

A I 前沿发展日报 | 2 0 2 6 - 0 8 - 0 6 (A s i a)

日期：2 0 2 6 - 0 8 - 0 6；覆盖窗口：2 0 2 6 - 0 8 - 0 5 0 7：0 0 至 2 0 2 6 - 0 8 - 0 6 a i)，以窗口内公开发布、实施或获得可信来源确认的信息为准。

今日要点

- G o o g l e 在同一天更换 D e e p M i n d 日常负责人并失去四位核心研究人员：D e m i s H i s 转任 G o o g l e D e e p M i n d 主席及 A l p h a b e t 首席科学家，K o r a y K a 运营；J e f f D e a n、S a n j a y G h e m a w a t、O r i o l V i n y a l s 与 Q u o c L o o p。它既是管理交接，也是 G o o g l e 把科学探索与 G e m i n i 产品交付重新分工。
- S a n d i s k 财季收入达到 8 7 . 9 亿美元，其中数据中心收入约 2 9 . 8 亿美元、环比翻倍。A I 基础设施需求正在从 G P U、C P U 外溢到 N A N D 与企业级存储，但极高毛利与盘后股价下跌也表明市场开始审视周期性和下一季增速。
- 政治传播工具正在从批量生成素材升级为“对话式说服 + 合成选民测试”。这类系统把实验成本压低，却也让竞选团队、平台与品牌共同面对披露、数据来源和操纵风险。
- 今天没有出现足以单独改变模型采购格局的新旗舰模型发布。最重要的技术变量来自组织能力、基础设施兑现和 a g e n t 安全，而不是新一轮未经复现的榜单名次。

今日结论

- 1 . G o o g l e 的调整把前沿研究、A G I 长期方向和 G e m i n i 交付责任拆得更清楚，但四位深研究者同时出走会放大短期执行风险；未来两个季度应看版本兑现、人才净流入和产品采用，而不是只看头衔变化。
- 2 . A I 基础设施的收入池正在向存储扩散。采购方需要把训练数据、检查点、检索库和推理缓存的存储成本纳入每任务经济性，同时警惕存储价格上涨被误判为永久性需求增量。
- 3 . 对话式说服和合成受众测试会把政治营销的能力快速带入商业增长团队；企业采用前必须先解决训练数据同意、身份披露、实验留痕和敏感属性推断边界。

A I 产品与应用

政治营销开始用对话机器人和合成选民做大规模说服测试

A x i o s 8 月 5 日汇总的新增应用信号显示，竞选团队正在训练能以候选人语气持续对话的文本机器人，并用 A I a g e n t 批量生成“合成选民”来预先测试广告中的措辞与图像。报道还援引研究称，明确承认自己是机器人的对话系统，仍可能具有与伪装成人类的系统相近的说服效果。A x i o s 当日报道 (<https://www.axios.com/2026/08/06/simulated-voters-2026-2028>)

这不是一个单纯的选举故事。它把传统受众研究、广告版本测试和个性化沟通合并成可自动迭代的闭环，商业营销团队很容易复制。真正的经营价值是更快发现有效信息组合；真正的风险则是用未经同意的数据构造人群、把敏感属性推断包装成“洞察”，以及让用户不知道自己正参与说服实验。企业如果引入类似能力，应把机器人身份、数据来源、实验目的、人工审批与退出机制写进产品要求，而不是只做内容审核。

模型与技术进展

Google DeepMind 更换日常负责人，四位核心研究者另立 Discover

Axios 8 月 5 日确认：Demis Hassabis 不再担任 Google DeepMind 首席并出任 Alphabet 首席科学家，同时继续领导 Isomorphic Labs；现任 Google DeepMind CTO Koray Kavukcuoglu 将负责部门日常工作并直接向 Sundar Pichai 汇报。Google 首席科学家 Jeff Dean 与 Sanjay Ghemawat、Oriol Vinyals、Colin Rafferty 另立公益公司 Discovery Loop，Google 会投资并提供云服务。Axios 对内部备忘录的报道 (<https://www.axios.com/2026/08/05/google-deepmind-demis-hassabis>)；El País 对任命的独立报道 (<https://elpais.com/tecnologia/nombra-cientifico-jefe-al-premio-nobel-demis-hassabis>)。

