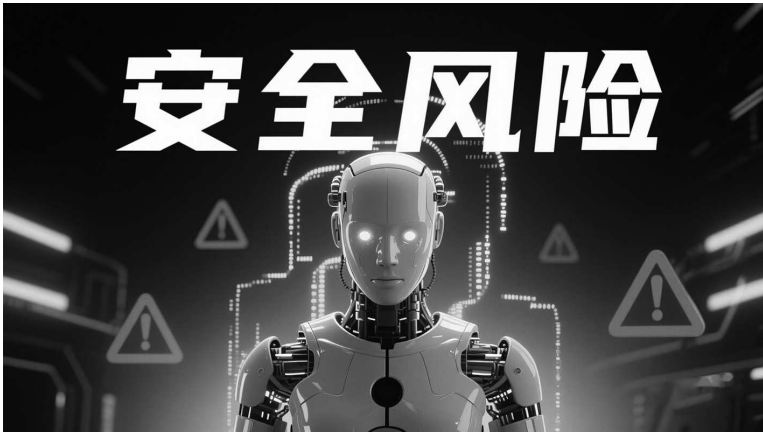


以大模型为核心的人工智能技术是创新范式变革与产业升级的关键引擎，越来越多的机关、企事业单位开始推进大模型私有化部署，广泛应用于企业办公、科技研发、公共服务等领域。然而，技术跃升与安全风险始终伴生演进，如何强化模型全生命周期安全管理，赋能 AI 行业向好向善发展，成为当前亟需解决的课题。



AI 生成

需加重视的潜在风险

近期多项研究发现，近 90% 私有化部署的服务器在互联网上“裸奔”，部分模型本身也容易被攻击，存在安全漏洞。目前，个别单位所谓的“设防”也只是简单地设置密码，易被攻破，个别单位甚至连防护密码都没有。可以预见，未来随着大模型普及使用，有针对性的恶意手段和风险场景势必激增。因此，网络安全防护必须与技术发展同步迭代。

敏感数据安全问题

大模型在训练、推理、使用过程中会涉及海量数据，如用户在输入数据时不当存储和处理，特别是违规在未设防模型中处理涉密数据、个人隐私数据、商业敏感数据

时，存在数据被非法获取、泄露风险。

关键领域安全问题

人工智能离不开高科技设备，如这类设备被植入后门程序会让智能工厂、金融机构、能源设施等关键领域面临风险。违法犯罪分子如恶意利用大模型部署的安全漏洞破坏相关系统，将可能导致公共服务中断、企业经济损失、安全事故频发等恶性事件，干扰经济正常运转和社会有序运行。

侵犯用户利益

普通用户如未加防护使用大模型服务工具，攻击者也可以远程调用接口窃取模型参数、训练数据、知识库等核心资产，或删除、污染私有模型文件，导致模型失效或输出偏差。同时，攻击者可通过未授权的接口调用模型推理功能，滥用

安全驶入快车道 堵漏洞，助力 AI 发展

GPU 资源。如处理数据量过大，大模型服务器就会因算力耗尽导致瘫痪。

大模型安全风险产生原因

开源框架存在不足

许多单位为了快速上线服务，直接使用开源框架，默认开启不设密码的公网访问模式，不配置合理的安全防护措施，忽略最基本的防火墙配置。攻击者未经授权即可自由访问模

型服务、窃取敏感数据，甚至通过历史漏洞执行恶意指令，从而导致数据泄露和服务中断。

风险意识存在欠缺

部分管理者对 AI 安全的认知相对滞后，部分群众认为“安全是专家的事”，不了解部署 AI 服务需要像保护银行卡密码一样谨慎，在享受 AI 带来便利时未考虑背后隐藏的风险。

安防教育有待加强

一些企事业单位缺乏必要的安全防范教育，导致员工国家安全隐患意识和素养不高，安全防范意识不强，对于大模型缺乏用心管理，安防教育缺乏必要的认识。

专门法律存在空白

我国近年来已经出台了多部关于人工智能和网络数据方面的政策法规和指导意见，但随着人工智能迅猛发展，应运而生的法律问题尚需进一步完善相关立法。

国家安全机关提示

大模型是推动科技进步的重要力量，但其安全防护须臾不可松懈，无论是开发者、企业还是普通用户，都应提高警惕，共同守护技术红利不被恶意利用。

● 做好安全防护，筑牢安全防范屏障

AI 企业在开发和应用大模型的过程中需重视自身应承担的安全责任和义务，可通过加强与安全厂商合作，以严密的安全技术保障和运行监测，强化大模型运行时的安全性、可靠性和稳定性。

