 DOI: https://doi.org/10.12349/iser.v7i8.11574

An Applied Research on the Use of Artificial Intelligence and Big Data Technologies in the Identification and Governance of Network Ecosystem Risks

Guoxiang He

Zhongxian County Cybersecurity and Information Center, Zhongxian County, Chongqing, 404300, China

Abstract

Risks within network ecosystems are characterized by rapid propagation, high concealment, and a broad impact scope; consequently, traditional approaches—such as manual inspection and point-specific security measures—are increasingly inadequate for meeting the governance requirements of complex network environments. Artificial intelligence and big data technologies can be employed to conduct comprehensive analysis of network traffic, user behavior, log data, content information, and security incidents, thereby enhancing risk detection capabilities, anomaly identification capabilities, and collaborative response capabilities. This paper examines the practical needs for identifying and managing network ecosystem risks within the context of network engineering applications, explores ways to leverage AI and big data technologies in data collection, model-based anomaly detection, trend analysis, and engineering-driven incident response, and proposes optimization measures to provide a valuable reference for cyberspace security governance.

Keywords

artificial intelligence; big data technology; cybersecurity ecosystem risks; risk identification; cyber engineering

人工智能与大数据技术在网络生态风险识别治理中的应用研究

何国翔

重庆市忠县网络安全和信息中心，中国 · 重庆 404300

摘　要

网络生态方面存在的风险有着传播速度较快、具备较强隐蔽性、影响范围比较广泛等多项特点，以往传统的人工巡查、单点防护这类方式，已经很难满足复杂网络环境之下的治理要求。人工智能和大数据技术可以针对网络流量、用户行为、日志数据、内容信息、安全事件进行综合分析，以此提高风险发现能力、异常识别能力、协同处置能力。本文结合网络工程的应用场景，对网络生态风险识别治理的现实需求予以分析，探讨人工智能与大数据技术在数据采集、模型识别、趋势感知、工程化处置当中的应用途径，并且提出优化举措，从而为网络空间安全治理提供一定参考。

关键词

人工智能；大数据技术；网络生态风险；风险识别；网络工程

1 引言

在互联网平台、云计算系统、移动应用迅猛发展的当下，网络生态风险展现出多源化、链式化、智能化的趋势。虚假信息传播、恶意流量攻击、异常账号行为、数据泄露、网络诈骗等一系列问题，不但对用户权益造成了影响，而且还给平台运行秩序、网络工程安全带来了挑战。网络工程领域有必要在链路监测、日志采集、边界防护、异常识别、联动处置等多个环节建立更为智能的治理模式。人工智能与大数据技术相互融合加以应用，能够提高风险识别的精度、响应的效率，促使网络生态治理从被动处理朝着主动防控的方向转变。

2 网络生态风险识别治理的现实基础

2.1 网络生态风险类型呈现复杂化特征

网络生态风险从原本单一的信息安全问题，发展成了内容、行为、技术、传播风险相互交织共同存在的状况。在内容方面，有着虚假信息、恶意营销、不良信息扩散等情况，行为方面会呈现出批量注册、刷量控评、异常登录、欺诈交易等现象，技术方面涉及恶意扫描、DDoS 攻击、接口滥用还有数据窃取等问题。不同的风险常常相互叠加，比如说异

【作者简介】何国翔（1987–），男，中国重庆人，本科，工程师，从事网信专业、网络生态治理研究。

常账号可能会借助脚本去传播有害内容，恶意流量也许会把数据爬取行为给掩盖起来 [1]。网络工程环境是由服务器、网关、防火墙、数据库和终端节点一起构成的，风险识别需要依赖跨系统、跨数据源的综合分析机制。

2.2 传统治理方式难以适应高频动态风险

传统网络生态治理主要依靠人工审核规则匹配、事后处置等方式，在风险类型比较稳定的时候能够发挥一定作用。然而在面对那些高频变化隐蔽传播且会跨节点扩散的风险时，其响应能力明显欠缺。规则库的维护依靠人工经验，对于变形词伪装链接异常脚本、新型攻击方式的识别存在滞后情况。人工巡查很难覆盖海量的平台内容实时流量、系统日志。网络工程系统每天都会产生访问记录认证日志 DNS 请求接口调用、安全设备告警等内容，如果缺少自动化关联分析，风险常常在扩散之后才会被发现，治理效率很难满足现实需求。

