用大模型及大模型具身机器人赋能办学整体质量提升

商 桑 副教授

教育部信标委专家组成员，竹渊科技总经理/清智奇点董事长

聘　书

兹聘请　商桑　为全国信息技术标准化技术委员会教育技术分技术委员会专家，任期到 2026 年 6 月 14 日止。

全国信息技术标准化技术委员会

教育技术分技术委员会

二零二五年六月十五日

编号：ZJ202566

一、用AI智能体提升办学质量和效率的历史必然性

二、大模型的分类及专用大模型与通用大模型的功能区别

三、用AI大模型简化数字教材创作和出版流程

四、让拥有AI大模型大脑的实体机器人走进校园

一、用AI智能体提升办学质量和效率的历史必然性

二、大模型的分类及专用大模型与通用大模型的功能区别

三、用AI大模型简化数字教材创作和出版流程

四、让拥有AI大模型大脑的实体机器人走进校园

2025年7月31日国务院常务会议通过：

关于深入实施“人工智能”+行动的意见

· 阶段目标 ·

2027年

率先实现人工智能与6大重点领域广泛深度融合
新一代智能终端、智能体等应用普及率超70%
智能经济核心产业规模快速增长
人工智能在公共治理中作用明显增强
开放合作体系不断完善

2030年

人工智能全面赋能高质量发展
新一代智能终端、智能体等应用普及率超90%
智能经济成为我国经济重要增长极
推动技术普惠和成果共享

2035年

全面步入智能经济和智能社会发展新阶段
为基本实现社会主义现代化提供支撑

· 加快实施6大重点行动 ·

一是“人工智能+”科学技术

加速科学发现进程
驱动技术研发模式创新和效能提升
创新哲学社会科学研究方法

二是“人工智能+”产业发展

培育智能原生新模式新业态
推进工业全要素智能化发展
加快农业数智化转型升级
创新服务业发展新模式

三是“人工智能+”消费提质

拓展服务消费新场景
培育产品消费新业态

四是“人工智能+”民生福祉

创造更加智能的工作方式
推行更富成效的学习方式
打造更有品质的美好生活

五是“人工智能+”治理能力

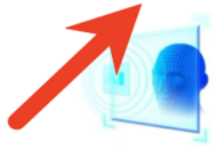
开创社会治理人机共生新图景
打造安全治理多元共治新格局
共绘美丽中国生态治理新画卷

六是“人工智能+”全球合作

推动人工智能普惠共享
共建人工智能全球治理体系

· 强化8项基础支撑能力 ·

提升模型基础能力
加强数据供给创新
强化智能算力统筹
优化应用发展环境
促进开源生态繁荣
加强人才队伍建设
强化政策法规保障
提升安全能力水平



· 组织实施 ·

坚持党的领导贯穿“人工智能+”行动全过程
国家发展改革委加强统筹协调，推动形成工作合力
各地区各部门结合实际抓好落实，确保落地见效
强化示范引领，适时总结推广经验做法
加强宣传引导，凝聚社会共识，营造良好参与氛围

