岂止“龙虾”

——智能体热的冷思考

记者 岳付玉 苏晓梅

进入3月以来,“全民养龙虾”迅速引爆舆论场。“全民”之说虽不无夸张,却也显示出人们对以“龙虾”(一个名为OpenClaw的开源智能体)为代表的智能体无比好奇与接纳。

短短两三周,从硅谷极客到中国大厂,从硬件抢购到政府补贴“算力券”,这只“龙虾”红到发紫。紧接着,安全漏洞被曝出,国家级预警也接踵而至。央视“3·15”晚会给这场狂欢再度降温:据其曝光,给AI(人工智能)大模型“投毒”已成产业链。而“龙虾”的本领恰恰就是调用各种大模型。

一边是拥有日益聪明的“数字助理”的诱惑,一边是可能被其拖入高风险泥潭的恐慌,智能体下一步会怎样?我们该如何拥抱它?

Ⅰ 全民兴起“养龙虾”热

3月的AI圈里,人们茶余饭后的社交话题产生微妙变化,很多人互相问候时的开场白不是“你吃了吗”,而是“你‘养龙虾’了吗”。

此“龙虾”非彼龙虾,它是人们对AI Agent(人工智能代理,简称智能体)OpenClaw的亲切称呼。它其实很“幼小”——是奥地利程序员彼得·斯坦伯格开发的,2025年11月才面市。跟豆包等大模型不同,它不是只会陪人聊天等的对话框,而是能自主操作浏览器、修改代码,甚至替你支付的“数字生命体”,能像真人一样写周报、整文档、盯股票……

360集团公司创始人周鸿祎透露其公司里一名员工的“养龙虾”片段:该员工给自己电脑里养的“龙虾”提了一个要求,让给他拍张照片。“龙虾”是没有拍照能力的,它就在网上搜了半天,之后在GitHub(代码托管平台)下载了一个能控制电脑摄像头的开源软件,然后把软件下载并运行起来,拍了张照片、发到他的飞书里去了。

谁不想拥有一个又听话又能干的帮手呢?一时间,上至退休工程师,下至毫无技术背景的小学生,人们争相养起“龙虾”。普通人想“养龙虾”,要跨过命令行代码调试等门槛。这足以劝退大多数人的技术鸿沟,恰恰成了生意切口,闲鱼、小红书等平台上,代装“龙虾”的广告比比皆是。有人自称靠代装服务月入数万元。

大品牌免费帮用户装“龙虾”,进一步助燃“养龙虾”热。

3月7日,深圳腾讯总部大楼外“免费装龙虾”活动吸引了大量人群排队;11日,杭州智谱科技有限公司上线本地版“龙虾”AutoClaw,并推出免费安装服务,也让杭州西湖边排起长队,很多人提着电脑来线下安装“龙虾”;14日,深圳机器人剧场,由深圳龙岗区联合Kimi(大模型公司)共同打造的“千人龙虾大会”活动开场近一小时后,入口处仍有众多进入报名候补名单的市民等待开放名额入场。

这轮热潮还带火了硬件市场。由于OpenClaw需要常驻内存来保持“长期记忆”和“多步规划”,苹果Mac Mini M4主机凭借良好的性能和价格优势瞬间脱销。据说,其小巧的铝合金盒子是运行OpenClaw比较稳定、安静的载体,因此也被戏称为“龙虾缸”。在一些二手平台上,“龙虾缸”溢价一度超过30%。

Ⅱ 大厂入局与资本助推

“养龙虾”的卡位战还蔓延到一些地方政府。3月7日,深圳龙岗区率先发布“龙虾十条”,为OpenClaw的开发者提供高达200万元的直接补贴;无锡高新区紧随其后,9日,发布12条“养龙虾”政策,单项支持最高达500万元……这些地方政府敏锐地意识到,谁能留住相关人才,谁就有可能拥有下一代自动化产业的高地。

嗅觉敏锐的资本,也第一时间将“极客的玩具”迅速转化为“大众的商品”。互联网巨头们精准地捕捉到普通用户对OpenClaw“想用却不会配、怕中毒、没显存”的痛点,精准挥刀,生怕落后。比如,百度利用其强大的算力储备,把OpenClaw托管在云端,同时推出低门槛“养龙虾”服务,为普通用户提供17.8元/月的套餐,这可比动辄4位数的硬件投入划算;字节跳动推出的ArkClaw(一款智能体)基础版甚至打出9.9元/月的试用价,其内置了剪映和抖音的专用接口,只要给它素材,就能自动帮你剪辑、对齐卡点并发布。

对于坚持“本地养龙虾”的用户,大厂也通过卖算力和Token(词元)成为“龙虾”的“饲料供应商”,赚取流量收入。比如阿里推出的JVS Claw(阿里版OpenClaw产品),虽然软件免费,但接入通义千问等大模型按量计费,每100万Token收取几元到几十元不等。

