网络安全态势感知技术在信息系统中的应用

姜婧茹
南通大学　江苏省南通市　226019

摘　要：网络安全态势感知技术在信息系统中的应用信息技术飞速发展且网络空间持续扩张，使得网络安全问题越发突显，传统被动防御安全策略应对复杂多变的网络安全威胁已经力不从心。网络安全态势感知是一种主动防御技术，可全面感知网络环境里的安全要素并实时监测、分析和预测网络安全状况，给信息系统安全防护带来强大支撑。本文系统地梳理了网络安全态势感知基本概念、理论框架和关键技术，着重分析数据采集与预处理、安全事件检测与识别、态势评估与预测等核心技术及其实现方法，并且探讨它在政府、金融、能源、医疗等关键信息基础设施的应用实践，剖析应用时面临的数据质量参差不齐、实时性要求高、安全知识不好表达等技术挑战。研究显示，依托大数据分析、人工智能和可视化技术的态势感知系统能有效提高信息系统安全防护能力，达成从被动响应向主动防御的转变。不过现在态势感知技术还存在感知数据不全、分析模型精度不够、威胁预测能力不足的问题，以后的研究要加强多源异构数据融合处理、深度学习与知识图谱相结合的智能分析以及态势预测方法的创新，促使网络安全态势感知技术在信息系统安全保障方面深入应用与发展。

关键词：网络安全；态势感知；信息系统；安全防护；智能分析

1 引言

全球数字化转型加速使网络空间变成国家经济、社会运行的关键基础设施，但网络攻击手段变得多样且复杂让传统安全防护机制难以应对不断涌现的安全威胁，2023 年网络安全行业报告表明全球因网络攻击遭受的经济损失超 6 万亿美元且该数字每年以 15% 速度增长，在政府、金融、能源、医疗这些关键信息基础设施领域尤其如此，网络安全事件频频发生既影响业务连续性又严重威胁国家安全与社会稳定，于是网络安全态势感知技术在这种情况下作为主动防御手段出现并能实时监测、分析、预测网络环境中的安全状况给信息系统全方位的安全防护支持从而成了当下网络安全领域研究的热点。

网络安全态势感知技术关键是采集与处理多源异构数据并运用人工智能和大数据分析方法来精准评估网络安全状态且动态预测之，这几年这一技术在多个行业广泛使用，拿金融来说态势感知系统能快速甄别异常交易行为并对潜在网络攻击预警，在能源方面则通过实时监控工业控制系统运行状态来有效防止关键基础设施遭受定向攻击，不过实际应用时仍有不少挑战像数据质量有好有坏、实时性要求高、安全知识不好表达之类的问题，并且现有的态势感知系统在感知范围、分析精度和预测能力上还有很大提升空间，所以以后的研究要聚焦于多源数据融合处理、智能分析模型优化以及创新的态势预测方法才能进一步发展网络安全态势感知技术让信息系统的安全保障能力从被动响应变成主动防御。

2 网络安全态势感知关键技术分析

2.1 数据采集与预处理技术

在网络安全态势感知里，整个系统的构建以数据采集与预处理技术为基础，由于网络空间快速拓展且攻击手段日益多样化，信息系统每日产生的海量数据涵盖流量日志、用户行为记录、系统运行状态、外部威胁情报等，其来源广泛、形式多样，包含结构化、半结构化、非结构化数据类型，但原始数据噪声大、冗余高、格式不统一，直接用于安全分析很困难，所以高效的数据采集与预处理技术相当关键，这几年像 Hadoop 和 Spark 这样的大数据平台技术框架在数据采集方面广泛应用，依靠分布式存储和计算能力可实现实时捕获大规模数据并初步清洗，针对数据质量问题，研究者提出不少预处理方法，如异常值检测、数据归一化、特征提取、降维等，这些技术能有效提升数据质量，给后续安全分析打基础，在金融、能源等行业尤其如此，因为它们业务场景复杂又高度敏感，数据采集的全面性与准确性直接影响安全防护效果，统计显示 2022 年全球超 30% 的网络安全事件由数