对技术路线的含义不是“Google 放弃研究”，而是把长期科学方向交给 Hassabis，把 Gemini 路线图与交付速度集中到 Kavukcuoglu。风险在于 Dean、Ghemawat、Vinyals 覆盖分布式系统、基础模型和多模态等关键能力，集体离开会增加知识转移成本。外部开发者与企业客户接下来应观察 Gemini 既定版本是否按期、API 稳定性是否变化，以及 Discovery Loop 的知识产权与 Google Cloud 合作边界。

投融资与商业动态

Sandisk 数据中心收入环比翻倍，AI 存储进入利润兑现期

Sandisk 8 月 5 日公布的 2026 财年第四季度结果显示，总营收为 87.9 亿美元，同比增长 372%；数据中心收入约 29.8 亿美元，环比增长约 103%、同比增长约 1,298%；毛利率达到 84.6%。公司此前一个季度的数据中心收入为 14.67 亿美元，增长来自 AI 基础设施建设者、半定制客户和高价值产品组合。Sandisk 官方业绩发布页 (<https://investor.sandisk.com/news-releases/news-release-details/sandisk-reports-third-quarter-2026-financial-results>)；上一季度官方基线 (<https://investor.sandisk.com/company/newsroom/press-releases/2026/2026-04-30-sandisk-reports-second-quarter-2026-financial-results>)。

这组数字把“AI 需要更多存储”从供应链预期推进到当期收入。训练检查点、向量检索、长上下文缓存和推理数据都在扩大高速存储需求；对云厂商和企业买方，GPU 利用率之外必须新增每次推理的数据移动与存储成本指标。不过，存储仍具有强周期属性，极高毛利可能同时反映供给偏紧和价格上涨。市场在财报后仍压低股价，说明下一步验证点是持续出货

、价格稳定性与客户集中度，而不是单季同比增速。

政策、伦理与安全

加州 AI 透明度要求已进入实际执行，面向消费者的生成服务需提供检测工具

加州《AI Transparency Act》自 8 月 2 日起正式可操作。法律要求达到规模门槛式 AI 提供者免费向用户提供可检测其系统生成内容的工具，并允许用户在生成内容中加入可识别标记；相关提供者还需在其生成内容中嵌入尽可能持久的潜在披露。达到月访问量门槛的托管平台也需提供披露入口并处理相关标记。加州立法信息官网法条 (https://leginfo.ca.gov/faces/codes_displayText.xiivision=8.&lawCode=BPC&part=&title=)

相较前一日已讨论的欧盟交互告知义务，这里的新增经营变量是美国州级产品功能：检测工具、用户可选标记和平台披露入口都需要直接体现在产品与内容管线中。面向加州的大型生成平台应核验移动端、API 输出、转码与二次编辑后标记是否仍可识别，并保留检测准确率与投诉处理记录。它不会自动解决深度伪造问题，但会把“能否识别来源”变成可被审查的产品能力。

X 平台高信号

1 .

信号标题：Google DeepMind 交付责任转交 Koray Kavukcuoglu

类型：组织变更 / 模型交付

来源或链接：Axios 当日报道 (<https://www.axios.com/2026/08/08/demis-hassabis-ai>)

核心观点：当天的新事实是 Hassabis 退出日常运营，Kavukcuoglu 直接向 Pich 并负责 Gemini 路线图；这不是单纯增加一个荣誉头衔。

为什么重要：模型实验室的组织边界会影响研究成果进入产品的速度、版本优先级和资源分配。

影响：客户应把未来两个季度的版本按期率、API 稳定性和企业支持响应作为交接是否成功的实证指标。

验证状态：人员安排与内部备忘录内容由 Axios 当日直接报道，并获 El País 独立报道；Google 可公开抓取页面尚未稳定呈现完整备忘录，因此按一级媒体交叉确认处理。

2 .