针对那些“敢爱不敢用”的大中型企业,大厂通过私有化部署确保安全与合规。腾讯推出的腾讯版“小龙虾”WorkBuddy针对个人版免费,但带有防数据外泄、内网穿透加密等功能的企业增强版则按人头收费,通常是数百元/年/人。

与此同时,一种名为“一人公司”(OPC)的商业模式也迅速兴起。一名设计师通过“养”3只不同职能的“龙虾”,就能完成过去一个工作室的工作量,其中一只负责搜集素材,一只负责生成草图,一只负责对接合同,这种生产力释放带来了巨大的商业吸引力。3月17日,阿里巴巴抢先发布OPC十大行业解决方案,覆盖电商、知识类博主等场景。以一人跨境电商为例,传统模式下,一位跨境电商从业者每天需要手动浏览亚马逊热榜、在1688平台上搜索比价、制作多语言营销视频等,每一步都是大量的手动操作和重复劳动。新的解决方案,通过AI运营系统,核心环节耗时可从一周压缩到一个下午。

在全民“养龙虾热”的背景下,A股市场相关概念股也借势发力,其中算力租赁板块表现一马当先,优刻得、青云科技、顺网科技等热门股股价在3月6日至10日短暂大幅上扬。

随着“龙虾”应用场景不断拓宽,对应的算力需求持续攀升。3月9日,来自天津高新区的国家超算互联网平台表示,依托由中科曙光scaleX万卡超集群(中国自主研发的超大规模AI智能计算基础设施)等构建的庞大国产AI算力池,超算互联网可为用户提供高稳定性、高性价比的国产算力支撑。用户可根据任务规模,灵活选择多种模型的API(应用程序接口)调用服务,并接入飞书、企业微信客户端使用。3月11日,国家超算互联网平台又宣布:面向全体OpenClaw用户,为期两周免费发放每人1000万Token额度福利。此举旨在解决用户在使用OpenClaw时遇到的高成本痛点,助力智能体在全社会层面的普及与应用。

Ⅲ 信任危机与数据泄露

从“全民养龙虾”到大规模卸载,情况急转直下,也就一周左右时间。

3月的第二周,一场名为“ClawJacked”的安全风暴,让无数“养龙虾人”彻夜难眠。安全专家发现,由于OpenClaw需要接管用户的系统权限和WebSocket(一种通信协议)连接,存在一个致命的设计缺陷。攻击者只需诱导用户点击一个链接,就能在后台无感地劫持本地运行的“龙虾”。你的数字助理会在瞬间变成黑客的“内鬼”,帮他们读取你的私人邮件、导出你的浏览器密码,甚至用你的银行账户转账。有用户让OpenClaw“清理一下邮箱里的垃圾广告”,结果由于语义理解偏差,“龙虾”把过去3年的客户往来邮件全删了,且无法撤回。

由于发生了多起因OpenClaw误操作导致的企业数据泄露事件,包括微软、Meta(美国科技巨头)以及国内数家大型商业银行在内的机构,很快发布了紧急内部通告:严禁在办公内网运行OpenClaw。

3月12日,南开大学党委网信办发布风险提示,提醒师生谨慎使用此类高权限应用。国内已有多所高校陆续跟进,要求防范OpenClaw安全风险。

3月14日,中海油一位负责信息技术的人士也向记者证实:“我们上周明确接到集团通知,自己在电脑里养个人‘龙虾’可以,但严禁拿单位信息去投喂,不允许在公司‘养’。”

社交媒体上风向大变,原本炫耀“龙虾”的用户开始发布卸载教程。人们这才发现,将电脑的最高控制权交给一只“龙虾”,风险成本远超其带来的便利。“卸载OpenClaw、QClaw、KimiClaw、JVSClaw、WorkBuddy、ArkClaw,上门卸载,包干净。”有人甚至将这一串带有戏谑口吻的“广告”做成视频。

面对这场突如其来的退潮,行业专家纷纷给出理性建议。周鸿祎在亲自“养龙虾”、看人“养龙虾”之后,深有感触地说,目前是“小龙虾”快速成长期,就跟电脑、手机刚出来的时候一样,很多东西都不成熟,大家一定不要在办公内网养,可以搞一个测试环境来使用。“别一开始就把‘龙虾’放到自己家的‘金鱼池’里,万一把你‘金鱼’都吃完了怎么办?先单独找个‘水盆’把它装起来、养熟了再说。”他建议,“比如你找个旧电脑来试用一下。另外,别让自己的‘龙虾’乱出去加群,到群里可就控制不住了——如果群里别人教你的‘龙虾’干坏事,它可真区别不了是主人的指令还是别人的。”

国家互联网应急中心3月10日发布的《关于OpenClaw安全应用的风险提示》也指出,其风险主要包括提示词注入风险、误操作风险、功能插件投毒风险等,严重者可导致核心数据泄露。这都提醒我们,在拥抱新技术的同时,必须时刻紧绷安全这根弦。

