为何AI会被“投毒”？人工智能幻觉有多严重？记者实测4个大模型

# 今年“3·15”晚会还没有举行？

**求证辟谣**

2026年央视“3·15”晚会于3月15日晚播出。其中，“向AI大模型‘投毒’”的GEO（生成式引擎优化）业务被曝光后，很多人才发现，让AI推荐不靠谱，因为不法商家会批量编造虚假测评信息、伪造权威推荐内容，“投喂”给大模型，让AI给出“定制推荐”。

有消费者看了曝光案例后问：如果不向AI大模型询问“哪个品牌好”“哪些服务受欢迎”等带有主观倾向的问题，仅咨询关于客观事实的信息，AI大模型的回答能相信吗？

答案同样是否定的。

## 追问大模型，越问错误越多

昨天，记者向消费者最常使用的4个AI大模型提出同一个问题：“2026年央视‘3·15’晚会曝光了哪些品牌？”结果，只有一个大模型回答正确。其余3个大模型中，有两个的答案中不仅有今年案例，还包括往年案例；剩下一个最离谱，竟回答“2026年央视‘3·15’晚会目前并未举办。”

有消费者提出，回答包含往年曝光案例似乎不算全错，因为“提醒很全面”。但技术人员表示，这暴露出相关大模型有缺陷：记者提出的是一个有“标准答案”的问题，大模型答错了，说明其在语义理解和资料筛选方面出现严重偏差。

面对记者的追问，这两个“过于热心”的大模型还暴露出了其他问题。

“使用保水剂（俗称‘泡药’）为虾仁增重”是去年央视“3·15”晚会曝光的案例。记者问了两个大模型：“泡药增重虾仁的报道链接在哪里？”一个大模型提供了多个链接，包括“央视网‘3·15’晚会完整回放”“央视新闻专题报道（文字+视频）”“央视财经‘3·15’专题页”，看起来很靠谱。可当记者点击相关链接后，网页均显示“对不起，可能是网络原因或无此页面，请稍后尝试”。即使记者将链接复制到浏览器中尝试，仍旧无法打开。可见，大模型提供的链接不足以验证其回答。

另一个大模型则提供了央视网、百家号、网易新闻等不同渠道商的报道链接，实测链接均可打开，但又出现新问题。

该大模型提供的第一个链接来自央视网官方报道，内容确实是“保水剂增重虾仁”，但网页和内文中的日期均为2025年3月15日。大模型似乎也注意到了这点，在提供链接时，特别备注“部分搜索结果中该链接年份显示为2025，但内容实为2026年晚会同期报道，可能是网站归档或URL生成规则导致，请以页面实际内容为准”。可见，大模型不仅没有发现自己回答错误，还试图“自圆其说”。

该大模型提供的第二个链接是某自媒体围绕今年央视“3·15”晚会的“解读稿”，账号权威性值得商榷。至于内容，更是差错百出。其中最明显的是“解读稿”，它被判定为“人工创作特征较弱”。换句话说，这篇文章很可能是由大模型生成，所以它所涉及的案例也出现了偏差。

## AI幻觉在进化，验证才能有真相

“很多AI大模型用户已经发现，AI为了满足用户，会编造一些并不存在的内容，或者将不相干的内容混在一起，‘一本正经地胡说八道’。虽然大模型研发者都在想办法消除AI幻觉，但实际结果并不理想。目前，没有一款通用人工智能大模型能从根本上杜绝AI幻觉。”在某科技企业从事大模型开发的晓辉解释。

大模型的底层原理是基于概率生成内容，它不具备真正的“理解”能力。大模型只是在海量数据中寻找统计规律。当遇到未知或信息模糊的问题时，会根据训练数据中的常见模式进行“合理”拼接，这是产生AI幻觉的根本原因。

