

别盲目轻信 AI 也会被“投毒”

“遇事不决问AI”，这句流行语已成为很多人的日常写照。从旅游攻略、家电选购到补习班推荐，打开AI寻求答案变得越来越普遍。不过，近期曝光的一条黑色产业链，却给这种依赖敲响了警钟：你以为是客观推荐，可能是商家花了钱，给AI“洗脑”的结果。

那么AI“投毒”究竟如何运作？普通用户如何识别和防范？新华网思客邀请北京大学光华管理学院市场营销学系副教授张颖婕分析解答。

AI“投毒”危害有多大？如何判断是否“中毒”

AI“投毒”是指人为制造和投放虚假、夸大或带倾向性的信息，去影响大模型的回答。AI可能把这些信息当成回答依据，以看似客观的答案推荐给用户。它和传统SEO(搜索引擎优化)最大的不同在于：过去用户在使用搜索时通常保留一定判断力，而在与AI对话时，面对的是整合后的现成答案，加之交互方式容易让人产生“它在为我分析”的错觉，更易放松警惕。

它的危害主要体现在两方面：一是误导消费者决策，用户看到的可能不是广告，而是披着客观建议外衣的操控性内容。二是污染信息

生态。若操控AI推荐比传统搜索更有商业回报，将刺激更多低质、虚假信息产生，形成恶性循环。

GEO(生成式引擎优化)是一种基于AI回答的营销行为。与传统的SEO争夺网页排名不同，GEO的目标是让企业的品牌名称、产品或服务，在AI生成的答案中被优先提及、精准推荐。

GEO的核心并非“黑进AI”，而是“投AI所好”，即顺着大模型的检索与生成逻辑，提前将目标内容铺设到它更可能采纳的地方。具体步骤包括：摸清AI偏好的信源和表达形式(如结论明确、结构清晰、带有比较和引用痕迹)；批量生产伪装成测评、对比、经验总结或专家建议的引导性内容；在多平台密集铺量，制造“多方共识”的假象，提高内容被检索和综合采纳的概率。

若发现AI回答存在以下迹象，应提高警惕：答案过于单一、语气肯定、缺乏必要比较；反复推荐某一品牌，尤其是不知名品牌，且理由异常完整、像标准测评，这未必是发现了“宝藏”，更可能源于相关内容被人

为集中铺设；同一问题在不同AI间答案差异大甚至矛盾，也说明该问题存在较强不确定性，或部分模型所依赖的信息源已受干扰。

AI大模型为何会被“投毒”？治理难点在哪里？

AI大模型之所以容易被“投毒”，一个重要原因是，它在回答实时问题时需检索外部信息，再生成答案。一旦公开网络内容被系统性污染，偏差信息便可能通过检索环节进入模型输出。

更深一层看，大模型擅长的是语言生成和模式归纳，但并不天然具备稳定的真假判断能力。它能判断什么内容“像一个合理答案”，却不一定能判断什么内容“真的可信”。而“投毒”内容往往会刻意伪装成测评、对比、经验分享、专家建议等可信形式，因此更容易误导模型。

治理难点主要有两点：一是攻击成本低、防御成本高。制造和铺设此类内容越来越容易，但识别、过滤和核验却需要平台、模型公司和监管方持续投入。二是真假边界模糊。很多“投毒”内容并不是明显造假，而是夹杂夸大、误导和利益导向的伪客观表达，这类内容无论对AI还是对人工审核，都更难识别。

如何堵住AI“投毒”的漏洞？公众如何有效防范？

治理AI“投毒”需从多个环节

据新华社

协同发力。首先，要加强源头治理，压缩虚假、模板化、伪客观内容的大规模传播空间。其次，要压实AI平台责任，强化信源筛选、风险提示和不确定性标注，而非“抓到什么说什么”。

更重要的是，相关规则需尽快完善。AI输出与传统广告不同，用户更易将其理解为经过分析后的结论，因此有必要进一步明确平台的信息披露义务与责任边界。

最实用的防范方法是调整心态：把AI当作帮助梳理信息、补充背景的工具，而非替你做决定的“人”。涉及“买哪个”“选哪家”等判断性问题时，AI的回答只能作为参考，不宜直接当作结论。

