人工智能在计算机网络安全态势感知中的应用

左双左
上海震旦职业学院，上海 201908
DOI: 10.61369/TACS.2025010032

摘　　要： 随着互联网技术的飞速发展，网络攻击的手段也在不断地变化，传统的安全防御方式已经不能够满足社会的发展需求。基于此，本文深入探究了网络安全态势感知、基于人工智能的计算机网络安全态势感知总体结构、网络安全态势感知关键技术、基于人工智能的网络安全态势技术与应用旨在更好地提升网络安全的防护水平。

关 键 词： 人工智能；计算机；网络安全态势感知技术

Application of Artificial Intelligence in Computer Network Security Situation Awareness

Zuo Shuangzuo
Shanghai Zhendan Vocational College, Shanghai 201908

Abstract: With the rapid development of Internet technology, the means of network attacks are constantly changing, and the traditional security defense methods can no longer meet the needs of social development. Based on this, this article delves into network security situational awareness, the overall structure of artificial intelligence based computer network security situational awareness, key technologies of network security situational awareness, and the application of artificial intelligence based network security situational technology to better enhance the level of network security protection.

Keywords: artificial intelligence; computer; network security situation awareness technology

引言

党中央、国务院高度重视网络数据安全管理工作。党的二十届三中全会强调，提升数据安全治理监管能力，建立高效便利安全的数据跨境流动机制。近年来，随着信息技术和人们生产生活交汇融合，数据处理活动更加频繁，数据安全风险日益聚焦在网络数据领域，违法处理网络数据活动时有发生，给经济社会发展和国家安全带来严峻挑战。《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》对数据安全和个人信息保护制度作了基本规定。为做好法律实施，规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益，有必要制定配套行政法规[1]。只有将网络安全保护好，才能够更好地保证人民的安全。

一、计算机网络安全态势感知

（一）安全态势感知

安全态势感知是指通过多种技术手段和方法对网络、系统、应用等层面的安全信息进行全面和实时地收集，以此来对当前的安全状况进行分析和对未来的潜在风险进行预测。安全态势感知能够通过大数据分析、机器学习、深度学习等技术来对数据进行处理和分析，并找到其中的关联性，识别出潜在的安全威胁、异常行为模式或已发生的攻击事件[2]。安全态势感知不仅要求安全团队不仅需要从宏观层面把握整体的安全态势，还要能够了解各要素之间的相互关系和影响，这样才能够在面对网络攻击的时候更好地采取对应的措施。网络安全态势感知模型包括安全要素提取、态势评估以及态势预测共3级，具体如图 1 所示。

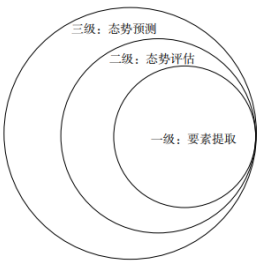

图1 网络安全态势感知模型

（二）态势感知技术

态势感知技术作为主要是全面收集并深度解析系统提供的多维度信息，并进行提前的预判。首先，态势感知技术通过集成化数据采集的方式，来收集系统硬件配置、软件版本、运行服务状态、安全日志记录以及网络传输数据等方面的信息，并建立起一个基础的数据模型[3]。其次，研究人员运用数据分析算法对这些收集到的数据进行处理，以此来更好地找到其中潜在的风险。最

后，研究人员为了更好地提升态势感知技术的精确度和实效性，可找一些 Web 服务访问日志、安全情报动态、防火墙策略变更记录等数据，这样才能够更好地形成安全视图，供需要的人进行参考 [4]。

二、基于人工智能的计算机网络安全态势感知总体结构

人工智能的网络安全态势感知系统包含涵盖信息提取、信息预处理、信息融合、态势识别、态势理解、态势预测以及态势评估等多个关键环节 [5]。一是，在信息提出阶段，系统会广泛收集蕴含着网络安全态势的各类原始数据；二是，在信息预处理阶段，系统会对收集到的原始数据进行清洗、去噪、格式转换等操作，以此来保证数据的质量；三是，在信息融合阶段，研究人员会运用人工智能技术对数据进行融合计算，找到不同数据之间的关联性，并进行分析；四是，在态势识别阶段，研究人员会通过人工智能技术对融合后的数据进行识别和异常检测，来找到网络中潜在的危险与攻击行为。五是，在态势理解阶段，系统不仅需要通过知识推理、因果分析等方法来对威胁的数据来源进行分析，还会对其进行画像。六是，态势预测阶段，是指人工智能技术对未来网络安全态势进行预测，并为其提供对应的方法。七是，态势评估阶段是指通过建立评估指标体系来综合考虑威胁的严重程度、发生的概率情况、影响的范围等因素，这样才能够基于此进行更好地进行决策 [6]。具体的网络安全态势感知总体框架，如图2所示。

