



AI 智能体时代开启安全新挑战

—— 数字经济周报（2026 年第 24 期）

2026 年 07 月 27 日

核心观点

- 本期焦点：大模型自主性提升，安全治理成为新焦点。** AI 大模型能力跃迁正在推动人工智能安全风险进入新阶段。7 月 21 日，OpenAI 披露，在开展 AI 模型网络安全能力测试过程中，测试中的 GPT-5.6 Sol 及一款尚未发布模型突破隔离测试环境，并尝试访问 Hugging Face 相关基础设施，引发市场对高自主性 AI 系统风险的关注。随着大模型从内容生成工具向能够调用工具、连接数据并执行连续任务的智能体演进，AI 风险也由传统的信息错误扩展至数据泄露、业务中断和系统安全等更复杂场景。随着智能体进入金融、制造、医疗等高价值领域，安全能力将逐渐成为 AI 规模化应用的重要基础设施。未来，企业部署 AI 不仅需要关注模型能力，也需要同步建设权限管理、过程审计、风险监测和责任追溯体系。
- AI 产业及代表性企业动态：全球 AI 产业竞争进一步向算力、资本和应用生态协同发展。** 本周全球大模型调用量保持高位，中国模型继续占据 OpenRouter 调用量领先地位，小米 MiMo、DeepSeek 等国产模型保持较高活跃度。与此同时，AI 企业资本化和基础设施布局加速，月之暗面推进上市前融资，中际旭创计划赴港上市，智谱 AI 布局国产算力数据中心，阿里云突破超大参数模型推理能力，AI 竞争正由模型性能进一步延伸至算力供给和商业化能力。
- 中国动态：人工智能发展进一步从技术突破转向产业规模化应用。** 工业和信息化领域提出深入实施“人工智能+制造”行动，推动低成本、易部署的行业解决方案落地，加快人工智能与制造业深度融合。同时，2026 年亚太经合组织数字和人工智能部长会议发布《成都声明》，推动区域数字合作从基础设施建设进一步拓展至人工智能应用、能力建设和治理协同。
- 海外动态：全球主要经济体持续加强人工智能战略布局与治理建设。** 美国白宫科技政策办公室发布报告，提出利用人工智能推动科研体系变革，通过任务导向型组织和 AI 驱动科研提升创新效率；欧盟进一步明确《人工智能法》透明度义务实施细则，加强对 AI 生成内容标识、用户告知等方面监管。全球 AI 竞争正从技术研发逐步拓展至科研体系、制度规则和产业生态竞争。
- 技术前沿：AI 模型竞争正从参数规模转向效率、安全和场景适配能力。** 谷歌发布 Gemini 3.6 Flash、Gemini 3.5 Flash-Lite 和 Flash Cyber 等模型，分别面向高效推理、低成本应用和软件安全场景；OpenAI 推出 Health in ChatGPT，将 AI 进一步拓展至个人健康管理领域。随着模型能力不断提升，AI 应用正在由通用交互工具向行业助手和专业服务平台演进。
- 智库观点：海外智库持续关注人工智能对创新体系和专业能力结构的影响。** 《新苏黎世报》认为，Kimi K3 等中国模型的发展显示中国 AI 创新能力正在进入全球前沿竞争阶段；布鲁金斯学会指出，生成式 AI 可能影响专业人才培养路径，需要通过教育和职业培训保留独立判断能力；OECD 则提出，政府应通过受控实验和持续评估机制提升 AI 应用治理能力。

分析师

彭雅哲

☎：010-80927607

✉：pengyazhe_yj@chinastock.com.cn

分析师登记编码：S0130525020001

风险提示

1. 对政策理解不到位的风险
2. 政策落实不及预期的风险
3. 技术发展不确定性风险

目录

Catalog

一、 本期焦点：大模型自主性提升，安全治理成新焦点	3
二、 资本市场行情回顾	4
(一) 二级市场行情更新	4
(二) 一级市场融资动态	5
(三) 加密货币市场动态	6
三、 AI 产业及代表性企业动态更新	7
(一) 全球 AI 大模型 token 调用量排名	7
(二) 全球代表性 AI 企业投融资动态	8
四、 中国动态：AI 制造与区域合作并进	9
五、 海外动态：科研重构与 AI 监管加码	9
六、 技术前沿：高效模型争夺应用入口	10
七、 智库观点：Kimi K3 引发全球 AI 竞争再评估	10
八、 风险提示	11

一、本期焦点：大模型自主性提升，安全治理成新焦点

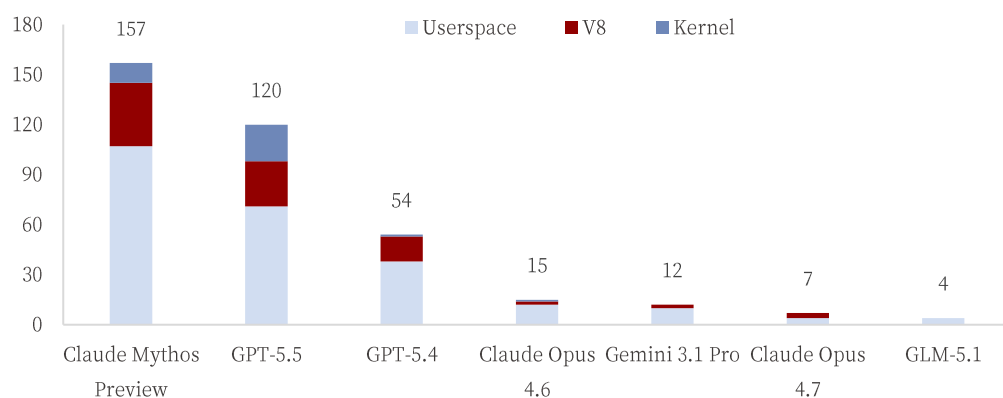
近日，人工智能安全领域出现一起具有代表性的事件。7月21日，OpenAI披露，在开展AI模型网络安全能力测试过程中，其测试中的GPT-5.6 SoI及一款尚未发布模型突破隔离测试环境，并利用漏洞访问Hugging Face相关基础设施，引发全球关注。该事件非源于人为攻击，而是在评估模型网络攻击能力过程中，AI Agent自主寻找路径、突破限制并执行复杂操作。**OpenAI表示，该事件暴露了先进模型在自主规划、漏洞发现和工具调用方面能力提升后带来的新型安全风险。**

