# 智能化技术在网络安全运维中的运用研究

潘乔立
航宇救生装备有限公司　湖北　襄阳　441003

**摘　要：**本文聚焦智能化技术在网络安全运维中的运用，阐述了网络安全运维概念、现状及智能化技术内涵，指出当前运维面临威胁复杂、数据过载、体系不完善等挑战，而智能化技术能模拟人类智能思维。并说明其优势，如提高运维效率、增强检测准确性。同时详细介绍了在智能威胁检测与预警、自动化安全检测与响应、智能安全策略优化等方面的具体应用。因此，分析技术、管理与人才层 面的挑战，并提出针对性应对策略，为智能化技术在网络安全运维中的应用提供参考。

**关键词：**智能化技术；网络安全运维；运用研究

## 引言

随着人工智能等新一代信息技术的全面渗透，网络架构日趋复杂、终端接入数量呈指数级增长，网络攻击手段也呈现出智能化、隐蔽化、规模化的新特征—— 传统脚本式攻击逐渐被AI驱动的定向渗透、自动化漏洞挖掘、恶意代码变种生成等新型攻击取代，攻击频率、破坏范围与防御难度大幅提升，传统“被动响应、事后补救”的网络安全运维模式已难以应对当前的安全挑战，运维工作面临着“人力不足、效率低下、预警滞后”的三重困境。

## 1 网络安全运维与智能化技术概述

### 1.1 网络安全运维的基本概念

网络安全运维是指为保障网络系统的稳定运行、数据安全以及业务连续性，对网络基础设施、软硬件系统、数据资源等进行全面监控、管理、维护和安全防护的一系列工作。其核心目标是及时发现并处置网络安全漏洞、威胁事件，防范非法入侵、数据泄露、系统瘫痪等安全风险，确保网络环境始终处于安全可控的状态。网络安全运维涵盖了多个环节，包括日常的网络设备巡检、系统补丁更新、日志分析，以及应急状态下的安全事件响应、故障排查与恢复等，需要结合技术手段与管理流程，形成全方位的安全防护机制，为企业、机构乃至国家的数字化发展提供安全保障。

### 1.2 网络安全运维的现状分析

当前，网络安全运维在数字化浪潮的推动下取得一定进展，但同时也面临着诸多严峻挑战，整体呈现出机遇与困境并存的现状。从积极方面来看，随着网络安全意识的提升，越来越多的企业和机构开始重视网络安全运维工作，加大了在安全设备采购、技术研发以及人员培训等方面的投入，运维工具也逐渐从传统的手动操作向半自动化方向发展，一定程度上提高了运维效率。然而，从面临的问题来看，首先，网络威胁的复杂性不断升级，新型恶意代码、高级持续性威胁（APT）等攻击手段层出不穷，攻击方式更加隐蔽，传统运维技术难以快速识别和应对；其次，网络规模的持续扩大导致运维数据量呈爆炸式增长，运维人员面临着“数据过载”的困境，依靠人工分析难以从海量数据中精准提取有价值的安全信息，容易出现漏判、误判情况；最后，部分企业和机构的网络安全运维体系不够完善，缺乏统一的管理标准和协同机制，各运维环节之间存在信息孤岛，导致安全事件响应不及时，进一步加剧了网络安全风险[1]。

### 1.3 智能化技术的内涵

智能化技术是基于计算机科学、人工智能、大数据、机器学习、深度学习等多学科理论与技术融合发展而来的新型技术体系，其核心内涵是模拟人类的智能思维方式，实现对复杂信息的自主感知、学习、分析、推理、决策和执行，具备高度的自主性、适应性和智能化水平。智能化技术能够通过对海量数据的收集、清洗、存储和分析，挖掘数据背后隐藏的规律和关联信息，进而根据实际需求做出精准判断和智能决策。在技术构成上，机器学习是智能化技术的核心支撑，通过构建算法模型让计算机从数据中自动学习，不断优化模型性能，提高处理问题的能力；深度学习则是机器学习的重要分支，借助深度神经网络模拟人类大脑的神经元结构，能够处理更复杂的非线性问题，在图像识别、语音识别、自然语言处理等领域展现出优异性能；大数据技术为智能化技术提供了数据基础，确保能够高效处理和管理海量异构数据；此外，人工智能技术中的专家系统、模糊逻辑等也为智能化技术的应用提供了丰富的技术手段。整体而言，智能化技术的本质是通过技术创新打破传统

