欢迎扫码订阅
《科普时报》

科普时报

2025年12月5日
星期五
第412期
今日16版

科技日报社主管主办　科普时报社出版　国内统一连续出版物号CN 11-0303　代号1-178

壶口瀑布出现“双彩虹”

受上游水库调节放水影响，位于山西吉县和陕西宜川县交界处的黄河壶口瀑布水量增大，飞溅的水雾在阳光照射下形成“双彩虹”，吸引了众多游客。图为12月3日在黄河壶口瀑布景区拍摄的“双彩虹”景观。　新华社发　吕桂明　摄

AI嵌入系统，你的手机还安全吗

□ 科普时报记者　陈　杰

这两天，直接把AI大模型塞进操作系统的“豆包助手”手机，火出圈了！

这款头顶“系统级AI”光环的手机，一上架就“秒空”，二手平台售价翻倍也一机难求。只不过，人们看中的并非手机本身，而是好奇系统级AI真能“看懂”屏幕，并跨APP协同“干活儿”吗？

“系统级AI，其实是将以往装在手机里的AI应用，直接‘种’进系统层，也就是现在手机厂商争相发力的‘端侧大模型’。”赛智产业研究院院长赵刚解释，过去的AI助手像是手机里的“房客”，仅在APP里活动；系统级AI更像是“管家”，手握系统级权限，能直接调动手机核心功能，跨APP完成复杂任务。

这些“管家”的“超能力”，源于智能体（Agent）技术的广泛应用。它能通过分析屏幕的文本、图像信息，结合语音指令理解用户意图，并自动将诸如“下周一想去上海”等简单指令，拆解成查机票、订酒店、做攻略等一连串子任务，再模拟或调用系统的点击、输入等操作，依次打开各APP，把事情一一办妥。

更贴心的是，这些“管家”从不添乱。“由于是嵌入操作系统，它要么是一个小悬浮窗，要么在后台默默处理任务，完全不影响手机的正常使用体验。”赵刚说。

只是，面对如此聪慧的AI助手，人们很难不对其“忠心”起疑：自己的聊天记录、支付密码等敏感信息，真的不会被AI获取和利用吗？

中国信通院数安智库专家曾令平坦言，系统级AI确实存在多重风险。“顶格的系统权限如同开‘后门’，可读取屏幕上的所有信息，包括各种隐私数据；模拟点击功能可能被恶意利用，威胁资金安全；部分厂商权限开通不透明，责任划分模糊，也会放大安全隐患。”

“不过也别太担心，规范AI的‘围墙’一直在修建中。”曾令平说，技术层面，数据脱敏、差分隐私等保护手段正被广泛应用；系统级AI涉及支付等关键操作时，也会要求用户手动点击确认；聊天记录等关键信息，只有得到授权后才会本地化存储，不会上传云端；手机出厂前，也会默认遵循“最小权限原则”。政策法规层面，从《生成式人工智能服务管理暂行办法》到《人工智能安全治理框架》，也都在给AI“立规矩”。

事实上，系统级AI因数据可本地化处理，比AI应用更具安全优势，这也是手机厂商加码端侧大模型的原因之一。

“豆包的入局，让这一赛道有了‘软硬结合’新动能，会吸引更多AI厂商跟进。”赵刚认为，这也将加速“未来手机”的成型——它们会成为仅保留人机交互与可视化功能，用于AI推理的边缘节点。也会将各类APP“降级”为可被调用的功能模块或服务，甚至完全消失。

最新消息显示，包括微信及多家银行客户端在内的APP已明确拒绝“豆包助手”手机登录，理由是存在安全风险。只是，很多人并不认同这一解释。

本期导读

编辑：陈　杰　美编：纪云丰　编辑部热线：010-58884135　投稿邮箱：kepushibao@kepu.gov.cn　印刷：新华社印务有限责任公司