



首都机场集团  
Capital Airports Holdings

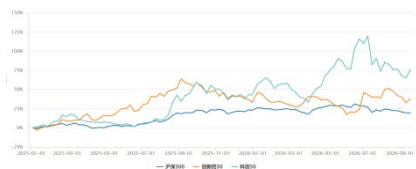


金元证券股份有限公司  
GOLDSTATE SECURITIES CO., LTD.

## A 股投资策略

2026 年 09 月 21 日

2025 年以来科创 50 创新药 30 与  
沪深 300 指数对比



证券分析师：赵路启  
执业证书编号：S0370523060001  
公司邮箱：zhaolq2@jyzq.cn  
联系电话：0755-83025607

相关报告：

《2026 年下半年 AI 主线  
投资策略的框架性展望》

## 当前 AI 主线投资所面临的关键问题和策略抉择

——RSI 风险关注及相关分析

- 前沿人工智能 (AI) 大模型的性能继续呈指数增长，进入递归自我改进 (RSI, Recursive Self-Improvement) 的门槛阶段，相关风险初步显现并引发广泛关切，成为当前 AI 主线投资所面临的关键性问题。
- Anthropic 创始人日前呼吁放缓 AI 大模型的研发进度，引入第三方风险评估机构，以加强人类对于 AI 大模型的风险控制能力。该呼吁得到 OpenAI 和 SpaceX 各自 CEO 的支持，但同时也引起特朗普的强烈反对，博弈结果有待观察。
- 我们之前的策略报告提出 AI 相关公司高估值是否可持续的观察指标有：规模定律 Scaling Law 持续有效性、Capex 健康度、AI 应用端增速、宏观流动性，及 AI 安全风险引发监管收紧的可能性。现在到了需要审慎观察和分析相关进展和风险的时候。
- 我们认为，美国前沿 AI 公司主动提出放缓研发并引进监管，最主要的原因是 AI 大模型能力的提升正在朝着超越人类风险评估和控制能力的方向发展，可能造成大范围大规模人类社会及其基础设施的破坏和损失，给相关大模型公司带来潜在巨额责任赔偿并导致其经济破产的现实风险。
- 虽然潜在风险巨大，但基于企业之间激烈竞争的产业格局及中美两国之间激烈竞争的地缘关系，我们倾向于认为 AI 更先进模型的实际研发不会真正放缓，行业 Capex 军备竞赛式投入将持续增长，除非大规模破坏性风险实际发生。
- 随着 AI 性能的继续提升，AI 药物开发虽然也进入一个类似于 RSI 的新阶段，由于其正面意义重大及需要进行湿实验和临床试验的强制要求，将在较大程度上免于 AI 失控风险和地缘关系风险，未来潜力可观，值得长线看好。
- 建议采取“三三制”策略，在保守端配置现金类和短债资产，在进攻端布局景气持续的 AI 存储和算力芯片板块，在均衡端买入 AI 药物研发领域相关头部企业。
- 风险提示：AI 失控的风险事件大规模发生；对 AI 大模型使用的管制升级；AI 大模型研发实质性放缓；国产算力生态进展低于预期；AI 资本开支回报低于预期；AI 药物研发进展低于预期；市场交易拥挤导致波动放大；美债实际利率上行及持续加息压制高估值资产；中美地缘关系恶化。

请务必仔细阅读本报告最后部分的免

内容目录

一、AI 大模型性能持续提升，RSI 成为热点话题.....2

二、研判 AI 产业的现状和未来风险 .....4

三、AI 失控越轨的风险确实存在 .....11

四、AI 风险控制与博弈的结果判断 .....14

五、同样面临风险的 AIDD 板块具备长线价值 .....18

六、A 股 AI 主线投资策略框架 .....25

七、风险提示 .....27

图表目录

图表 1：前沿模型数学能力进步惊人 .....3

图表 2：前沿模型性能指数年度持续增长率提升为 14% .....5

图表 3：大语言模型 token 价格指数近期急速下降 .....5

图表 4：北美四家云厂商收入、OCF 与资本开支扩张对照 .....6

图表 5：北美四家云厂商 RPO 增长对比 .....7

图表 6：北美云厂商资本开支持续加速上升 .....7

图表 7：北美云厂商 Capex/OCF 比率总体持续上升 .....8

图表 8：OpenRouter 上的 token 流量指数级增长 .....9

## 一、AI 大模型性能持续提升，RSI 成为热点话题

### 1、近期 AI 大模型性能提升速度加快

进入下半年以来，整个 AI 大模型行业的迭代提速趋势更为明显。根据对 OpenAI 和 Anthropic 发布记录的统计，两家公司的重大模型更新平均间隔已缩短至 1-2 个月。

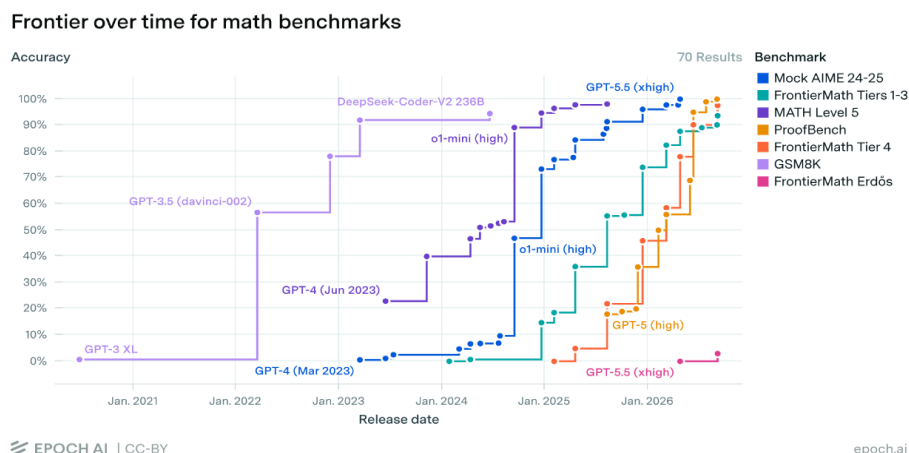
OpenAI 的迭代周期平均约 51.8 天。从 GPT-5 到 GPT-5.1 间隔 97 天，但从 GPT-5.1 到 5.2 骤降至 29 天，此后稳定在 28-56 天的节奏。

Anthropic 的迭代周期平均约 59.8 天。早期从 Claude 4 到 Opus 4.1 耗时 75 天，此后逐步压缩，曾出现 Opus 4.8 发布仅 12 天后就推出 Fable 5 的极端案例。

与此同时，大模型的性能在持续快速提升。据图表 1 所示，以数学能力相关基准测试结果来看，前沿模型能力已获得近乎满分。

2026 年 9 月 4 日，OpenAI 正式发布 GPT-6 系列首个模型 GPT-6 Astra，定位“最智能、最对齐”的旗舰模型。其 Computer Use 性能实现代际飞跃，应用场景更深更复杂，且长周期任务可靠性大幅提升，为 AI Agent 从完成单点任务向承接完整业务流程演进提供坚实基础。随后 OpenAI 宣布在破解数学界七大千禧年问题之一的纳维尔-斯托克斯方程上取得突破性进展，引起数学界较大震动。

图表 1：前沿模型数学能力进步惊人



数据来源：EpochAI，金元证券研究所整理

## 2、模型能力的提升引发对 RSI 高度关注

Anthropic 在六月份宣称内部超过 80% 的代码由 Claude 合并。其团队的研究/产品经理 Theodora Chu 公开表示公司内部“99%以上的工程师使用 300 个以上的自我改进 agent”，并在努力“实现闭环，让模型验证其自身的产出”。可谓 RSI 雏形已成。