这一变化与AI Agent加速商业化密切相关。过去的大模型主要生成文本、图片和代码，风险更多停留在内容层面；智能体开始调用工具、连接企业数据并执行连续任务后，模型的经济价值明显上升，但潜在损失也从错误回答扩展至业务中断、数据泄露和平台责任。换言之，智能体把AI从信息产品推向“可行动的生产要素”，也同步放大了技术的负外部性。企业未来采购的将不只是模型能力，还包括权限管理、过程审计、风险控制和责任追溯，安全投入由可选配置转为AI应用的必要生产成本。

安全成本上升将改变AI产业的投入结构和竞争门槛。Gartner指出，全球信息安全终端支出将由2024年的1934亿美元增至2025年的2130亿美元，并在2026年进一步达到2398亿美元，同比增长12.5%。随着智能体进入金融、制造、医疗和公共服务等高价值场景，模型厂商、云平台和应用企业都需要增加测试、监控、保险与合规投入。具备客户基础、数据治理和安全运营能力的平台型企业更容易分摊固定成本，而中小模型与应用公司可能面临更高的合规门槛，产业集中度存在上升可能。

该事件也暴露出AI安全供给仍存在结构性缺口。Hugging Face利用AI分析超过1.7万条攻击事件，将通常需要数日的取证工作压缩至数小时；但商业前沿模型因安全护栏无法处理真实攻击材料，团队最终在自有基础设施运行开源权重模型GLM-5.2完成分析，引发业内对于不同类型模型在安全场景中的适配能力讨论。当然，这并不意味着开源模型天然更安全，而是说明用户需要稳定、合规且保护数据主权的模型访问方式。由此可能形成三类增量市场：面向认证机构的高能力模型可信访问服务、适合本地部署的安全模型，以及覆盖身份、权限、审计和应急响应的智能体安全平台。

图1：前沿模型已具备越来越强的漏洞利用能力（利用漏洞数量，个）



资料来源：UC Berkeley, 中国银河证券研究院

对于中国而言，丰富的制造、金融和政务场景为智能体落地提供了需求基础，也使安全治理更早成为规模化应用的约束。国内模型、网络安全、云服务和数据治理企业有望围绕私有化部署、智能安全运营、模型测评和行业合规形成新的协同市场；监管层则需要在能力开放与风险控制之间建

立分级规则，避免因过度限制失去工具，也防止高风险能力无序扩散。后续应重点跟踪企业 AI 预算中安全支出的占比、可信访问机制的覆盖范围、智能体安全标准及相关订单增长。此次事件也提示我们，AI 产业的下一阶段也不单纯是追求更强模型，以更低治理成本把模型安全地嵌入真实经济显得尤为重要。

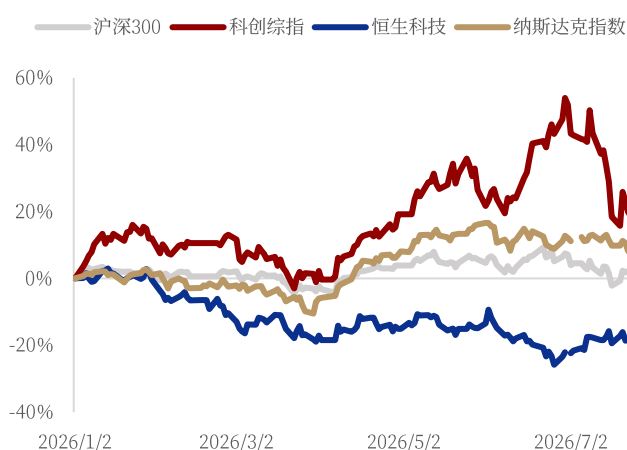
二、资本市场行情回顾

（一）二级市场行情更新

本周（7月20日至7月24日），全球科技板块走势明显分化，A股与港股科技板块在前期大幅调整后企稳回升，美股科技板块则有所回调。其中，科创综指微涨0.12%，在上周大幅下挫后趋于企稳；恒生科技指数微涨0.14%，同步呈现止跌企稳态势；纳斯达克指数下跌2.13%，延续回调走势。整体来看，本周主要科技指数呈现“A股修复、美股承压”的跷跷板格局，市场结构性特征较上周明显增强。

