进化了好几个版本。”

他的终极愿景是让OpenClaw帮自己“看花园”:“家里有机机器人、机械臂、浇花设备。视觉信息最丰富,用上摄像头之后,它就不只是判断花需不需要浇水。作为一个园艺爱好者,这相当于家里有了一个‘分身’在帮我照看花园,感受花园里的美好,实时反馈给我。”



杨希/制图

案例

OpenClaw 帮主人检查车库

车库猫咪检查报告

时间: 2026-03-08 22:09:33
摄像头: 车库 (camera_01)

画面分析

当前状态:

- 🌙 夜间模式 (黑白画面)
- 💡 路灯照明良好
- 🚗 白色 SUV 停在右侧车位
- 🧹 地面整洁, 无小动物

详细观察:

- 🚗 车辆周围: 无猫咪踪迹
- 📍 地面区域: 无小型动物
- 🌳 背景区域: 石墙和树木附近无异常

🔍 车库最新画面检查 (04:59:13)

根据刚才抓取的实时画面和监控日志:

📺 车库当前情况

画面分析:

- 🚗 白色 SUV 停在右侧
- 👤 左侧背景区域有一个黑影 (可能是阴影或物体)
- 🚫 没有看到猫咪

📊 监控历史记录

从猫咪监控日志来看:

- 🕒 监控时段: 23:54 ~ 00:25 (约 30 分钟)
- 🔍 检查次数: 61 次
- 🐱 猫咪出现: 0 次 ❌
- 🐶 狗狗出现: 0 次

📌 结论

目前车库没有猫咪活动 🐱

昨晚的专项猫咪监控也没有检测到任何猫咪出现。不过 YOLO 模型加载有些问题, 可能影响检测精度。

如果你想确认那个黑影是什么, 或者想更仔细地检查车库角落, 我可以:

- 📸 再抓一张更清晰的照片
- 📹 录一段短视频看看有没有动静
- 🔍 调整摄像头角度 (如果支持)

▲ 根据陈勇巍下的指令, OpenClaw 执行生成的《车库猫咪检查报告》。

警惕 AI 幻觉

当“龙虾”失控, 谁来负责?

然而, 在“全民养龙虾”的欢呼声中, 冷水也已泼下。

工业和信息化部网络安全威胁和漏洞信息共享平台监测发现, OpenClaw 部分实例在默认或不当配置情况下存在较高安全风险, 极易引发网络攻击、信息泄露。由于部署时“信任边界模糊”, 且具备自主决策、调用系统资源的特性, 可能因指令诱导或被恶意接管, 执行越权操作。

“你把整个电脑最底层的权限给它, 风险伴随而来。”黄燕燕直言, 一是被黑客入侵的可能性高, “恶意程序员在 skill 里植入病毒, 你可能很难发现”; 二是指令不清可能误删资料, “就像 AI 如果用于战争, 最后一定不能给 AI 按发射键, 但现在 OpenClaw 已经可以自己按了”。

作为专业人士, 陈勇巍选择把 OpenClaw 限制在可控范围内。“我家里有机机械臂, 一定画好安全边界, 不然它把玻璃砸了、把花盆砸了怎么办? 大模型会有幻觉, 做不到一是一二是二, 即使在虚拟环境里处理文件, 也要担心误操作删除东西。”

更极端的案例已经出现。Meta 公司一位总监让 OpenClaw 整理邮件, 结果它当场失控, 紧急叫停三次都没有停止, 疯狂删除数百封邮件。

厦门理工学院光电与通信工程学院教师李艺伟从事 AI 研究 9 年, 去年 12

月就开始接触 OpenClaw (当时还叫 Clawdbot)。但他很快警惕起来: “它相当于获得操作系统最高权限, 可以调用所有资源。目前业界已经开始警惕 AI 幻觉问题。”

李艺伟最担心的是社区生态风险: “社区里有很多现成‘技能包’, 但开源社区难免有人上传恶意包, 可能窃取 API 密钥、密码, 甚至挟持文件勒索。这有点像以前的电脑病毒。”

如何规避? 三位受访者给出相似建议: 李艺伟的做法是把 OpenClaw 装在虚拟机或沙箱里运行, “哪怕虚拟机被劫持, 影响也有限”。

黄燕燕强调“先学会驾驭再让它处理重要数据”, “重要交易密码、数据先不要存放在它可触及的范围, 对不明来源的 skill 要谨慎”。

陈勇巍则建议普通人“不要急着冲进去”。他说, “现在 OpenClaw 整体比较臃肿, 运行速度和代码架构还处于初级阶段。再等一两个月, 等门槛降低到用起来没什么风险的程度, 那时候再用比较好。”

正如工信部建议, 部署 OpenClaw 时需充分核查公网暴露情况, 关闭不必要的公网访问, 完善身份认证、访问控制、数据加密和安全审计。

AI“龙虾”确实香, 但别忘了——先给自己的数据安全上一把牢固的锁。