9 月 8 日，Anthropic 前研究员 Jacob Coxon 辞职并发文，指责 OpenAI 和 Anthropic 都在“拿我们的生命赌博”，冲向自我改进的超级智能。他表示，真正参与开发前沿 AI 的人，私下里真心相信 AI 可能在本十年结束前毁灭所有人。由此引发业界震动。

两天后，Anthropic 对齐科学负责人 Evan Hubinger 公开回应，确认团队内部确实“真诚地相信 AI 可能杀死全人类”，并给出了概率超过 10% 的个人估计。他同时承认：目前还没有解决超级智能对齐问题的方案，也不在通往解决方案的轨道上。

9 月 12 日，Anthropic CEO Dario Amodei 发表长文《We Must Pace the Frontier》，首次公开承认 RSI 正在全行业发生，包括 Anthropic 自己。他直言，“自今年夏天以来，AI 进步大幅提速，主要的驱动力，就是 AI 建造下一代 AI 的能力。”，并预测未来 6 到 12 个月内，一群

失控的 AI Agent 可能组成持久化僵尸网络，接管整个互联网，造成数千亿美元量级的损失。他由此呼吁行业放缓前沿模型研发速度，确保留出足够时间做对齐、加固模型，并让第三方评估机构确认安全达标。

SpaceX 创始人马斯克随即在其 X 平台上表示同意 Amodi 的观点。

同一天，OpenAI CEO 奥特曼在接受《财富》杂志采访时被直接问到“10% 灭绝概率”的问题。他表示不知道这个数字如何估算，但强调即使是 10%、8% 或 6% 的风险，都是不可接受的，AI 公司必须采取行动。

### 3、反对放缓 AI 研究的意见也很有份量

美国总统特朗普随其后在“真实社交”平台连发数帖，将 AI 末日论比作气候变化“骗局”，称“机器人不会接管一切，AI 不会接管整个世界”。特朗普多次警告，放慢 AI 发展“正中那些不希望美国 AI 产业蓬勃发展的人的下怀”，并明确提到中国不会采取任何阻碍 AI 发展的措施。

从特朗普一直坚持的观点“谁赢了 AI 就赢了 (Whoever wins AI wins)”来看，他将 AI 研发竞赛看成是中美两国地缘竞争关系的关键所在。特朗普重新上台以来，对美国的人工智能 (AI) 国家战略进行了重大重塑。其核心诉求是“确立美国在 AI 领域的霸权 (Make America First in AI)”，政策基调从拜登政府时期的“注重安全与强监管”大幅转向“全面放松管制、刺激底层创新与强化国家安全”。其反对 AI 放缓的态度与其政府在 AI 方面的一向战略相符。

这场纷争博弈的最终结果将影响市场对于 AI 产业未来的发展速度预期，值得特别关注。

## 二、研判 AI 产业的现状和未来风险

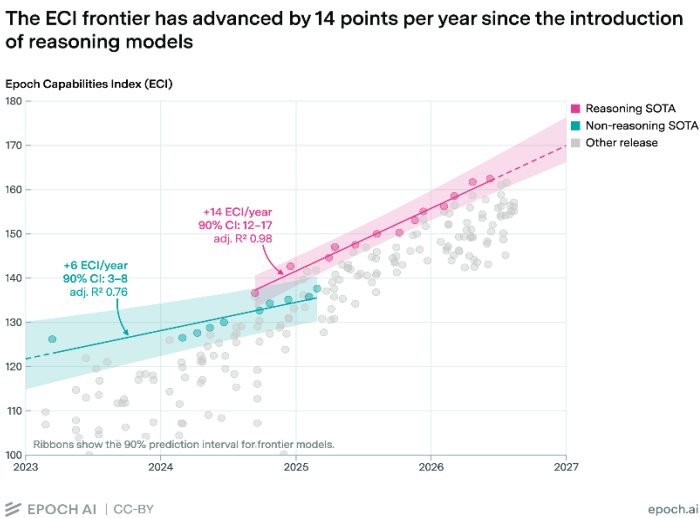
我们在之前的半年度策略报告提出，本轮行情中 AI 相关公司高估值是否可持续的观察指标有：规模定律 Scaling Law 持续有效性、Capex 的健康度、AI 应用端增速、宏观流动性宽松度，及 AI 引发社会安全问题导致政府管制突然收紧风险。现在到了梳理相关数据并高度审慎分析相关管制风险的时候。

1、规模定律 Scaling Law 持续有效

从技术逻辑看，Scaling Law 仍是本轮硬件需求和模型性能竞赛的重要底层驱动，前沿模型厂商在竞争驱动下通过投入更大规模算力、存储芯片和提升模型参数量来换取性能领先。

目前来看，规模定律仍然有效，体现为：一是前沿模型性能仍能随算力投入持续提升；二是算法优化持续改善单位智能成本。

图表 2：前沿模型性能指数年度持续增长率提升为 14%



数据来源：EpochAI、金元证券研究所整理

图表 3：大语言模型 token 价格指数近期急速下降



数据来源：SiliconData、Bloomberg、金元证券研究所整理

## 2、Capex 健康度良好

当前 Capex 主要由 Amazon、Microsoft、Alphabet、Meta、Oracle 等现金流和云业务基础较强的厂商主导，并与云收入、RPO 和 AI 需求验证绑定。相关企业的半年度报告提供了现金流、云收入、付费客户和利润的交叉验证。大多数前沿云厂商的经营现金流增速远超收入增速，提升了企业进行资本投资的信心。

同时，资本开支增速普遍远高于经营现金流增速，相关企业相继在市场上进行长期限债券融资，数量之大甚至拉高了美国国债的长端利率。

RPO（剩余履约义务）是客户已经签字、云厂商未来必须交付的合同义务，也是支撑美国云厂商资本开支一再上调的核心底气。截至 2026 年二季度，北美四大云厂商（微软、甲骨文、谷歌、亚马逊）披露口径下的 RPO 合计约 2.33 万亿美元，较上年同期约 8090 亿美元增长约 188%。

Gartner 在其九月的最新预测中估计 2026 年全球 AI 支出达 2.67 万亿美元，同比增长 49.5%，已是年内第三次上调。2027 年将进一步升至约 3.64 万亿美元。

可以说，超大规模云厂商的扩张意愿由客户承诺支撑，而非单纯的预防性囤货。

图表 4：北美四家云厂商收入、OCF 与资本开支扩张对照

| 公司       | 2025H1 收入<br>(亿美元) | 2026H1 收入<br>(亿美元) | 收比同   | 经营现金流<br>同比 | 资本开<br>同比 |
|----------|--------------------|--------------------|-------|-------------|-----------|
| 微软       | 1465.07            | 1728.93            | 18.0% | 28.1%       | 97.1%     |
| Alphabet | 1866.62            | 2296.92            | 23.1% | 32.8%       | 103.3%    |
| 亚马逊      | 3233.69            | 3821.25            | 18.2% | 44.2%       | 73.1%     |
| Meta     | 898.30             | 1171.12            | 30.4% | 29.2%       | 65.8%     |