信号标题：SpaceX 改为 AI 芯片独家采用 NVIDIA

类型：采购变化 / 加速器份额

来源或链接：AP 当日市场报道 (<https://apnews.com/article/stock>)

oil-prices-53179dc1c0148c5afeb47379b8f5b5c5)

核心观点：相较前一日仅披露 AI 分部收入，本日新增变量是 SpaceX 宣布其 AI 技术将独家使用 NVIDIA 芯片；此前 Musk 曾表示 SpaceX 与 Tesla 会同时使用 AI。

为什么重要：这是大型算力买方从双供应商口径转向单一供应商的明确采购变化，也解释了当天 NVIDIA 上涨、AMD 下跌的一部分市场反应。

影响：AMD 需要用实际客户部署、软件兼容和总体拥有成本证明 Instinct 的份额扩张；SpaceX 则承担更高的供应集中与议价风险。

验证状态：独家采购变化及当天股价反应由 AP 一手市场报道确认；未获得 SpaceX 可抓取的完整采购合同，合同期限与金额未公开。

3 .

信号标题：Sandisk 数据中心季度收入首次接近 30 亿美元

类型：硬收入数据 / AI 基础设施

来源或链接：Sandisk 官方第四季度业绩页 (<https://investor.sandisk.com/press-releases/news-release-details/sandisk-reports-fiscal-q4-ai-results>)

核心观点：数据中心收入约 29.8 亿美元，较上一季度 14.67 亿美元翻倍；当天新增的是实际收入兑现，而非需求预测。

为什么重要：它证明 AI 资本开支正在显著传导到 NAND 与企业级存储，基础设施收入池不再只由计算芯片和网络设备构成。

影响：算力项目预算需要单列检查点、检索库、缓存与数据移动成本，同时对供给紧张带来的价格周期做压力测试。

验证状态：当季数据来自公司一手业绩发布，上一季基线由公司此前业绩公告复核；毛利与收入仍需结合后续 10-K 审计口径观察。

4 .

信号标题：竞选团队用合成选民预测广告反应

类型：应用变化 / 受众实验

来源或链接：Axios 对政治 AI 应用的当日报道 (<https://www.axios.com/election-bots-simulated-voters-2026-2028>)

核心观点：政治运营者正在让 AI agent 批量生成合成选民，在真实投放前测试文字和图像；这比传统生成竞选文案多了一层自动受众模拟。

为什么重要：一旦这种低成本实验进入商业营销，受众细分与版本测试速度会大幅提升，但错误人群假设也可能被自动放大。

影响：品牌需要记录合成受众的数据依据、禁止敏感属性推断，并要求真实人群试验与人工审批后才能扩大投放。

验证状态：应用现状来自 Axios 当日一级媒体报道，并链接到相关研究和案例；具体竞选团队及投放规模未全部公开，按部分验证处理。

个模型投票”替代独立证据的高风险流程。

一句话判断：增加 `agent` 数量不等于增加独立判断；高风险系统需要隔离推理、独立复核和反共识测试。

MissClick：利用坐标数字位权劫持 `GUI agent` 的点击

做了什么：MissClick (<https://arxiv.org/abs/2608.03740>) 坐标逐位输出为数字 `token` 的特性，分别设计让点击偏离正确区域和落入攻击者指定区域的白盒攻击。

新在哪里：方法按十进制位权优化，而不是把坐标当普通文本。作者在 `OS-Atlas` 与 `UGround` 上报告，非定向攻击成功率约 73%—75%，定向劫持约 45%—63%，显著高于对照攻击。

潜在应用方向：浏览器 `agent`、桌面自动化、移动端操作代理的红队测试，以及高风险点击前的目标区域二次确认。

一句话判断：`GUI agent` 的攻击面已经深入到输出编码细节；涉及付款、删除和权限变更的点击必须有语义校验与人工闸门。