据采集不完全或者预处理不当造成，这更突显这项技术的重要性。

2.2 安全态势指标体系构建

网络安全态势感知的核心内容之一是构建安全态势指标体系，其目的在于借助科学合理的指标设计全面反映网络环境中的安全状况。完善的指标体系需综合考量网络资产、威胁情报、漏洞信息、攻击行为等诸多维度并结合具体行业特性定制化设计，如在政府与医疗领域，除关注传统入侵检测率和恶意代码传播速度外，还得格外重视数据泄露风险和隐私保护水平。为提高指标体系的实用性和可操作性，研究者引进层次分析法（AHP）、模糊评价模型等数学工具来量化不同指标权重以评估整体安全态势 [1]。与此同时，伴随人工智能技术发展，基于机器学习的动态指标调整方法兴起，此方法能依据历史数据和当前环境变化自动优化指标参数。不过，构建统一且通用的指标体系仍存在不少挑战，多源异构数据融合时保证指标一致性与兼容性尤为困难。相关统计显示，2021–2023 年由于指标体系不完善，安全误报率平均上升 15%，可见该领域研究还有很大改进空间。

2.3 多源数据融合与态势评估算法

实现网络安全态势感知的关键技术是多源数据融合与态势评估算法，该算法旨在从分散数据里提炼有价值信息并达成对当下安全状况的整体认知。实际应用时，网络环境数据来源非常多，有内部监控系统、外部威胁情报平台以及第三方合作机构提供的补充数据，且这些数据异构性很强、更新频率很快，所以得用先进融合算法整合信息。近些年，基于深度学习的融合模型优势明显，像卷积神经网络（CNN）、循环神经网络（RNN）在流量模式识别、时间序列分析里广泛应用，从而提高数据关联性与预测精度，并且知识图谱技术也被引入态势评估中，构建实体关系网络能更直观地揭示潜在安全威胁路径 [2]。不过，现有算法应对新型攻击手段不够理想，在零日漏洞利用、高级持续性威胁（APT）检测时误判率高。调查显示，2022 年中国关键信息基础设施领域大概 40% 的安全事件没及时发现，主要原因是融合算法覆盖范围有限。以后的研究应该致力开发更智能、自适应的评估算法以应对越来越复杂的网络威胁。

2.4 态势预测与可视化技术

网络安全态势感知中态势预测与可视化技术是重要部分，二者负责把抽象数据变成直观决策支撑，其中态势预测技术主要靠时间序列分析、回归模型、强化学习等方法，通过学习历史数据推断趋势来对可能发生的攻击行为预先预警，像在能源行业，实时监测和预测电网运行数据能有效防止分布式拒绝服务（DDoS）攻击损害供电系统，并且可视化技术借助图表、热力图、三维建模等形式助力管理者迅速明白复杂网络安全状况，近年引入虚拟现实（VR）、增强现实（AR）技术后进一步提高了可视化的交互性和沉浸感，不过目前态势预测技术有局限性，尤其在突发性或者未知类型的攻击面前预测准确率低，并且可视化界面设计要兼顾专业性和易用性以满足不同层次用户需求，数据表明 2023 年上半年全球因态势预测不准造成的安全损失比去年同期增加了 20%，可见这一领域急需技术创新和突破，以后的研究应着眼于提升预测模型的泛化能力以及可视化表达的精准度以便更好地服务于信息系统的安全保障工作。

3 网络安全态势感知在信息系统中的实际应用

3.1 企业级信息系统的安全态势感知实践

企业级信息系统的复杂性对企业级信息系统而言，其复杂性对企业级信息系统的复杂性让态势感知技术有了更高的要求，因为不同业务场景下安全需求差别很大且感知模型的通用性受限，并且企业内部普遍有数据孤岛从而使数据采集和整合存在挑战，不过部分领先企业开始探寻基于云原生架构的态势感知解决方案依靠统一数据平台达成跨部门、跨系统协同防御，就像某个跨国制造企业引入边缘计算技术后成功解决工业控制系统数据传输延迟问题进而提升态势感知实时性和准确性一样，这些做法显示企业级信息系统安全防护正在从传统边界防御迈向全域感知并且态势感知技术的应用给它提供了稳固的技术支持 [3]。

3.2 关键基础设施的安全态势感知应用

国家经济和社会运行的关键基础设施是命脉，其网络安全事关国家安全和社会稳定，这几年能源、医疗、交通等领域遭受网络攻击的事情频频发生，就像 2021 年美国 ColonialPipeline 公司被勒索软件攻击致使全美多地燃油供应中断那样，这些事表明关键基础设施急需网络安全态势感知技术，实践当中态势感知系统把物联网传感器、工业控制协议解析工具还有威胁情报共享平台集在一起构建起覆盖物理层、网络层和应用层的全方位安全监测体系，例如某个省级电网公司在调度中心部署态势感知平台，实时监控电力设备运行状况和网络流量，成功预警并阻断一起 APT 攻击，