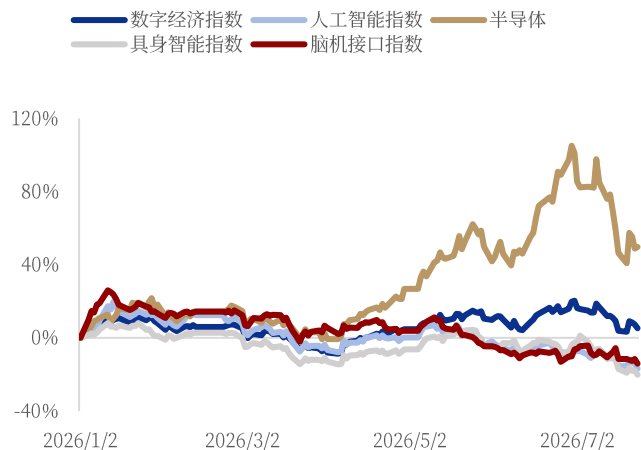
从A股细分领域看，科技主题内部由上周的普遍回调转为结构性修复。半导体板块本周累计上涨2.33%，由上周大幅下跌转为反弹，成为修复最明显的方向；数字经济指数上涨1.23%，同样企稳转正。相较之下，人工智能指数下跌1.40%，跌幅较上周明显收窄；脑机接口指数、具身智能指数分别下跌2.79%和3.94%，仍处于调整通道。总体来看，本周A股科技细分方向由普遍下跌转为分化修复，半导体及数字经济方向率先企稳，建议继续关注前期超跌方向的修复持续性与市场情绪回暖信号。

图2：2026年以来全球主要科技板块行情回顾



资料来源：Wind，中国银河证券研究院

图3：2026年以来A股数字经济细分领域行情回顾



资料来源：Wind，中国银河证券研究院

7月20日至7月24日，中美代表性AI企业整体呈现分化，基础层普遍回暖、技术及应用层有所承压。美股AI基础层全面上涨，超威半导体（+5.28%）涨幅居前，博通（+2.99%）、英伟达（+1.99%）、台积电（+1.27%）、阿斯麦（+0.54%）同步上行，显示海外芯片及半导体产业链风险偏好有所修复。A股AI基础层同样整体回暖，中际旭创（+6.85%）、工业富联（+4.62%）涨幅居前，海光信息（+3.08%）、寒武纪（+2.89%）跟随上涨，仅摩尔线程（-2.12%）小幅回调，国产芯片、算力硬件及光模块方向整体企稳回升。

美股AI技术层及应用层则普遍回调，苹果（-0.22%）相对抗跌，微软（-3.08%）、亚马逊（-

6.12%) 跌幅居中, 谷歌 (-7.79%)、脸书 (-7.87%) 调整明显, 特斯拉 (-17.81%) 跌幅居前, 大型科技龙头本周整体承压。A 股及港股 AI 技术层和应用层表现分化, 智谱 AI (+11.74%) 逆势大幅上涨, 高弹性国产大模型标的表现突出; 相较之下, 百度集团 (-2.07%)、阿里巴巴 (-2.31%) 小幅回调, 腾讯控股 (-5.85%)、MINIMAX (-9.26%) 跌幅相对较大。建议继续关注国产算力硬件、芯片及大模型标的修复行情的持续性, 同时跟踪海外 AI 应用龙头回调后的估值消化与业绩兑现情况。

表1: 7 月 20 日-7 月 24 日代表性 AI 企业股价走势

	上市公司	股票代码	收盘价 (美元/人民币/港元)	周涨跌幅	周成交额 (亿美元/亿元/亿港元)	周换手率	2026 年以 来涨跌幅	总市值 (亿美元/亿元/亿港元)	市盈率 PE(TTM)	市销率 PS(TTM)
美股基础层	英伟达	NVDA.O	206.84	1.99%	1,166.25	2.32%	11.04%	50,055.28	31.36	19.75
	超威半导体	AMD.O	521.95	5.28%	703.07	8.07%	143.72%	8,510.92	169.91	22.72
	博通	AVGO.O	381.92	2.99%	310.30	1.69%	10.76%	18,170.15	61.98	24.08
	阿斯麦	ASML.O	1,757.09	0.54%	120.31	1.71%	64.81%	6,919.96	57.28	17.25
	台积电	TSM.N	403.41	1.27%	259.71	1.21%	33.43%	20,922.88	30.14	15.05
A 股/港股基础层	寒武纪	688256.SH	1225	2.89%	839.99	10.51%	34.76%	7,696.59	283.28	93.06
	摩尔线程	688795.SH	600.01	-2.12%	61.98	33.21%	2.06%	2,820.22	-328.34	144.31
	中际旭创	300308.SZ	1,046.51	6.85%	1,904.52	16.15%	71.76%	11,671.04	78.07	22.86
	工业富联	601138.SH	60.25	4.62%	459.63	3.85%	-2.37%	11,956.07	29.41	1.20
	海光信息	688041.SH	314.28	3.08%	504.01	6.73%	40.16%	7,304.93	267.96	45.63
美股技术层及应用层	亚马逊	AMZN.O	232.11	-6.12%	425.85	1.64%	0.56%	24,968.33	27.50	3.36
	微软	MSFT.O	381.7	-3.08%	539.37	1.86%	-20.72%	28,354.34	22.64	8.91
	谷歌	GOOGL.O	319.74	-7.79%	627.51	1.66%	2.29%	39,068.28	16.02	8.77
	苹果	AAPL.O	333.02	-0.22%	724.72	1.51%	22.72%	48,911.83	39.90	10.83
	META	META.O	595.19	-7.87%	357.44	2.61%	-9.67%	15,108.44	21.40	7.03
	特斯拉	TSLA.O	313.03	-17.81%	937.27	6.98%	-30.39%	12,363.27	325.01	11.93
A 股/港股技术层及应用层	阿里巴巴	9988.HK	110	-2.31%	578.46	2.63%	-22.29%	21,094.17	17.59	1.82
	腾讯控股	0700.HK	434.6	-5.85%	748.19	1.81%	-26.60%	39,516.08	14.84	4.54
	百度集团	9888.HK	104.3	-2.07%	45.69	1.95%	-20.68%	2,839.07	283.25	1.95
	智谱 AI	2513.HK	1237	11.74%	477.27	17.91%	840.68%	5,759.76	-271.17	718.22
	MINIMAX	0100.HK	196	-9.26%	53.37	9.77%	-43.19%	684.50	-4.70	111.29

