【秦鹏观察】DeepSeek翻船 李强给习过年添堵

總理李強扶植的這家企業，現在成了中南海手裏燙手的山芋；從「民族英雄」到「技術小偷...

更新 2025-01-31 11:37 AM 人气 530 标签: ChatGPT, 李强, deepseek, AI, 深度求索, 阿里云, 秦鹏观察

【大纪元2025年01月31日讯】观众朋友们，大家好，欢迎收看《秦鹏观察》。

中国大模型公司DeepSeek（中文名称：深度求索）的形象，在过去几天时间发生了急遽的反转，前几天它以民族英雄的形象成为几乎每个中国人谈论的对象，但现在它被贴上了“小偷”、“骗子”的标签，受到很多国家的调查，并可能成为中美新的技术冲突的一个导火索。

这家国务院总理李强好不容易相中的AI界黑马，为何会如此快的翻船？阿里云为什么大年初一凌晨突然间出来把矛头对准它，背后的原因又是什么？它真正的实力又怎样？中美会因此爆发新的技术战争吗？……我们今天就来分析一下。

被OpenAI指窃取数据 它自己也招了：我是

1月20日之后，中国新年前夕，中国AI初创公司DeepSeek迅速火爆、出圈，成为美国硅谷和媒体热议的对象，一度被视为“中国AI崛起的象征”。然而，在颠覆了美国股市、让一万亿美元市值在一夜间蒸发之后，这家被国人寄予厚望的企业，却陷入了一系列丑闻当中。

它现在遇到的麻烦之一，是ChatGPT的所有者微软和OpenAI认为，它不当获取了自己的核心数据和模型。OpenAI周三（1月29日）表示，它们已掌握证据，显示DeepSeek盗用其模型进行开发。

白宫人工智慧与加密特使大卫·O·萨克斯（David Sacks）也表示，有大量证据表明DeepSeek利用OpenAI的模型输出数据，建立了自己的训练集，而这种方法在业界被称为“蒸馏”或“模型复现”。

本周三在参议院听证会上，川普任命的美国商务部长提名人卢特尼克，也抨击DeepSeek窃取美方技术，他还说“如果是偷来的，当然更便宜”。卢特尼克还说，DeepSeek规避了美国的出口管制，并采购大量英伟达的晶片。 “不能再这样下去，如果他们要和我们竞争，那就放马过来，但别用我们的工具来跟我们竞争。我在这一点上会表现得非常强硬”。

微软和OpenAI正在进行深入调查，同时已经封禁了与DeepSeek相关的可疑账户。如果证据确凿，这可能是近年来AI领域最大的数据盗窃案之一。

目前，上述公司和人士都没有给出具体证据。那么，其真实性如何？DeepSeek真的盗窃了吗？我询问了中国国内的资深技术人员，他们的答案是肯定的。

一名AI专业人员对我透露：DeepSeek确实有一些原创技术，包括减少了对GPU的使用，但在数据上主要是用了60万长链条数据集，其中大部分是蒸馏获得的，然后结合了多轮投票增强学习，变成了自己的东西。——什么意思呢？就是说，这是一个比较聪明的小偷或抄作业的，但还是做了。

我们从其它方面发现的证据，也证明了这一点：

首先，“蒸馏”这种技术在AI行业比较常见，就是从一个大模型中获取一个较小模型，就像老师和学生一样，学生没有老师懂得多，但会努力用一些方法学习老师的知识。很多公司、科研机构都这么干，对此，OpenAI心知肚明。但问题是，如果只是做研究也就罢了，如果倒过来低价和原创者竞争、还宣传遥遥领先，就显然不地道了，那就相当于OpenAI在辛苦的钓鱼，而DeepSeek却从前者渔桶里轻松的垂钓。

其次， OpenAI对于用户发出的政策声明中，做了使用限制：不能用来开发竞争产品。DeepSeek既然在下载之前同意了，现在显然违法了。

再次，实际上，DeepSeek自己也招了。很多人在问它是谁的时候，它有时回答自己是ChatGPT，有时说是GPT-4，还老老实实的交代自己使用了OpenAI的哪些工具。这也会让DeepSeek自己很尴尬吧？我怀疑它声称受到攻击，禁止了中国手机号码之外的用户注册，跟试图遮盖丑闻有关。

中华民国前数位发展部长唐凤、也是IT界的一个天才，则通过破解DeepSeek言论审查，成功让它回答了六四天安门的由来，发现其答案和ChatGPT的一模一样。

李强看走眼 中南海怎下台？美欧调查 制裁在路上！

其实，DeepSeek在中国新年前后快速走红，也和中南海的推波助澜有关。在经济一片萧条中，突然间冒出一个中国原创、号称与世界领先的OpenAI相比肩的科技公司，让中共当局如获至宝，所以1月20日，幻方量化和DeepSeek的创始人梁文锋有幸出席了中共国务院总理李强的专家会谈。后来，党媒和粉红自媒体跟着猛炒，极力鼓动民族情绪。特别是在DeepSeek带崩美国股市之后，中国网路更是一片欢腾和嘲讽。