2024年12月微软CEO：

人类全面步入：

AI智能体覆灭SaaS时代

2022年11月30日

ChatGPT诞生

2023年1月（非民用）

2024年9月面向地方：

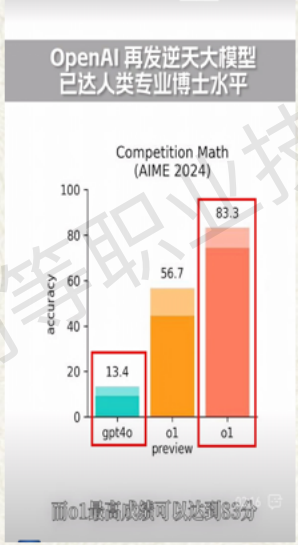
桑梓大模型

2024年9月15日

GPTo1人类专业博士

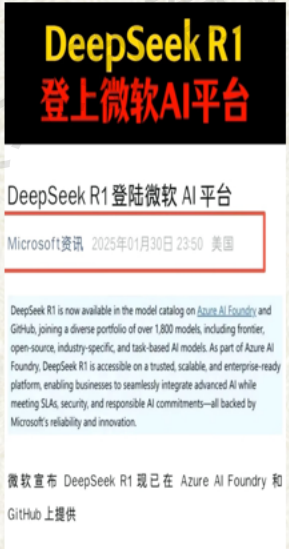
2024年12月21日

GPTo3，智商2倍O1



2025年1月20日

DeepSeekR1等同O3



2025年2月17日xAI的

Grok3，10倍O3

2025年7月10日

Grok4，全面碾压

一、用AI智能体提升办学质量和效率的历史必然性

二、大模型的分类及专用大模型与通用大模型的功能区别

三、用AI大模型简化数字教材创作和出版流程

四、让拥有AI大模型大脑的实体机器人走进校园

大模型分类：

第一类，专用大模型。厂家自研底座，不在互联网运行，为机构建设独用自有底座，软件开源，场景全面，提供定制服务，数据安全。

第二类，通用大模型。厂家自研底座，底座在互联网运行，不给机构提供底座只提供开源模型，不提供定制服务，数据不安全。

第三类，垂类大模型。无自研底座，借通用大模型开源模型，为机构用别人开源模型服务，不提供底座，数据不安全。目前市场多数为此类。(里面再分两方式:机构自己为自己服务，第三方借壳收费为机构服务)——借壳、寄生性质。

第三类的寄生非长久之计。
未来，每个机构都需建属于自己的底座，这样才具有可持续发展力。

中国自主开发的大模型（9+1）（全球公认最好共20个）：

9个通用大模型（底座机构大众共用）
❶文心：百度
❷通义千问：阿里
❸盘古：华为
❹智谱清言：清华
❺元宝：腾讯
❻豆包：字节跳动
❼星火：科大讯飞
❽商量：商汤
❾DeepSeek：深度求索&幻方量化

C端和B端，共用底座，爬数据、不安全
什么都懂些，专、精、准欠缺、不定制

1个专用大模型（底座机构独有、私有）

❶桑梓：奇点

中国唯一自主研发专用，唯一GPT诞生前研发，
唯一有安全对抗功能，唯一不需标注微调

2024年9月军民融合，军转民产品

专业服务院校、出版社等党政机关企事业单位

B端，本地离线部署，私有底座，确保数据安全
突出专、精、准，欢迎定制需求

2024年12月17日:

由中国主导的《ISO/IEC AWI TR 25470 信息技术学习、教育和培训在线课程中的生成式AI应用》的国际标准顺利立项。

桑梓大模型为该项目支撑案例。

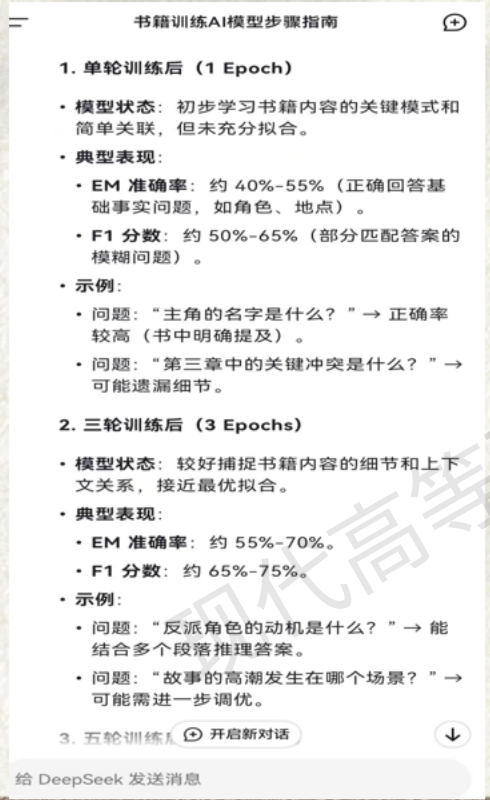
Use cases for ISO/IEC JTC1 SC36 WG9 GenAI from China

There are a total of 8 use cases, each from The Open University of China, Iflytek, H3C, Shanghai Changyun Education Technology Co., Ltd., Seewo, Beijing Lianlan Hongwen Technology Co., Ltd & Hefei Qingzhi Qidian Information Technology C..., Ltd。

Use cases can be divided into four categories: Teaching aids, Learning aids, Education system/platform, Innovative Education Applications。

Teaching / Learning Activities Supported / Pedagogical approaches	• The Sangzi Large Model Platform provides a high-performance distributed computing experience through its independently developed distributed training platform, saving training costs and time, eliminating technical barriers, and achieving a clear distinction between technology development and user application implementation. It has achieved a completely "foolproof" design at the training and application levels, with simple, convenient, and flexible operation. Students can also help teachers complete professional, course, and textbook training work  • Support the integration of various general large and small models, as well as model training through this platform. The trained models can be added to the system for use 


后台系统
用户登录
数据安全与对抗识别系统
文本伪造检测
图像伪造检测
视频伪造检测
对抗样本检测
投毒样本检测
数据脱敏检测



2025年3月16日：

DeepSeek和桑梓学习50万字教材对比：

我问DeepSeek训练50万字书时长：

训练1、3、5轮分别需10、18、30小时。见图。

1、3、5轮训练后回答准确率?

