然语言指令规划步骤、自动执行复杂任务的‘数字员工’。”

“以往的AI大模型即便技术再成熟，也始终局限于各自的领域，无法实现跨领域的协同运作，而‘龙虾’的核心优势在于其打通了不同领域的大模型壁垒，真正调动起所有大模型的功能与价值。”于静雯解释道，“因此，可以说OpenClaw对于AI行业来说，是具有桥梁性、纽带性的颠覆性创新。”

热潮之下，不少地方积极响应。据不完全统计，截至3月12日，深圳龙岗区、无锡高新区、合肥高新区、苏州常熟市、南京栖霞高新区、杭州萧山区等多地出台“龙虾”的相关支持政策，还有一些地方政府推出面向公众的“小龙虾”免费部署服务。

“龙虾”暗藏多重安全隐患

全民“养虾”的热情之下，第一批尝试者的体验却并非都是好评。

“整体来说感觉不如网上宣传得那么神奇。”李垚坦言，用好“龙虾”需要开放电脑上各类应用的控制权限，出于谨慎他没有打开过多权限，因此觉得“效果有限”。

于静雯分析，OpenClaw的核心能力在于对各类应用、工具的操作与控制。而想要实现这一功能，使用者必须向其开放大量的应用授权，包括邮箱、办公软件、各类平台后台等。“这就好比你想请人把家打扫干净，就得把家里所有房间的钥匙交给对方。”她比喻道，相应地，全量的应用授权可能会给部署“龙虾”的个人和企业带来数据泄漏风险。

3月10日，国家互联网应急中心发布的《关于OpenClaw安全应用的风险提示》（以下简称《提示》）中明确指出，为实现“自主执行任务”的能力，该应用被授予了较高的系统权限。然而，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。

《提示》显示，截至目前，OpenClaw已公开曝出多个高中危漏洞，一旦这些漏洞被网络攻击者恶意利用，则可能导致系统被控、隐私信息和敏感数据泄露的严重后果。“对于个人用户，可导致隐私数据（如照片、文档、聊天记录）、支付账户等敏感信息泄露；对于企业，可导致核心业务数据、商业机密泄露，造成难以估量的损失。”于静雯分析说。

北京市汉鼎联合律师事务所执业律师周子川表示，为完成用户指令，“龙虾”在没有控制权限的情况下，可能在全网直接或间接收集大量各类数据，其获取数量、访问权限、数据敏感程度等，往往超出用户控制范围，严重的可能构成非法获取计算机信息系统数据罪、侵犯公民个人信息罪。

“此外，目前很多用户为了图便利，找第三方花钱部署‘龙虾’，但这些第三方未必具备安全防护条件，极易导致设备数据暴露，攻击者可通过恶意代码执行等方式远程控制设备，窃取敏感信息。”周子川补充道。

热潮之中，更需守好安全底线

今年的政府工作报告提出，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。

“‘龙虾’的出现，为AI智能体的落地应用提供了新路径。若能规范使用，就能很好发挥现有AI智能体的作用，大幅提升个人和企业的工作效率。”于静雯表示，推动“龙虾”良性发展，关键在于平衡便利与安全。

“‘龙虾’等AI智能体呈现出的新技术特征，使现有的关于AI的法律问题更加复杂。”周子川举例说，如最重要的“权责归属模糊”问题，当“龙虾”等AI智能体基于用户指令执行操作并造成侵权或其他违法违规行为时，开发者、部署者、使用者之间如何归责、确定责任的大小，需要法律进一步明确。

对于AI产品的开发者和服务提供者，周子川建议，一方面，应积极履行个人信息保护法等规定的合规义务，如数据处理日志满足日志留存和可追溯的要求。另一方面，在具体操作中也应增强法律合规意识，如加强AI权限管理、加强提示词审核等，降低安全风险。

国家互联网应急中心发布的《提示》也给出具体建议：相关单位和个人用户在部署和应用OpenClaw时，应对运行环境进行严格隔离，使用容器等技术限制OpenClaw权限过高问题，同时严格管理插件来源，持续关注补丁和安全中心。

“用户在‘养龙虾’前，首先要全面评估其价值与风险，判断自己是否真的需要它解决问题，再决定是否部署。”于静雯提醒，使用过程中，也务必做好数据分区和隐私保护，“不盲目跟风，将自己的隐私和数据安全暴露于风险之中”。

编辑/燕子（hchwyx7810@sina.com）