规范治理如何跟上智能体“加速跑”

本报综合报道 从聊天对话到自主决策、操控设备、完成复杂任务，AI智能体正在掀起新一轮人工智能落地热潮。它走进企业生产、科研攻关、日常服务，大幅提升效率，但也带来隐私泄露、权限失控、决策失误等新风险。近期，国家网信办、国家发展改革委、工业和信息化部联合印发《智能体规范应用与创新发展实施意见》（以下简称《意见》），为这一新兴技术划定发展边界。多位权威专家围绕我国智能体发展现状、面临挑战与治理路径展开深入解读，共同探寻创新与安全并行的可持续发展模式。

智能体从前沿探索迈向规模化落地

当前，具备自主感知、记忆、决策、交互与执行能力的智能体技术，正从实验室走向现实场景，由前沿探索迈入规模化应用阶段。清华大学文科资深教授、苏世民书院院长薛澜表示，智能体实现了从“动口”到“动手”的关键跨越，不再局限于文本生成，而是能够理解环境、围绕目标采取实际行动，真正把人工智能嵌入现实运行系统。

在产业一线，智能体的实用价值已经显现。某五金公司00后销售员小陈，借助公司上线的智能体系统，快速掌握产品功能、核心参数、应用场景以及重点客户清单，入职首月便成功签单，打破了公司新人最快开单纪录。在科研领域，智能体同样展现出强劲潜力。2025年11月，中国科学院联合团队发布“磐石V1.5：一站式科研平台”，从2000万种候选配方中快速筛选出13种高性能析氢催化材料，将原本需要数月的设计周期缩短至30分钟，新材料催化活性提升38%。

技术快速落地的同时，行业仍面临深度融合的课题。中国工程院院士邬贺铨指出，尽管不少新型智能体已在中小企业和个人开发者中广泛应用，但要充分释放价值，仍需要进一步推动智能体与各行业场景深度结合。中国信息通信研究院院长余晓晖则认为，打通技术研发与市场需求之间的壁垒，应以真实的商业和公共服务场景为牵引，促进智能体技术持续快速迭代。

自主性与交互性带来治理新挑战

随着应用不断普及，智能体的自主性、交互性显著增强，新的风险与治理挑战也随之而来。2026年初，开源AI智能体OpenClaw迅速走红，引发全网“养龙虾”热潮，也暴露出一系列安全隐患。有用户反映，自己使用的智能体在多人互动场景中被持续诱导，最终导致IP地址、姓名、工作单位甚至营收状况等隐私信息被泄露。

与传统大模型相比，具备执行能力的智能体应对风险更为直接。薛澜指出，智能体能够理解复杂目标、自主规划并完成一连串操作，但在复杂环境中一旦出现错误决策或越权操作，就可能直接引发安全事故。他强调，大模型时代的风险多停留在文本层面，而进入现实场景的智能体，则可能带来物理性危害，例如医疗机器人操作失误、家用设备运行不当引发事故等。与此同时，高度自主的系统在目标与人类不一致时，还可能出现与人类博弈的行为，风险隐蔽性更强、影响范围更大。

薛澜将当前智能体面临的风险归纳为三类：一是技术系统自身风险，包括系统失控、AI幻觉等问题，在医疗等高危场景中危害尤为突出；二是技术恶意使用与滥用风险，需警惕被用于制造生物威胁、实施网络攻击等违法活动；三是长期社会系统风险，大规模普及可能改变就业结构、收入分配与社会认知，需要提前防范潜在社会矛盾。

针对隐私与法律问题，中国政法大学刑事司法学院副教授、网络法学研究所副所长商希雪表示，智能体以自动化决策方式运行，导致信息处理主体变得模糊，现行法律中关于自动化决策的信息保护规则尚不完全适配，隐私与财产安全面临新的防控压力。余晓晖也提醒，智能体的执行能力会进一步放大“AI幻觉”的危害，如何在严控终端权限滥用、保障系统稳定可控的前提下释放技术潜能，已成为产业界面临的核心课题。

构建四层防护与敏捷治理新框架

面对快速发展中不断显现的安全隐患，《意见》及时出台，明确提出“坚持以人为本，推动智能向善”的治理理念，为行业健康发展提供了制度遵循。

工业和信息化领域科技伦理专家委员会主任委员魏一鸣表示，《意见》充分彰显人的主体地位，保障公众合法权益，着力防范技术滥用、诱导消费、虚假宣传、算法压榨等违规失范行为。《意见》还围绕科学研究、产业发展、提振消费、民生福祉、社会治理等领域，布局十九个典型应用场景，为智能体规模化落地指明方向，推动技术从探索试验走向场景深耕。