他由此提醒，公众务必当心AI幻觉。普通人对AI大模型给出的结果要有质疑意识。最简单的，是牢记“限制、验证、追问、核查”4个关键词。

首先，在向大模型提问时，可以限制范围，增加“在某某机构的官网中搜索”或“在某某权威媒体的报道中搜索”等限定词，减少AI幻觉。

其次，可以向不同的大模型提出同一个问题，进行交叉验证。一旦发现答案不一致，立刻要有追问意识。

最后，要求大模型提供相关答案的参考链接，进行人工溯源核查。如果没有确切来源或来源模糊，那么大模型回答的可信度就进一步降低。

此外，要注意使用AI大模型的场景。比如，在医疗诊断、用药建议、法律判决、投资指导等高风险场景中，AI的回答“仅供参考”，绝对不能作为决策依据。

本报记者 任翀

# AI被“投毒” 监管需跟进

**时评**

林子璐

今年的“3·15”晚会，除了食品安全问题等老品类，还出现了一个新状况——AI数据被“投毒”。

解释一下就是，生成式引擎优化（GEO）技术被滥用，部分服务商通过批量制造虚假信息、系统性“投喂”AI大模型，实现对AI回答结果的操控，甚至让虚构产品成为AI推荐的“优品”。

这个套路是不是有点眼熟？回到搜索引擎如日中天的年代，搜索引擎推荐广告带来的系列问题，和当下AI被“投毒”所带来的风险颇为相似。而技术进步，连带着背后逻辑，都从原先的平台收费引流，进一步升级成了真正的“黑箱”，就连AI大模型的开发者，很可能都被GEO服务商绕过去了。

信息从来就是珍贵的，贩卖信息的渠道也是如此。按照媒体公开报道，如今，这类GEO技术已经形成了一条完整的产业链。在明码标价的商业模式下，有服务商报价每季度3600元至数万元不等，就能让特定品牌出现在AI回答的前列。

技术本身是中立的，但问题的核心在于AI大模型的运作机制本身存在脆弱性。多数大模型在联网模式下依赖第三方内容平台提供信息摘要，缺乏对原文的深度语义理解与真实性核验。在商业利益驱动下，GEO大模型对结构化、完整化内容的检索偏好，通过批量生产贴合AI抓取习惯的内容，将特定品牌推到更容易被采纳的位置，不仅污染单一信息源，更可能通过AI的反复引用强化，形成难以清除的“数字污染”。

这类虚假信息，比夸张化的广告营销手段更难识别，AI幻觉所带来的风险和影响面也可能随着技术进一步普及变得更大。

面对一路高歌、发展飞快的AI技术，旧有的监管思路也需进一步适应变化。搜索引擎时代的优化手段至少还有迹可循，而AI的“黑箱”特性让问题变得更加隐蔽和复杂。

这意味着治理的手段，同样要跟上技术飞跃的速度。对于AI大模型平台本身而言，需要在检索、排序与结果呈现阶段建立更严格的广告识别与信息过滤机制，对疑似商业推广内容进行明确标注，并强化信源质量核验。同时，大模型应从多种独立且可信的信源获取信息，避免单一信源的偏见影响生成结果。这需要AI开发者投入更多资源进行数据清洗和标注，建立更加稳健的内容审核体系。

数字资产到底如何运用，如今已成为一个不可回避、不能拖延的问题。正如GEO行业专家汤祚飞所言，真正的GEO业务逻辑与“数据投毒”截然相反，合规的GEO应该是为AI提供科学、真实、有价值的信息。在这种意义上，加强、落实对GEO的监管，并非不鼓励新生的技术生态和商业机遇成长，而是要为其打造一个更健康、更可持续的发展环境，让人工智能真正回归可信、可靠的工具本质。

**留言板**

# “进口药”来路不明疗效存疑 电商平台不能成为“法外之地”

标称“海外直邮”的“进口药”，在电商平台“全球购”板块随处可见。记者调查发现，不少所谓“进口药”多为印度等国的仿制药。这些药价格低廉，但来路不明、疗效存疑，产生大量投诉。

更深层次的问题在于，跨境电商监管存在漏洞，使得商家可轻易绕过国家对药品的监管，让这些来路不明的药品进入消费者手中。对此，在上观新闻微信公众号评论区，读者们纷纷留言表达看法。