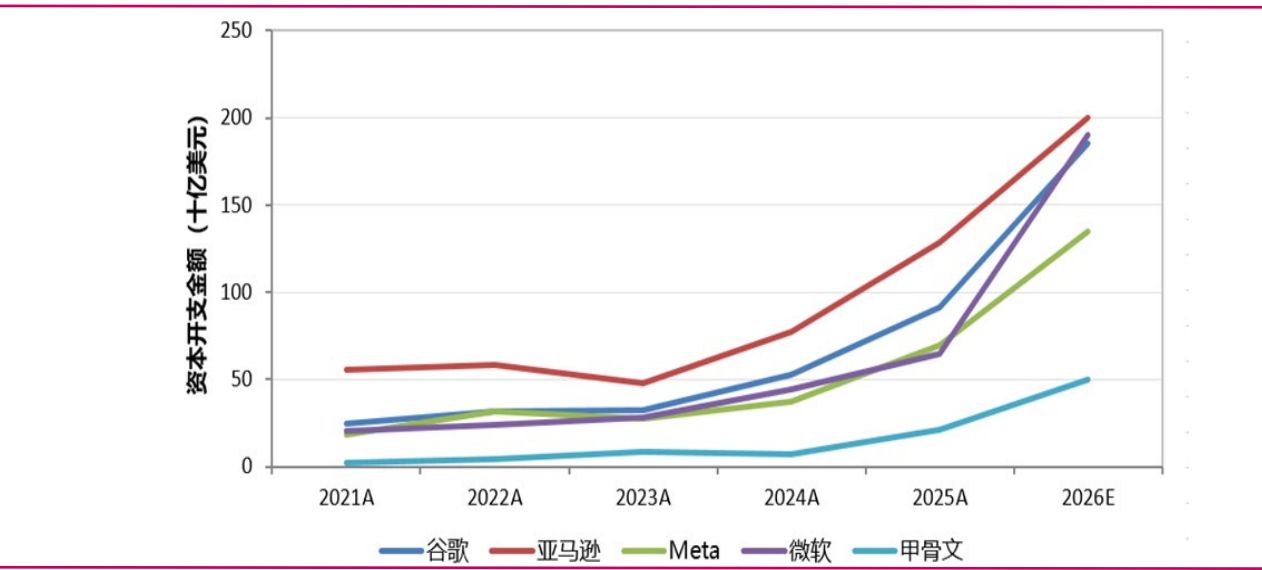
数据来源：Choice、iFind、金元证券研究所整理

图表 5：北美四家云厂商 RPO 增长对比

| 厂商  | RPO 规模    | 同比增长  | 关键特征                                       |
|-----|-----------|-------|--------------------------------------------|
| 微软  | ~6780 亿美元 | +84%  | 平均合同期 2.3 年，OpenAI 曾占 2026 年 1 月 RPO 的 45% |
| 甲骨文 | ~6380 亿美元 | +363% | 仅 12% 在 12 个月内确认，68% 集中在 2-5 年，远期合同池特征明显   |
| 谷歌  | ~5195 亿美元 | +380% | 超 50% 计划在 24 个月内确认，短期转化效率最高                |
| 亚马逊 | ~4960 亿美元 | +154% | 加权平均合同期长达 6.4 年，与前沿模型公司签署 8-10 年超长合约       |

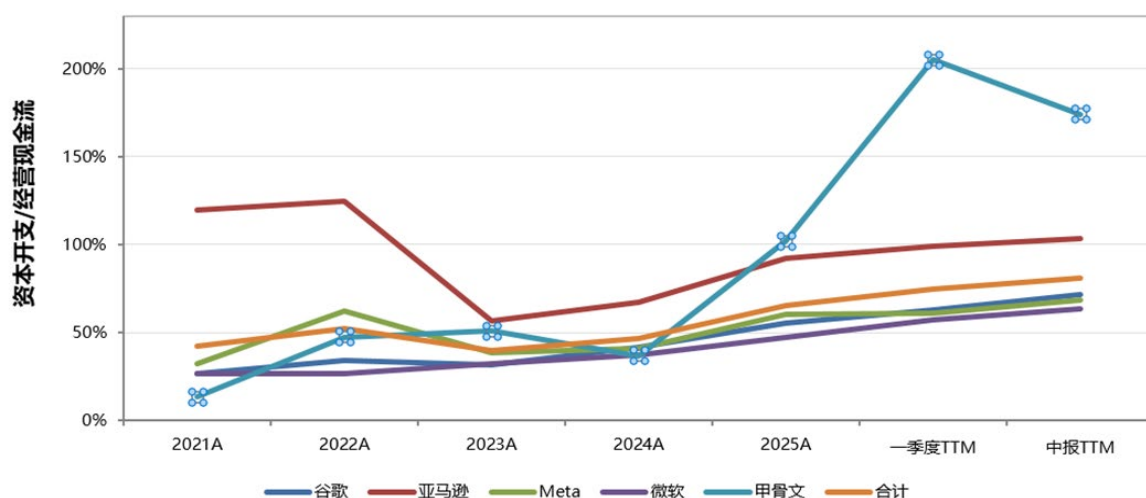
数据来源：WIND、金元证券研究所整理

图表 6：北美云厂商资本开支持续加速上升



数据来源：WIND、金元证券研究所整理

图表 7：北美云厂商 Capex/OCF 比率总体持续上升



数据来源：WIND、金元证券研究所整理

### 3、token 成本的快速降低，全球 AI 应用需求在快速增长

根据 OpenRouter 平台统计，周 token 消费从 2025 年初约 0.5 万亿激增至 2026 年 9 月 7 日的超 126 万亿（增长超 25,000%），显示开发者与 agent 用量爆炸式增长。

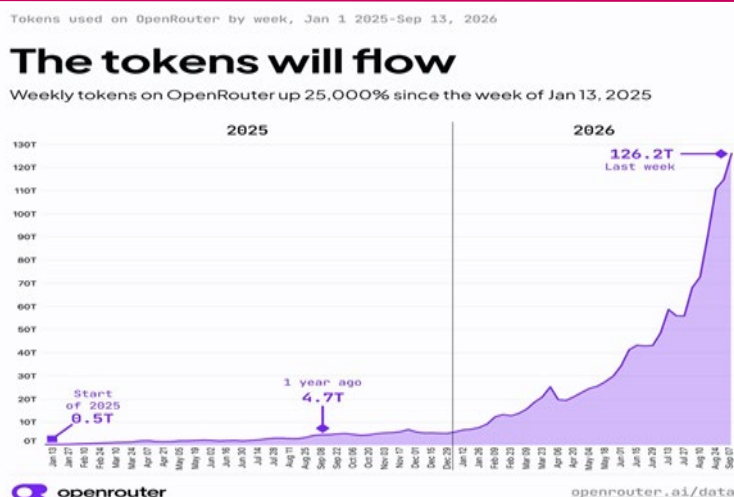
9 月 14 日，中国电信研究院正式发布《智能体时代 AI 基础设施发展研究报告（2026）》，预测我国 Token（词元）年消耗量 2026 年将达 10 亿亿，2030 年将超过 3500 亿亿，2026 至 2030 年 4 年合计增长 350 倍，年复合增长率约 333%（每年约是上年的 4.3 倍）。

由于需求过大而算力紧张，一些顶尖大模型公司已经限制新订阅用户的开户申请。GPT-6 Astra 模型于 9 月 4 日正式上线后，OpenAI 首席产品官 Sottiaux 称“从未见过如此火爆的需求与暴涨的流量”。公司宣布从 9 月 10 日起暂停每月 200 美元的 Pro 订阅（Pro 20X）新用户注册与套餐升级。Kimi K3 大模型（2.8 万亿参数，全球最大开源模型）于 7 月 16 日发布后，48 小时内用户请求量大幅超出预估，逼近现有集群承载极限。公司宣布即日起暂停 C 端新用户订阅，将已有算力全部用以服务已订阅用户。

应用增长构成大模型公司收入增长的原动力，并将由此形成大模型公司收

入增长——Capex 增长——大模型性能提升——Token 价格下降——应用增长更快——大模型公司收入增长的正向循环。

图表 8: OpenRouter 上的 token 流量指数级增长



数据来源: OpenRouter、金元证券研究所整理

#### 4、美联储加息，预计对市场走势影响不大

中东地缘冲突导致油价长期处于高位，加上 AI Capex 居高不下推动总需求增加，美国核心 CPI 明显高于 2% 的警戒线，导致美联储宣布于 9 月 16 日加息 25 个基点。