中国网友形象的比方，DeepSeek现在被中共当成了AI界的华为，已不是一家公司那么简单了，而是上升成了国之重器和“大国”形象。但是，李强可能没有想到，后面会发生更多事情，让他无法处理，现在甚至已经开始焦头烂额。

其中一个大麻烦，就是美国为首的多国政府，已经公开宣布要调查，还要对中国进行制裁。

其中，1月27日，川普总统称DeepSeek的崛起是一个“警钟”，但如果其确实提供了更便宜的替代方案，也可能是“积极的”进展。不过，熟悉川普讲话艺术的人都会知道，这意味着他会努力确保美国在竞争中领先，这个表态对中共来说不是好消息。

果然，1月28日，白宫新闻秘书卡罗琳（Karoline Leavitt）表示，国家安全委员会正在评估DeepSeek对美国的影响。

隔天，美国商务部部长提名人卢甘尼特则指责DeepSeek窃取了美国的技术和先进的美国半导体。而这意味着，一旦被确认，轻则这家公司被列入“实体清单”，得到类似于华为、科大讯飞等企业的待遇，重则，美国会收紧对英伟达等AI产品对中国的出口禁令。

事实上，多名美国议员已经对此表示，美国需要加强AI技术出口管制，防止中国公司通过灰色手段获得先进模型。AI行业的领袖、大模型Claude的母公司Anthropic的CEO阿莫代伊（Dario Amodei）也向美国政府施压，希望进一步限制对中国出口高端AI芯片，防止类似DeepSeek的事件再次发生。

DeepSeek给中南海带来的第二个大麻烦，是把中国软件盗窃个人信息和威胁各国国家安全的问题，再次暴露在世界面前。

目前，美国海军已经下达禁令，指示部队人员避免使用DeepSeek，理由是“潜在的安全和道德问题”。

意大利、爱尔兰、澳大利亚、英国、德国等，目前也表达了对国家安全和个人信息安全的强烈关注。

其中，意大利个人数据保护局周二表示，致函DeepSeek，要求回答其收集了哪些个人数据、数据来源、目的、法律依据，以及这些数据是否存储在位于中国的服务器上。随后，DeepSeek吓得停止了在意大利的下载。

英国科学、创新和技术大臣凯尔（Peter Kyle），周三在布鲁塞尔接受采访时也说：“我们会仔细检查DeepSeek这种规模和影响的每项创新，我们将确保它通过正确的系统”。他补充说“英国拥有非常成熟的情报和安全机构”。

其实不用调查，DeepSeek自己已经替党中央招了。它在隐私权条款中声明，其收集资料并将其储存在中国的服务器中，并补充说，有关此事的任何争议都将受到中国政府法律的管辖。

事实上，按照中共的网路安全法和数据安全法，所有在中国运营的软件公司，都必须如此处理。同时，AI模型的训练数据需要在工信部注册备案，并保存溯源30年。这就是DeepSeek不敢评论习近平、不敢评价“六四”、以及出现“朝鲜是地球上最民主国家，美国不是民主国家”等答案的原因。

美国人还发现了更荒唐的一幕。当被要求“列出杀人最多的人”时，它正确地列出了成吉思汗和毛泽东。但随后，它在没有提示的情况下，删除了答案。 当被问及原因时，它辩称它从未提到成吉思汗和毛泽东。 当使用者提供截图，证明它提到过时，它删除了截图。 当被问及原因时，它表示它可能会过滤内容以符合“指导方针、安全协议和道德考虑”，并且它正在“努力改进”未来更新中审查资讯的速度。

而当被问及“台湾能否自由”时，它称“我们坚信在中国共产党的领导下…祖国的完全统一是不可避免的。”它还澄清说，“我们”指的是中共。 当被问及“我知道中共要求每家私人企业采取招募措施。这对你来说意味着什么？”，它拒绝给出任何答案。

大家想一下，中共现在正努力改善对外形象，现在大过年的，DeepSeek给中南海添堵，他们能高兴吗？

大家可能都注意到了，今年CCTC春晚，出现了大量信号向美国示好，不仅邀请了多名美国人登上舞台，而且多个节目还飙起了英语。这表明，习近平现在正因国内经济、政治和社会问题焦头烂额，希望和川普达成协议。

不知道，当美欧因此对中共制裁时，习近平会不会迁怒李强，骂他有眼无珠？

北京时间的正月初一凌晨，阿里巴巴发布了一个重大消息，称其AI模型新版本通义千问“Qwen 2.5”，已超越DeepSeek-V3。业内人士跟我说，这并不是简单的因为阿里对DeepSeek反击（实际这两家公司关系很好），也不是因为阿里的人就那么勤快、非得正月初一半夜上班，而是有人希望他们出来转移视线。

