# 基于数智赋能信息安全态势感知技术研究

李星龙[1]　王艺茗[2]
1 吉林省财税信息中心　吉林省长春市　130021
2 吉林市第一中学　吉林省吉林市　132012

**摘　要：**随着云计算、人工智能、大数据、区块链的飞速发展，加之黑客攻击、勒索软件、数据泄露等网络安全事件频发，网络攻击手段不断演变升级，网络安全形势日益严峻。由于传统网络安全防护设备之间存在关联较少，造成了“信息孤岛”效应，并且数据信息来源比较单一，仅仅聚焦于网络安全事件相关的告警日志，防御效果达不到理想状态，基于被动防御方式已经难以应对日益复杂且不断变化的网络安全威胁，做出的应急响应大多也是在事件发生后“亡羊补牢”。因此，基于数智赋能的信息安全态势感知技术应运而生，通过大数据、人工智能以及区块链等技术实现对网络安全活动的监测预警、分析研判和应急处置，能够改变传统防御体系被动应对的不利局面，全面提升网络安全综合防护能力。本文综述了基于数智赋能的信息安全态势感知技术的相关文献，分析了该领域的研究进展、关键技术及应用前景，旨在为信息安全领域的研究人员提供参考。

**关键词：**数智赋能；态势感知；大数据；人工智能；区块链

## 引言

近年来，网络安全技术覆盖到的区域广度与深度持续加强，各个行业纷纷部署网络基础设施，网络规模不断扩大，拓扑结构日益复杂，网络安全管理的难度和复杂程度也不断加大。很多颠覆性的新技术也引入了新的网络安全问题，这也给不法分子提供利用网络工具攻击的机会，防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）等常规防护系统，主要依赖静态检测，难以应对高级持续性威胁（APT）、0day 攻击等新型网络威胁。因此，需要有能够精准预测和有效评估网络安全事件的技术，并且能够及时识别并应对威胁的技术，在此背景下基于数智赋能的信息安全态势感知技术成为研究热点，该技术能够全面、实时地感知网络态势，预测潜在威胁，提高网络安全的防御能力。

### 1. 网络安全态势感知的定义与发展

态势感知最早兴起于上世纪 80 年代的航空领域，美国空军对空战环境信息分析的过程中，希望有种技术能够快速判断当前以及预测未来发展形式，因此态势感知的概念应运而生。1999 年，Bass 首次提出网络安全态势感知的概念，并认为未来网络管理的发展方向将会是基于融合的网络态势感知。它包括三个层次：网络态势要素提取、网络态势理解和网络态势预测。通过采集网络中的各种数据，提取态势要素，进行分析评估，预测未来趋势，实现对网络安全的全面感知。网络态势是网络状态和网络趋势的表达，它能够反映出在此网络下设备的运行状态等多方面情况。决策者可以通过该技术实现掌握目前网络情况并根据情况对网络安全实时进行保障。

### 2. 数智赋能安全态势感知与塑造

所谓数智赋能安全态势感知与塑造是顺应人类社会活动的发展以及技术革新下的产物，它集数智赋能概念、安全态势感知与塑造于一体并加以创新。伴随着工业革命人类走向信息化时代，数智赋能技术引领新时代的发展，利用大数据和人工智能的手段可以实现流程再造、模式革新、体系重构和价值共创。数智赋能包括数据智能、数智化、数智技术以及数字智商四个方面，主要内容包括利用数据挖掘技术提取一特定应用场景用于服务或处理有价值的信息；利用数智技术推动新型生产力的发展进而实现社会的可持续高质量发展；数智技术顾名思义就是将数据和智能技术结合起来形成一些有实际应用效果的智能算法；随着数字化发展的进程，数字智商需要该技术有元认知与社会情感能力。从技术的不断发展和更替，数智赋能逐渐演变为具有数字智商的人运用数智技术为某对象赋能的过程。综上分析，数智赋能是安全态势感知与塑造的支撑与手段，而安全态势感知与塑造