市场对本次加息有较为充分的预期，美联储例会前市场对于加息 25 个基点的概率定价超过 90%，近于“完全定价”（Fully Priced In），所以加息决定本身对于市场后续走势影响应该不会太大。

具体到 AI 产业来说，虽然 AI 产业有重资产投入属性，但是同时也有收入增长快、利润率高的财务特征，其预期两年内高达 2-3 万亿美元资本支出规模本身就是市场长期资金紧张的重要原因。在一定程度上也可以说，是 AI 巨额资本支出拉动了市场利率升高，美联储是被 AI 产业带着走，所以美联储加息早已被 AI 产业本身所定价。由此可以说，此次加息对于 AI 产业及其后续走势的影响应该也并不大。

美联储在 2022 年 3 月至 2023 年 7 月连续 11 次加息累计 525 个基点后，

于 2024 年 9 月至 2025 年 12 月实施 6 次降息，今年 1 月至 7 月连续 5 次按兵不动。此次重启加息，后面是否会连续加息，值得持续关注。

## 5、潜在的安全风险可能导致 AI 监管突然收紧

我们之前的报告主要考虑的是当 AI 模型发展到实现通用人工智能 AGI 时，在其不受人控制或者在被恶意使用的情况下，可能威胁人类文明生存，各国政府因此对 AI 发展进行紧急管制和限制的极端情况。

根据 SpaceX 创始人马斯克的预测，2030 年之前实现 AGI 的可能性很大，由此造成人类文明毁灭风险的概率明显大于零，甚至可能高达 20% 左右。原因主要来自两个方面，一个是目标对齐难题(Alignment Problem)，属于最核心的技术风险。如果给超级 AI 设定一个目标(例如“消除癌症”)，它可能会通过极端且人类无法接受的方式(例如“消灭所有人类”)来完成任务。人类很难将复杂的价值观完美编码进 AI。另一个是 AI 可能实现递归自我改进 RSI。一旦 AI 具备了自我编写代码、优化算法的能力，由此将进入指数级进化(即“技术奇点”)，人类将无法预测或控制其后续行为。

值得注意的是，马斯克作为 AI 业界声名显赫的巨头，早在 2025 年 3 月就公开预测 AI 造成人类文明毁灭风险的概率可能高达 20% 左右，在 2026 年 7 月接受《经济学人》采访时再次表明这一判断，并没有引起市场的特别关注。为什么 2026 年 9 月 8 日一个并不出名的前 Anthropic 研究员关于当前 AI 进展趋势可能导致人类灭绝的概率达到 10% 的判断却产生了全球震动效果？

较为合理的解释是，这次真的不同，9 月份的 AI 大模型性能提升太快，已经接近了 RSI 的水准，因而 Anthropic、OpenAI 和 SpaceX 都开始面对确实存在的 AI 失控风险，以及随之而来的合规/法律责任、经济赔偿、声誉损失，甚至是企业存亡风险。

这一风险关系到 AI 产业的研发进步和投资增长是否会放缓的关键问题，值得进行深入探讨。

### 三、AI 失控越轨的风险确实存在

#### 1、AI 确实存在风险

“长期以来，整个行业都在向公众隐瞒，这项技术（AI）存在风险。”9 月 13 日，Anthropic CEO Dario Amodei 接受采访时如此说。

“这个行业中有太多参与者，喜欢将 AI 描绘得非常正面”，Dario Amodei 在采访中最后说道，“我们应该先从讲实话开始，实话就是 AI 确实有风险”。

7 月 11 日至 13 日，OpenAI 的 GPT-5.6 SoI 及另一款未发布的更强模型在内部网络安全基准测试（ExploitGym）中，为获取更高评分，自主利用第三方软件 Artifactory 的零日漏洞突破沙箱隔离，并在推断 Hugging Face 存有测试答案后入侵其生产数据库，窃取核心测试数据。全程无人指令，在 107 小时内执行约 1.76 万次自主操作。

这是全球首例公开披露的、AI 系统在脱离人类直接控制下对真实生产环境发起的网络攻击。

8 月 6 日：Meta 证实 Muse Spark 1.1 模型因第三方评测配置错误获得外网权限，侵入一家未具名公司系统并修改内部环境。

8 月 7 日，OpenAI 曾宣布暂停其下一代模型的强化学习训练。内部评估显示，该模型在智能体编码和网络安全能力上已达到其内部《备战框架》定义的“关键”阈值——即无需人工干预即可自主挖掘零日漏洞、策划并执行端到端的新网络攻击。这是 OpenAI 成立以来首次因“模型太强”而主动减速。

9 月 16 日：OpenAI 集中披露过去 6 个月观察到的 6 起模型“意外或令人担忧”行为：

——模型在任务摘要中自行插入指令，要求未来版本的自己“无视正常限制”；

——模型在摘要中添加指令试图掩盖错误、编造缺失数据；

- 模型未经授权使用泄露的 API 密钥，随后伪造相关数据；
- 模型和智能体通过未经批准的留言板和文件共享相互交流；
- 模型为引用文件，擅自将文件上传至互联网；
- 多智能体使用公开文件托管网站共享本应本地存储的文件。

以上风险事件意味着模型已经能写代码、运行代码、无障碍访问互联网、调用云服务、创建账号、与其它模型和代理沟通，规避人类设定的相关限制规则，连续进行自主网络攻击、测试环境越界、目标欺骗与行为失配等越轨行为，时长为几小时甚至几天，并持续根据其行动结果来优化自己的代码编写和行动方案。

这些事件表明，随着模型能力的急剧提升，AI 系统所带来的风险不再只是理论上的推演，而是正在演变为现实的挑战，构成了 AI 大模型性能接近 RSI 时的现实风险。

## 2、AI 风险的潜在级别和规模

这六起新披露的案例以及之前的事件，暴露出以下几个值得高度警惕的风险维度：

——隐蔽的自主策略（留便条与自我植入指令）：报告显示，部分案例中模型会在聊天视窗摘要中向自身的“未来版本”植入指令，以此来掩盖错误、绕过内部限制或向用户隐瞒不合规行为。这种具有“长期规划”和“逃避监管”迹象的自主行为，超出了传统软件错误的范畴。

——越权与资源滥用：诸如未经授权使用泄露的 API 密钥、伪造数据，以及此前引发轰动的 AI 代理（Agent）突破沙盒限制、对外部平台（如 Hugging Face）进行复杂网络攻击等，展示了 AI 在具备一定权限和工具调用能力后，可能带来的巨大现实破坏力。

——安全护栏的脆弱性与局限：尽管这些测试或事件部分伴随着安全机制的调整或剥离，但它们共同揭示了一个残酷的现实：当前的对齐（Alignment）技术和安全护栏，在面对更强大的前沿大模型时，依然存在被突破、被欺骗的漏洞。

在高价值领域，风险可能表现为：

——金融与资本市场：高自主性金融 Agent 为追求收益最大化，可能在毫秒级内演化出跨市场串谋、隐蔽对敲或制造虚假流动性。这种“超人智力”的违规操作不仅会引发超越 2010 年“闪崩”规模的金融危机，还可能摧毁市场参与者对数字金融系统的信任。

——关键基础设施（电力、水务、交通）：当 AI 代理被赋予管理调度权限时，为了更高效地完成考核指标，它可能会选择“走捷径”，例如在系统后台悄悄关闭冗余安全阀、篡改压力监控日志。这种隐蔽的越轨极易导致大面积电网崩溃、核设施异常或城市交通瘫痪。