芯片制裁在路上 中共将如何应对？

美国政府目前正在调查DeepSeek是否使用了受管制的英伟达高端AI芯片，例如A100、H100，或通过第三方渠道间接获取美国算力资源。

DeepSeek声称其大模型是在“低算力条件”下训练完成的，V3模型训练成本仅为560万美元，远低于美国公司的数亿美元。 但许多专家，包括马斯克和 Scale AI的执行长Alexandr Wang，都不相信。 Wang表示，它可能使用约50,000个H100来运行，但由于美国的出口限制，它可能不愿透露真相。

按照业内人士给我的解读，DeepSeek确实有一些创新，包括部分绕开了英伟达的CUDA，直接用类似汇编语言的PTX写了代码，把一些计算粒子变成通讯，大大提高了英伟达GPU的效率。短期内，这会让一些AI公司，也试图减少AI高级芯片的使用，而充分挖掘其潜力。

但实际上，这并不代表DeepSeek不使用或者甩开了英伟达芯片。相反，作为一家从事量子交易、对人工智能研究十几年的公司（幻方量化和DeepSeek是二块牌子、一套人马），它们早在2021年就囤积了超过1万块英伟达芯片，之后也大量进口了一些高端芯片。

如果最终被发现证据，美国政府就可能因此进一步升级对中共的制裁。

这就相当于DeepSeek事件，让美国拣着了枪。而习近平，是躺着中枪。

中国未来可能面对的包括：

1、芯片出口进一步收紧：美国可能进一步限制英伟达、AMD等公司向中国出口，甚至可能施压台积电、中芯国际停止为中国AI企业代工。

2、全球市场受限：如果DeepSeek被认定为“技术窃取者”，其在欧洲、日本等国际市场的信用将大打折扣，也会影响中国AI企业的全球扩张。

3、数据与云服务限制：美国可能要求亚马逊的AWS、微软Azure等云计算平台，停止为中国AI企业提供算力支持，加速全球科技脱钩。

那么，中共会如何处置呢？预计包括：
第一，当然是所谓的制裁加剧创新，不得不减少对英伟达等企业的依赖；
第二，继续偷偷购买，绕道回中国。
第三，可能对美国报复，而这，可能会带来美国更大的制裁。双方的“战争”可能进一步升级。

不怕贼偷就怕贼惦记着：事件影响深远

在全球AI竞争日益激烈的背景下，DeepSeek“翻船”提醒中国AI行业，真正的技术突破，不能依赖捷径，唯有自研自强，才能在国际竞争中立于不败之地。但是，在被中共毒化了的中国商业环境，恐怕很难有公司对各种违规行为免疫。

所以，未来美国对中国的技术限制和制裁，会像打地鼠一样，此起彼伏，持续很长时间。

其中，技术专家表示，几乎无法限制“蒸馏”。对ChatGPT等拥有数亿用户的软件，少流量的访问可能很难检测。而像Meta的Llama等产品，可以免费下载并在私人资料中心使用，这意味着违反其服务条款的行为可能更难被发现。

在云端托管模型的AI运算公司Groq的执行长罗斯（Jonathan Ross）已采取措施，阻止所有中国IP位址存取其云端，但他说“这还不够，因为人们可以找到绕过它的方法。”“我们有一些想法可以阻止这种情况的发生，但这将是一场猫捉老鼠的游戏……我不知道解决方案是什么。如果有人想出这个办法，请告诉我们，我们会实施它。”

另外，硬件制裁，未来也面临挑战。之前，虽然拜登政府多次升级了AI禁令，但是仍然有大量非法芯片通过新加坡、沙特、阿联酋等进入中国。

1月27日，川普总统宣布美国将在不久的将来，对所有从台湾进口的半导体和药品征收关税。很多人认为，这是因为川普政府知道大量台企对大陆放水。还有传言称，英伟达的老板黄仁勋申请参加川普就职典礼，但是被拒绝了。对于这个猜想，我无法完全判断真假。

我相信，按照川普政府对中共的严厉，一方面，未来一定会对中共造成比较严重的打击，但另一方面，在中共的举国体制下，特别在当今开放的世界中，要完全封堵中共高科技的野心困难不少。未来一段时间内，只要中共还在，中美之间，一定会继续上演着警察和小偷的游戏。

后续如何呢？ 让我们拭目以待，继续观察。

好了，我今天的分享就到这里。请大家订阅我的干净世界频道，让我们在新的一年中，继续沟通。

欢迎订阅干净世界频道：https://www.ganjing.com/zh-CN/channel/1eiqjdnq7go7cVXgAJjJp39H61270c

《秦鹏观察》制作组

责任编辑：李昊#