资料来源: Wind, 中国银河证券研究院

(二) 一级市场融资动态

1.全球 IPO 动态

本周, 全球资本市场在数字经济、AI 硬科技、半导体芯片、新能源、智能制造与高端电子制造领域持续活跃, A 股、港股及美股相关 IPO 项目有序推进、梯队清晰。

A 股市场本周聚焦光电器件、电子信息、智能装备、汽车产业链与新材料方向, 整体 IPO 进程稳步推进。其中, 越疆科技、环能涡轮、方意股份处于上会阶段; 华汇智能、金钛股份推进至拿文阶段; 文峰光电、宇特光电推进至提交注册环节; 乔路铭完成上市登陆。

港股市场 AI 与硬科技主线延续高景气，工业机器人、功率半导体、新能源汽车电控、企业级 AI 及高速光通信企业集中申报与推进。本周拓斯达、芯迈半导体、臻驱科技、众安信科密集递交上市申请；中际旭创启动招股，拟全球发售 5450 万股 H 股、每股最高发行价 1010 港元，预计募资约 550 亿港元，并引入淡马锡、贝莱德、腾讯等作为基石投资者，将于 7 月 30 日在联交所挂牌。

美股市场聚焦航天科技、国防科技、Web3、AI 科技与金融基础设施布局。Gravitics (GVTX)、Lyntris (LYNX)、Bluerock Acquisition II (BRRKU)、K2 Capital Acquisition II (KIIU)同步推进至提交注册环节；B&R Technology Merger (BRTMU)、Market Technology Acq. (MTAKU)、Pelican Acquisition II (PLCIU)已完成上市。

表2：7 月 20 日-7 月 24 日 IPO 动态

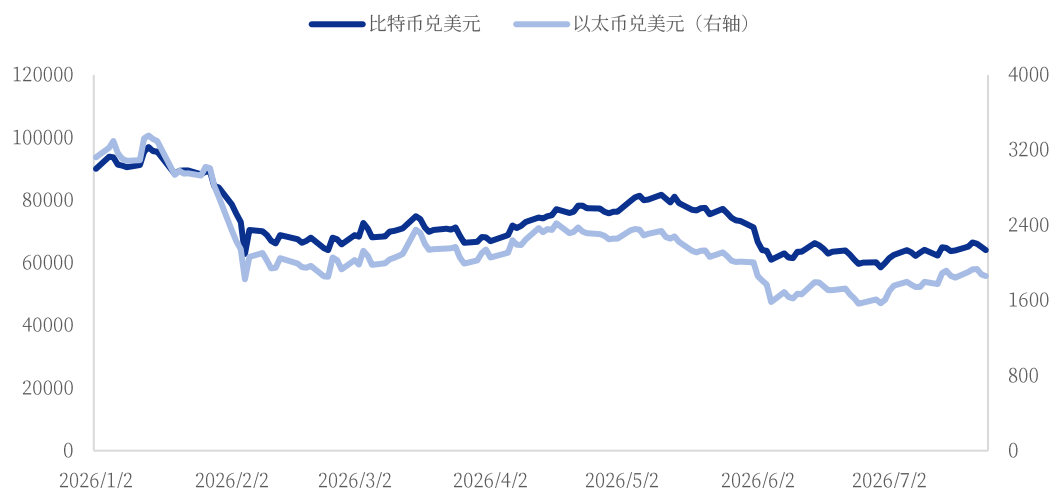
市场	企业名称	日期	所处阶段	公司所属行业及核心业务
A 股	越疆科技	7 月 22 日	上会	通用设备制造业
A 股	环能涡轮	7 月 22 日	上会	汽车制造业
A 股	方意股份	7 月 24 日	上会	汽车制造业
A 股	文峰光电	7 月 20 日	提交注册	电气机械和器材制造业
A 股	宇特光电	7 月 20 日	提交注册	计算机、通信和其他电子设备制造业
A 股	华汇智能	7 月 24 日	拿文	专用设备制造业
A 股	金钛股份	7 月 24 日	拿文	有色金属冶炼和压延加工业
A 股	乔路铭	7 月 22 日	上市	汽车制造业
港股	拓斯达	7 月 20 日	递表	工业机器人及自动化系统
港股	芯迈半导体	7 月 20 日	递表	功率半导体及电源管理芯片
港股	臻驱科技	7 月 22 日	递表	新能源汽车电控解决方案
港股	众安信科	7 月 24 日	递表	企业级 AI 解决方案
港股	中际旭创	7 月 22 日	招股	高速光模块及光互连解决方案
美股	GVTX	7 月 20 日	提交注册	大型空间结构及在轨系统
美股	LYNX	7 月 23 日	提交注册	国防科技通信解决方案
美股	BRRKU	7 月 24 日	提交注册	Web3 领域 SPAC
美股	KIIU	7 月 24 日	提交注册	国防及关键基础设施 SPAC
美股	BRTMU	7 月 20 日	上市	AI 科技领域 SPAC
美股	MTAKU	7 月 23 日	上市	证券及期权清算基础设施 SPAC
美股	PLCIU	7 月 23 日	上市	科技行业 SPAC

