委员在这里

全国政协委员周鸿祎建议：
支持中小企业低成本构建垂直领域智能体

3月4日，全国政协委员、360集团创始人周鸿祎围绕人工智能高质量发展提出他的建议。

他认为，我国人工智能产业正逐步形成“电力-算力-智力-人力-安全力-生产力”协同推进的“六力模型”，为“人工智能+”行动落地夯实基础。围绕这一体系构建，周鸿祎今年重点关注推理算力布局优化、智能体公共服务平台建设以及安全智能体规模应用等方向。

在周鸿祎看来，电力优势正持续转化为通用算力。通用算力分为训练算力和推理算力，但算力本身并不直接创造产业价值。只有消耗推理算力运行的智能体，才能将通用模型能力转化为懂行业、懂场景的“专用智力”，再由“懂AI又懂业务”的专业人才进行规划与治理，并在安全能力护航下运行，最终形成稳定、可持续的生产力。在这一转化链条中，智能体成为连接各要素、推动生产力形成的关键引擎。人工智能已从“大模型能力竞争”迈向“智能体规模应用阶段”。

周鸿祎
360集团供图

> 周鸿祎认为，相关部门应支持兼具“安全+AI”能力的企业打造安全智能体产品，在重点领域批量部署，推动场景化应用。

优化推理算力布局：夯实智能体发展底座

随着百亿级智能体进入产业场景，推理算力的重要性日益凸显。当前我国训练算力稳步提升，但面向推理任务的专用集群仍存在结构性缺口，专用推理芯片能力亟需突破。

围绕这一问题，周鸿祎认为，应在全国一体化算力体系框架下出台推理算力布局指导政策，建立“全国统筹+区域细化”的布局体系，在重点产业区域建设低时延、高密度的推理算力集群，通过调度机制提升资源利用效率。同时鼓励专用推理芯片国产化发展，实现产业链自主可控，支撑智能体技术的深度应用。

智能体规模化落地仍面临三方面挑战

在调研中，周鸿祎发现，智能体规模化落地仍面临三方面挑战：一是技术转化门槛较高，通用模型难以直接融入企业业务流程；二是安全保障能力不足，智能体参与关键业务操作，风险管控难度提升；三是复合型人才储备不足。

针对上述问题，他指出，应实施技术与人才“双线赋能”，由相关部门牵头建设普惠型智能体公共服务平台和智能体课堂。平台集成模型能力与行业工具，提供全流程服务，支持中小企业低成本构建垂直领域智能体。同时推行“以模治模”的安全防护机制，发布安全智能体场景适配指南，开展技能培训与认证，培养“既懂AI又懂业务”的专业人才。

推行“以模治模”：用AI治理AI

在“六力模型”中，“安全力”是保障体系稳定运行的重要一环。周鸿祎指出，当前安全领域面临三方面挑战：一是传统安全体系智能化水平不足；二是“黑客智能体”兴起，网络攻防形态从过去的“人和人”对抗升级为“人和机器”的不对称对抗；三是AI自身风险加剧，一旦与业务系统深度结合，可能带来更复杂的安全隐患等问题。

他认为，安全行业亟需转型，加快推行“以模治模”，用AI治理AI。相关部门应支持兼具“安全+AI”能力的企业打造漏洞处置、攻击溯源分析等系列安全智能体产品，在关键信息基础设施、工业互联网等重点领域批量部署，推动场景化应用。同时鼓励行业龙头企业联合科研机构创新，将具备实战能力的安全智能体产品纳入优先采购目录，推动规模化应用。

周鸿祎表示，人工智能已进入体系化协同阶段。只有在夯实基础能力、完善应用生态、强化安全保障的基础上，统筹推进各要素协同发展，才能不断提升产业转化效率，推动人工智能高质量发展。

华西都市报-封面新闻记者 雷强

全国政协委员张云泉：
建议行业主管部门将终端智能体纳入监管范围

3月4日，全国政协委员、中国科学院计算技术研究所研究员张云泉接受华西都市报、封面新闻记者专访时表示，建议补贴消费者购买智能体订阅服务，由政府与人工智能企业共担成本，还可探索将提升职业技能相关的编程辅助、研究工具等AI应用支出看作职业教育，列入个税专项附加扣除。