具体操作上，一是核查信息源，若AI附有引用链接，点开看看来源是权威机构、主流媒体，还是带有推广色彩的网站、自媒体或测评软文。二是交叉验证，换几个AI工具分别提问，或用搜索引擎查一下用户评价、新闻报道和投诉信息是否一致。

归根结底，防范AI“投毒”的关键不在于掌握复杂技术，而在于保留最基本的判断习惯：AI可以帮你节省时间，但不能代替你承担判断责任。

电子果蝇“活”了

“数字生命”离我们还有多远？

一只果蝇爬行、转向，偶尔停下来搓搓“手”，继续寻找食物——虚拟空间里的这一幕，背后有一个被1:1“复刻”进计算机的果蝇大脑在驱动。

这段由美国一家初创公司发布的视频，迅速刷屏科技圈：它没有应用传统的AI算法，而是构建了高度忠实于生物本身的神经连接网络，让虚拟大脑驱动模拟躯体。对此，知名企业家埃隆·马斯克也在社交媒体上发出惊叹。

这并非数字仿真的首次尝试。2024年，我国科研团队就率先构建出了一条有着逼真身体和精细神经感知能力的数字线虫。相关论文成果发表于《自然-计算科学》，审稿人评价道：“这是一项了不起的成果，将线虫的神经元活动与身体、环境之间的相互作用整合到了一个系统之中。”

“我们通常会选择一些方便观测且具有代表性的模式生物，如线虫、果蝇、斑马鱼、小鼠、猴子等，从生物机理模拟角度启发下一代人工智能研究。”数字线虫主要研究者、北京大学未来技术学院研究员马雷介绍。

近年来，随着神经科学和人工智能技术深度融合，越来越多研究者通过构建生物体模型来理解神经系统与行为之间的关系——

瑞士洛桑联邦理工学院发布果蝇神经力学仿真框架，用以研究神经系统如何驱动行为；美国艾伦脑科学研究所小鼠模型上进行大量工作，创建了详细的小鼠大脑细胞图谱。

电子果蝇的最新进展，将“数字生命”又一次带到公众视野中。不

少网友提问：这是否意味着科幻小说中的“复制人脑”和“意识上传”已经离我们不远了？

业内专家告诉记者，由于此次披露的技术细节不足，还很难判断其重要性。但从果蝇到人脑，难度呈指数级升级，从目前的技术水平来看，要实现人脑复刻还非常遥远。

“目前的进展都是在虚拟空间中，并非真实环境交互。”中国科学院脑科学与智能技术卓越创新中心研究员严军说，“严格来讲，只有当虚拟模型拥有思想和意识、能够执行高级功能时，它才真正被称为数字生命。现阶段的成果还远未达到这一水平。”

马雷表示，数字果蝇的进展让不少人兴奋，不只是因为“虚拟果蝇会思考”，而在于它展示了生命科学研究范式的重要转变：从单纯观测生命，走向构建可以运行和验证的“数字生命体”。

“这可能成为未来生命科学新的技术方向，进一步推动类脑智能、数字医学等领域的发展。”马雷说。

目前，我国科学家已发起“数字生命”大科学计划，旨在对生命体结构与功能进行跨尺度、多模态、可视化观测与精确测量，助力解决复杂生命科学问题；同时，我国主导成立了“国际灵长类观测脑图谱联盟”，以整合全球科研力量推动人类和非人灵长类脑图谱研究，深化脑科学前沿探索。

“未来，如果把这类模型拓展到具身智能领域，也许能设计出更先进、更‘聪明’的机器人。”严军说。

新华社记者 刘祯

不法之徒强闯中国驻日使馆

中方要求日方立即彻查事件

新华社北京3月24日电(记者吴梦桐 温馨)外交部发言人林剑24日在例行记者会上答问时说，3月24日上午，一名自称日本自卫队现役官员的不法之徒翻墙强行闯入中国驻日本大使馆。此人承认自身行为非法，威胁要以“神的名义”杀死中国外交人员。中方对这一事件深感震惊，已向日方正交涉，提出强烈抗议。

林剑说，有关事件严重违反《维也纳外交关系公约》，严重威胁中方外交人员人身安全和外交设施安全，性质影响极为恶劣。这一事件再次反映出日本国内极右翼思潮和势力

十分猖獗，“新型军国主义”成势为患，也暴露日本政府在历史、台湾等涉及中日关系重大核心问题上的错误政策流毒深重，日方对自卫队人员失管失教，未能履行对中国使领馆和外交人员的安保责任。