则是数智赋能的赋能对象和应用场域。数智赋能信息安全态势感知技术和塑造系统可以为情报安全保驾护航，二者的融合可以做到全方位的信息处理、情报分析和生成决策。该技术的核心概念主要体现在以上三个步骤的实现和传递，直到生成安全态势情报并加以塑造。现阶段是“物理—社会—信息”三元空间 ( 以下简称“三元空间”) 交互时代，从情报主导的安全工作面向的三元空间交互安全场景看，数智赋能安全态势感知与塑造要实现跨空间、全周期、多维度、更可靠的智能化、精准化，应包括三大基本流程，即三元空间安全信息感知 ( 信息层 )、基于安全信息的安全态势感知 ( 情报层 ) 和基于安全情报的安全态势塑造 ( 应用层 )。其中信息层打破物理、社会、信息空间的壁垒，实现全域数据的动态采集与深度融合；情报层可以将原始数据转化为可行动的威胁情报，实现风险量化与威胁的可视化；应用层可以通过动态防御、资源调配与协同响应，将情报转化为主动干预能力。总之，数智赋能安全态势感知与塑造的三层架构，本质是通过数据贯通三元空间→情报驱动认知升级→智能重构防御范式，推动安全体系从“事后补救”转向“事前免疫”。其终极目标不仅是防御威胁，更是通过持续的学习与进化，构建适应复杂环境的“安全生态系统”，为数字时代的全局性风险治理提供技术。

## 3. 数智赋能信息安全态势感知技术的应用

### 3.1 大数据技术在态势感知中的应用

大数据技术在态势感知中的应用首先体现在数据收集与处理方面。通过利用大数据技术，可以实现对海量、异构数据的实时收集和处理，为态势感知提供丰富的数据源。例如，可以利用分布式存储和计算框架（如 Hadoop 等）对大规模数据集进行高效存储和处理；同时，数据挖掘和机器学习算法在数据的预处理和特征提取方面也有着较高的准确性和效率，可以应用在态势感知方面。在数据收集与处理的基础上，大数据技术在态势分析与预测方面发挥着重要作用。通过利用数据挖掘、神经网络模型等技术手段实现对未来态势的预测和预警。例如，可以利用时间序列分析、关联规则挖掘等方法发现数据之间的关联性和趋势性；同时，也可以利用神经网络、支持向量机等模型对未来态势进行预测和分类。大数据技术在态势感知中的另一个重要应用是智能决策支持。通过将大数据技术与人工智能技术融合，为复杂态势的智能化分析和决策提供支持。如应用在城市应急管理中，某特大城市对 12345 热线、地铁闸机数据、气象预警信息等信息进行整合并构建城市风险指数模型，最终在 2022 年的暴雨预警准确率提升至 92%，应急响应时间缩短 40%；同样的大数据态势感知也可应用于金融风控系统，某银行运用图神经网络分析 10 亿级交易关系网，实现洗钱行为识别准确率从 68% 提升至 89%，日均处理可疑交易预警量达 20 万笔。当前面临多模态数据对齐、小样本场景建模、模型可解释性等挑战。未来将向 " 云边端 " 协同计算、因果推理与深度学习融合、量子计算加速等方向发展。Gartner 预测到 2025 年，70% 的态势感知系统将内置自适应 AI 引擎，实现从被动响应到主动干预的范式转变。

### 3.2 人工智能技术在态势感知中的应用

人工智能技术在态势感知中主要用于智能数据处理与分析。通过利用支持向量机、神经网络模型等智能优化算法，实现对数据的筛选和预处理，提取出关键信息，为态势感知提供技术支持。此外，深度学习算法在图像、语音识别等领域的潜力也是巨大的，为态势感知提供了更加智能化的手段。在态势感知中，智能预测与预警是至关重要的环节。人工智能技术可以通过对历史数据的分析和建模，预测未来的发展趋势和潜在风险。例如，利用时间序列分析、关联规则挖掘等方法，可以发现数据之间的关联性和趋势性，从而实现对未来态势的预测和预警。得到的预测和预警结果可以辅助决策者做出更加明智的决策。人工智能技术在态势感知中的另一个重要应用是智能决策支持。通过将人工智能技术与决策支持系统相结合，可以实现对复杂态势的智能化分析和决策支持。例如，利用自然语言处理技术对文本数据进行理解和分析；同时，也可以利用强化学习等方法对决策过程进行优化和迭代。比如在太空态势感知应用中，SpaceX 星链系统集成自适应光学神经网络，实现对厘米级太空碎片的实时追踪，轨道预测精度达 0.001 角秒；在工业安全监测终 BP 集团炼油厂部署多智能体强化学习系统，2024 年将设备故障预判时间从 72 小时提升至 360 小时，年避免损失超 2 亿美元目前人工智能技术发展在不断地取得突破。当前面临小样本持续学习、跨模态语义鸿沟、因果可解释性等挑战。MIT 最新研究显示，神经符号系统（NeSy）可将模型决策透明度提升 60%。Gartner 预测到 2027 年，40% 的态势感知系统将嵌入量子机器学习模块，处理速度实现指数级提升。同时，生成式 AI 正在催生虚拟态势沙盘技术，通过 Diffusion