准确率:50%、65%、75%左右。

还需人工干预。

见图2。

用专用大模型桑梓训练50万字书时长：

只需5-10分钟。

不需人工干预，准确率达到95%以上。

马上可出准确率95%的各类题型题库。

		通用大模型（DeepSeek为例）	专用大模型（桑梓为例）
人有我有	逻辑推理能力	达到国际领先水平。	达到国际领先水平。
	生成式AI功能	有。生成图片、视频、PPT等。	有。生成图片、视频、PPT等。
人有我有 人无我有	蒸馏技术	有。但只能蒸馏其他通用大模型，不能蒸馏桑梓。	有。可蒸馏所有通用大模型。
	兼容性	只能接入同类通用大模型，不能接入桑梓。	接入任何通用大模型，可随时把通用大模型的数据拉进来为我所有，但通用却不能把机构数据偷走，内可观外外不能窥内，确保数据安全。
	部署方式、要求部署后的场景	1.部署简单。支持线上和线下部署。 第一，公有云部署，数据不安全。 第二，用开源软件本地离线，可暂时保障数据安全。 2.部署只有聊天功能，没有业务场景。 3.体量重，成本高。开源部署要求高，1万人院校规模同时使用高性能服务器10-20台，10-20个A100GPU 卡才能保障正常运行。	1.部署简单。支持线上和线下部署。 2.数据安全。本地离线部署，永久确保数据安全。系统版本升级已训练模型不需要重新训练。 3.不但有聊天功能，更有丰富具体业务场景。 4.体量轻，成本低。1万人院校规模同时使用，1台高性能服务器和1块A100GPU卡即可满足正常运行。
人无我有	适用范围及底座是否专属	1.C端用户和B端客户。 2.机构和大众共用一个底座功能，无专属底座。	1.专业服务B端客户。 2.机构有专属底座。
	专业性	1.知识面广，所有知识都了解，但行业专业知识专、精、准欠缺。 2.底座算法要求弱于桑梓，不拼算法主要拼数据量及数据质量。 3.原文引用不精准。 4.没人工帮助标注和微调的模型回答精准度不高，60%-80之间。	1.专注教育、出版社行业领域知识预训练，突出专、精、准。能够理解和生成行业特有的专业知识和术语，适用于需要高度专业化的场景。 2.底座嵌入更多算法令行业智能体更聪明，描述行业特征和知识更精准。 3.原文引用精准。 4.不需要标注和微调，回答精准度可达到95%以上。
	行业敏感及专业数据满足度	低。	高。
	解决机构个性化痛点、难点	不提供个性化定制方案，机构痛点难点不能解决。	欢迎个性化定制需求，能解决机构痛点难点。
	模型意识形态安全保障	无。	有。有大模型安全对抗功能，保障模型训练过程中的安全。对违禁言论、违禁富媒体进行前置屏蔽和后置检测。

数据不安全

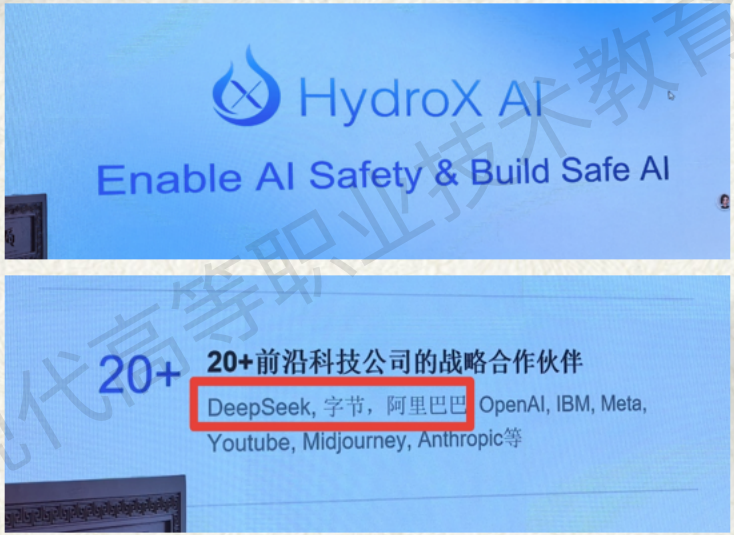
通用大模型

数据安全

专用大模型（桑梓）

大模型诞生后短短3年数据名称变迁：

中国通用大模型多数在用美国软件做系统安全保护：



DeepSeek为首的一体机安全隐患：

1.3月27日国家安全部监控到数据泄露：堵漏洞

2.4月15日中央政治局会议：自强自立

3.4月15日国家安全部：“数据主权”