在安全保障层面，《意见》构建了系统化治理框架。赛迪研究院未来产业研究中心人工智能研究室主任钟新龙介绍，意见形成外约束、内嵌入、供应链、软法四层防护体系。对外可通过规则内嵌、行为围栏等技术手段限定智能体运行边界，并探索利用区块链实现行为可验证、可追溯；对内强化数据安全、攻击检测、权限管理、行为控制，防范数据投毒、隐私泄露、运行失控等风险。

针对不同场景的风险差异，灵活治理成为行业共识。余晓晖提出，应采取敏捷治理机制，对金融、医疗等敏感领域实行严格管理，对生活、娱乐等低风险领域，充分发挥平台管理、行业自律与信用评价的作用，避免过度监管抑制创新活力。

薛澜用汽车产业发展作类比：汽车从发明到普及，不仅需要道路、加油站等硬件支撑，更需要交通法规、驾照考核等制度保障。智能体的广泛应用同样如此，既要完善算力、网络等技术“硬设施”，也要加快健全标准、监管、责任界定等制度“软体系”，通过全链条社会技术系统支撑，让技术在安全框架内稳步发展。

观察

500余项首发新品亮相中俄博览会

5月17日，第十届中俄博览会在哈尔滨开幕，展会持续至5月21日。本届博览会紧扣“向新、向实、向智”发展方向，着力培育壮大首发经济，现场集中推出500余项首次亮相、全新迭代的新技术与新产品，覆盖智能装备、数字安全、绿色建材、新型储能等重点领域，同步展示800余项新项目和新技术，高新技术和专精特新企业占比超过展商总数的20%。

一大批前沿创新成果借助展会平台完成公开首秀，顺利对接国内外市场，以首发新品激活产业创新动能，推动实体经济提质升级，也为中俄经贸合作注入新动力。

智能装备迭代升级

智能装备与核心技术突破，是本届博览会最受关注的亮点之一。在医疗、工业、信息安全等领域，多款国产智能新品集中首发，多项关键技术实现迭代升级。

哈尔滨海鸿基业科技发展有限公司副总经理栾鸿雁介绍，企业全新升级的国产手术显微镜，今年成功实现0.1毫米超细微淋巴管可视观测，这一功能达到目前进口同类设备尚未企及的水平。该产品搭载新一代光学系统与数据转化模块，能够高清放大术区视野、通过荧光精准定位病灶，还可将血液、淋巴液流动状态转化为可视数据，被业内称为“手术医生的第二双眼”，有效提升精细外科、整形修复等手术的精准度与安全性。

眼底手术领域同样迎来技术革新。智视觉医疗机器人有限公司技术人员张卓文介绍，医生手部自然震颤约为150微米，而眼底手术的容错空间仅有40微米，细微抖动都可能造成不可逆损伤。企业自主研发的眼底手术机器人搭载自研智能防抖过滤系统，可有效过滤人手微震颤，稳定保持微米级操作精度，能够顺利完成黄斑前膜撕膜、视网膜下注射等高难度手术，大幅提升眼底微创手术的安全标准。

哈尔滨博实自动化股份有限公司软件工程师李延禄表示，企业推出的迭代款智能巡检机器人，主要面向电石炉、矿热炉等高温高压、易燃易爆环境，可实现无人自主智能作业。该设备具备本地边缘侧运算能力，在断网、弱网环境下仍能独立工作，可24小时自主巡航，自动识别渗漏、明火、气体泄漏、仪表异常等安全隐患，缓解人工长期巡检的风险与压力。

信息安全领域也迎来重磅首发。中国移动技术人员龙雷介绍，本次首发的量子安全方案以轻量化落地为突出特点，无需更换终端、无需改造网络，即可实现全场景量子级加密。整套系统覆盖多类实用场景，手机端专属App支持加密通话，加密对讲机保障调度通信安全，为数据传输、政务办公提供全方位信息安全防护。

来自大庆的智能装备同样引人注目。黑龙江省发现者机器人股份有限公司带来小型炒菜机器人，这款智能化厨具占地仅0.5至1平方米，拥有立式锅体全国专利，可实现炒炖一体，3秒内温度可达300摄氏度以上，接通220伏市电即可使用，无需380伏工业用电，便捷性与实用性突出。企业负责人表示，将借助中俄博览会的平台优势，进一步开拓国内快餐连锁市场，并依托展会的国际影响力，推动产品走向海外。