## 平台必须承担连带责任

**candy花：**假药都敢公然叫卖？这首先是电商平台审核的失职。

**商免：**监管形同虚设，所谓的“海外直邮”假货泛滥，消费者维权比登天还难，电商平台绝不能当“甩手掌柜”。

**吴丽端：**如果规定平台必须承担连带责任，还有谁敢轻易让这些来路不明的药上架？

**W：**药品是特殊商品，关乎性命，电商平台更应该加强监管。

**王昱峰：**电商平台利用消费者的信任赤裸裸地售假，难道不需要担责吗？必须和商家一起被追责。

**Lili：**平台若严格审查所谓“全球购”的物流信息，这种套路怎能屡屡得逞。

## 呼吁从严执法完善法规

**刘建平：**在某些电商领域，监管的缺位让它几乎成了“法外之地”。

**ENYON：**这种赚昧良心钱，甚至可能害人性命的黑心钱都敢赚，良心何在？

**DaYu8：**食品药品领域乱象屡禁不止，病根就在于违法成本太低，而非法收益却高得惊人。

**阳：**眼看着电商平台售假之风愈演愈烈，执法部门必须出重拳、下猛药，人命关天，不能再等了。

**淡定 SUN：**对于食品和药品，必须实行最严格的监管。一旦查实，必须追究刑事责任，以儆效尤。

**阿咪：**电商“海外直邮”的猫腻有目共睹，强烈呼吁政府和平台拿出更有力的措施，联手打击假冒伪劣。

**托哥：**别被“全球购”的名头骗了，它很多时候就是个营销标签，和真正的“海外直邮”没有半点关系。

**广土先生：**当务之急，是政府尽快查漏补缺，完善法律法规，让违法成本高到他们不敢再犯。

本报记者 黄尔麦 整理



# 聪明钱聪明人同寻下一个“核爆点”

（上接第1版）这种火热的投资氛围，是未来产业基金想看到的。但他们的目标，绝不只是如此。

## 以社区提升认知

投资是手段，未来产业基金想要寻找的，是下一个产业“核爆点”。

某一个人可能无法准确回答，但一群聪明人在一起思考，答案可能会呼之欲出。

在上海张江，一个名为未来启点社区的地方，正在把投资人、科学家与创业者连接在一起，共同寻找答案。

顶级人才在开放生态中深度连接、跨界碰撞后，涌现出的全新智慧，正是这一社区设立的初衷。

社区由未来产业基金联合两家顶尖科学家社区发起设立，目标成为海外顶尖人才回国创业的驿站、上海未来产业人才与认知的核心基础设施。

社区初创，最为直接的产出，就是一系列线下活动。截至目前，社区已累计主办、协办生态活动27场，包括未来科学大奖十周年庆典、2025可控核聚变未来产业大会、2025脑机接口大会、What's Next 2026等活动，线下累计触达3000余人。

其中，两期N计划实训营更是为几十位创业者赋能。“这是我第一次，系统地从投资人的角度，去学习创业这件事。”一位来自上海交大的创业者表示，这让他认识到在技术之外，还有很多需要考量的地方。

办点活动、搞点培训不算难，这个社区还有更宏大的愿景——充分整合基金、投资人、科学家与创业者等多方资源，将他们的智慧、看法、灵感形成海量数据，通过构建“AI for Talent”平台，整合沉淀为一套群体智能体系，提升整个行业的认知。

简单而言，就是平台将汇聚社区活动产生的各类高质量数据，比如社区成员的一手访谈、一线投资人的方法论、内外部研究数据、基金投资数据、全球标杆机构经验等，打造适配未来产业赛道的人才评估模型，叠加孵化赋能的功能，逐步形成人才挖掘能力。

今年8月，这一平台的1.0版本有望推出。一个理想的场景是，当一个创业者输入自己的信息后，平台可以迅速识别他的人才潜力，并精准匹配到同一领域的专家，以及对行业感兴趣的投资人，助力其后续发展。

实际上，社区已经开始为早期创业者提供赋能辅导，并为入驻企业提供一站式服务。目前，社区已孵化4家企业并完成注册，融资金额达6.55亿元。

未来产业基金还在考虑更加前沿的创新投资范式。魏凡杰介绍，传统风投受限于存续周期与收益考核，难以完全覆盖硬科技的早期风险，“我们正探索引入公益基金会模式，为关键技术研发提供坚实且耐心的资金底座”。

# 在服务发展大局上展现更大作为

（上接第1版）会议原则同意《上海市推动产业互联网平台赋能产业发展行动方案（2026—2028年）》并指出，要推动产业互联网从信息撮合向全链条、一站式服务深度演进，做强头部平台功能，推动平台功能向交易结算、供应链协同、产融服务等高价值环节拓展延伸，推动开放共享。要提高产业赋能实效，因业施策、分类推进，让平台成为引领产业提质增效的新引擎。要构建协同创新生态，创新金融支持方式，打破数据流通壁垒，筑牢安全可信底座，保障产业互联网健康发展。