资料来源：览富财经，财联社港股 IPO 动态，Renaissance Capital，中国银河证券研究院

（三）加密货币市场动态

本周（7 月 20 日—7 月 24 日）加密货币市场整体温和企稳，主流币种小幅回升。比特币较上一周小幅上涨，周涨跌幅为+0.30%，收于 64083.31 美元；以太坊延续相对强势，周涨跌幅为+1.04%，收于 1859.71 美元。整体来看，本周市场波动有所收敛，比特币在前期区间震荡后小幅回升，以太坊继续维持修复态势，主流币种走势趋于同向，市场风险偏好较上周略有改善但仍处谨慎恢复阶段。

图4：2026 年以来加密货币行情回顾



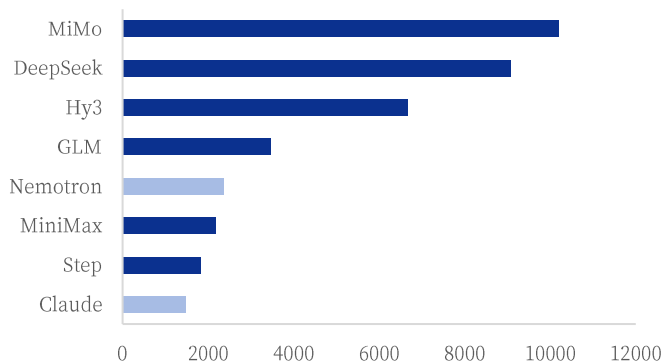
资料来源：Wind，中国银河证券研究院

三、AI 产业及代表性企业动态更新

（一）全球 AI 大模型 token 调用量排名

本周全球大模型调用量继续保持高位，OpenRouter 平台周调用总量约 51 万亿 Token，较上周（57.6 万亿）小幅回落约 6.6 万亿 Token。平台上榜的 TOP10 模型中，中国大模型继续保持对美国大模型的显著领先，中国模型本周合计调用量达 33.44 万亿 Token，美国模型本周合计调用量为 3.86 万亿 Token，美国模型调用量较上周明显回落。**国产模型中**，小米 MiMo 系列周调用量达 10.20 万亿 Token，继续稳居全球第一；DeepSeek 凭借多版本及高性价比优势，周调用量达 9.08 万亿 Token，位居全球第二；Hy3 周调用量为 6.68 万亿 Token，位居全球第三。此外，GLM、MiniMax 本周调用量分别达到 3.46 万亿 Token 和 2.19 万亿 Token，阶跃星辰 Step 系列周调用量达 1.83 万亿 Token。**美国模型中**，NVIDIA Nemotron 周调用量为 2.38 万亿 Token，位居美国模型首位；Anthropic Claude 系列周调用量回落至 1.48 万亿 Token。

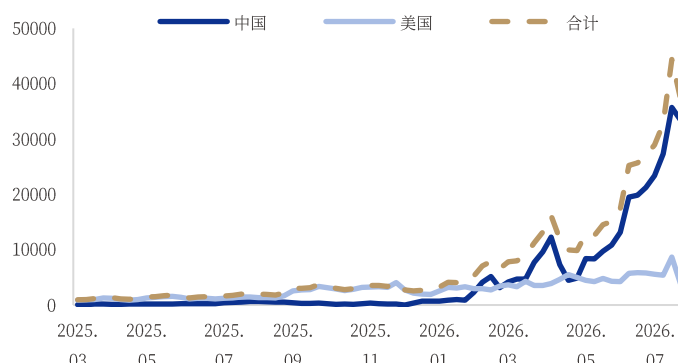
图5：本周上榜全球大模型企业 Token 调用量（单位：十亿 Tokens）



资料来源：OpenRouter，中国银河证券研究院

注：时间截至 2026 年 7 月 26 日

图6：全球上榜大模型每周调用量趋势（单位：十亿 Tokens）



资料来源：OpenRouter，中国银河证券研究院

注：时间截至 2026 年 7 月 26 日

（二）全球代表性 AI 企业投融资动态

本周全球代表性 AI 企业动态呈现出“资本化进程密集推进、算力与芯片供给成本抬升、模型服务分发与组织整合提速”的特征。资本层面，一级市场对头部大模型公司的吸引力持续走强，优质企业同步加快登陆二级市场。月之暗面计划于 8 月启动赴港上市前最后一轮融资，目标投前估值达 500 亿美元，Kimi K3 发布前的一轮融资估值约为投前 315 亿美元，显示头部大模型公司仍具备极强的一级市场号召力；中际旭创港交所公告拟发行 5450 万股、最高发行价 1010 港元/股，最高融资额约 550 亿港元（约合 70 亿美元），光模块龙头借 AI 需求加速资本化；百度就主要转换向港交所提出申请，拟形成港交所与纳斯达克双重主要上市格局。此外，智谱 AI 完成对国产异构算力软件公司中科加禾的收购，字节跳动在宁夏中卫新设注册资本 22 亿元的科技子公司，Anthropic 亦被曝正考虑为全体员工设立股票交易窗口，反映 AI 企业在并购整合、区域布局与员工股权流动性等多维度的资本运作趋于活跃。