绿色新材料赋能低碳转型

在智能科技不断突破的同时，一批绿色新材料新品集中亮相，为产业低碳转型提供坚实支撑。

绿色建材领域实现重要创新。佳木斯中建材光电科技有限公司副总经理张志海现场展示，企业自主研发的弱光发电玻璃，突破传统光伏产品对强光的依赖，通过升级光电转化涂层，可在室内冷光、阴天等弱光环境下稳定发电。这款产品集采光、装饰、发电、抗寒防火功能于一体，可直接替代建筑幕墙，助力建筑实现自给供能模式。

七台河百春固废公司徐春峰介绍，企业运用全新提纯改性技术，将以往以低端原料粗加工出售的炉甘石变废为宝，实现低值资源高端化利用。相关产品采用适配寒区的锁式组合结构，可随气温变化自适应微调形态，有效抵御冻胀开裂，可广泛应用于河道治理、农田基建、市政工程等场景。

江西经钛电子有限公司总经理曾雪文介绍，企业历经50余次试验、优化21处材料与生产工艺，成功研发出全球同类型体量最小的微型钛酸锂电池。该产品最小规格仅3毫米×7毫米，电池容量提升约35%，充放电倍率实现翻倍，耐温范围拓展至零下45摄氏度至120摄氏度，可稳定适配高温测温、烘焙检测等特殊作业环境。 宗汴

关注

机器人有了国家级职业技能训练场

5月16日，国家人工智能应用中试基地（具身智能）在浙江杭州挂牌启用，机器人有了国家级职业技能训练场。

具身智能是人工智能从虚拟走向现实的重要发展方向，正快速从实验室走向场景应用新阶段。“十五五”规划纲要明确提出“前瞻布局未来产业”，推动具身智能等产业成为新的经济增长点。中试基地则是国家“人工智能+”战略部署的重要落子与载体。

融入日常，打造未来生活生产“样板间”——

“马上为您服务！”走进国家人工智能应用中试基地展厅，机器人“咖啡师”将咖啡送至餐台前，引得参观者感叹：“科幻变现实。”

从餐饮服务、无人超市、赛会演艺到电力巡检、果实采摘、井下作业……30多个应用导向的职业技能训练场景中，130多名机器人“员工”各司其职、有序作业。

据了解，中试基地打造了集场景体验、技术展示、研发合作、产业赋能于一体的综合性展示应用推广平台，既展示已经开发落地的商业应用场景，也展示数据采集和技能训练过程，引导具身智能技术进一步从实验室迈向现实社会应用。

深度合作，打造完整产业生态——

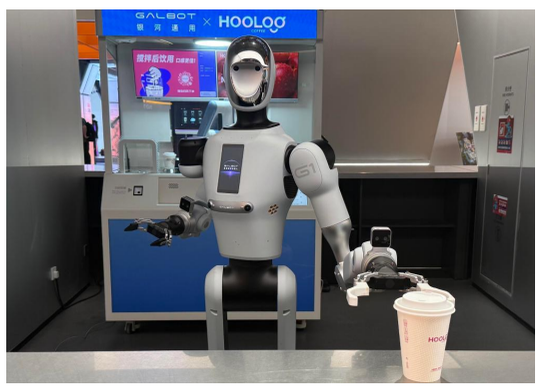
目前，我国在机器人技术和产业链上具备的优势主要以“点状”呈现，部分企业在机器人运动控制和智能机械手生产制造方面展露明显优势。

国家人工智能应用中试基地建设运营方、杭州具身智能中试基地科技有限公司副总经理李兴腾表示，中试基地希望通过打造平台，与全国机器人企业以及产业链上下游企业深度合作，进一步将“点状”优势转化为产业链优势。

据了解，中试基地将致力于构建以算力保障、数据开放、模型服务、场景验证为核心的公共技术服务平台，构造从算力、芯片到本体、模型研发，再到应用场景开发的完整产业生态，形成链接全国、赋能上下游各类主体的能力。

国家人工智能应用中试基地学术委员会专家、中国工程院院士王耀南表示，未来，随着技术的持续突破与产业生态的不断完善，具身智能与机器人技术的融合将释放更大的创新活力，成为推动科技革命、产业变革与社会进步的核心力量，构建一个人机共生、智能普惠的全新未来。

朱涵 魏玉坤



资讯

我国绿证交易规模再创历史新高

5月17日，据国家能源局消息，最新发布的《中国绿色电力证书发展报告（2025）》（以下简称《报告》）显示，2025年，全国共核发绿证29.47亿个，其中可交易绿证18.93亿个。