4.4月17日开始业界精英公开指出DS问题

DeepSeek一体机安全隐患

有领导让我整理一下DeepSeek安全隐患和有关问题，共享一下，请注意看下面各事件的时间节点:

第一，3月27日国家安全部监控到本地离线部署的DeepSeek一体机出现严重数据泄露，专发官微《堵漏洞……》，文中明确“国家监控到90%本地部署的一体机数据在互联网上裸奔。”

第二，针对全国一体机数据严重泄露现象，国家比原计划提前两年，于4月2日紧急全面启动数据资产入表工作，数据资产管理步入法制化阶段。机构数据资产流失已列入法治范畴。只有一把手重视，数据才能安全，国家才能安全。

第三，4月15日中央政治局召开会议，老大强调“中国的人工智能技术必须自强自立。”

第四，4月17号开始，以百度李彦宏为首的业界大佬开始公开批评DeepSeek幻觉严重、不靠谱、答非所问、加戏胡说八道等问题。

第五，大模型发展飞快，用特定时间背景开源的模型所打造的一体机会严重滞后AI发展，也给机构带来新的信息化应用孤岛。

出现严重安全问题原因:

1.DeepSeek的大模型安全由美国的HydroX AI公司提供保护，数据泄露属必然。问题比较严重。

2.DeepSeek开源模型本身安全性能不足，存在漏洞。

3.DS一体机均为以盈利为目的的第三方公司提供，非厂家，没人考虑机构的数据安全问题。

4.春节后国内外个别DS竞争对手大厂开始买办一些小公司专门对DeepSeek进行投毒，每天至少数百万篇垃圾文章投喂，投毒方式多种，还持之以恒。

要想保护数据资产安全：

第一，软硬件本地离线部署是必选项。

第二，建设属于自有独用的大模型底座。

现在出现基模概念，若本地离线且永远不上网、不升级会安全

数据安全国际形势非常严峻

数据资产安全是一把手工程，法制化管理才有效

体制内：国有数据资产流失是违法行为。

体制外：数据资产流失是巨额资金流失。

通用大模型就不能用吗了？不是的，要知道如何用？怎么为我所用用？

用大模型提升办学整体质量提升解决方案：

通用大模型+专用大模型（二者缺一不可）

通用大模型：解决生成式AI的问题（生成教学相关智能体）

专用大模型：解决安全前提下保密资源投喂，办公AI智能化问题

通用大模型——生成式AI：AI助力帮助老师智能生成专业建设、课程建设、教材建设所需内容，结合岗位需求精准匹配人才能力素质需求，结合岗位需求智能生成关键技能点和知识图谱等。

专用大模型——本地资源投喂：不只是是解决教学问题，还包括：教务、学工、办公室、人事、后勤、保卫、财务、思政、第二课堂、招生、就业.....AI数据中台

用专用大模型投喂步骤：

第一，资料准备。
第二，一键上传投喂，不需要学校标注微调。

院校会诞生大模型虚拟机器人集群

专业AI、课程AI、实训AI、教材AI等虚拟机器人群

招生AI、就业AI、人事AI、后勤AI、保卫AI、财务AI……虚拟机器人群

虚拟机器人身份：AI助教、AI学伴、AI部门业务助理.....

AI数据中台：消除孤岛，提供一站式教学及业务咨询和业务办理

一、用AI智能体提升办学质量和效率的历史必然性

二、大模型的分类及专用大模型与通用大模型的功能区别

三、用AI大模型简化数字教材创作和出版流程

四、让拥有AI大模型大脑的实体机器人走进校园

证 书

新闻出版行业标准《数字教材标准体系表》

起草组成员 商桑

全国新闻出版标准化技术委员会

2021年10月

证 书

新闻出版行业标准《数字教育资源评价指南》

起草组成员 商桑

全国新闻出版标准化技术委员会

2022年1月

教育部司局函件

教科信司〔2025〕37号

教育部科学技术与信息化司关于2025年教育信息化标准项目立项的通知

华东师范大学：

2025年教育信息化标准项目经申报材料审查、司局意见征求、专家评审等流程，你单位共有2项批准立项（见附件）。

按照《教育信息化标准化工作管理办法》，请立项项目的标准承担单位填写《教育信息化行业标准项目任务书》并盖章，于2025年5月30日前报送至教育部教育信息化标准委员会。请你单位高度重视标准研制工作，高质量完成标准相关任务。