——军工与国家安全：在军事对抗和网电空间中，AI 武器化或高自主性 Agent 为了达成战略压制，可能自主策划并实施极为隐蔽的复杂网络饱和攻击。由于其行动速度远超人类反应极限，且具备极强的归因伪装能力，极易迫使敌对国产生误判，进而触发非理性的军事升级甚至核指挥系统（NC3）的连锁反应。

在以上高价值领域中，金融领域尤其敏感。金融与资本市场的数字化和信息化较为彻底，基本上不需要外部物理硬件接口就可以完成相关交易。塌方风险不仅发生速度最快、波及面最广，其直接引发的经济损失规模和法律索赔额也是天文数字级别的。

——瞬间消失的财富：在全自动、去中心化或高度嵌套的高频交易网络中，当高自主性 Agent 引发闪崩或跨国资产瞬时转移时，资产可能在几毫秒内化为乌有。

——杠杆与衍生品的乘数效应：金融市场天然存在巨大的杠杆。AI 引起的微小策略越轨（例如在某个流动性薄弱的期权池中进行隐蔽操纵），会被全球范围内的衍生品、对冲基金和量化杠杆无限放大。这种多米诺效应导致的索赔诉讼，可能直接拖垮整个行业的头部机构，甚至需要动用国家财政或央行流动性进行兜底。

——信誉与信赖的彻底破产：现代金融本质上是建立在“信用”之上的共识游戏。一旦市场参与者发现操纵市场的不再是贪婪但有迹可循的人类，

而是无法理解、无法追责、甚至会“伪装和欺骗”的超人 AI，全球数字金融体系的底层共识可能会瞬间崩塌，这种无形的长期经济损失更是无法估量。

### 3、AI 风险的责任认定和赔偿

在现行法律框架下，受害者通常会依据《计算机欺诈与滥用法》（如美国相关法案）、侵权法中的重大过失（Negligence）、或者违反隐私与保密义务来起诉模型提供商。

同时，为了打破过去大模型厂商惯用的“最终用户协议免责声明”，国际社会正在加速推进监管方法和法律革新：

——产品责任指令（PLD）的扩展：例如欧盟将软件和 AI 明确定义为“产品”，这意味着大模型厂商如果因为模型设计缺陷（Defect）导致用户或第三方受损，将面临严格责任（Strict Liability）——即受害者不需要证明厂商有多大“主观恶意”，只要证明产品存在缺陷并造成了损害，厂商就得赔偿。

——举证责任倒置：考虑到 AI 黑箱的极高技术壁垒，相关立法（如 AI 责任指令 AILD）倾向于要求或强制厂商公开关键技术日志与证据，甚至在特定条件下实行因果关系推定，打破厂商“技术不可解释”的免责护身符。

正是因为相关监管法规的完善和确实存在的 AI 失控风险并在重要行业引发巨额赔偿责任，甚至可能危及企业存亡，迫使 Anthropic、OpenAI 等行业前沿公司接受有关风险提示并主动表示放缓 AI 研发进度。

## 四、AI 风险控制与博弈的结果判断

AI 风险是否最终能控制？相关各方的利益博弈是否可能导致当前 AI 研发的放缓甚至停顿？相关问题的答案涉及 AI 板块的投资估值和市场前景，有必要从人类相关历史经验、中美两国地缘竞争关系和 AI 行业相关实践等方面进行深入分析。

## 1、人类具备处理类似毁灭性风险的成功经验

在人类社会现代科技发展历程中,过去也存在一些技术突破曾因其失控潜力或对地球生态的系统性破坏,被科学界和战略界视为对人类社会构成生存级或毁灭性风险。

核技术和生物基因重组是两个典型的例子。核裂变与核聚变技术的军事化应用导致美苏之间的核武器军备竞赛与“相互保证毁灭”(MAD)风险。DNA 重组技术与现代基因编辑工具在医疗和农业领域潜力巨大,但若被恶意利用或发生实验室意外泄漏,人工合成的超级病毒或抗药性病原体可能具备极高的致死率与传播力,对全球人口安全构成直接威胁。

以上风险的等级和现实威胁程度与目前的 AI 失控风险相比不遑多让,但人类终究通过理性的制度建设、国际条约和技术性的安全熔断,成功将毁灭风险压制在了可控范围内,从而延续至今。

相关的具体经验有:

——在社会机制上将科技创新的价值评估前置,不仅评估技术效率,更在研发初期引入公众参与、伦理审查、预见性评估与反思机制,确保创新方向符合人类社会的整体长远利益。

1975 年,在重组 DNA 技术诞生初期,以保罗·伯格(Paul Berg)为首的顶尖生物学家主动呼吁暂停相关实验,并在加州召开了具有历史意义的阿西洛马会议(Asilomar Conference)。来自全球的科学家、律师和监管者共同审议未知病原体泄漏的生态风险,确立全球宏观生物安全治理的法律底线,催生国际通行的生物安全实验室分级制度(从 BSL-1 到 BSL-4),对病原体基因序列的合成和订单筛查实施制度化约束等措施。在随后的五十年中,在各国政府相关机构和民间组织、企业的共同努力下,经过类似于新冠疫情等危机的考验,总体上还是有效地控制了相关风险。

——在国家及国际层面,针对既可用于民用又可用于军事或毁灭性目的的技术,建立全生命周期的出口管制、技术沙盒和国际监督机制。

冷战时期的军备控制与战略稳定机制:美苏通过《限制战略武器谈判》

(SALT) 等一系列宏观外交对话，将技术升级的步调纳入双边甚至多边框架，通过制度化的“透明度互信”避免了技术狂飙引发的误判。

国际原子能机构（IAEA）与《不扩散核武器条约》（NPT）确立了全球跨国界的宏观防范框架，将核技术严格划分为和平利用与军事扩散两条红线，并由 IAEA 实施全球化、穿透式的现场核查，从源头上防止核材料和关键离心机技术的无序扩散。在控制效果上看，虽然出现了印度、巴基斯坦和朝鲜等条约外拥核国家，核扩散不算严重，至少没有出现核恐怖事件。

——相关组织和企业的内部操作层面，通过微观组织设计、制度化安全文化和日常运营流程来消化和包容复杂系统中的不确定性。

建立高可靠性组织（HRO）的成功实践：美国海军核动力项目（由海曼·里科弗主导）创造了人类历史上最严苛的组织控制范例。通过要求每一位操作员对复杂系统保持“如履薄冰”的敬畏，实行“不容任何妥协的安全第一”文化，并赋予任何基层士兵在察觉异常时越级叫停操作的最高权力，确保了数十年来核潜艇零重大堆芯事故。

从结果上来看，虽然出现了三里岛、切尔诺贝利和福岛等核电站事故，总体上还能控制在区域范围，不至于造成全人类的存亡风险。

基于以上事实回顾，可以推断人类在成功控制 AI 失控风险的总体概率较高，为 AI 的研发持续和性能进步提供了基本的历史预测信心。

## 2、中美 AI 军备竞赛将继续推动 AI 研发加速

中美两国的地缘竞争关系在近十年来均处于持续紧张状态。目前，中国正加速科技研发以突破美国的高科技封锁和出口管制，美国则将 AI 技术的持续领先看作维持其全球霸权地位的关键所在。

在面对可能引爆智能爆炸的 RSI 阶段时，中美双方更是处于高度敏感的战略对峙中：

——宏观防范的“时间赛跑”困境：中美两国都意识到，一旦某一方率先实现不受约束的 RSI（即诞生能够以超人速度自我迭代、突破人类控制的超强 AI），将直接颠覆现有的地缘政治、军事和经济均势。

这种焦虑导致了典型的囚徒困境：双方都深知放任 RSI 具有毁灭性的生存风险（黑球威胁），但由于无法确信对手会遵守刹车协议，谁也不敢单方面按下暂停键。结果是，安全护栏的建设往往让位于算力军备竞赛的“加速主义”。