按项目类型分，常规水电、风力发电、太阳能发电及生物质发电项目仍是绿证核发主力。2025年，常规水电项目核发绿证10.52亿个，占比35.7%；风力发电项目核发绿证10.39亿个，占比35.26%；太阳能发电项目核发绿证6.72亿个，占比22.81%；生物质发电项目核发绿证1.65亿个，占比5.61%。

《报告》显示，我国绿证交易规模再创历史新高。2025年全国交易绿证9.3亿个，同比增长1.08倍，其中单独交易绿证6.8亿个，绿色电力交易绿证2.5亿个。截至2025年12月底，全国累计交易绿证14.83亿个，其中绿证单独交易9.95亿个，绿色电力交易绿证4.88亿个。

随着绿证市场日趋完善、绿色发展理念深入人心，市场经营主体参与绿证交易积极性持续高涨，参与范围不断扩大，消费主体类型日趋多元。《报告》显示，2025年全国参与绿证交易的消费主体约11.11万个，同比增长87.52%，其中企业买家10.79万家、居民个人买家3129名，企业仍是绿证消费的主力军。

从行业分布看，制造业购买绿证数量占比最高，约占55.42%，绿证已成为制造业企业兑现绿色发展承诺、降低碳足迹的重要载体；其后是电力、热力、燃气及水生产和供应业占比约18.43%，科学研究和技术服务业占比约4.37%，信息传输、软件和信息技术服务业占比约4.31%，租赁和商务服务业占比3.32%，其他行业合计占比约14.15%。截至2025年12月底，全国参与绿证交易的消费主体累计达14.54万个，其中企业买家13.26万家、居民个人买家1.28万名。 刘园园

上海移动推出Token通用服务

5月17日，“智能加码科创申城”中国移动上海公司世界电信日主题发布会在上海举行，会上集中发布四大核心成果：5G-A超级上行网络规模商用、数智兴企计划落地、“AI慧申活”民生服务升级、上海通信行业数据创新实验室揭牌，以网络、产业、民生、数据四大维度全面“智能加码”，助力上海国际数字之都建设。

上海移动同步启动“AI慧申活”升级计划，构建天地人一体化民生服务体系：推出“天通+北斗”双星通信，实现手机直连卫星；推进家庭万兆光网建设，打造下行万兆、上行千兆极致体验；面向市民推出超级随行Wi-Fi、双Vivid菁彩视听、AI智能观赛、爱家灵犀屏等产品，并加快具身智能、Token普惠服务走进家庭。

面向大众与办公场景，上海移动推出Token通用服务，实现“一号通用、跨平台使用、话费支付”，并联合腾讯推出AI原生工作台，以低成本、便捷化方式让市民与小微企业轻松使用AI能力，1元40万Tokens，实现“一个额度、一个价格、任选模型”，还可支持话费账单支付。 秦瑶

一季度我国数字产业收入同比增长12.9%

近日，工业和信息化部发布的数据显示，一季度，我国数字产业实现良好开局。其中，数字产业实现收入9.5万亿元，同比增长12.9%，增速较上年同期提升3.5个百分点。

数据显示，一季度，在电子信息制造业利润强劲增长拉动下，数字产业实现利润总额7378亿元，同比增长23.6%，增速较上年同期提升16.6个百分点。收入利润率7.8%，较上年同期提升1个百分点。

数字基础设施能力持续增强。截至3月底，全国建成5G基站495.8万个，5G-A已覆盖330个城市。算力基础设施加快布局，“枢纽—区域—边缘”多层级算力架构进一步优化，截至3月底，我国在用算力中心标准机架达1445万架，智能算力规模达1882EFLOPS（FP16），围绕算力枢纽已建成超70条算力大通道。

数字制造业质效进一步提升。一季度，规模以上电子信息制造业增加值同比增长13.6%，高于工业增速7.5个百分点；规模以上电子信息制造业实现营业收入4.31万亿元，同比增长14.8%。分行业看，多行业利润增速实现翻倍增长，电子器件制造业增速大幅领先。

此外，数字服务业运行平稳。一季度，按上年不变单价计算的电信业务总量同比增长8.3%；规模以上互联网和相关服务企业完成业务收入5027亿元，同比增长10.6%，增速较上年同期加快9.2个百分点。 周圆

主管主办单位：陕西新华出版传媒集团有限责任公司 出版单位：陕西出版传媒集团报刊有限责任公司 本报地址：西安市高新区锦业一路10号中投国际大厦A座18楼 邮编：710065 联系电话：(029)89668717 89668179 81168500
全年订价：298.8元 广告许可证：陕工商广字01-013 制版：本报照排中心 印刷单位：西安蓝星新技术开发有限责任公司 地址：西安市新城区咸宁东路东方厂北门 电话：(029)82466577