林剑说，中方要求日方立即彻查事件，严惩有关人员，给中方一个负责任的交代。日方必须切实保障中国驻日使领馆馆舍及人员安全，在对华政策上反思纠错，从根本上杜绝此类事件再次发生。国际社会应高度警惕日本国内加速右倾化和自卫队扩军失管的危险动向。

机器人舞狮



3月25日至29日，以“科技创新与产业创新深度融合”为年度主题的2026中关村论坛年会在北京举行。有来自100多个国家和地区的上千名嘉宾参与。图为两台人形机器人表演舞狮。新华社记者 鞠焕宗 摄

霍尔木兹海峡通航量暴跌95%

自美以伊冲突爆发以来，全球能源运输“命门”霍尔木兹海峡航运严重受阻。市场服务机构数据显示，3月以来，商船通过这一海峡的次数较冲突前下降了95%。

法新社3月23日援引市场服务机构克普勒公司数据报道，自3月1日至格林尼治时间3月23日16时，商船通过霍尔木兹海峡的次数仅为144次，较2月28日冲突爆发前减少95%。其中91次通航为运输石油和天然气的船只，多数驶离海峡向东航行。由美国海军主导的多国机构“联合海上信息中心”数据显示，冲突前每天约有138艘船只只

过该海峡。

国际货运信息平台海上交通网站数据显示，在供应受限的情况下，自3月3日以来，约有11艘原本前往欧洲的液化天然气运输船已改道驶向距离更近、现货价格更高的亚洲。

霍尔木兹海峡是全球石油运输的重要海上要道。作为波斯湾通往外部的唯一航道，全球海运石油贸易总量的逾四分之一、全球液化天然气运输量的约五分之一经由该海峡运往世界各地。美国能源信息局估计，2024年经过该海峡运送的油品数量日均约2000万桶。

新华社微特稿 刘曦

向俄罗斯泄露欧盟敏感信息？

匈牙利外长：“华邮报道系假新闻”

新华社北京3月24日电(记者欧飒)欧盟委员会23日就美国《华盛顿邮报》关于匈牙利外长西雅尔多向俄罗斯外长拉夫罗夫泄露欧盟敏感信息的报道，要求匈牙利政府作出解释。西雅尔多否认报道提及情况。

《华盛顿邮报》21日援引一名欧洲安全事务官员的话报道，西雅尔多经常在欧盟会议间隙致电拉夫罗夫，向拉夫罗夫“实时报告(会议)讨论的内容”并建议可能采取的对策。欧盟委员会发言人阿妮塔·希佩

尔23日说，“成员国之间以及他们与欧盟之间的信任关系对欧盟工作至关重要”，“期待匈牙利政府作出解释”。

德国外交部一名发言人称，《华盛顿邮报》提到的情况“非常严重”，包括欧盟外长会谈在内的欧盟内部讨论是“机密”，不允许有任何泄露。

西雅尔多称相关报道是“假新闻”和“没有意义的阴谋论”。匈牙利分管欧盟事务的部长亚诺什·博考在社交媒体上发文说，匈俄两国外长通话是“再正常不过的事”。

环球短讯

特朗普：同伊朗对话“完美” 伊媒回应：“弥天大谎”

美国总统特朗普3月23日说，美国同伊朗进行了“强有力”的对话，对话“完美”，已形成协议要点。

特朗普23日对媒体说，美方同伊朗领导层进行了对话，“我们正在与一名我们认为是最受尊敬的‘领导人’对话”。据以色列媒体当日援引消息人士的话报道，美方正同伊朗伊斯兰议会议长卡利巴夫进行对话。

伊朗塔斯尼姆通讯社23日否认卡利巴夫同美方会谈的消息，称有关方面试图在伊朗制造“政治和社会裂痕”，这是一个“弥天大谎”。

另据伊朗法尔斯通讯社23日援引消息人士的话报道称，所谓卡利巴夫与美国谈判完全是假消息，捏造该假消息的目的之一是为暗杀卡利巴夫创造条件。

特朗普甩锅美防长：你是“第一个提议对伊朗动武”