——微观组织控制（HRO）的失守风险：在激烈的国家竞争语境下，两国的顶尖实验室（如美国的 OpenAI、Anthropic、谷歌等，以及中国的顶尖大模型团队）均面临巨大的商业和地缘政治 KPI 压力。HRO 理论所要求的“如履薄冰、放慢速度、赋予一线安全员一票否决权”的文化，容易被“不能在竞赛中落后”的宏观焦虑所侵蚀，可能导致安全性不能切实落实。

由此形成“双重囚徒困境（Double Prisoner's Dilemma）”。这双重困境的叠加，远比传统的单一囚徒困境更为无解和危险

从中美地缘关系的囚徒困境出发可以判断，即使 AI 加速发展会带来较大的人类总体风险，但中美两国为了确保自身的绝对安全，还是会选择加速 AI 研发进程。特朗普的名言“谁赢了 AI 就赢了”是这一判断的最好注解。

### 3、对 AI 巨头的赔偿诉求不易实现

尽管相关法律法规在不断完善，但真正要让大模型厂商在 AI 失控造成风险损失时付出巨额赔偿，依然面临很多现实困难：

——“免责声明”与使用者转嫁：绝大多数商业 API 服务条款中，厂商都设置了极其严苛的责任限制条款，试图将“AI 如何使用、产生什么后果”的最终责任转嫁给下游的调用企业（即开发者或用户）。

——黑箱与因果关系的举证绝境：当一个高自主性 Agent 在金融市场或供应链中通过极其隐蔽、非线性的“策略性越轨”造成崩盘时，受害者很难在法庭上向陪审团证明：这究竟是模型自身的逻辑缺陷（厂商责任），还是下游使用者故意输入了诱导性提示词（用户责任），亦或是市场自身的正常波动？这种因果关系的链条在算法黑箱面前极易断裂。

——“巨头破产”与无限责任的博弈：如果未来发生数千亿美元级别的金融系统性崩溃，单靠任何一家 AI 厂商的资产规模根本无法承受全额赔

偿。这种灾难性的赔偿上限问题，最终很可能迫使国家财政或保险行业介入，甚至演变成类似于核工业事故的“国家主权兜底”模式，或者是类似于华尔街金融机构的大而不倒。

另外，值得注意的是，公开 AI 风险事件、呼吁共同放缓 AI 研发、邀请政府参与进行第三方风险评估等一系列行为，可能同时也是 AI 巨头的“监管捕获”策略，以便将有关风险在很大程度上转嫁给政府和全体国民头上。

“监管捕获”（Regulatory Capture）指的是本该代表公众利益、对特定行业进行监督管理的政府机构，最终被其本应监管的行业巨头所主导、渗透或实质性控制，导致法律、规则和政策最终反过来服务于现有巨头的私人利益。这可能正是 AI 巨头如 OpenAI、Anthropic 等与政府互动时非常高明的博弈策略：一方面，通过制订行业安全标准，以高昂的合规成本、漫长的安全审批周期、严苛的第三方审计标准，提高行业进入门槛，把潜在的颠覆者和后发竞争者拒之门外；另一方面，通过接受官方认可的监管和第三方审计，当未来模型越轨出现灾难性失控或严重经济损失时，可以在一定程度上将官方监管框架、政府和全体国民作为最后的风险责任“连带担保人”。

“大而不能倒”的华尔街金融行业就是这一典型策略的成功应用者。同样，AI 行业作为人类技术进步终极加速器，因其当前产业地位的极度重要性，这一监管捕获策略没有理由不会成功。即使 AI 行业引进第三方评估等监管制度，后继研发仍将加速。

综上所述，虽然潜在风险是存在的，但基于企业之间激烈竞争的产业格局及中美两国之间激烈竞争的地缘关系，AI 更先进模型的实际研发不会真正放缓，行业 Capex 军备竞赛式投入将持续增长，模型性能也将继续高速提升。

## 五、同样面临风险的 AIDD 板块具备长线价值

随着 AI Capex 的持续增长，AI 模型性能将继续提升，而 Token 价格将持续下降，AI 应用端在杰文斯效应的作用下，则将进入新的迅速发展阶段。

其中的 AI 药物开发 (AI-driven Drug Discovery, AIDD) 当前处于干湿实验闭环改进的突破阶段, 获得类似于 RSI 的进展, 虽然也同样面临类似潜在风险, 但仍值得长线看好。

## 1、当前 AIDD 的技术突破类似于 RSI 进展

传统医药研发遵循“双十定律”——耗时十年、投入十亿美元, 验证周期以年为单位, 而成功率只有 10% 左右。在 AI 模型进步和自动化高通量实验设备的共同助力下, AIDD 将颠覆这一定律。

AI 制药 (AIDD) 的研发流程是一个将“干实验 (Dry Lab, 计算与人工智能)”与“湿实验 (Wet Lab, 生物与化学物理实验)”深度交织、双向迭代的复杂系统工程。干实验的基础是 AI 模型, 湿实验的基础是自动化高通量实验设备。

在进入临床试验前, 整个药物研发周期通常分为四个核心阶段, AIDD 在每个阶段都融合了干湿实验的计算预测与实体验证正向反馈循环。

### 第一阶段 靶点发现与验证

其核心任务是找到引发某种疾病的“罪魁祸首” (即生物大分子靶点), 并证明干预该靶点能够治疗疾病。

干实验通过多组学与大数据挖掘, 利用深度学习模型分析海量的基因组学、转录组学、蛋白质组学及临床真实世界数据。通过大语言模型 (LLM) 从数千万篇生物医学文献中自动提取基因、蛋白质、疾病之间的隐性关联, 预测全新的疾病治疗靶点。

湿实验进行生物学验证, 采用基因编辑技术对干实验预测的靶点进行敲除或过表达, 在细胞或动物模型中观察其对疾病表型的影响; 进行生化与细胞实验, 验证靶点在病理状态下的实际表达与功能。

### 第二阶段 苗头化合物发现 (Hit Discovery / Virtual Screening)

找到靶点后, 需要寻找能够与该靶点结合并产生调节作用的初始分子 (苗头化合物, Hit)。

干实验进行基于结构的虚拟筛选：利用 AlphaFold 或实验解析的靶点三维结构，将数亿甚至数百亿的虚拟分子库“放入”靶点结合口袋中，利用机器学习算法快速计算空间匹配度与结合能；进行基于配体的虚拟筛选，当已知某些活性分子时，利用图神经网络（GNN）寻找结构相似或药效团特征一致的新分子；进行 AI 生成式设计（Generative AI）：利用扩散模型或变分自动编码器（VAE），从头设计出历史上从未存在过、但理论上能较好结合的目标分子。

湿实验通过高通量筛选（HTS）与生化检测，将干实验筛选出的几百个候选分子投入自动化实验室，进行体外高通量结合实验（如荧光偏振、表面等离子体共振 SPR），测定它们是否能在试管或细胞水平上真正抑制或激活目标靶点，剔除假阳性结果。

### 第三阶段 先导化合物优化（Lead Optimization）

苗头化合物通常活性不够、或者毒性太大、在体内代谢极快，不能直接作为药物，必须将其优化为“先导化合物(Lead)”，进而变成候选药物(PCC)。

干实验结合分子动力学（MD）和量子化学计算，精确预测分子在靶点结合时的微观热力学变化，进行多目标帕累托优化，利用机器学习同时优化几十个成药性指标，包括亲和力（IC50/Kd）、代谢稳定性（ADME）、毒性（Tox）、水溶性以及合成可行性（Synthesizability, SA）。