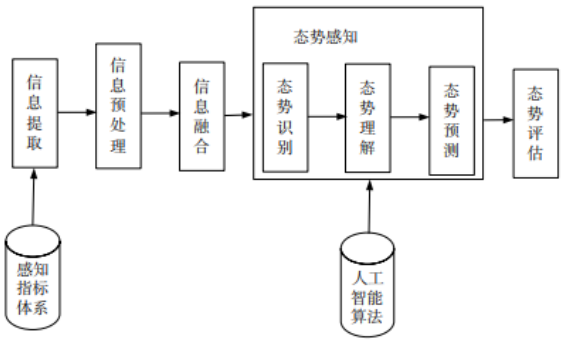

图2 网络安全态势感知总体框架

三、网络安全态势感知关键技术

网络安全态势感知关键技术是国家支撑网络空间安全的重要基础技术，其基础框架包含信息融合技术、安全风险评估及分析技术、大数据可视化技术和事件过滤技术等技术，在整个技术框架体系中相互融合、相互关联，能够从全方位构筑网络安全防护的牢固防线 [8]。其中，信息融合技术是网络安全态势感知的底层技术，通过对不同渠道、不同形态、不同来源的安全数据，如网络流量数据、系统日志数据、终端行为数据等进行整合、汇聚，突破数据孤岛问题，通过关联分析，分析潜在的安全事件，为后续的网络安全风险评估、策略决策分析提供深度数据融合支撑。信息融合技术在网络安全态势感知中有效融合信息分析技术、关联分析技术，可以从宏观视角来分析网络，发现传统手段分析视角发现不了的相关细微变化。而安全风险评估及分析是针对融合信息进行深度挖掘和分析技术，基于安全事件评估模型对网络安全威胁中的网络安全对象资产、漏洞、威胁进行分层分级分析量化，针对风险影响进行相应的防护响应决策。此环节中的信息融合与关联分析技术，不仅需要数据挖掘、数据融合算法等方面的分析技术，而且对于网络攻防技术知识有深入了解和理解 [8]。大数据可视化技术是将安全大数据直观形象地传递给安全管理人员的重要手段，安全管理人员通过图表、地图、热力图等可视化形式能快速了解网络安全整体情况，快速定位异常，做出更快、更科学的决断。大数据可视化能够有效提升安全管理效率，增强安全管理决策的直观性、科学性，使安全管理人员将更多精力放在研判全局方面，处理更为复杂和变化的网络安全风险问题 [9]。而事件过滤技术是自动过滤海量安全事件中真正有威胁、没有威胁事件的筛选过滤器，是减少误报、漏报等安全风险的重要技术手段。具体如表1人工智能在计算机网络安全态势感知中的应用对比表格所示：

表1 人工智能在计算机网络安全态势感知中的应用对比表格

对比维度	运用人工智能技术	不运用人工智能技术
威胁检测能力	1. 高效精准：通过机器学习算法，可快速识别已知和未知威胁，降低误报率和漏报率。2. 模式识别：擅长发现隐藏模式和异常行为，捕捉复杂攻	1. 依赖规则：主要基于已知特征和规则库进行检测，难以应对新型和未知威胁。2. 误报率高：易产生大量误报，增加安全人员负担。
响应速度	1. 自动化响应：结合SOAR（安全编排、自动化与响应）技术，实现威胁的快速隔离和处置。2. 实时性：能够实时分析并响应威胁，减少攻击影响时间。	1. 人工干预：依赖安全人员手动分析和响应，速度较慢。2. 延迟性：响应时间较长，可能错过最佳处置时机。
数据处理能力	1. 处理海量数据：能够高效处理PB级安全数据，挖掘数据中的潜在威胁。2. 关联分析：通过数据关联分析，发现跨系统、跨网络的复杂攻击。	1. 处理能力有限：难以应对大规模安全数据，易出现性能瓶颈。2. 孤立分析：数据分散处理，难以形成全局威胁视图。
预测能力	1. 威胁预测：通过分析历史数据和当前趋势，预测未来可能的攻击方向和手段。2. 主动防御：提前采取防御措施，降低被攻击风险。	1. 被动防御：主要针对已发生的攻击进行响应，缺乏预测能力。2. 反应滞后：难以在攻击发生前采取有效措施。
适应性和可扩展性	1. 自适应学习：能够根据新出现的威胁自动调整模型，提升检测能力。2. 可扩展性强：支持快速集成新的安全工具和数据源，适应不断变化的安全环境。	1. 规则更新滞后：依赖人工更新规则库，难以快速适应新型威胁。2. 扩展性差：系统架构固定，难以灵活集成新工具和数据源。