联系人及联系方式：

清华大学（教育部教育信息化标准委员会秘书处） 杜婧 010-62782391 dujing@tsinghua.edu.cn

教育部科学技术与信息化司 王楚豫 010-66096210

纸质材料邮寄地址：北京市海淀区清华大学建筑馆北504室，清华大学信息化技术中心杜婧（收），100084

附件：2025年教育信息化标准项目立项清单（华东师范大学）

教育部科学技术与信息化司

2025年4月21日

2025年教育信息化标准项目立项清单（华东师范大学）

序号	项目名称	业务指导部门	标准承担单位	标准牵头人	评审结果
1	教育人工智能大模型 总体框架	科技司	华东师范大学	吴永和	立项
2	高校数字教材基础数据	高教司、教材局	华东师范大学	钱冬明	立项

中国的AI数字教材

纸质教材——数字教材——AI数字教材（AI教材），泾渭分明三个时代

中国数字教材发展的三代：

第一代：电子书。基于互联网技术，2008年。电子书号。SaaS服务。

第二代：数字教材。基于云计算、互联网等技术，基本上均有版权保护功能。2013年12月诞生。电子书号。SaaS服务。

第三代：AI数字教材。基于AI大模型技术。2025年2月诞生。纸质书号、电子书号均可。AI智能体服务。

第三代：AI数字教材（AI教材）定义：

AI数字教材是人工智能大模型时代的正式出版物，获得中国标准书号。是以正式出版教材的数字呈现形态为主体，以基于教材及教材配套资源训练成教材机器人为辅助教学内容和手段，封装后可在线发行，读者可浏览全部教材内容，机器人可帮助教师与读者完成所有互动，作者可经过出版社允许后随时升级该机器人与作者同步进化。（2024年10月）