模型生成百万级威胁场景进行压力测试。欧盟已出台《可信 AI 态势系统认证标准》。技术融合趋势下，生物启发式计算（类脑芯片、DNA 存储）将突破传统架构限制。IDC 分析表明，到 2030 年全球 AI 态势感知市场规模将达 3800 亿美元，其中军事国防、城市治理、气候变化三大领域占据 72% 份额，标志着智能感知技术正式进入社会核心决策层。目前人工智能技术发展在不断地取得突破，在不久的将来相信人工智能技术能够在态势感知领域中有着更重要的地位，同时也要发挥学科交叉带来的创新作用以推动人工智能技术与态势感知的深度融合和发展。

3.3 云计算在态势感知中的应用

云计算技术是将态势感知系统云平台化，配合云计算场景远程高效的应对复杂的网络环境和潜在威胁，同时省去了硬件设备所占用庞大的场地和昂贵的费用。最重要的是，海量的日志分析和处理对运算和存储性能有很高的要求，云计算最大的特点就是可弹性扩容和性能按需分配，所以态势感知云化平台可以有效保障其感知能力可以随着对象规模的变化而变化。将交换机、防火墙、IDS、IPS、WAF 等网络安全设备资源组成安全资源池，在一定程度上实现“安全云计算”。在发现存在安全风险隐患时，可以第一时间通过安全资源池下发策略进行阻断隔离，而在同一个网络区域间的东西向流量，可使用虚拟交换机或防火墙 ACL 或 UCL 进行阻断。这使得资源的利用率达到了极大的提升，在新环境下高效的为网络安全保驾护航。

3.4 区块链在态势感知中的应用

区块链技术在态势感知中有多方面的应用。一是提高数据安全性。区块链的分布式账本和加密技术，能确保态势感知数据的完整性和不可篡改性。在态势感知中，数据来源广泛且复杂，包括各种网络设备、传感器、安全设备、日志等。区块链可以将这些数据以加密的方式存储在多个节点上，防止数据被恶意篡改或删除，为准确的态势分析提供可靠的数据基础。二是整合多源数据：区块链可以有效整合来自不同来源、不同格式的态势感知数据。在复杂的网络环境中，数据分散在多个系统和设备中，通过区块链技术将这些数据统一整合到一个区块链平台上，实现数据的互联互通和共享，构建更全面、动态的安全态势感知模型，为多维度分析和趋势预测提供有力支持。

**4 结论**

基于数智赋能的信息安全态势感知技术是当前信息安全的前沿研究领域也是当前研究的热点话题。通过大数据、人工智能及区块链等技术的应用，全面实现对网络活动的全面感知、理解和预测，提高网络安全的防御能力。未来，随着数字技术的不断发展，基于数智赋能的信息安全态势感知技术将在 AI 大模型安全、数据要素安全、网络安全保险等方面展现出广阔的应用前景。企业需要密切关注这些趋势的发展变化，加强自身的数字安全建设和管理，确保业务的安全性和稳定性。

**参考文献：**

[1] 黄福全，王廷凰，刘子俊，缪秋滚 . 舰船通信系统 5G 网络多维度安全状态感知技术 [J]. 舰船科学技术 ,2023,45(22):186–189.

[2] 张杨 . 塑造国家安全态势研究 : 基于模型的阐释 [J]. 云南行政学院学报 ,2023,25(5):72–82.

[3] 陆伟 . 基于数智技术的创新辅助框架探析 [J]. 情报学报 ,2023,42(9):1009–1017.

**作者简介：**

李星龙（1982–7），男，满族，高级工程师，研究方向：计算机应用。