药企纷纷接入DeepSeek

医药行业从“试错”转向“预测科学”

▶ 孙立彬

近期，和众多其他行业一样，中国制药行业也迎来拥抱DeepSeek的热潮，包括上海复星医药（集团）股份有限公司（以下简称“复星医药”）、云南白药集团股份有限公司（以下简称“云南白药”）、江苏恒瑞医药股份有限公司（以下简称“恒瑞医药”）、信达生物制药（苏州）有限公司、维亚生物科技（上海）股份有限公司等在内的众多企业纷纷宣布接入DeepSeek。业内专家表示，DeepSeek正在引发医药行业从“试错法”向“预测科学”转变。

制药企业热情异常

一份名为《恒瑞医药管理总部文件》近日广为流传，恒瑞医药董事长孙飘扬亲自发起，指示全面应用DeepSeek，涉及各部门、分公司、子公司。该公司还成立了专项工作小组，推动DeepSeek在药物研发、临床诊断等领域的落地。

复星医药则在自主研发的PharmAID决策智能体平台上接入Deepseek-R1。该平台构建了覆盖医药创新研发场景的全生命周期智能决策网络，将在新药分子结合点位预测、构象预测、结合机制分析、毒理优化、医学写作、临床信息萃取等方面提升药物研发效率，加速科研成果转化。

中药龙头企业云南白药发布消息称，集团于2月9日结合工作实际，上线DeepSeek。据了解，目前云南白药数字员工“白小柒”“重小楼”已接入DeepSeek，为员工提供企业内部知识检索、文案创作、辅助制定营销方案等智能化工具，显著提升了生产力和工作效率。

公开信息显示，越来越多的药企结合自身实际情况引入DeepSeek大模型，以提升在药物研发、供应链优化、公司管理等诸多方面的效率。

粤港澳大湾区精准医学研究院原创新药研究中心主任粟武表示，与其他AI模型相比，DeepSeek的优势在于开源和较低的使用成本；在执行具体任务时能以更少的资源达到相近精度的结果。

除此之外，制药企业纷纷接入DeepSeek的原因还源于该模型优异的性能，例如领先的推理能力、完整的思维逻辑和卓越的模型性能。

为新药研发带来新变化

众所周知，药物研发过程投入大、耗时长，而在AI的助力下，新药研发的效率将显著提升。近年来，社会各界对AI可能给新药研发领域带来的革命性变化充满期待，但AI制药成果大多还处于早期研究阶段。DeepSeek能带来哪些新变化呢？

粟武认为，在新药研发领域，由于DeepSeek开源，研发人员就可以根据本企业的需求定制相应的工作模块，并以企业内部的数据进行训练，使相关的AI模型快速定向进化，助力特定研发任务的推进。

业内人士表示，DeepSeek其底层技术已展现出改写医疗范式的巨大潜力，比如其已经大大解决了成本问题，凭借更为先进的神经网络，大幅减少了专家输入的需求，进而提升工作效率。

此外，同类AI系统在基因治疗、合成生物学、中药现代化等领域的突破性进展，为DeepSeek提供了明确的技术参照系，通过其卓越的性能进行深度学习，有望模拟药物与生物分子的相互作用，预测药物的活性、毒性和代谢途径等。这种预测能力不仅提高了研发成功率，而且为药物的个性化治疗提供了可能性。

技术落地面临挑战

当然，DeepSeek在新药研发领域的应用还处于探索阶段，还有很长的路要走，正如华泰证券指出的，尽管DeepSeek在算法效率上取得了突破，但技术落地仍面临诸多挑战。例如，医疗数据隐私监管趋严，模型训练成本可能上升等。

而这些挑战不仅仅存在于DeepSeek，而是所有大模型共同面临的问题。

粟武表示，AI会颠覆性地改造药物研发全流程，从靶点确证、分子设计、先导化合物发现直至临床方案的设计等。但AI的作用像是放大器，正确和错误的影响都会被放大。药物研发人员最希望的大模型是以可靠的数据进行针对性训练的模型，除了通用数据，还需要引入药物研发的专业知识和数据库，才能使AI在处理药物研发的任务时理解行业术语，数据运用更加精确可靠。