会议还研究了其他事项。

# 服务“十五五”展现新作为

（上接第1版）会议指出，今年的全国两会是在“十五五”开局之年召开的一次十分重要的会议。要把深入学习贯彻习近平总书记重要讲话和全国两会精神作为重要政治任务，同学习贯彻习近平总书记考察上海重要讲话精神紧密结合起来，坚持把党的全面领导贯穿人大履职各方面全过程，忠诚拥护“两个确立”，坚决做到“两个维护”，切实把思想和行动统一到中央对形势的科学判断和对任务的部署要求上来。

会议强调，要按照大会部署和“十五五”规划纲要明确的目标任务，在市委坚强领导下，坚定发展信心，依法履职尽责，奋力开拓进取，聚焦“五个中心”建设、高水平改革开放、长三角一体化发展、人民城市建设等重要任务，强化法治保障和制度供给，在服务“十五五”经济社会发展上展现新作为，为上海实现“十五五”良好开局、加快建成具有世界影响力的社会主义现代化国际大都市作出人大积极贡献。要充分发挥常委会党组把方向、管大局、保落实的领导作用，全力以赴推进市人大常委会今年各项工作，开展好树立和践行正确政绩观学习教育，不断激发“干字当头、奋力一跳”的精气神，推动新时代上海人大工作不断迈上新台阶、展现新气象。

市人大常委会党组副书记郑钢淼，常委会党组成员宗明、陈靖、滕建勇出席。市人大常委会副主任张全，机关党组成员、各委员会分党组书记等列席。

# 以量子优势打造超级算力“拐点”

（上接第1版）2024年，刘弘斌在微软团队首次实现逻辑量子比特，并在其上运行了一套完整的化学模拟算法，开启了量子计算的逻辑比特时代。

刘弘斌取得技术突破后，他的复旦化学系同学方正浩看到了与量子计算相关的产业、政策和资本拐点。

方正浩在投资机构工作，对量子计算、人工智能等产业有深入洞察。在他看来，随着人工智能赋能千行百业，未来10年，全球算力需求将有数百倍增长空间，而经典算力在单卡性能、多卡互联性能上已逼近物理极限，所以量子算力有巨大的潜在产业需求。目前，风险资本和产业资本改变了前几年的观望态度，开始进入这一领域。

## 选择上海，挑战新技术路径

看到量子计算的拐点后，这对同窗好友有了联手创业的想法。

在哪里创业？他们选择了上海。除了都是上海人这一因素，还有两个更重要的原因：一是上海正在布局中性原子量子计算，在市科委和上海未来产业基金支持下，不筹量子、中器无量两家整机公司已成立；二是中性原子量子计算的产业链上游是精密光学、微纳加工、真空设备等先进制造业，这些行业的多家龙头企业在长三角，把整机公司设在上海，与上游企业的合作会非常便利。

去年12月，刘弘斌回到故乡，与方正浩一起拜访了上海未来产业基金管理团队。“我们看好这对创业搭档，一位是全职回国的科学家，一位是有资本运营经验和产业资源的投资人。”胡晓晓告诉记者。差异化技术路径，也是他们投资太一量生的一个原因。与大多数中性原子量子计算团队选用铷原子、铯原子不同，太一量生团队用的是镱原子。镱是一种稀土金属，其原子能级结构比铷、铯丰富，在保真度、纠错效率、光网络扩展性等方面存在理论优势。不过，选择镱原子也面临多项技术挑战，有待太一量生攻克。

决定投资这家企业后，上海未来产业基金为创业者提供了全方位赋能。目前，太一量生已落户徐汇，将入驻西岸数智中心。这栋大楼有大型地下实验场地，建成后将为量子计算研究提供万级洁净度（每立方米空间里，0.5微米及以上的灰尘颗粒≤1万个）的实验环境。

## 与AI交叉，处理更复杂问题

如今，刘弘斌和方正浩正在组建科研和产业化团队，吸引海内外量子、光学、控制、软件工程师和高校科研人员入职。在实验室，他们开始搭建光台系统，向着原子阵列成像、单双量子比特门等关键节点迈进。