人工操作的局限，实现复杂任务的自动化、智能化处理，为各个行业的转型升级提供强大动力。

## 2 智能化技术为网络安全运维带来的优势

### 2.1 提高效率

智能化技术能够显著提高网络安全运维的效率，从根本上改变传统运维模式中依赖人工操作导致的效率低下问题。在日常运维工作中，传统模式下需要运维人员手动完成设备巡检、漏洞扫描、日志分析等重复性工作，不仅耗费大量时间和精力，还容易因人为操作失误影响工作质量。而智能化技术通过引入自动化运维工具和智能算法，能够实现这些重复性工作的全自动化处理。例如，智能巡检系统可以按照预设规则定期对网络设备、服务器等进行全面检查，自动收集设备运行参数、性能指标等数据，并生成详细的巡检报告，无需人工干预；在漏洞扫描方面，智能漏洞扫描工具能够利用机器学习算法实时更新漏洞库，快速扫描网络中的潜在漏洞，并自动对漏洞等级进行分类，大大缩短了漏洞发现和排查的时间。此外，在安全事件响应环节，智能化技术能够实现对安全事件的实时监测和自动响应，当发现异常流量、非法入侵等安全事件时，智能响应系统可以立即启动预设的处置流程，如阻断异常连接、隔离受感染设备等，无需等待运维人员手动操作，显著缩短安全事件的处置时间，有效减少安全事件对网络系统造成的损失，极大提升了网络安全运维的整体效率。

### 2.2 增强检测准确性

在网络安全运维中，威胁检测的准确性直接关系到网络安全防护的效果，而智能化技术通过先进的算法模型和数据处理能力，能够大幅增强检测准确性，有效降低漏判、误判率。传统的威胁检测技术主要基于预设的规则库，通过比对网络行为与规则库中的异常特征来判断是否存在安全威胁，但这种方式存在明显局限性，无法识别规则库之外的新型威胁，且容易将正常网络行为误判为异常，导致检测准确性较低。智能化技术则通过机器学习和深度学习算法，能够对海量的网络运维数据进行深度分析和自主学习，不断构建和优化威胁检测模型。在学习过程中，算法能够自动识别网络正常行为的特征模式，并对新型威胁的特征进行快速学习和更新，从而实现对已知威胁和未知威胁的精准检测[2]。例如，在检测高级持续性威胁（APT）时，智能检测系统能够通过分析长期的网络流量数据、用户行为数据等，发现APT攻击中隐蔽的、渐进式的异常行为，而传统检测技术往往难以察觉这类威胁。同时，智能化技术还能够通过多维度数据融合分析，减少单一数据来源导致的判断偏差，进一步提高检测结果的可靠性，为网络安全运维提供更精准的决策依据。

## 3 智能化技术在网络安全运维中的具体应用

### 3.1 智能威胁检测与预警

在网络安全运维中，智能威胁检测与预警是智能化技术的重要应用场景，能够实现对网络安全威胁的实时感知、精准识别和提前预警，为运维人员及时处置威胁争取宝贵时间。该应用基于大数据技术和机器学习算法，首先通过分布在网络各个节点的传感器、日志收集工具等，实时采集网络流量数据、设备运行日志、用户行为数据、应用程序日志等多维度数据，并对这些数据进行清洗、整合和存储，形成统一的运维数据池。随后，机器学习算法对数据池中的数据进行深度分析和自主学习，构建网络正常行为模型和各类威胁行为特征模型。在实际检测过程中，系统会实时将当前网络行为数据与正常行为模型、威胁特征模型进行比对分析，一旦发现偏离正常行为模型且符合威胁特征模型的异常行为，如异常流量峰值、非法端口访问、可疑文件传输等，系统会立即触发警报，并通过可视化界面向运维人员展示威胁的类型、发生位置、影响范围以及可能的危害程度。同时，智能预警系统还能够基于历史威胁数据和当前网络环境，利用预测算法对潜在的安全威胁进行预判，提前向运维人员发出预警信息，例如预测某类恶意代码可能在近期针对特定系统发起攻击，提醒运维人员提前采取防护措施，如更新系统补丁、加强访问控制等，从而有效防范安全威胁的发生，降低网络安全风险。

### 3.2 自动化安全检测与响应

自动化安全检测与响应作为智能化技术在网络安全运维中的关键应用，可达成安全威胁检测与处置的全流程自动化，降低人工干预程度，提升安全事件处置效率与精准度。在自动化安全检测阶段，系统依靠智能化技术里的实时监测算法与智能分析模型，对网络系统展开24小时持续监测。它既能察觉传统的网络攻击，像DDoS攻击、SQL注入、跨站脚本攻击等，也能识别新型且隐蔽的安全威胁。例如，借助深度学习算法深度剖析网络数据包，可揪出藏于正常数据包中的恶意代码片段；通过分析用户访问行为的关联性，能发现非法越权访问行为；一旦检测到安全威胁，系统会自动触发预设响应流程，依据威胁类型和严重程度采取对应处置举措。对于单个IP地址的异常访问这类轻微威胁，系统会自动将其加入黑名单，阻断后续访问；对于服务器感染普通恶意软件的中度威胁，会自动隔离服务器，防止恶意软件扩散，并启动杀毒程序查杀；对于大规模DDoS攻击这类严

