“智能体”首次写入政府工作报告

代表委员关注智能体规模化应用

▶ 本报记者 罗晓燕

“智能体”首次写入政府工作报告。今年政府工作报告提出，打造智能经济新形态，深化拓展“人工智能+”，促进新一代智能终端和智能体推广。全国两会期间，智能体成为代表委员们关注的热点话题之一。

从概念走向实干

智能体是人工智能（AI）领域一个重要概念，是指能够自主感知环境、做出决策并执行行动的智能实体，它可以是一个程序、一个系统或是一个机器人。

“人工智能已从大模型能力竞争迈向智能体规模应用阶段。”全国政协委员、360集团创始人周鸿祎在接受采访时表示，大众对人工智能的认知往往停留在“搜索或通用问答工具”阶段，但如果将AI打造成垂直领域的智能体，赋予其特定思维方式，其专业能力将远超普通人。

在调研中，周鸿祎发现，智能体规模化落地仍面临3个方面挑战：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。

对此，周鸿祎建议，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”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“懂AI又懂业务”的专业人才。

“人工智能正从生成式问答迈向智能体执行新阶段。智能体具备工具调用、跨系统协同、多步骤任务执行能力，正在成为各行业智能化升级的新型生产要素组织方式。”全国政协委员、天娱数科董事长贺晗表示，当前欧美科技巨头已展开智能体生态军备竞赛，试图通过底层协议、开发框架、应用入口垄断产业主导权。对我国而言，抢抓智能体发展窗口期，是巩固上一轮大模型追赶成果、避免生态层面再次受制的关键。

构建安全可控生态

“当前，AI智能体正在从概念走向规模化应用，成为驱动新质生产力发展的关键引擎。然而，不同厂商、不同框架开发的智能体互不联通，生态碎片化严重。”全国人大代表、国宏嘉信资本董事长冼汉迪建议，将智能体通信协议（A2A）及标准研究纳入国家科技战略布局。

具体而言，冼汉迪建议设立“智能体互操作关键技术与标准研究”国家重点研发计划，支持建设“智能体互操作技术国家工程研究中心”；构建协同标准化推进机制，加快研制国标、行标或团标。设立“多智能体协同应用示范项目”，支持龙头企业构建开源开放生态。此外，完善法律、监管与伦理治理框架，建立安全与伦理评估指南，明确主体责任，确保技术发展安全、可信、可控。

“过去的几年，国内基础大模型能力大多集中在自然语言处理和多模态生成上，对支撑高级智能体稳定运行所必需的复杂推理、长链条决策规划与跨系统调度等关键能力尚有不足。”贺晗在调研中发现，当前国内产业界工具接口与组件生态呈现碎片化，“烟囱”式智能体偏多。同时，我国针对智能体行为审计、越权熔断等关键环节缺乏系统的安全标准、监管规则与技术防范工具。

为推动智能体安全有序发展，贺晗提出3个方面建议。

一是强化顶层设计，建设可信智能体运行底座。他建议出台智能体产业创新发展指导意见，设立国家级产业赋能重大专项，采用揭榜挂帅、赛马机制支持产学研协同；在重点行业试点可信智能体运行底座，与生成式AI备案衔接，降低企业合规成本，打造真用管用的标杆案例，引导产业从拼参数转向拼场景、拼价值。

二是推动标准统一工作，打造互操作产业生态。制定智能体接口与互操作标准，明确交互数据格式、权限认证、计费机制等统一标准，打破厂商封闭状态，形成“基座大模型按需调用、终端工具全面开放”的网状生态架构。推动国内标准向国际转化，提升我国在智能体领域的标准定义权。

三是构建包容审慎监管框架，设立智能体安全“沙盒”与权限审计机制。针对具备系统操作执行权限的高级智能体出台安全监管指南，要求建立可追溯决策日志与人类随时干预的“一键熔断”功能；建设行业级“智能体插件与技能安全认证库”，设立行业级“智能体创新应用安全‘沙盒’”，在受控环境内开展前沿测试，在安全可控前提下给予技术创新试错空间。