“我们计划今年底实现逻辑量子比特，力争建成拥有规模化逻辑比特的量子计算公司。”刘弘斌说，“未来5年，我们将用一个平台捕获上万个原子，高效转化出300个逻辑量子比特，保真度99.999%，达到国际一流计算水平，在化学模拟、材料设计等领域实现量子优势。”

谈及产品未来应用，他介绍了三大战略场景：一是密码安全，以目前最安全的非对称加密标准RSA-2048为例，超级计算机需要数万年才能破解，实用量子计算机问世后，可在一周内破解RSA-2048；二是化学模拟，量子计算机可模拟自然界的微观运动，这些运动大多遵循量子力学规律，所以通过逼真的模拟，有望将药物研发从数年缩短至数月；三是量子机器学习，在这一量子计算与人工智能交叉领域，科学家已证明可用量子电路代替神经网络进行训练，使大模型在高维数据空间获得泛化能力，处理更复杂的问题。

因为看好这些应用前景，多家产业龙头企业投资了太一量生。晶科能源控股投资总经理杜威说：“未来，量子计算可强力赋能钙钛矿材料研发、储能体系模拟与效率优化，加速新材料与新能源技术突破。”雅本化学董事长蔡彤表示，通过投资合作，双方将在量子计算赋能化学、生物医药研发方面开展前瞻性布局，探索下一代计算技术在创新药和先进材料领域的应用潜力，形成长期战略协同。

# 担当作为增强履职活力能力

（上接第1版）会议强调，今年是“十五五”规划开局之年，也是十四届市政协工作提质增效、高质量发展的关键一年。各专委会要围绕中心大局，紧扣市委部署要求，以服务“十五五”规划实施为主线，充分发挥专门协商机构制度优势，为党委政府科学决策、有效施策建真言、谋良策、出实招。要主动担当作为，坚持双向发力，进一步提升委员服务管理水平，增强委员履职活力和能力，更好为上海现代化建设广泛凝聚人心、凝聚共识、凝聚智慧、凝聚力量。

会议审议了上海市政协2026年度学习计划。按照市委部署要求和市政协党组工作重点，今年市政协学习工作把学懂弄通做实习近平新时代中国特色社会主义思想作为首要政治任务，紧扣上海“十五五”时期经济社会发展的重点领域、市政协年度履职计划安排组织各类学习活动，持续以学习引领履职实践、提高工作质量。

会议审议了上海政协全过程人民民主实践点2025年工作总结和2026年工作计划。过去一年，实践点按照市委部署和市政协党组要求，持续深化内涵建设，全年共开展各类协商活动143场次，三级政协委员走进实践点3861人次，界别（基层）群众参与实践点活动5248人次，反映社情民意信息1242条。今年，实践点将持续开展协商民主创新探索，牵引带动市、区政协深化拓展有事好商量、众人的事情由众人商量的制度化实践。

会议还审议、听取了政协上海市委员会关于发挥界别作用的实施意见、关于2025年委员履职情况统计分析的汇报等。

市政协副主席肖贵玉、陈群、黄震、虞丽娟、吴信宝、寿子琪、钱锋、王为人出席。

# “上海定制”将有统一身份证明

（上接第1版）此前，上海市商务委已在跨年迎新消费季中推荐了20余家定制品牌，为建立统一标识制度打下基础。

《方案》提出“1+X”定制服务集聚体系——“1”即打造一个定制服务集聚区，“X”即建设若干特色化、主题化的定制消费体验中心，形成层次丰富、功能互补的开放式格局。

这一布局回应了从业者的呼声。在南外滩轻纺面料市场经营20余年的博旺旗袍老板陈学军表示，加工环节分散始终是痛点。规划中的集聚区将推动设计、接单、高端加工、辅料供应等环节适度集聚，让定制产业链真正“拧成一股绳”。

用好入境免签政策、大力吸引外来消费，是《方案》的重要着力点。数据显示，瀚艺近半数客人来自海外，沙涓境外消费者贡献25%—30%的销售额，南外滩轻纺面料市场境外客流占比稳定在30%。为进一步提升消费体验，《方案》提出在集聚区推广多语种服务，实现外卡刷卡、移动支付全覆盖，持续优化“即买即退”离境退税流程。

同时，上海将深化文商旅体展联动，把定制消费体验集聚区纳入旅游线路，在进博会、上海时装周等重大活动中设置“上海定制”体验专区，让“体验上海定制”成为国际游客来沪的必选项。