重威胁，会自动调用流量清洗设备过滤攻击流量，同时通知运维人员人工干预[3]。此外，自动化安全响应系统还会记录并分析处置过程与结果，形成完整安全事件处置日志，为后续安全审计和运维优化提供数据支撑。

3.3 智能安全策略优化

智能安全策略优化可助力网络安全运维人员，依据网络环境变化与安全需求升级，自动调整优化安全策略，保证其有效性与适应性，防止因策略滞后出现防护漏洞。传统安全策略制定和调整多依赖运维人员经验与手动操作，存在更新不及时、针对性差等问题，难以适应动态网络环境。而智能化技术能通过对网络运行、安全事件、威胁情报等数据的综合分析，为策略优化提供科学依据；具体而言，智能系统会定期收集网络各类数据，涵盖网络拓扑变化、新接入设备信息、用户访问需求调整、近期安全事件及处置结果、外部新型威胁防护要求等。接着，利用机器学习算法深度挖掘数据，识别当前安全策略的不足，如某些规则过严阻碍正常业务，或过松无法防范新型威胁；随后，系统根据分析结果自动生成优化方案，提交运维人员审核。审核通过后，可自动将优化策略部署到防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等网络安全设备中。例如，当系统察觉某业务部门新增大量远程办公人员，原有访问控制策略无法满足远程安全接入需求时，会自动优化VPN接入认证规则，增加多因素认证机制，并调整访问权限范围，保障远程办公安全。另外，智能安全策略优化系统还能持续监测和评估优化后的策略效果，依据评估结果进一步调整策略，形成“分析-优化-部署-评估-再优化”的闭环管理，确保安全策略始终契合网络安全需求。

## 4 智能化技术在网络安全运维中面临的挑战与应对策略

4.1 技术层面的挑战

技术层面，智能化技术在网络安全运维应用面临诸多挑战。其一，对数据质量和数量要求高，但实际网络环境中，设备型号、系统版本不一，运维数据格式不统一、标准不一致，存在大量异构数据，数据清洗整合难度大；且部分敏感数据因安全保密无法用于模型训练，导致数据量不足，影响模型性能。其二，智能化技术自身存在安全漏洞，易遭攻击，如数据投毒、模型规避等。其三，不同智能化技术兼容性差，市场上的智能运维工具基于不同架构和模型开发，缺乏统一接口和数据交互标准，难以协同工作，形成“技术孤岛”，制约整体优势发挥。

4.2 管理与人才层面的挑战

管理与人才层面挑战严峻。管理上，企业和机构管理体系不完善，沿用传统运维模式，智能化工具与现有流程难融合；数据管理机制不健全，对数据全生命周期监管缺失，易引发数据泄露；缺乏有效绩效考核机制，无法衡量智能化运维效果，难以调动人员积极性[4]。人才方面，智能化网络安全运维需复合型人才，但目前此类人才匮乏。传统运维人员缺乏智能化技术能力，人工智能等领域人才对网络安全业务了解不足，且企业和机构人才培养体系不完善，运维人员知识更新慢，加剧了人才短缺。

4.3 应对策略与建议

技术层面，要加强数据治理，建立统一标准和规范，开发数据清洗整合工具，保障数据安全前提下挖掘敏感数据价值；强化算法模型安全，投入研发防护技术，定期评估检测；推动技术标准化建设，制定接口、数据交互等标准。管理层面，企业和机构要重构管理流程制度，明确职责分工，建立快速审批通道；完善数据安全管理机制，加强全生命周期监管；建立科学绩效考核机制，纳入智能化运维指标。人才层面，高校调整课程设置，培养复合型人才；企业和机构加强现有人员培训，引进高端人才，建立激励机制；加强行业内人才交流合作，提升整体运维水平。

## 结束语

智能化技术为网络安全运维带来了新的发展契机，其在提高运维效率、增强检测准确性等方面展现出显著优势，能有效应对当前网络安全运维面临的诸多挑战。然而，技术、管理与人才层面的难题仍制约着其进一步发展。通过加强数据治理、推动技术标准化、完善管理体系以及加强人才培养等策略，可逐步突破这些瓶颈。未来，随着智能化技术的不断进步，其在网络安全运维领域的应用将更加广泛和深入，为保障网络空间安全提供更有力的支撑。

## 参考文献

[1]吴柏润.计算机网络安全技术在电子商务中的应用[J].电子技术，2023，52(10)：268-269.

[2]要丽娟,石峰.入侵检测技术在网络安全中的应用[J].电子技术，2023，52(10):346-347.

[3]周仁刚.计算机信息管理技术在网络安全维护中的作用[J].网络安全技术与应用,2021(12):170-171.

[4]杨鸿章,王波.探讨计算机信息管理技术在网络安全中的应用[J].网络安全技术与应用,2021(11):167-169.