

强“智”铸“链” 国产高端装备多点突破

决胜“十四五”收官战之际，我国高端装备产业正在以“智”为刃突破技术壁垒，以“链”为脉畅通全球市场，聚焦关键举措，全力冲刺目标，为制造强国建设筑牢根基。

以“智”破局 攻坚核心技术短板

全球最大吨位全地面起重机械、全球最长陆上风电叶片、16 米级超大直径盾构机、重载铁路“动力之王”的全球最大功率电力机车、国内电压等级最高和容量最大的海上风电电抗器……“十四五”期间，制造业大省湖南涌现出一大批高端装备创新成果。

记者近日从湖南等地行业一线获悉，高端装备产业正集中力量突破关键核心技术瓶颈。在集成电路领域，相关企业持续提升产能与质量，“中国芯”应用比例不断提高，多个关键环节自主可控取得进展。针对航空发动机、深海深空装备等“卡脖子”领域，研发投入持续加大，技术迭代加速推进。

智能制造升级成为重要抓手。数控机床、工业机器人等关键装备自主化水平提升全面推进，汽车、能源等行业成

套装备智能化改造成效显著。三一重能韶山叶片工厂的智能化实践颇具代表性，其采用全智能辅助定位、机器人激光引导等技术，实现叶片生产全流程自动化管理，为行业提供了可借鉴范本。

龙头企业引领作用凸显。三一重工等企业在智能制造、新能源等领域布局新项目，带动行业技术水平整体提升。

“在超级技术窗口期，三一正围绕‘全球化、数智化、低碳化’开启第三次创业，在智能制造、新能源等方面大举投资。”三一重工董事长向文波说。

以“链”聚力 构建协同产业生态

长沙作为全球知名的“工程机械之都”，多家龙头企业在“十四五”期间取得标志性成果：三一重工夺得全球挖掘机销量冠军；中联重科海外营收占比超过 50%；铁建重工成功研制超大直径盾构机主轴承，完成盾构机全产业链自主化的“最后一环”。当前，工程机械企业一边加快高端化、智能化、绿色化转型，一边抓紧布局新赛道、新产品，持续强链、延链、补链。

这是我国高端装备产业构

建协同生态的一个侧影。当前，高端装备产业集群建设呈现强劲势头。记者从湖南省工业和信息化厅了解到，近年来，湖南形成了省、市、县三级大抓产业集群建设的强大合力，国家级产业集群建设取得突破。其中，长沙工程机械等 5 个产业集群成为国家先进制造业集群，15 个中小企业特色产业集群进入国家中小企业特色产业集群，数量均居全国前列。

衡长株潭特高压输变电装备产业集群自入选“国家队”以来，发展提速。集群内特高压变压器、轨道交通牵引变压器等多款产品市场占有率全球或全国领先。湘雁输变电产业服务中心负责人晏华衡表示，特高压输变电装备产业正迎来前所未有的发展机遇，地方政府将抢抓集群入选国家级先进制造业产业集群的有利契机，加大创新投入、完善产业链生态链供应体系，引进更多高端创新项目，培育具有国际影响力的龙头企业。

在国内产业集群建设提速的同时，高端装备国际供应链合作也不断深化。第三届中国国际供应链促进博览会上，中国中车、广汽集团等展示的产业链协同成果，彰显了我国高

端装备产业的体系竞争力。

以“策”助推 多维发力谋突破

新建产线、更新设备、技术改造……走进湖南省衡阳市衡南高新区，多家输变电产业链上的企业里一片繁忙景象。

冲刺收官，各地产业园区加快行动。衡南高新区管委会副主任李孟炎表示，“十四五”规划收官之年，园区将继续加大精准招商力度，做好企业服务，招引输变电产业的重点供应商，增强“特高压输变电”配套能力，进一步提升产业链供应链的完整性。

各地政府也在积极出台政策，比如，黑龙江出台支持高端智能农机装备产业高质量发展若干政策措施，对智能农机企业研发投入给予 50% 上浮补助，支持大马力拖拉机、智能农业机器人等整机及关键零部件攻关，单个项目最高支持 5000 万元；重庆打出“组合拳”推广应用首台（套）装备，促进装备制造业优化升级。

标志性产品接连取得突破，为高端装备产业冲刺“十四五”目标提供了关键支撑与强劲动力。今年以来，我国企业在人形机器人、人工智能

等领域取得的标志性成果，不仅为高端装备产业构建技术底座，更持续释放新质生产力的乘数效应。数据显示，全国已累计培育 421 家国家级智能制造示范工厂，建成万余家省级数字化车间和智能工厂，推进近万家中小企业数字化改造。