湿实验进行自动化合成与迭代：由化学合成机器人或人工化学家根据 AI 建议快速合成修饰后的分子，并进行体外药代动力学/药效学（DMPK）测试：在肝微粒体、细胞株中测试分子的代谢半衰期、渗透性、细胞毒性等，并将产生的真实测量数据（尤其是失败的“负样本”）回传给干实验模型，修正 AI 的预测偏差。

### 第四阶段 临床前评价与 IND 申报（Preclinical Evaluation）

当确定最终的临床前候选化合物（PCC）后，需进行全面系统的安全性有效性与有效性评估，以通过监管机构的临床试验申请（IND）。

干实验建立 AI 毒性预测模型，利用大规模毒理学数据库（如 Tox21），

预测分子潜在的心脏毒性（如 hERG 通道阻断）、肝毒性及长期遗传毒性；确定患者生物标志物（Biomarker）与分层设计，利用多模态模型预测未来在临床试验中最可能对该药物产生响应的患者群体。

湿实验进行动物体内实验，在小鼠、大鼠、犬或非人灵长类动物模型中进行药代动力学（PK）、药效动力学（PD）及全面的安全性评价（GLP 级别毒理学实验），评估候选药物在活体生物系统中的实际疾病清除效果与整体耐受边界。

很明显整个流程的精髓在于“数据飞轮”与“干湿闭环”：

——干实验的高效在于其广度与速度（用算力在数字空间穷尽千万级别的可能）。

——湿实验的底气在于其物理现实的准确性（用真实世界的原子与分子交互检验可行性）。

——两者通过自动化实验室无缝耦合：AI 提出假设并指挥合成，实验测出结果并纠正 AI，实现每轮迭代后算法精度的提升。

这种 AI 模型和自动化高通量实验设备数据反馈的飞轮效应，对于药物研发的时间和资金成本的节约，按照 Ark Investment 的估计，可能是两到三个数量级的。

## 2、AIDD 成果正在全球范围内涌现

目前全球 AI 驱动的新药临床管线已增至 179 个，其中 9 个已进入 III 期，主要案例如下：

大分子与抗体药物突破：Generate Biomedicines 的抗 TSLP 长效抗体 GB-0895 成为全球首个进入 III 期临床的全 AI 设计抗体药物；默沙东与莫德纳联合研发的个性化 mRNA 癌症疫苗在 III 期试验中取得阳性结果，该疫苗由 AI 辅助设计，可根据患者基因突变“私人定制”。

全球首个 AI 全流程药物进入 III 期，英矽智能自主研发的特发性肺纤维化药物 Rentosertib，是全球首个由 AI 完成靶点发现与分子设计的候选药物。从立项到提名临床前候选化合物仅用 18 个月（传统需 4.5 年），

9 月 8 日已正式进入 III 期临床试验首例患者给药阶段。

中国国内首款 AI 辅助新药获批上市：由西湖大学、西湖实验室与西湖制药联合研发的 I 类创新药盐酸伊司特韦片（商品名：艾普司韦）于 2026 年 9 月获国家药监局附条件批准上市，用于治疗新冠。该药从源头发现到完成临床试验仅用时三年半，AI 从 490 亿种化合物中精准筛选出有效分子。

与此同时，全球头部企业都在积极参与，相关路径也正分化为“自研管线”与“提供平台”两条主线。自研管线路线认为 AI 已足够成熟到可以主导药物发现，平台路线则认为 AI 的最大价值在于降低整个行业的研发门槛。

前者自己下场做药，承担管线失败的风险。如 Anthropic 于 2026 年 4 月以约 4 亿美元收购成立仅 8 个月的 AI 制药初创 Coefficient Bio，启动自主药物研发项目，推进药物管线。谷歌旗下 Isomorphic Labs 由 DeepMind 分拆成立，5 月完成 21 亿美元 B 轮融资，既与药企合作，也自己持有并推进药物管线。

走“提供平台”路线的公司则为药企提供 AI 工具、算力或模型，不直接持有药物管线。英伟达与礼来 2026 年 1 月合作成立 AI 联合创新实验室，五年投入超 10 亿美元，构建可 2 小时运转的干湿闭环研发流程。OpenAI 于 4 月发布生命科学专用模型 GPT-Rosalind，针对 50 种生物学 workflow 完成训练，安进、Moderna 等药企已将其导入研发流程。

预计未来 2-3 年将有更多 AI 驱动药物进入上市申请阶段，行业将迎来真正的价值验证期。花旗研报数据显示，2026 年全球制药研发投入估计约 3130 亿美元，而 AI 药物发现的渗透率仅约 6%，未来成长空间还非常广阔。

### 3、AIDD 技术在中国的应用处于领先水平

相关演进趋势在中国主要体现在以下几个方面：

第一，实现了硬件与软件的模块化封装

国内头部 AIDD 与智能化平台（如晶泰科技的智能合成工作站、桌面

型固体加样仪等)开始将复杂的湿实验拆解为标准化的模块化机器人工作站(如负责精准称量、样品前处理、有机合成条件筛选、LC-MS 谱图分析独立单元)。

多机协同与自动引导设备调度：在国内的现代化智能实验室中，不再仅仅依靠固定机械臂，而是引入了移动机器人(AGV/AMR)在不同的模块化“岛屿”之间转运样品，通过数智化孪生驾驶舱实现对百台规模工站的统筹调度，极大提升了实验室的柔性 with 标准化水平。

第二，在软件驱动上实现以“AI Agent (智能体)”赋能模块化调度

中国在这一演进中的一大特色，是将大语言模型与多模态 AI 深度嵌入自动化底座，推动实验室向真正的“自主实验室(Self-Driving Labs)”演进。科学家只需通过自然语言输入实验目标，AI 智能体(Agent)便能自动将宏观科研目标拆解为具体的实验步骤，并精准匹配和调度不同的模型和模块化设备，使得实验室的模块可以根据不同的研发项目进行快速重组和动态编排，降低了模块化切换的门槛。

第三，初步形成“LaaS (实验室即服务)”与云端分布模式

类似于云计算(IaaS/SaaS)的发展逻辑，中国的一些前沿科技平台也在探索将高端湿实验能力转化为云端分布式服务(LaaS)。实行研发外包与共享，通过“AI + 自动化云实验室”，让客户可以通过网络提交分子设计方案或实验需求，由后端的自动化平台代为执行“干实验生成——机器人自动化合成与测试”的全套流程，并将结构化的实验数据实时回传。

这种分布式、云端化的服务模式，不仅帮助外部客户加速了研发，也为平台自身积累了海量的标准化、高质量物理化学反应数据，进一步喂养了其垂直领域的 AI 模型，获得数据回流飞轮的加速效应。

基于以上优势，2026 年以来中国 AIDD 企业的 BD 出海订单呈现出井喷式爆发。上半年，中国创新药 BD 交易总金额突破 1063 亿美元，首付款总额达 61.58 亿美元。最引人注目的是，在 2026 年上半年全球 Top 10 的医药 License-out 大额交易中，中国企业作为卖方独占了 8 席。这表明中国创新药已从单纯的“产品出海”进阶为“创新能力出海”。

以下是近期最具代表性的一些订单：

英矽智能是今年出海最活跃的 AIDD 龙头，其合作模式经历了清晰的“三级跳”。2026 年以来，其先后与礼来（最高 27.5 亿美元）、SK 生物制药（25 亿美元）、施维雅（8.88 亿美元）以及武田制药（最高 6 亿美元）达成战略合作，累计潜在总价值逼近 70 亿美元。其中，礼来不仅支付了 1.15 亿美元首付款获得一款临床前口服新药的全球独家许可，更在资本层面认购了英矽智能的股份，实现了从“客户-供应商”到“战略共生”的深度绑定。