从DeepSeek横空出世到Seedance炫酷刷屏……人工智能迎来爆发式发展，正进入以智能体为重要形态和应用载体的新阶段，驱动经济社会实现更深层次、更广范围的转型升级。

张云泉认为，我国智能体应用在个人工具、移动生活、企业服务等多个领域已展现出蓬勃活力，相关技术与商业创新不断涌现。构建一个规则有序、协同高效、安全可控的智能体生态，是关乎人工智能国家战略落地的关键。

智能体生态面临商业困难 建议加大落地引导和支持

智能体作为新兴业态，张云泉认为其整体生态构建仍面临商业化困难、协同规范不完善、安全基础不牢固等基础性、结构性挑战，制约了产业的健康、可持续与高质量发展。

比如，在C端智能体方面，个人用户付费意愿远低于海外，国内绝大多数产品为免费使用，而国外通常为每月20美元的订阅服务模式。

他举例，以OpenAI为例，其2025年的200亿美元营收中，有不少是由1500万-2000万付费用户所贡献，显著高于国内。

而在B端行业应用方面，我国企业用户更倾向本地化部署和定制化开发，导致MaaS（模型作为服务）等智能云服务市场难以规模化，极大限制了大模型企业的盈利能力。

张云泉建议，通过政策引导、补贴等方式，大力培育个人及企业应用市场。对企业应用，建议加大对智能体行业落地的引导和支持，在非敏感领域减少私有化部署，鼓励央国企采用MaaS等方式，构建智能体应用生态。

张云泉
受访者供图

> 张云泉建议，规范数据采集和使用边界，禁止无差别读取手机、电脑等屏幕内容，确保采集范围与具体功能相匹配。

直接与手机屏交互存在风险 应制定智能体互操作性标准

当前，部分智能体使用直接与手机屏幕上的应用界面进行交互（GUI路线，即图形用户界面操作），来完成跨应用任务（如一句话点餐、订酒店和购物比价等服务），一定程度上提高了用户使用效率，创造了新体验。

但业界专家提醒，类似做法若不通过应用官方提供的标准连接和开发者许可来实施，会带来生态和安全风险。

张云泉建议相关部委指导行业协会牵头，参考国际主流的智能体通信协议（如MCP、A2A等）与意图框架接口标准，组织产业各方共同制定智能体互操作性标准与行业公约。

比如，标准应明确要求，无论采用图形界面（GUI），还是通过官方应用编程接口（API）实现功能，禁止任何形式的权限滥用和模拟操作绕过授权。

此外，对通过标准认证的产品给予政策支持，同时推动建立价值共享机制，鼓励终端厂商通过流量回馈、数据协作等方式与开发者共享生态收益。成熟的标准应积极推动上升为国家标准，并参与国际标准制定，从而构建规则统一、接口开放、利益共享的可持续发展生态。

以截屏方式过量搜集用户数据 应禁止无差别读取手机等内容

在智能体应用落地过程中，仍存在个人信息保护与数据安全意识不强的问题，部分企业将产品创新凌驾于个人隐私与数据安全保护之上。张云泉透露，尤其是部分终端智能体以截屏方式过量搜集用户数据、敏感数据上云，不仅威胁用户数据安全，更影响大模型产业的国际化发展。

他表示，中美人工智能竞争不仅限于国内市场，更要在全球市场中抢占话语权和主导地位。由于海外主流市场普遍对隐私、安全高度审慎，一些依托于未授权截屏形态的智能体应用极有可能难以出海。

他呼吁强化底线监管，筑牢安全可控的发展基础防线。建议行业主管部门参照国际治理通行做法，将终端智能体纳入监管范围。落实个人信息保护法中对数据处理者的安全主体责任要求，制定细化监管标准或指南，明确大模型企业、终端厂商、应用企业等主体在数据安全上的责任边界。

张云泉还建议，规范数据采集和使用边界，禁止无差别读取手机、电脑等屏幕内容，确保采集范围与具体功能相匹配。构建端云协同场景下的数据安全屏障，形成覆盖端侧、云侧处理及两者协同全过程的系统性安全设计，并推动建立第三方独立检测与核查机制，对厂商的端云协同架构进行周期性安全评估。

华西都市报-封面新闻记者 粟裕