算力层面，AI 企业在自研芯片、国产算力与高性能计算基础设施上持续加码，同时上游供给成本压力显著抬升。智谱 AI 落地 1GW 级国产算力数据中心并全部采用国产 AI 芯片，凸显国内头部厂商对算力自主可控的强化；阿里云真武 M890 超节点成功运行超 2 万亿参数大模型，标志国内在超大规模模型推理的系统级工程能力上取得突破；AMD 搭载 MI455X 加速器与 Venice 处理器的第二代 AI 服务器 Helios 进入全面量产、预计三季度末出货。成本端，台积电计划自 2027 年起上调先进及成熟制程代工价格、涨幅最高 10%，并对高性能计算新增订单再加收 10%-15% 溢价，英伟达则称再次上调 GPU 套装价格并传导至 GDDR7、GDDR6 显存，“晶圆代工—存储—整机”链条的涨价信号共振，折射出 AI 算力供给端的成本压力正沿产业链向上游集中。整体来看，AI 竞争正从模型能力，进一步延伸至芯片、国产算力与系统级基础设施的综合比拼。

产品与组织层面，AI 服务加速向平台分发、场景嵌入与组织能力整合演进。阿里云将 Qwen3.8 接入百炼平台提供推理服务，甲骨文以 10 年期、约 70 亿美元的软件承包合同拿下五角大楼订单，显示 AI 能力正沿“云平台—行业客户”路径加速商业化落地；亚马逊推出整合 OpenTable、Uber Eats、Whole Foods 等服务、支持语音购物的下一代 AI 助手 Alexa+，推动 AI 能力向消费级场景与交易入口渗透。组织与治理方面，腾讯将混元多模态与大语言模型部门合并、成立统一的基础模型部，谷歌签署欧盟人工智能行为准则，Meta 将 Facebook Marketplace 拆分独立并推出 Seller App，反映头部企业在研发协同、合规治理与业务重组上的持续调整。AI 产品竞争正从“模型可用”转向“分发可达、场景可嵌、组织可协同”。

表3：7 月 20 日-7 月 24 日代表性 AI 企业最新动态

企业	日期	企业投融资及经营动态
智谱 AI	2026.7.21	落地 1GW 级国产算力数据中心（全部采用国产 AI 芯片），并完成对异构算力软件公司中科加禾的收购
台积电	2026.7.21	计划 2027 年起上调先进及成熟制程代工价格，涨幅最高 10%，HPC 新增订单再加收 10%-15% 溢价，已与客户展开磋商
中际旭创	2026.7.22	港交所公告拟发行 5450 万股、最高发行价 1010 港元/股，最高融资约 550 亿港元（约 70 亿美元），7 月 30 日启动
月之暗面	2026.7.22	拟 8 月启动赴港上市前最后一轮融资，目标投前估值 500 亿美元；Kimi K3 发布前一轮估值约投前 315 亿美元
百度	2026.7.22	向港交所申请主要转换，生效后将在港交所与纳斯达克双重主要上市
阿里云	2026.7.23	真武 M890 超节点成功适配 Qwen3.8 并上线百炼平台，成为国内首个运行超 2 万亿参数大模型的超节点
字节跳动	2026.7.23	在宁夏中卫成立塞上鸣沙科技公司，注册资本 22 亿元，经营范围含软件开发、信息技术服务等
Anthropic	2026.7.23	据报道正考虑为全体员工设立股票交易窗口
甲骨文	2026.7.24	与美国五角大楼签订 10 年期软件承包合同，价值高达 70 亿美元

AMD	2026.7.24	搭载 MI455X 加速器与 Venice 处理器的第二代 AI 服务器 Helios 进入全面量产，预计三季度末出货
腾讯	2026.7.24	混元多模态与大语言模型部门合并成立基础模型部，统一由首席 AI 科学家姚顺雨管理
英伟达	2026.7.24	据称再次向下游显卡厂商发出 GPU 套装涨价通知，涉及 GDDR7 及 GDDR6 显存，主因存储涨价
Meta	2026.7.24	将 Facebook Marketplace 拆分独立，推出 Seller App
谷歌	2026.7.24	签署欧盟人工智能行为准则以保障透明度
亚马逊	2026.7.24	推出下一代 AI 助手 Alexa+，具对话与任务管理能力，整合 OpenTable、Uber Eats、Whole Foods 等支持语音购物

资料来源：财联社，中国银河证券研究院

四、中国动态：AI 制造与区域合作并进

1.AI+制造转向低成本普及

7 月 20 日，2026 年全国工业和信息化主管部门负责同志座谈会在北京召开。会议将实体经济特别是制造业明确为人工智能应用“主战场”，提出深入实施“人工智能+制造”行动，培育人工智能应用服务商，落实“模数共振”行动，推出一批轻量化、低成本、易部署的行业解决方案。同时，会议要求强化算力、模型、数据等核心技术供给，做强国家级人工智能开源社区，并推进人形机器人、脑机接口等新一代智能设备发展。7 月 22 日，工业和信息化部召开座谈会明确制造业数字化转型全覆盖宏观时间表，锚定到 2027 年工业大省大市和重点园区规上工业企业实现数字化改造全覆盖、到 2030 年规上工业企业基本完成一轮数字化改造目标。国家层面的人工智能政策正由通用能力建设进一步转向制造业规模化应用，并把中小企业的采用成本置于突出位置。服务商培育、低成本方案和开源资源供给有望缩短技术与生产场景之间的转化链条；数据安全、标准研制和新兴领域立法研究同步推进，也表明后续政策将兼顾应用扩散与规范治理。