避免了可能发生的大型停电事故。

3.3 态势感知技术应用中的挑战与对策

显著成效虽已取得，但发展面临的诸多挑战依旧存在，其中感知数据全面性不足是首要问题，因为企业或机构内部多种异构系统并存会使数据格式不统一、采集标准不一样等，进而可能导致感知结果有偏差，比如在部分政府机构里，老旧信息系统无法与现代化态势感知平台无缝衔接就影响了整体安全防护效果，并且实时性要求高这一因素也重要地制约着技术应用，像高频交易、智能制造等场景下，毫秒级延迟或许就会产生严重后果，这就使得态势感知系统性能要求被提得极高。

上述挑战面前，研究者和从业者积极探寻创新解决方案，因为多源异构数据融合技术能有效整合不同渠道安全信息以提升感知数据的完整性和准确性，例如有家科技公司开发出基于区块链的数据共享机制，使各方在保护隐私的同时达成数据互通，并且深度学习与知识图谱相结合给智能分析带来新途径，不但可提高威胁检测精度，还可推理预测潜在安全风险，就像某能源企业实践时，带知识图谱的态势感知系统识别出隐藏攻击链路，为企业赢得宝贵应急响应时间。

4 结论

现代信息系统安全防护以网络安全态势感知技术为核心手段，该技术正逐渐突破传统被动防御的局限性并给复杂多变网络威胁的应对带来新解法 [4]。这几年，政府、金融、能源和医疗等关键信息基础设施对网络安全需求不断提高使态势感知技术重要性越发突显。统计显示，2022 年全球网络安全市场规模超 1500 亿美元且态势感知相关技术占比大幅增长，估计未来五年其年均增长率还会保持两位数，这一趋势说明态势感知技术在理论研究方面有重要进展且实际应用价值得到广泛认同。

当前的技术体系面临着不少挑战，首先在数据采集和预处理环节，数据质量有好有坏，而且多源异构数据融合的时候，保证数据完整一致是个急需解决的难题。其次，在安全事件检测和识别方面，分析模型的精度需要提高，因为新攻击手段面前，现有模型缺乏泛化能力。还有在态势评估和预测环节，威胁预测的准确性和及时性限制着技术发展，这些都导致态势感知系统实际部署时很难完全符合高实时、高可靠性要求。

上述瓶颈被基于大数据分析、人工智能和可视化技术创新实践所突破是有可能的，就像深度学习跟知识图谱相结合能大大提高安全事件识别的效率和准确性并且可视化技术能让复杂网络态势的呈现更直观，以后的研究重点应放在多源异构数据高效融合处理方法上以探寻更智能的分析模型并用创新的态势预测方法让系统主动防御能力再上一个台阶，此外行业间加强协作、推进标准化建设也会给技术推广和应用提供很大支撑，技术不断成熟后，网络安全态势感知在保障信息系统安全方面会起更重要的作用且推动网络安全防护由被动响应向主动防御彻底转变这是可以预料到的 [5]。

参考文献：

[1] 苏忠 ; 林繁 ; 陈厚金 ; 赖建荣 ;. 网络安全态势感知系统的构建与应用 [J]. 信息网络安全 ,2014(05):79-83.

[2] 成春雨 ;. 基于信息分类的变电站网络安全态势感知系统设计 [J]. 自动化应用 ,2022(08):59-62.

[3] 罗传军 ; 崇晓峰 ; 张珊 ; 王艺 ;. 网络安全态势感知系统在天津气象信息网络中的应用 [J]. 网络安全技术与应用 ,2024(05):121-123.

[4] 王军 ; 张勇 ;. 网络安全态势感知在铁路信息安全的应用 [J]. 信息安全研究 ,2019(07):73-80.

[5] 刘冬兰 ; 刘新 ; 张昊 ; 于灏 ; 马雷 ; 赵晓红 ;. 基于大数据的网络安全态势感知及主动防御技术研究与应用 [J]. 计算机测量与控制 ,2019(10):235-239.