2.3 网络工程场景为智能治理提供数据基础

网络工程系统具有较强的数据采集和运行监测能力，为智能化风险治理提供了重要基础条件。路由器、交换机、防火墙、入侵检测设备、WAF、负载均衡、数据库审计系统和应用服务器等设施，在运行过程中能够持续产生访问路径、连接状态、接口响应、用户行为、流量峰值和异常事件等数据。这些数据既能反映网络系统运行状态，也能揭示潜在风险活动。通过镜像流量采集、NetFlow 分析、日志集中管理、探针部署和安全设备告警接入，可以构建较为完整的数据链路，使不同层级、不同来源的风险信息能够被统一汇聚。大数据平台负责对原始数据进行清洗、去重、标准化和关联分析，人工智能模型则在海量数据中提取异常模式，识别隐藏在正常访问行为中的风险特征。

3 人工智能与大数据技术在风险识别中的应用路径

3.1 基于多源数据融合构建风险感知体系

对网络生态风险进行识别时，需要把内容数据、行为数据、流量数据、日志数据整合起来，以此建立统一的风险感知基础。大数据技术能够把分散于网络边界、应用系统、数据库还有用户管理模块里的信息进行集中采集、清洗、关联。在工程实践当中，可以借助日志采集代理来汇聚服务器日志，利用流量探针获取访问特征，凭借安全设备接口同步告警信息，并且从业务系统里提取账号行为数据。数据进入平台之后，要完成时间同步、字段标准化、异常值处理、标签标注，从而确保模型输入稳定可靠。多源融合能够弥补单一数据判断存在的不足，当登录失败、高频接口调用、异地访问、异常流量同时出现的时候，系统就能够更早识别出账号被盗或者自动化攻击风险。

3.2 运用人工智能模型提升异常识别能力

人工智能技术具备从复杂数据里学习隐蔽特征的能力，进而提高网络生态风险识别的精准度。针对内容风险，借助自然语言处理模型能够识别虚假宣传、诱导性表达、恶意文本，针对图片、视频等多媒体内容，结合计算机视觉模型可检测违规画面、二维码链接、伪造内容。面对行为风险，机器学习模型能分析登录频次、访问路径、点击节奏、设备指纹、接口调用规律，进而发现异常账号、脚本访问、批量操作行为。对于网络攻击风险，依据流量特征、协议字段、连接状态、请求间隔建立检测模型，以此提高对异常扫描、暴力破解、恶意爬取的识别能力。

3.3 利用大数据分析实现风险趋势研判

大数据技术的价值并非仅仅局限于存储、检索方面，其更重要的意义在于能够支持风险趋势的分析、趋势感知。网络生态风险一般具备周期性、区域性、群体性等特征，仅仅凭借单次告警是很难体现出整体风险变化情况的。通过对访问量、异常账号数量、攻击来源、热点话题、违规内容传播路径、设备告警频次进行持续分析，能够了解风险演化的规律。网络工程平台能够把实时流处理与离线分析结合在一起，实时流处理的作用是捕捉突发流量、异常登录、安全告警，离线分析则是用于复盘风险来源、模型效果、处置结果 [2]。趋势研判还能够对资源调度起到辅助作用，当攻击流量不断上升时，能及时对防火墙策略进行调整、扩展带宽防护、对负载均衡进行优化并且加强重点接口的限流，促使治理从单点处置朝着整体管控转变。

4 网络工程视角下的智能治理机制构建

4.1 建立分层防护与联动处置架构

人工智能、大数据技术若要发挥治理功能，则需融入网络工程防护模式之内。可以依据网络边界层、平台应用层、数据资源层还有业务管理层来建立分层防护架构。网络边界层着重部署防火墙、入侵防御、流量清洗、访问控制设备，以此阻断明显带有恶意的流量。平台应用层借助 WAF、接口鉴权、验证码、限流策略、异常行为检测来降低业务风险。数据资源层强化数据库审计、敏感数据识别、访问权限控制。业务管理层承担内容审核、风险研判、处置复盘任务。各层之间要经由统一安全运营平台达成告警汇聚、策略联动。当模型识别出异常行为之后，系统能够自动触发限流、封禁、二次验证、人工复核或者溯源分析。分层防 4.2 完善风险识别模型训练与评估机制

智能治理系统所呈现出的效果，其关键在于模型质量，而模型质量又与样本数据、特征工程、评估机制紧密相关。网络生态风险样本存在变化速度较快、标注难度较大、类别不均衡等特性，企业或者平台需要建立能够持续更新的数据集，把历史风险事件、人工审核结果、安全设备告警、处置结论融入模型训练之中。针对数量较少的高危样本，可以采用样本增强、迁移学习、人工标注复核等方式来提高模型的识别能力。在模型上线之前，应当对准确率、召回率、误报