构建“软硬协同”安全底座 抢占AI发展制高点

▶ 本报记者 李争粉

当前，人工智能（AI）正在以空前的广度与深度成为国家未来竞争力的关键变量。伴随全球主要经济体加快布局“主权AI”，我国如何在激烈的国际竞争中发挥优势、突破核心瓶颈？此话题成为今年全国两会代表委员热议的焦点。

多位代表委员围绕AI安全、算力底座、软硬协同、生态构建等方面建言献策，共同指向以安全为基、以创新为翼、以协同制胜的AI高质量发展路径。

筑牢全域风险防护屏障

“在数字化浪潮与国家战略交汇的关键节点，必须用‘AI+安全’双轮驱动筑牢现代化产业体系根基。”全国政协委员、奇安信集团董事长齐向东表示，网络与数据安全需求正在持续扩张，AI既是提升生产力的核心工具，也是驱动安全行业迈上新台阶的最强引擎。AI与安全互为支撑、攻防互促，实战化对抗场景不断淬炼AI技术成熟度，推动产业在风险与应对的动态平衡中行稳致远。

齐向东表示，AI技术革新在重构IT体系的同时，也带来前所未有的安全风险。AI“投毒”、模型“幻觉”、智能体“武器化”等新型威胁快速蔓延，安全威胁从数字空间向物理世界传导，威胁量级呈指数级增长。愈是面对复杂风险，体系化、实战化的安全防护能力愈加成为刚性需求。

全国人大代表、科大讯飞董事长刘庆峰表示，我国AI产业发展迅速，但仍面临两大突出挑战：首先，模型研发对进口算力依赖度高，国产算力“好用、易用、迭代快”生态不完善；其次，面向下一代AI的交叉前沿布局不足，兼具AI与数学、量子、类脑、微电子等背景的复合型顶尖人才短缺。

激活自主可控核心动能

破解AI发展瓶颈，既要筑牢安全防线也要夯实算力根基。全国政协委员，麒麟软件有限公司党委书记、董事长谌志华表示，算力即资源、智能即生产力，这已成为全球共识。在由算法、算力、数据、产业链与治理体系构成的系统性竞争中，我国拥有超大规模市场带来的场景“红利”、完整工业体系支撑的应用优势、国产大模型快速崛起的技术底气，以及数据中心集群的成本优势，但同时面临高端算力供给不足、底层原创技术有待突破的现实挑战。

“突破高端算力瓶颈，不能依赖单点硬件突围，必须转向体系化协同，充分发挥新型举国体制优势，实现从分散攻关向战略整合跨越。”谌志华认为，其核心路径是强化“算力—系统—应用—模型”纵向贯通，而国产操作系统正是承上启下的关键枢纽。

刘庆峰建议布局国家级人工智能专项，组织国家实验室、领军企业和科研院所协同攻关，加强在国产算力平台上的大模型研发和生态建设。

构建开放共赢全球格局

释放AI最大效能，离不开场景与数据的双轮驱动。谌志华建议，推动国资央企与行业龙头开放全场景数据资源，建设安全合规的国家级高质量语料库与垂直行业知识库；政府引导、市场运作相结合，并依托国产操作系统安全可信能力，打通数据流通壁垒，让AI技术在工业、医疗、交通、金融等真实场景中持续迭代，加速形成“数据驱动、系统支撑、算法涌现”的良性循环，让AI真正赋能千行百业。

AI制图：刘琴

构建自主可控、开放共赢的创新生态，是抢占AI发展制高点的长远之计。谌志华建议国家加大底层根技术研发投入，支持壮大国产开源AI生态，汇聚多方力量协同攻关核心技术，在开放合作中筑牢自主根基。

谌志华表示，要以“国家队”担当加快技术“出海”，依托开源社区提升国际话语权，将中国操作系统与人工智能的技术优势、生态优势转化为全球竞争力，让中国方案惠及世界。

刘庆峰建议，强化在自主可控算力平台上的AI研发和生态建设，布局下一代AI重大专项。研发脑启发的新一代模型架构，实现面向高能耗与可解释性等瓶颈的突破，为我国在下一代人工智能竞争中赢得先机。