AI制图：杨天

网络安全厂商竞相采用DeepSeek

▶ 孙立彬

近日，国际数据公司（IDC）发布相关分析认为，DeepSeek或成未来网络安全行业首选基础大模型。据了解，DeepSeek上线至今，已有包括安博通、安恒信息、北信源、观安信息、霍因科技、华云安、绿盟科技、奇安信、启明星辰集团、山石网科、天融信、亚信安全等在内的众多国内网络安全厂商宣布接入DeepSeek大模型能力，并将进一步进行能力融合，越来越多的安全智能体正在尝试采用DeepSeek作为大模型底座。

网络安全厂商为什么选择DeepSeek？

IDC认为，首先，DeepSeek采用的“专家混合架构”（MoE），在同等算力下实现了更高的推理效率，可显著提升实时威胁分析和自动化安全响应的能力。其次，相比于同等规模的大模型训练成本，DeepSeek更具有优势，可最大程度节约企业投入成本，对于最终用户来讲，其部署训练及使用大模型的意愿和能力也将显著提升。此外，DeepSeek的开源生态通过GitHub、Hugging Face等平台吸引了全球开发者参与优化与安全测试，形成了充满活力的协同创新生态。在性能方面，DeepSeek模型在数学、代码和自然语言推理等任务上表现出色，尤其在复杂逻辑推理场景中展现了强大的深度思考能力，可为威胁检测、告警验证等场景提供更智能的解决方案。

不过，在DeepSeek赋能网络安全行业的同时，IDC也发现，在大模型时代，AI的开放性与复杂性带来了前所未有的安全挑战，大模型安全问题已不容忽视。

从安全视角出发，无论何种使用场景，大模型或GenAI（生成式人工智能）的使用都可能会给最终用户带来新的安全风险。如训练安全：大模型训练数据质量把控不过关，使用有偏见的数据训练生成的大模型会持续输出有偏见的输出；在模型训练过程中大量高质量数据需要被集中在一起，数据泄露风险会陡然加大。基础设施安全：大模型运行所依赖的硬件设施、软件框架、操作系统等，若存在漏洞，会极大影响大模型的稳定与安全运行。内容安全：大模型生成内容可能存在不准确、不合规、个人敏感信息或企业机密信息以及存在侵权可能的内容；输入内容可能存在恶意攻击指令会干扰模型推理预测，造成不良后果。应用安全：在应用层面面临传统网络安全问题和应用框架安全双重风险，如DDoS攻击、SQL注入、恶意插件、跨站脚本攻击等。

针对这些新安全问题，IDC调研发现，目前，已经有越来越多的网络安全公司和大模型公司将关注重点放在大模型或GenAI工具的安全能力检测以及安全防护的方向上，推出了一系列的针对大模型或GenAI工具的安全检测和安全防护解决方案。当前大模型安全检测与防护解决方案包含了大模型攻防检测、输入内容安全检测、生成内容安全检测、代码安全检测、模型训练与防护、数据保护、访问控制与API防护几个大的方面。

DeepSeek后又有两款大模型开源

本报讯（记者 张伟）2月18日，阶跃星辰和吉利汽车集团联合宣布，将双方合作的视频生成模型阶跃Step-Video-T2V和语音交互大模型阶跃Step-Audio两款Step系列多模态大模型向全球开发者开源，即日起可在跃问APP内体验。这是继DeepSeek后又有两款大模型向开发者开源。

阶跃星辰是吉利汽车集团的科技生态战略合作伙伴。在两款大模型的研发过程中，双方展开了深度合作，在算力算法、场景训练等领域优势互补，显著增强了多模态大模型的性能表现。此次联合开源的行动，旨在促进大模型技术的共享与创新，推动人工智能的普惠发展。这一举措也将为开源世界贡献多模态大模型能力，形成大模型开源世界的又一股中国力量。

吉利汽车集团CEO淦家阅表示，早在2021年，吉利就围绕芯片、软件操作系统、数据和卫星网搭建了端到端的自研体系和生态联盟，构建了完善的“智能吉利科技生态网”，驱动用户在智能驾驶、智能座舱上的体验不断进化。目前，吉利全栈自研的星睿AI大模型已经与阶跃Step-Video-T2V、Step-Audio等大模型完成了深度融合，将为用户带来更智能、更高阶的座舱交互与智驾出行体验，推动AI在智能汽车领域的普及。

据悉，阶跃Step-Video-T2V模型的参数量达到300亿，可以直接生成204帧、540P分辨率的高质量视频，这意味着能确保生成的视频内容具有极高的信息密度和强大的一致性；阶跃Step-Audio语音交互模型，能够根据不同的场景需求生成情绪、方言、语种、歌声和个性化风格的表达，能与用户自然高质量对话。