率、处理时延等指标展开测试，不能仅仅一味追求单一识别精度。在网络工程场景当中，如果误封正常用户或者误拦正常流量，将会对业务体验造成影响，所以模型阈值设置理应依据业务风险等级予以调整。

4.3 推动监测预警与人工审核协同运行

网络生态治理不能仅仅依靠机器判断，也不能单纯停留在人工凭借经验处理的方面。比较合理的做法是建立一种协同机制，这种协同机制包括机器识别、人工复核、策略反馈这几个部分。人工智能模型需要负责对数量庞大的数据进行初步筛选工作，能够快速识别出高风险内容、异常账号、恶意流量、可疑操作，人工审核人员则针对高风险或者边界模糊不清的事件作出判断，以此避免因算法误判而导致管理出现偏差。审核得出的结果应当及时返回到数据平台当中，成为模型优化、规则更新的重要参考依据 [3]。对于确定性比较高的风险，能够由系统自动采取拦截、限流、封禁、告警等措施，对于那些影响范围比较大或者涉及到用户权益的事件，则应该保留人工确认的环节。监测预警还需要形成等级化的处置流程，根据风险影响、传播范围、攻击强度来设置不同的响应级别。

5 人工智能与大数据治理应用的优化措施

5.1 加强数据治理与安全合规管理

网络生态风险识别离不开大量数据的支持，而数据采集、存储、使用均要符合安全合规的要求。在平台建设过程中，采集范围、使用边界、保存周期、访问权限都应当明确，防止出现过度采集、无序共享的情况。针对用户行为、账号信息、访问日志、敏感内容，要采取脱敏处理、分级授权、加密存储、日志审计等一系列措施，以此保障数据使用的安全。大数据平台还需要建立统一的字段标准、时间格式、事件编码，确保不同系统的数据能够准确关联。数据质量对模型判断有着直接影响，低质量样本可能会导致误判或者错误处置，所以应当完善数据清洗、标签审核、样本复核机制，让智能识别系统在保障用户权益的前提下达成风险防控。

5.2 提升平台工程化部署与运维能力

人工智能、大数据治理系统要有稳定的工程环境来给予支撑。在网络工程建设里，要依照业务规模、风险等级、实时处理需求，去合理地设计数据采集节点、计算资源、存储架构还有容灾方案。对于实时性要求比较高的识别任务，能够让边缘节点来完成流量的初步筛选、本地告警，中心平台则负责深入分析、模型训练、策略管理。安全运营平台还得和防火墙、WAF、入侵检测、日志审计、业务系统打通接口，从而让模型识别结果可以转变为限流、拦截、复核、告警等具体的处置动作。

5.3 建立持续评估与闭环优化机制

网络生态风险处于持续变动之中，相应的治理模式也要持续保持动态优化。企业需要建立起包括风险识别、处置反馈、效果评估、策略调整的闭环机制，定期对模型告警准确性、人工审核效率、风险处置时效、用户申诉情况展开分析 [4]。针对误报率偏高的风险类型，要对特征选择、模型阈值、规则条件予以优化，针对出现漏判的事件，则要对传播路径、数据采集盲区、处置流程短板进行复盘，进而补充监测维度。治理效果的评价不能仅仅聚焦于拦截数量，还应当综合考虑风险扩散控制、对正常业务的影响、系统响应时间、处置合规性等方面。

6 结语

人工智能跟大数据技术给网络生态风险识别治理带来了新的支撑途径。依靠多源数据采集、智能模型分析、风险趋势研判、工程化联动处置，能够有效提高网络风险发现跟治理效率。网络工程方向的应用不能只注重算法本身，还得重视日志采集、流量监测、边界防护、平台部署、运维管理等基础环节 [5]。未来实践里，要在数据安全合规、模型调整、多部门协同治理之间达成平衡，让智能技术切实服务于网络生态安全、平台秩序维护、网络工程系统稳定运行。

参考文献

[1] 张蓝天.人工智能和大数据技术在计算机网络安全防御系统中的多元化分析[J].信息与电脑,2026,38(12):159-161.

[2] 沈莉.大数据时代网络舆情治理能力提升研究[J].广州广播电视大学学报,2022,22(2):91-95+112.

[3] 姜金贵,卢至滔.信息生态视域下生成式人工智能驱动的网络舆情风险治理研究[J].情报探索,2026,(4):60-66.

[4] 侯勇,肖洋.应用生成式人工智能建构网络育人新生态的价值图景、潜在风险与行动策略[J].中国德育,2025,(22):15-20.

[5] 赵杰.智能推荐算法赋能网络舆论生态治理的逻辑理路与风险省思[J].中共乐山市委党校学报,2025,27(5):24-33.