北京交通大学中国高端制造业研究中心执行主任朱明皓等专家建议，决胜“十四五”之际，仍要加大对基础零部件和元器件、基础材料、工业基础软件、基础工艺及装备、产业技术基础等“五基”的支持力度，围绕重大装备短板环节开展技术攻关和产业化应用。同时，积极运用人工智能技术，推动“人工智能+装备”迭代升级、换道超车。

同济大学国家创新发展研究院研究员宫超则建议，通过举办“十四五”高端装备成就展及相关论坛，强化行业交流与科创分享，并可考虑将成就展“国际化”，为产业出海提供窗口。

业内人士表示，随着各项举措落地见效，高端装备产业有望圆满完成“十四五”目标，为中国式现代化提供坚实装备支撑。

（《经济参考报》记者 / 吴蔚、白田田）

0.01% 虚假训练文本可致有害内容增加 11.2%

警惕人工智能“数据投毒”

当前，人工智能已深度融入经济社会发展的方方面面，在深刻改变人类生产生活方式的同时，也成为关乎高质量发展和高水平安全的关键领域。然而，人工智能的训练数据存在良莠不齐的问题，其中不乏虚假信息、虚构内容和偏见性观点，造成数据源污染，给人工智能安全带来新的挑战。

数据是人工智能的基础

人工智能的三大核心要素是算法、算力和数据，其中数据是训练 AI 模型的基础要素，也是 AI 应用的核心资源。

——提供 AI 模型的原料。海量数据为 AI 模型提供了充足的训练素材，使其得以学习数据的内在规律和模式，实现语义理解、智能决策和内容生成。同时，数据也驱动人工智能不断优化性能和精度，实现模型的迭代升级，以适应新需求。

——影响 AI 模型的性能。AI 模型对数据的数量、质量及多样性要求极高。充足的数据量是充分训练大规模模型的前提；高准确性、完整性和一致性的数据能有效避免误导模型；覆盖多个领域的多样化数据，则能提升模型应对实际复杂场景的能力。



——促进 AI 模型的应用。数据资源的日益丰富，加速了“人工智能+”行动的落地，有力促进了人工智能与经济社会各领域的深度融合。这不仅培育和发展的新质生产力，更推动我国科技跨越式发展、产业优化升级、生产力整体跃升。

数据污染冲击安全防线

高质量的数据能够显著提升模型的准确性和可靠性，但数据一旦受到污染，则可能导致模型决策失误甚至 AI 系统失效，存在一定的安全隐患。

——投放有害内容。通过篡改、虚构和重复等“数据投毒”行为产生的污

染数据，将干扰模型在训练阶段的参数调整，削弱模型性能、降低其准确性，甚至诱发有害输出。研究显示，当训练数据集中仅有 0.01% 的虚假文本时，模型输出的有害内容会增加 11.2%；即使是 0.001% 的虚假文本，其有害输出也会相应上升 7.2%。

——造成递归污染。受到数据污染的人工智能生成的虚假内容，可能成为后续模型训练的数据源，形成具有延续性的“污染遗留效应”。当前，互联网 AI 生成内容在数量上已远超人类生产的真实内容，大量低质量及非客观数据充斥其中，导致 AI 训练数据集中的错误信息逐代累积，最终扭曲模型本身的认知能力。

——引发现实风险。数据污染还可能引发一系列现实风险，尤其在金融市场、公共安全和医疗健康等领域。在金融领域，不法分子利用 AI 炮制虚假信息，造成数据污染，可能引发股价异常波动，构成新型市场操纵风险；在公共安全领域，数据污染容易扰动公众认知、误导社会舆论，诱发社会恐慌情绪；在医疗健康领域，数据污染则可能致使模型生成错误诊疗建议，不仅危及患者生命安全，也加剧伪科学的传播。

筑牢人工智能数据底座

——加强源头监管，防范污染生成。以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规为依据，建立 AI 数据分类分级保护制度，从根本上防范污染数据的产生，助力有效防范 AI 数据安全威胁。

——强化风险评估，保障数据流通。加强对人工智能数据安全风险的整体评估，确保数据在采集、存储、传输、使用、交换和备份等全生命周期环节安全。同步加快构建人工智能安全风险分类管理体系，不断提高数据安全综合保障能力。

——末端清洗修复，构建治理框架。定期依据法规标准清洗修复受污数据。依据相关法律法规及行业标准，制定数据清洗的具体规则。逐步构建模块化、可监测、可扩展的数据治理框架，实现持续管理与质量把控。

国家安全机关将在以习近平同志为核心的党中央坚强领导下，全面贯彻总体国家安全观，与有关部门一道防范针对我人工智能领域的的数据污染风险，依法维护人工智能安全和数据安全，不断筑牢国家安全屏障。

（据“国家安全部”微信公众号）