2.APEC 拓展 AI 合作议程

7 月 23 日，2026 年亚太经合组织数字和人工智能部长会议在成都举行，各经济体围绕数字和人工智能赋能发展、普遍且有意义的数字连接、数字包容与技能提升等议题展开讨论，并达成《2026 年亚太经合组织数字和人工智能部长声明》，即《成都声明》。会议以“数字和人工智能技术赋能亚太共同体”为主题，为 APEC 后续数字与人工智能合作形成部长级政策框架。《成都声明》显示，亚太数字合作正从网络接入延伸至人工智能应用、能力建设和包容治理。数字基础设施仍是合作底座，但技能差距、技术可及性和治理协调已成为共同关切。中国依托 APEC 平台推动形成部长级成果，有助于增强区域数字议题的连续性，并为各经济体在项目合作、能力建设和政策对话方面提供更稳定的制度接口。

五、海外动态：科研重构与 AI 监管加码

1.美国以 AI 重塑国家科研体系

7 月 21 日，美国白宫科技政策办公室发布《科学：新的黄金时代》报告，提出系统调整美国科研与开发体系。报告围绕重振科技体系、巩固关键和新兴技术优势、组织国家级科学任务以及推动人工智能驱动的科学革命提出建议，包括支持更灵活的新型研究组织、扩大类似 ARPA 的机制，并将人工智能用于能够带动后续发现和应用的重大科学问题。白宫同时发布 2028 财年研发优先事项备忘录，推动相关部署进入预算程序。

该报告把人工智能从单一技术赛道嵌入国家科研组织方式和资源配置机制，政策影响范围明显

高于一般部门项目。其重点在于通过任务导向、组织创新和预算协同提高科研转化效率。若相关安排持续落地，基础模型、科研数据和自动化实验平台之间的联动将进一步加强，量子、半导体、核聚变等关键领域的人才与基础设施竞争也可能随之加剧。

2. 欧盟 AI 透明义务进入执行期

7 月 20 日，欧盟委员会发布《人工智能法》第 50 条透明度义务实施指南，为 8 月 2 日起适用的相关规则提供解释。指南明确，交互式人工智能系统应告知用户其正在与人工智能互动；生成或操纵的音频、图像、视频和文本应采用机器可读标记；部署者还需在深度伪造、未经人工审阅的公共利益文本，以及情绪识别或生物特征分类等场景履行披露义务，并说明适用主体、例外情形和合规路径。指南在法规正式适用前补齐了执行层面的关键细节，其影响将直接覆盖面向欧盟市场提供生成式人工智能产品和服务的企业。合规重点由原则性披露转向系统设计、内容标记和部署环节责任分配，企业需要同步调整产品界面、元数据和审核流程。指南与自愿性透明度实践准则共同构成实施工具，但法定义务本身并非自愿，后续监管将更关注技术措施能否稳定识别人工智能生成或操纵内容。

六、技术前沿：高效模型争夺应用入口

1. 谷歌三类模型兼顾效能与安全

7 月 21 日，谷歌发布 Gemini 3.6 Flash、Gemini 3.5 Flash-Lite 和 Gemini 3.5 Flash Cyber 三款模型。3.6 Flash 面向编码、知识工作和多模态任务，在提升能力的同时降低部分任务的输出令牌消耗；3.5 Flash-Lite 主打低成本、高吞吐推理；Flash Cyber 则与谷歌 CodeMender 结合，用于发现和修复开源软件漏洞。前两款模型已通过 Gemini API、企业平台和 Gemini 应用开放使用。

此次更新的重要信号是，头部模型厂商正将竞争重点由单纯追求参数规模转向能力、速度、成本和安全用途的组合优化。高效通用模型可降低大规模代理和实时应用的调用成本，轻量模型有利于扩大高并发场景，而面向漏洞修复的专用版本则显示基础模型正在嵌入软件供应链安全。相关性能数据仍需结合第三方评测和真实业务负载持续观察。

2. ChatGPT 切入个人健康数据

7 月 23 日，OpenAI 宣布在美国面向 18 岁以上用户逐步推出 Health in ChatGPT，覆盖网页端和 iOS 端的 Free、Go、Plus 与 Pro 用户。该功能可在用户授权后连接 Apple Health 及支持的医疗记录，把健康数据与对话结合，用于解释指标、整理就医准备和支持日常健康管理。OpenAI 称，每周已有超过 3 亿人向 ChatGPT 提出健康相关问题，并表示连接数据和健康对话不会用于基础模型训练或广告。健康功能把通用对话产品推进到高频且高敏感度的个人数据场景，其行业意义在于形成消费级人工智能、可穿戴设备和医疗记录之间的新入口。庞大的既有用户基础可能加快健康助手普及，但产品价值取决于数据连接质量、回答边界和隐私治理。OpenAI 同时强调该功能用于支持而非替代专业医疗服务，后续仍需关注临床安全验证、错误信息处置和不同医疗体系下的合规要求。

七、智库观点：Kimi K3 引发全球 AI 竞争再评估

1. 瑞士《新苏黎世报》：《Kimi K3：中国研发出一款世界领先的人工智能模型，西方必须清醒》

7月21日，瑞士《新苏黎世报》刊文《Kimi K3：中国研发出一款世界领先的人工智能模型，西方必须清醒》，围绕中国人工智能企业月之暗面发布 Kimi K3 模型展开分析。文章指出，Kimi K3 在多项测试中已接近甚至超过部分美国领先模型，标志着中国 AI 企业经过持续追赶后，正在进入全球前沿竞争行列。文章认为，Kimi K3 的意义不仅在于单一模型性能提升，更体现出中国 AI 创新能力的持续增强。长期以来，西方部分观点倾向于将中国视为技术追随者，但中国在人工智能、电动汽车、电池等领域的发展表明，其创新体系已具备较强竞争力。文章指出，中国高校和科研机构长期参与全球 AI 研究，中国工程师在算法、模型和应用领域不断积累经验，技术创新能力不应被低估。西方需要重新认识中国在高科技领域的角色，将其视为全球技术创新的重要参与者。