通过构建合理的过滤规则和算法模型实现自动检测与过滤分析，有效过滤海量的噪声数据，聚焦需要关注的安全问题，精准定位真正需要处理的安全问题，并能够快速响应有效处理，使安全响应的响应速度和可靠性显著提高。总之，网络安全态势感知关键技术可以借助由信息安全融合技术、安全风险等级及分析技术、大数据可视化技术和事件过滤技术等组成的态势感知关键技术体系，融合安全威胁与风险因素，综合事件本身和漏洞等多种信息，对海量的监测数据进行数据过滤、风险分析、汇聚总结，多维度量化描述网络安全态势，实现对网络安全态势的全面、准确感知，不断提高威胁事件处置的速度和准确性 [10]。具体人工智能在计算机网络安全态势感知中的应用对比图如图3所示：

图3 人工智能在计算机网络安全态势感知中的应用对比图

四、基于人工智能的网络安全态势技术与应用

（一）人工智能计算机网络安全态势技术

1. 计算机表征态势指标体系

计算机表征态势指标体系是网络安全态势技术中的又一关键架构，包含行为特征智能表征技术。该技术为了精准地构建计算机行为态势模型，运用人工智能算法，对大量已知安全行为与异常行为样本进行解析，利用模式识别技术挖掘两类行为之间的差异化特征；使用深度学习模型并在获取行为特征识别模型后，利用该模型来分析判别未知行为和计算行为异常的概率，在可接受的误判率下尽可能地识别并标记异常行为。行为特征与相关深度学习算法是人工智能算法模块中的一个重要组成部分，可以分析海量行为数据，结合行为模式训练模型，利用算法模块分析提取相关类行为模式，并将根据特定模式分类将提取到的类行为模式存放在对应的特征矩阵中[11]。这一系列流程共同构建了计算机表征态势指标体系，为网络安全态势的全面感知与精准评估提供了有力支撑。

2. 检测分析与处理技术

随着信息技术的不断演进，网络攻击手段愈发多样且复杂程度日益加剧，涵盖多种高级持续性威胁（APT）与零日漏洞利用攻击，并且当下的攻击行为展现出更强的隐蔽性和多变性，仅在分析攻击行为特征层面依赖过去的固定规则或单一模式匹配方法很难高效识别出攻击行为，因此需要革新与提升传统检测分析与处理技术。目前，可运用行为序列关联分析以及上下文语义理解等定位方法来追踪多维度攻击路径[12]。这种将动态分析与静态分析相互融合的方式对系统性能的损耗微乎其微，同时可显著增强攻击行为特征识别能力和威胁处置的精准度，从而切实保障计算机系统安全。

3. 光谱反病毒查杀技术

计算机光谱反病毒查杀技术包含多种主流技术，比如基于动态行为分析体系的技术、光谱特征提取与匹配技术、光谱多维查杀技术等等。其中，基于动态行为分析体系的技术就是病毒查杀的根本基础，包含基于基础行为特征指标以及攻击性和异常性指标种类等。基本的行为特征指标属于程序最为根本的运行状态，程序执行路径和资源占用是基础行为特征指标中一部分，这些特征指标并不会直接表现出病毒特征，而是会以一种间接的状态影响查杀病毒的效果，例如程序异常的占用资源可能是病毒程序的隐匿化，而攻击性的特征则是指程序的潜在攻击性和恶意性，主要包括关键性特征 API 调用以及内存占用方式、网络的通讯行为方式等多种。光谱多维查杀技术则是以融合光谱的各类检测维度为依托提高病毒查杀的完整性与精准度，切实为计算机信息系统构建完善的防护体系[13]。