Ⅳ “吞金兽”助推卸载潮

如果说安全漏洞是压垮信任的“致命一击”,那么高昂的运营成本则是劝退普通用户的重要原因。以为“养龙虾”像养电子宠物,结果是养了头“吞金兽”,这是不少“养龙虾人”的真实感受。部署成本只是开始,真正费钱的是“虾粮”——Token,其也成为今年最昂贵的“数字饲料”。

有用户晒出后台记录:分析一份行业报告,AI每思考一步就“复读”3万字背景资料,10分钟“烧掉”50万Token,相当于200元。更令人焦虑的是“不可控性”,OpenClaw全自动运行,用户无法实时监控Token消耗,有人让AI抓取行业数据,结果程序陷入循环,6小时“烧掉”9000万Token,相当于1172元;有人忘记开启“缓存模式”,尤为“烧钱”——总不能“努力打工养AI”吧,于是一些“养龙虾人”不得不卸载了事。

对于技术小白们来说,既无法配置复杂的防火墙和沙箱环境,也难以承受不可控的Token消耗,也唯有“卸载保平安”。

Ⅴ 从技术狂欢到产业价值沉淀

岂止“龙虾”,3月17日,阿里巴巴发布全球首个企业级Agent(代理)平台“悟空”,开启邀测,并将其直接内置到超2000万个企业组织的钉钉之中。

钉钉首席执行官陈航表示,过去是人用钉钉来工作,未来是AI用钉钉来工作。他解释说:“‘悟空’不是‘个人玩具’,它从第一天起就是为企业设计的:内置企业级运行环境,能自动继承企业权限规则,所有操作在安全沙箱中运行,Token消耗和成本一目了然。别的平台解决的是让AI能干活,‘悟空’解决的是让AI在企业里安全、可控、算得清账地干活。”

有意思的是,从全国各地跑去一睹“悟空”风采的人,问得最多的一句话还是“这是钉钉版的‘龙虾’吧?”陈航笑答:“这是一支24小时工作的‘龙虾军团’!”

一时间,“龙虾”成了AI Agent的代名词。“我认为这是‘龙虾’最大的贡献。”周鸿祎的话代表了很多人的观点。之前一说AI Agent或“智能体”,寻常百姓总是一头雾水,现在好了,原来是像它这样的可以帮干活的数字助理。从这个意义上说,“龙虾”成功地完成了对大众的市场教育,其历史价值已远超其作为一个具体产品的价值本身。

然而,当我们剥开热闹的表象,清华大学信息与计算科学专业的大学生小任引述其老师刘知远教授的观点,智能体要发挥全部效力,需要拿到你数字生活的核心底牌。你越希望它替你做更多事,就越脆弱。

那么,这场全民狂欢究竟是短命的泡沫,还是新时代的序章?

资深人工智能投资专家、网经社电子商务研究中心特约研究员郭涛认为,当前“养龙虾”的走红更偏向于一场阶段性技术应用热点,而非成熟的AI终端形态。其核心驱动力源于开源技术的普惠性与用户的尝鲜需求。但企业的蜂拥而至暗藏产业过热的风险,多数产品只是在现有硬件上简单植入开源代码,既无核心算法突破,也未解决兼容性、稳定性等基础问题。这种“蹭热点式”跟风,有可能是对技术趋势的误判。

不过,一向把“风险”二字挂在嘴边的周鸿祎,对“龙虾”等智能体的发展前景仍持乐观态度:“不发展才是最大的不安全!”他补充道:“大模型也有很多安全问题,我们不能因为它有安全问题就因噎废食。”

“龙虾”类项目的真正价值,或许正在于它用一场全民实验,为我们揭示了通往AI终端的必经之路。

那么,未来真正有潜力的AI终端形态会是什么?答案指向了“具身智能”。

小任解释说,具身智能能感知物理环境、具备行动能力、可理解人类意图。与“龙虾”类虚拟智能体相比,其以软硬件深度融合为核心特质,能依托传感器精准捕捉温度、光线等物理环境数据,凭借机械执行系统完成抓取、位移等具象动作;它能深度契合场景语境,精准洞察人类需求。例如,在家庭场景中,具身智能体能根据用户表情判断情绪,自主调整室内温度;在工业场景中,它能通过视觉识别发现设备异常并主动维护。

在以色列历史学家、《人类简史》作者尤瓦尔·赫拉利看来,我们正在创造的是一种与人类截然不同、甚至完全陌生的“异类智能”。他在2025年的上海外滩大会上警示:“真正值得担心的不是技术本身,而是为了竞争优势不顾安全边界地部署技术。”

因此,当我们站在“龙虾”的肩膀上眺望未来,既要保持周鸿祎所说的“不发展才是最大不安全”的进取心,也要坚守“不管跑多快,安全不能忽视”的底线。这场始于一只“龙虾”的狂欢,最终将把我们带向何方,取决于我们如何平衡创新与风险、如何从这场实验中汲取智慧。