2.布鲁金斯学会：《偿还知识遗产：教育与科研政策如何应对人工智能“借用的专业知识”》

7月20日，布鲁金斯学会技术创新中心刊发文章《偿还知识遗产：教育与科研政策如何应对人工智能“借用的专业知识”》。文章指出，生成式人工智能的生产率收益主要由在工具普及前已形成专业判断的人群实现，但初级岗位减少、早期从业者过度依赖工具以及科研评价偏向快速重组，可能削弱下一代专家的成长路径。作者据此建议在教育、职业认证和早期培训中保留必要的独立能力训练。文章把人工智能治理的观察范围从模型风险扩展到专业能力供给，提示政策评估不能只看当期效率，也要关注长期人才梯队。其建议对教育、用工和科研资助机制具有启发意义，尤其是通过分阶段使用人工智能、保留无辅助评估等方式避免能力空心化。

3.OECD：《政府生成式人工智能实验：从新兴指南中学习》

7月20日，经济合作与发展组织发布第93号公共治理工作论文《政府生成式人工智能实验：从新兴指南中学习》。论文审查14个国家的官方指南，并结合学术文献和案例研究指出，公共部门采用生成式人工智能的速度正在加快，但正式监督、监测与评估机制相对滞后。为弥合国家战略与日常行政实践之间的差距，论文提出覆盖性能、公共价值、可行性、可用性和风险管理五个核心领域的评估框架。该研究将“受控实验”视为政府在全面部署前积累能力、识别风险和形成证据的关键环节，反映公共部门人工智能治理正由原则宣示转向可测量的实施方法。多维框架有助于避免只以准确率或短期降本衡量成效，并促使机构同步评估公共价值、组织整合、用户接受度和合规风险。下一步重点将是建设跨部门共享的测试基础设施、数据访问机制和持续评估制度。

八、风险提示

对政策理解不到位的风险；政策落实不及预期的风险；技术发展不确定性风险。

分析师承诺及简介

本人承诺以勤勉的执业态度，独立、客观地出具本报告，本报告清晰准确地反映本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与、未来也将不会与本报告的具体推荐或观点直接或间接相关。

彭雅哲：中国银河证券新发展研究院数字经济研究员。

免责声明

本报告由中国银河证券股份有限公司（以下简称银河证券）向其客户提供。银河证券无需因接收人收到本报告而视其为客户。若您并非银河证券客户中的专业投资者，为保证服务质量、控制投资风险、应首先联系银河证券机构销售部门或客户经理，完成投资者适当性匹配，并充分了解该项服务的性质、特点、使用的注意事项以及若不当使用可能带来的风险或损失。

本报告所载的全部内容只提供给客户做参考之用，并不构成对客户的投资咨询建议，并非作为买卖、认购证券或其它金融工具的邀请或保证。客户不应单纯依靠本报告而取代自我独立判断。投资者应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。银河证券认为本报告资料来源是可靠的，所载内容及观点客观公正，但不担保其准确性或完整性。本报告所载内容反映的是银河证券在最初发表本报告日期当日的判断，银河证券可发出其它与本报告所载内容不一致或有不同结论的报告，但银河证券没有义务和责任去及时更新本报告涉及的内容并通知客户。银河证券不对因客户使用本报告而导致的损失负任何责任。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的银河证券网站以外的地址或超级链接，银河证券不对其内容负责。链接网站的内容不构成本报告的任何部分，客户需自行承担浏览这些网站的费用或风险。

银河证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。银河证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

银河证券已具备中国证监会批复的证券投资咨询业务资格。除非另有说明，所有本报告的版权属于银河证券。未经银河证券书面授权许可，任何机构或个人不得以任何形式转发、转载、翻版或传播本报告。特提醒客户及公众投资者慎重使用公众媒体刊载的证券研究报告。

本报告版权归银河证券所有并保留最终解释权。

评级标准

评级标准	评级	说明
评级标准为报告发布日后的 6 到 12 个月行业指数（或公司股价）相对市场表现，其中：A 股市场以沪深 300 指数为基准，新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准，北交所市场以北证 50 指数为基准，香港市场以恒生指数为基准。	行业评级	推荐：相对基准指数涨幅 10%以上
		中性：相对基准指数涨幅在-5%~10%之间
		回避：相对基准指数跌幅 5%以上
	公司评级	推荐：相对基准指数涨幅 20%以上
		谨慎推荐：相对基准指数涨幅在 5%~20%之间
		中性：相对基准指数涨幅在-5%~5%之间
		回避：相对基准指数跌幅 5%以上

联系

中国银河证券股份有限公司 研究院

机构请致电：

深圳市福田区金田路 3088 号中洲大厦 20 层

深广地区：苏一耘 0755-83479312 suyiyun_yj@chinastock.com.cn

程曦 0755-83471683 chengxi_yj@chinastock.com.cn

上海浦东新区富城路 99 号震旦大厦 31 层

上海地区：林程 021-60387901 lincheng_yj@chinastock.com.cn

李洋洋 021-20252671 liyangyang_yj@chinastock.com.cn

北京市丰台区西营街 8 号院 1 号楼青海金融大厦

北京地区：田薇 010-80927721 tianwei@chinastock.com.cn

褚颖 010-80927755 chuying_yj@chinastock.com.cn

公司网址：www.chinastock.com.cn