《基于大模型的网络攻击行为建模与防御技术要求》

编制说明

2026 年 4 月

一、工作简况

（一）任务来源

本项目根据中国互联网协会2025年团体标准制定计划（标准计划号：140-T/ISC-25），项目名称为“《基于大模型的网络攻击行为建模与防御技术要求》”的任务而进行制订。

（二）起草单位及主要起草人

本文件起草单位：国网河南省电力公司信息通信分公司、中国信息通信研究院、公安部第三研究所、北京邮电大学、广州汇智通信技术有限公司、零日信安（武汉市）技术有限责任公司、北京航空航天大学、中科数测科技有限公司、华兴中科标准技术（北京）有限公司。

本文件主要起草人：闫丽景、陈文弢、静静、马若龙、邵彦华、付文豪、詹前靖、刘欣然、王磊、王悦霖、白天锐、芦艺佳、肖蔚琪、李洁、周鸣一、黎立、董坤、董婧一、成瑾、李华、任国静、丁月。

（三）标准制定目的和意义

数字经济发展是国家现代化建设的重要引擎，网络安全作为数字经济发展的基石，其保障能力直接关系到国家主权、安全和发展利益。基于大模型的网络安全技术作为人工智能与网络安全深度融合的重要方向，凭借其强大的数据分析、模式识别与预测能力，已成为提升网络安全防御水平的关键突破口。《网络安全法》等法律法规明确要求“提升网络安全保障水平，防范网络违法犯罪活动”，为网络安全技术创新与标准建设提供了根本遵循。

基于大模型的网络攻击行为建模，是指利用大模型对海量网络攻击数据进行学习，提炼攻击特征、挖掘攻击路径、预测攻击趋势的技术方法；对应的防御技术则是在建模基础上，构建动态防护策略、实现精准拦截响应的安全机制。智能防御体系则是通过大模型与安全设备、数据平台的深度融合，将攻击建模、态势感知、防御响应等业务与数据进行整合，实现网络安全全流程动态管理。

随着数字社会建设的深入推进，关键信息基础设施、金融、能源等重点领域面临的网络攻击威胁持续加剧，勒索攻击、供应链攻击等新型攻击事件频发，对经济社会稳定运行和人民群众合法权益造成严重影响。行业依赖传统基于规则库的防御手段，存在检测滞后、适配性不足等问题，且在基于大模型的网络攻击行为建模与防御环节缺乏统一技术规范，存在显著安全风险，亟需通过标准制定填补技术空白，提升全行

业安全防御水平。本标准的制定可以补充完善我国网络安全技术标准体系，推动基于大模型的攻击防御技术规范化发展，同时也将有助于降低新型网络安全事件的发生概率，保障数字经济健康安全运行。

（四）主要工作过程

2025 年 12 月本团体标准由中国互联网协会正式立项，立项名称为：《基于大模型的网络攻击行为建模与防御技术要求》。

2025 年 12 月 5 日通过腾讯会议召开了本团体标准的第一次讨论会。本次会议确定了本标准的框架结构，收集了与会各单位对标准草案（初稿）的修改意见或建议，明确工作组各单位的工作分工，以及会后的具体工作安排。

2026 年 3 月 24 日通过腾讯会议线上召开了本团体标准的第二次讨论会。编制组就本团体标准第一次讨论后的修改情况、意见采纳情况进行了综合阐述。与会专家及代表对该项团体标准的定义内容、技术内容等进行了进一步的深入讨论和修改，编制组认真听取和记录了与会代表提出的问题和调整建议。

二、标准编制原则和依据

（一）编制原则

标准起草小组在编制标准过程中，以国家、行业现有的标准为制订基础，结合我国电子油泵产品的现状，按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定及相关要求编制。

（二）标准范围

本文件规定了基于大模型的网络攻击行为建模与防御的攻击行为建模技术要求、防御技术要求以及安全评估和测试等内容。

本文件适用于大模型在网络攻击检测、行为分析、威胁建模和防御措施中的应用，适用于大模型开发方、部署方、服务提供方和评估机构。

（三）标准主要内容与确定依据

1.攻击行为建模技术要求

本章节对攻击行为建模技术要求的攻击类型建模、行为特征提取、建模方法、建模结果验证与优化要求做出了规定。

依据：参考 GB/T 20986、GB/T 37027 等相关标准要求，结合行业需求和企业生产

实际。

2.防御技术要求

本章节对防御技术要求的总体要求、训练阶段、部署阶段、使用阶段、运营阶段做出了规定。

依据：结合行业需求和企业生产实际。

3.安全评估和测试

本章节对安全评估和测试的评估指标、测试方法、测试环境要求、测试报告要求做出了规定。

依据：结合行业需求和企业生产实际。

三、国内外情况简要说明

经查，暂无相同类型的国际标准与国外标准，故没有相应的国际标准、国外标准可采用。本标准达到国内先进水平。

四、与有关的现行法律、法规和强制性国家标准的关系

本标准的制定过程、技术要求的选定、试验方法的确定、检验项目设置等符合现行法律法规和强制性国家标准的规定。

五、重大分歧意见的处理经过和依据

本文件在制定过程中未出现重大分歧意见。

六、废止现行有关标准的建议

本标准不涉及对现行标准的废止。

七、其他应予说明的事项

无。

团体标准编制组

2026 年 4 月