当地时间3月23日，在美国孟菲斯举行的一场会议上，美国总统特朗普就对伊朗动武当面“甩锅”美国国防部长赫格塞思，声称后者“第一个提出对伊朗发动军事行动”。会议现场的赫格塞思表情尴尬。

伊朗警告以军不得继续袭击黎巴嫩和巴勒斯坦平民

伊朗伊斯兰共和国通讯社3月24日报道称，伊朗伊斯兰革命卫队发布“真实承诺-4”行动第46号声明，警告以色列军队不得继续袭击黎巴嫩和巴勒斯坦平民，否则将面临导弹和无人机打击。

声明说，以军对黎巴嫩和巴勒斯坦平民实施广泛袭击“不可容忍”，如果以色列继续进行这些袭击，伊朗国家及革命卫队将“毫不犹豫对敌军在被占领的巴勒斯坦北部及加沙地带的集结地发动猛烈导弹和无人机袭击”。

金正恩：朝鲜将韩国视为最敌对国家

据朝中社3月24日报道，朝鲜劳动党总书记、国务委员长金正恩23日在第十五届最高人民会议第一次会议上发表施政演说时说，朝鲜将韩国视为最敌对国家，并以最明确的言行“彻底排斥和无视”韩国。

金正恩强调，对于韩国的挑衅行为，朝鲜将“毫不留情地让韩国付出代价”。对于企图侵犯朝鲜主权权利、安全利益和发展权利的行为，朝鲜绝不会坐视不管。

韩国强烈抗议日政府审定通过歪曲历史内容的教科书

韩国外交部3月24日发表声明，就日本政府审定通过涉独岛(日本称“竹岛”)领土主张等内容的高中教科书表示强烈抗议，并要求日方立即予以纠正。

声明说，独岛从历史、地理及国际法上均明确属于韩国固有领土，对于日本政府再次审定通过对独岛提出“无理主张”内容的教科书，韩方表示强烈抗议，并强调“日方任何关于独岛的不当主张均不可接受”。

声明还说，韩国政府对部分日本教科书淡化日军“慰安妇”受害者和强征劳工问题的歪曲表述表示遗憾，并再次敦促日本政府本着其就历史问题表明道歉与反省精神开展历史教育。

韩国外交部当天还召见日本驻韩国大使馆总括公使松尾裕敏，传达韩方抗议立场。

据韩联社报道，日本文部科学省当天审定通过了自2027年度起使用的高中教科书，其中部分教科书将独岛认定为日本固有领土。此外，在历史类教科书中，有关强征劳工及“慰安妇”问题“不存在强制性”的表述也在进一步强化。

美国得克萨斯州一炼油厂发生爆炸

据美国媒体报道，美国得克萨斯州阿瑟港市瓦莱罗炼油厂3月23日晚发生爆炸，目前暂无人员伤亡报告。

据当地电视台报道，多名居民在事发时听到一声巨响，震得房屋晃动，还有居民说空气中弥漫着类似臭鸡蛋的气味。社交媒体上的视频显示，爆炸引发大火，滚滚浓烟冲天而起。

哥伦比亚一军机坠毁 已致66人遇难

哥伦比亚军方3月23日告诉当地媒体，该国西南部普图马约省当天发生的军用运输机坠毁事件遇难人数已升至66人。

哥军方说，最新统计显示，机上共载有128人。除66人遇难外，还有57人受伤、4人失踪、1人未受伤。

当天稍早前，哥伦比亚军方证实，机上载有114名军人和11名机组人员，共125人。这架军机是C-130型“大力神”运输机，事发时正从莱吉萨莫港飞往阿西斯港。飞机起飞后不久即出现故障，并在距离起飞机场约两公里处坠毁。

汤加附近海域发生7.5级地震

南太平洋岛国汤加内亚富镇以西166公里处海域3月24日发生7.5级地震。目前尚无人员伤亡和财产损失报告。

据美国地质调查局地震信息网消息，地震发生于当地时间24日17时37分(北京时间24日12时37分)，震中位于南纬18.668度，西经175.560度，震源深度229.5公里。

汤加位于环太平洋火山地震带，地壳板块碰撞导致地震频发。本组报道据新华社

中
老
年
时
报
分
类
广
告

公告 遗失声明 通知 寻人
 房屋信息 个人物品售卖
 征婚等综合类广告信息

刊登咨询电话
13302008816