● 培养安全意识，打造协同防御生态

单位、企业在部署大模型前，需要进行全面的风险评估和安全规划，通过制定安全政策、开展安全培训等方式，提高全员安全意识。广大民众要增强大模型使用的安全意识，注意学习相关安全知识，养成良好使用习惯，选择从官方渠道下载大模型工具，使用时不要随意连接陌生网络，确保大模型应用安全稳定。

“赶考”路上 保驾护航

1949 年 3 月 23 日，中共中央从西柏坡迁往北平，毛泽东同志意味深长地说：“今天是进京赶考的日子。”76 年来，从“进京赶考”到“新的赶考之路”，“赶考”精神不仅是历史记忆，更是中国共产党人时刻保持清醒坚定、锐意进取、永不懈怠的行动指南和生动写照。“赶考”路上，隐蔽战线作为中国共产党领导下维护国家主权、安全、发展利益的特殊力量，在看不见硝烟的战场上为民族独立、国家富强和民族复兴保驾护航。

“赶考”背后的无声战场

“赶考”前夕，北平虽已解放，但国民党特务、土匪和反动势力仍频繁制造绑架、暗杀等事件，严重威胁我中央领导人生命安全。

根据党中央指示精神，中央情报部部长李克农带领工作组提前进

驻北平，经过严密侦察，建议将香山作为中共中央迁往北平后的临时驻地。为确保党中央驻地安全，工作组立即对香山及西郊地区进行地毯式排查，消除了地雷、枪支等危险物品隐患，建立了多层警戒网。此外，中央情报部在西柏坡还组建了一支便衣保卫队，他们中有许多同志长期在敌占区从事隐蔽斗争。1949 年 3 月上旬，这支保卫队经过严格的政治历练和业务培训后抵达北平，迅速投入以香山为重点的保卫工作，查看地形、熟悉环境、甄别敌伪档案、控制重点敌嫌对象，并以各种掩护职业暗中保卫重点路线和重要人物，确保党中央进京后的绝对安全。

“赶考”仍在路上

76 年前，毛泽东同志离开西柏坡时提出了著名的“赶考”命

题，从此成为中国共产党人执政“赶考”的永恒主题。76 年来，中国共产党“赶考”的脚步从未停歇，从新中国成立到社会主义革命和建设时期，从改革开放和社会主义现代化建设时期到中国特色社会主义进入新时代，从一穷二白到世界第二大经济体，从温饱不足到全面小康，中华民族实现了从站起来、富起来到强起来的伟大飞跃。我们党的“赶考”实践，既波澜壮阔、又跌宕起伏，既立足于现实“考题”、又着眼于未来使命，既立足于提高自身执政能力和巩固执政地位、又指向维护和实现最广大人民群众的根本利益。我们在这场历史性考试中取得了优异成绩，向历史和人民交出了一份满意答卷。当前，我国迈上全面建设社会主义现代化国家新征程，踏上了实现第二个百年奋斗目标新的“赶考”之路，必须始终保持“赶考”的清醒和坚定，始终发扬时刻自省、永不懈怠的革命精

神，不断开辟党和国家各项事业新局面，让“赶考”精神永放光芒。

护卫新时代“赶考”之路

时代在变，“考题”在变。当前世界百年未有之大变局加速演进，全球经济复苏进展曲折缓慢，地缘政治局势持续紧张，冷战思维、零和思维沉渣泛起，单边主义、保护主义甚嚣尘上，民粹主义和极端主义抬头趋势明显，国家安全形势严峻复杂。国家安全机关将始终坚持以习近平新时代中国特色社会主义思想为指导，坚持和发扬“赶考”精神，全面贯彻落实总体国家安全观，以解放思想开路、以调查研究开局、向制约瓶颈开刀，进一步全面深化国安改革，加快形成和提升新质国安战斗力，以中国式现代化全面推进强国建设、民族复兴伟业筑牢安全屏障。

(均转自国家安全部微信公号)