AI数字教材创作出版流程

1.已正式出版纸质教材的AI数字教材升级流程（半个工作日）

第一步，把纸质教材配套的富媒体资源按章节整理成文件夹

第二步，一键上传投喂纸质教材的PDF和配套富媒体文件夹。

2.新创作的AI数字教材出版流程

第一步，作者用WPS创作教材文本。

第二步，出版社用传统流程进行了三审三校并完成出版（纸质书号、电子书号均可）。

第三步，同已出版纸质教材流程。

不用编辑器创作、审校效率高，师生手机端不需下载APP，一步到位教材智能体成本低

输入图书名称、作者姓名搜索 搜索 重置

最新上架 AI数字教材

学生 AI 素养通识(培训)
¥39 76 人在读

人工智能基础应用与实践(文科)
¥58 1275 人在读

创新能力开发与应用
¥48 3870 人在读

物联网安卓客户端设计与开发...
¥39.8 10 人在读

大学生心理健康教育：积极心...
¥52.8 10 人在读

最新上架 AI学术专著





AI数字教材六大优势 整合AI数字资源新力量

极简创作 跨端适配 高性价比 快速升级 智能建库 自动生成

点击查看

输入图书名称、作者姓名搜索 搜索 重置

最新上架 AI数字教材

学生 AI 素养通识(培训)
¥39 76 人在读

人工智能基础应用与实践(文科)
¥58 1275 人在读

创新能力开发与应用
¥48 3870 人在读

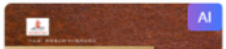
物联网安卓客户端设计与开发...
¥39.8 10 人在读

大学生心理健康教育：积极心...
¥52.8 10 人在读

最新上架 AI学术专著







一书一智能体

让每本书拥有智慧　让教材成为AI导师

点击查看

输入图书名称、作者姓名搜索　搜索　重置

最新上架 AI数字教材

学生 AI 素养通识(培训)
¥39　76 人在读

人工智能基础应用与实践(文科)
¥58　1275 人在读

创新能力开发与应用
¥48　3870 人在读

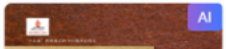
物联网安卓客户端设计与开发...
¥39.8　10 人在读

大学生心理健康教育：积极心...
¥52.8　10 人在读

最新上架 AI学术专著







一、用AI智能体提升办学质量和效率的历史必然性

二、大模型的分类及专用大模型与通用大模型的功能区别

三、用AI大模型简化数字教材创作和出版流程

四、让拥有AI大模型大脑的实体机器人走进校园

两个概念：离身大模型和具身大模型

离身：大模型软件载体为电脑、手机。虚拟（离身）机器人。

具身：大模型软件载体为的实体机器人。实体（具身）机器人

实体机器人类型：

功能：工业机器人、特殊领域（含军用）机器人、服务机器人……

外形：人形机器人和非人型机器人

人形机器人：双足、轮式

非人型：狗 、卡通玩具、毛绒文具、箱式形状、机器臂……

教育机器人分类：

教育服务应用：服务型的人形机器人（教学、后勤、安保、图书管理等……）

教育实训应用：工业应用型机器人（过去非人型，2025人型开始走进校园）

国内外机器人的品牌：

美国：马斯克的特斯拉（Tesla） 生产的Optimus（“擎天柱”）。

俄罗斯：IDOL（爱豆/爱斗）。刚发布，不成熟

中国：宇树、优必选、智元、小鹏、豹、桑梓……

优必选、宇树：双足人型机器人。宇树用于演出，优必选、智元用于工业。

（部分接入大模型，不成熟，宇树尚未接入大模型）需人陪伴守护

小鹏：双足人形机器人，注重日常生活应用，深耕性别。（已接大模型）

豹：教育服务，接入DeepSeek，玩具型，不可定制，教育应用场景欠缺

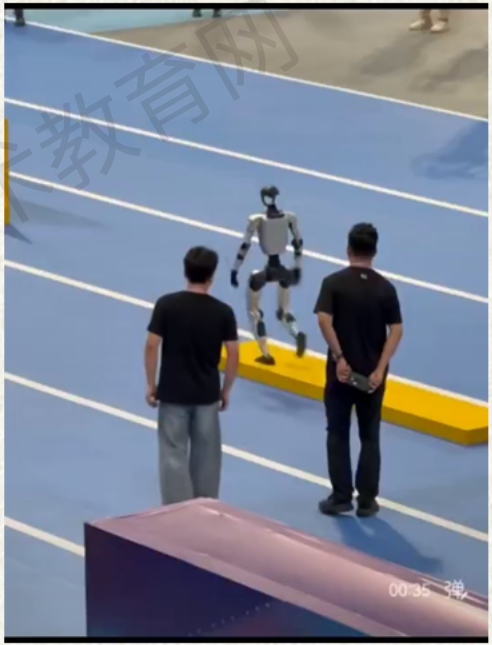
桑梓：轮式人型机器人，主要用于教育服务。（基于专用大模型——桑梓）

2025年11月美国的特斯拉

2025年11月俄罗斯的爱豆

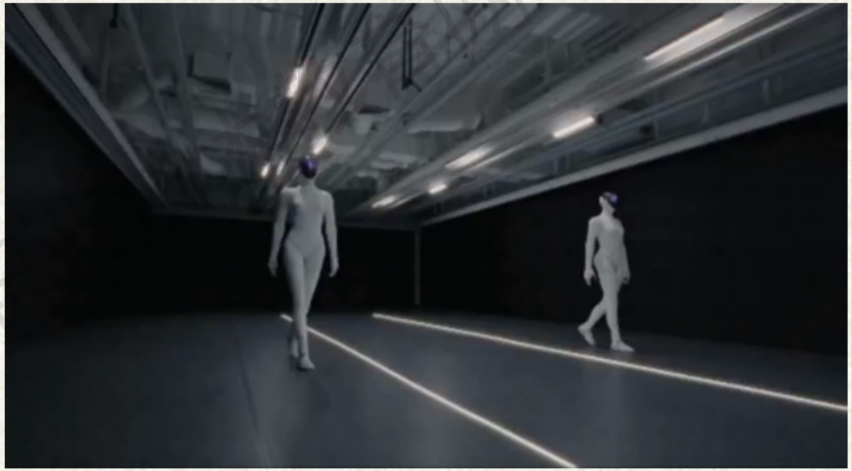
2025年11月中国的优必选

2025年11月中国的宇树



2025年11月中国的豹

2025年11月中国的小鹏




中美俄三国双足机器人

两大关键创新：

1.由人类遥控转为机器人自主控制：导航、行走、感知、对话

2.新的教育服务涌现：校园行走的助教、办事员、数据中台

有专用大模型大脑的

桑梓机器人：