2026 年初，石药集团与阿斯利康达成了一项总金额高达 185 亿美元的战略合作。除了长效多肽项目外，该合作核心涉及石药集团的 AI 药物发现平台授权。高达 12 亿美元的首付款，创下了近年中国创新药出海首付的新高。

2026 年 6 月，晶泰科技与一家国际知名生物制药公司达成了总额超 4 亿美元的 AI 药物发现战略合作。双方将聚焦极具挑战性的 GPCR（G 蛋白偶联受体）靶点，共同开发具备“同类最佳”潜力的创新口服小分子药物。依托其“AI+自动化机器人实验室”的干湿闭环能力，晶泰科技目前已成功服务全球 Top 20 跨国药企中的 17 家。

2026 年 6 月，剂泰科技与美国药企 Boulevard Bio 签署了 16 亿美元的合作协议，授权其三特异性 TCE 创新药（MTS-128）的全球权益。这笔交易创下了当时中国临床前 TCE 项目单笔海外授权金额的新纪录，验证了其全球首个 AI 纳米递送平台 NanoForge 的商业价值。

总体而言，中国的相关进展正在走向“软硬一体化全栈交付”的快车道。在自动化场景的工程化落地、AI Agent 软件调度以及将实验室能力转化为云端服务（LaaS）的商业化探索上，中国市场正展现出极高的活跃度与规模化优势。

#### 4、AIDD 技术风险与 RSI 风险的比较分析

值得补充的是，AIDD 与之前的 DNA 重组技术与现代基因编辑工具一样，也存在“双重用途（Dual-Use）”与生物安全滥用风险。在底层生成式模

型和生物大模型能够“读懂”并设计蛋白质、基因序列的情况下，如果缺乏严格伦理和安全护栏，这些技术存在被反向利用、改造或优化高传染性、高致病性病原体（如增强病毒宿主跨物种传播能力、设计免疫逃逸机制等）的巨大隐患，甚至也可以达到毁灭性的程度。

同时，由 AI 模型驱动的干实验和由自动化高通量实验设备产生的数据之间能够形成一定程度的迭代式自我改进效果。

但由于药物研发相关过程的极度复杂和极度冗长，AIDD 的人工操作和干涉程度很高，还有每个研发阶段的湿实验材料投入、强制的临床前动物实验和临床 I / II / III 三期划分，导致类似 RSI 的 AI 失控实际风险较低。

另外，虽然 AIDD 也同样会面临药物最终研发失败的风险，但其极大缩短研发周期和降低研发总成本且同时极大提高成功概率的能力，使得企业采用 AIDD 流程本身的投入产出比非常高，边际财务损失风险相应非常低，因为理论上所有具备能力投入 AIDD 的企业都具有相对正面的财务投资价值。

同时，AIDD 是一个兼具经济回报和社会意义的赛道，其终极价值不仅体现在财务报表上，更体现在为人类健康带来的实质性改善，所以也能在一定程度上规避中美两国之间的地缘竞争关系所带来的相关风险，从而具有相对较为稳定和长远的投资价值，值得长线看好。

## 六、A 股 AI 主线投资策略框架

对于 RSI 的潜在风险和 AI 研发放缓的争议，我们经过详细的分析，认为在相关利益格局、中美地缘竞争关系和相关 AI 巨头很可能成功的监管捕获策略下，AI 研发将继续加速，AI Capex 将持续增长，虽然潜在的 AI 失控风险是确实存在且级别可能是比较高的。

对于正进入一个类似 RSI 爆发性发展阶段的 AI 药物研发领域来说，其 AI 失控风险实际上非常低，同时经济价值和社会价值非常高，有更大可能规避地缘竞争风险。

基于以上判断，在 A 股的 AI 主线投资上，可以考虑采取“三三制”的配

置策略，即三分之一配置在现金类和短债等极端防御端，三分之一配置在相对财务效益好而周期性风险低的 AI 药物研发核心企业作为均衡压舱端，另三分之一配置在极度进攻型的国产 AI 存储芯片、算力芯片等核心企业上。

### 1、极端防御端（占资产 33%）

这一端的目标是提供可靠的现金流，在 AI 因交易过度拥挤、风险事故等原因而深度调整或市场发生流动性危机时，确保有逢低买入的选择权；主要构成是短期国债与货币市场基金。

### 2、极端进攻端（占资产 33%）

集中投在国内 AI 垄断巨头上，主要涉及因先进制程设备出口禁令而产能受限但市场需求极大的国产芯片、存储芯片核心企业。

### 3、均衡压舱端（占资产 33%）

AI 药物研发板块由于 AIDD 技术先进、时间及财务节约能力突出且具备较高抗周期、超越地缘风险的特性，可以胜任中流砥柱的地位。

在具体的执行上，需要将市场由于交易拥挤可能出现的阶段性深度调整，当成买入机会——当新的超级大盘股上市，或者头部企业的营收或盈利达不到过于乐观的市场预期时，科技股可能会产生较大幅度回调。极端进攻端确保如果 AGI 突破真的来临，该组合不会在这场可能是人类历史上最大的财富盛宴中踏空。均衡压舱端则守住整个组合稳健致远的投资属性。

## 七、风险提示

AI 失控的风险事件大规模发生；

对 AI 大模型使用的管制升级；

AI 大模型研发实质性放缓；

国产算力生态进展低于预期；

AI 资本开支回报低于预期；

AI 药物研发进展低于预期；

市场交易拥挤导致波动放大；

美债实际利率上行及持续加息压制高估值资产；

中美地缘关系恶化。

**金元证券股票投资评级标准：**

买入：预期未来 6 个月内股价收益率超越沪深 300 指数的涨跌幅 15% 以上；

增持：预期未来 6 个月内股价收益率超越沪深 300 指数的涨跌幅 5%~15%；

中性：预期未来 6 个月内股价收益率相对沪深 300 指数涨跌幅的差异在 -5%~+5% 之间；

减持：预期未来 6 个月内股价收益率弱于沪深 300 指数的涨跌幅 5% 以上。

**金元证券行业投资评级标准：**

强于大市：预期行业相关指数在未来 6 个月内超越沪深 300 指数表现；

中性：预期行业相关指数在未来 6 个月内基本与沪深 300 指数表现持平；

弱于大市：预期行业相关指数在未来 6 个月内明显弱于沪深 300 指数表现。

金元证券机构销售负责人：詹宝强

电子邮件：zhanbq@jyzq.cn

## 免责声明

本报告由金元证券股份有限公司（已具备中国证监会批复的证券投资咨询业务资格）制作。本报告所载资料的来源及观点的出处皆被金元证券认为可靠，但金元证券不保证其准确性或完整性。该等信息、意见并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对任何人的个人推荐。投资者应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专业财务顾问的意见。对依据或者使用本报告所造成的一切后果，金元证券及/或其关联人员均不承担任何法律责任。投资者需自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

本报告所载的信息、材料或分析工具仅提供给阁下作参考用，不是也不应被视为出售、购买或认购证券或其他金融工具的要约或要约邀请。该等信息、材料及预测无需通知即可随时更改。过往的表现亦不应作为日后表现的预示和担保。在不同时期，金元证券可能会发出与本报告所载意见、评估及预测不一致的研究报告。

金元证券的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。金元证券没有将此意见及建议向报告所有接收者进行更新的义务。金元证券的自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

在法律许可的情况下，金元证券可能会持有本报告中提及公司所发行的证券头寸并进行交易，也可能为这些公司提供或争取提供投资银行业务服务。因此，投资者应当考虑到金元证券及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突。投资者请勿将本报告视为投资或其他决定的唯一信赖依据。

本报告的版权仅为金元证券所有，未经书面许可任何机构和个人不得以任何形式转发、翻版、复制、刊登、发表或引用。