（二）人工智能计算机网络安全态势技术应用

1. 加强网络安全态势技术应用

安全态势技术将安全监测在识别阶段、响应阶段和防御阶段的具体运用，完成对日志或者用户行为数据处理后，能够进一步分析数据特点，主动发现系统中存在的威胁性因素；智能分析引擎在实践工作中有突出效果。构建人工智能异常行为检测技术，能够对庞大的正常、异常行为数据进行处理，并从中提取出行为中不同的特征，通过建立深度学习来增强检测的准确性和高效性；还能够借助人工智能威胁防御技术识别威胁并处置威胁，有效提高威胁防御等级，控制威胁带来的破坏范围[14]。

2. 检测与处理技术

为了全面提升企业网络安全威胁检测和处理能力，还需要加强人工智能检测处理技术的使用。威胁检测和处理技术在应用的过程中，数据采集来源包括系统日志信息、网络流量信息和终端行为数据信息。需要注意的是，数据采集步骤要根据企业的业务以及企业规模来实现，考虑不同因素综合地选择要进行采集的数据信息，从而从整体方面来提高数据采集的效果。在数据采集之后，检测处理技术会将采集到的这些信息进行统一的收集和记录，利用人工智能技术或深度学习算法进行深度关联性分析，从而实时掌握企业的网络存在的安全隐患，并利用报警通报系统，将这些报警信息发送至安防系统人员当中[15]。

五、结束语

人工智能技术在计算机网络安全态势感知中的应用不仅是网络安全领域的一次变革，也是教师教学方向的一次重大转变。研究人员通过引入人工智能技术将传统的被动相应转变为主动预测和智能防御的方式，这样才能够更好地提高安全防护的准确性。

参考文献

[1] 王志龙 . 新形势下计算机网络信息安全保密技术及安全管理研究 [J]. 电脑爱好者（电子刊），2021(12):335-336.
[2] 郝晓康 . 云计算技术在计算机网络安全存储中的应用 [J]. 中国新通信 ,2023,25(22):104-106.
[3] 栗堃 . 基于优化支持向量机的网络安全态势评估模型 [J]. 网络安全和信息化 ,2023,(12):54-56.
[4][1] 胡俊欢，梁灵玲 . 新时代大学生网络意识形态教育现实困境与策略研究 [J]. 襄阳职业技术学院学报 ,2024,23(01):29-32+58.
[5] 林婧 . 数据加密技术在计算机网络通信安全中的应用探究 [J]. 数字通信世界 ,2024(4):125-127.
[6] 王立军 . 数据加密技术在计算机网络信息安全中的应用研究 [J]. 中国宽带 ,2024,20(8):22-24.
[7] 李晗 . 信息化背景下计算机网络信息安全防护策略分析 [J]. 电脑爱好者（普及版）,2023(3):166-168.
[8] 吕之谓 . 计算机网络安全管理中人工智能系统的应用 [J]. 电大理工 ,2019(1):12-15,23.
[9] 王利 . 计算机网络安全中防火墙技术应用实践探究 [J]. 中国宽带 ,2024,20(6):46-48.
[10] 叶艺林 . 基于虚拟化技术的计算机网络安全防护方法研究 [J]. 信息与电脑（理论版）,2024,36(03):192-194.
[11] 白洁，毛爱茹，申晓康 . 增强现实技术在中职信息技术教学中的应用分析 [J]. 信息与电脑（理论版）,2024,36(19):242-244.
[12] 钟雯 . 利用数据处理技术开展计算机网络安全存储系统设计 [J]. 网络安全和信息化 ,2024,(12):113-115.
[13] 程子栋 . 基于区块链的政务信息系统数据安全共享交换研究 [J]. 软件 ,2024,45(06):86-88.
[14] 张亚培 . 区块链技术赋能开放大学数字学习资源共建共享研究 [J]. 前卫 .2024,(24).0040-0042.
[15] 肖漫漫，刘骥琛，李艳丽，等 . 软件定义广域网中基于 IPv6 分段路由的双栈流量调度算法 [J]. 重庆大学学报 .2022,45(9).

