网络安全视角下数据要素安全治理研究

唐　珂，宋　崴，张文瑾，柳碧岚，史晓莉
（中国人民解放军 96941 部队，北京　100085）

摘　要：“数据要素”是驱动数字经济发展的核心资源，其本质是通过数据资源的整合、加工和流通，释放数据价值，赋能业务决策、社会治理和经济增长。在网络安全领域，数据要素不仅仅是“原始数据”，而是通过采集、整合、加工、流通、应用等过程，能直接发挥其网络安全价值的数据资源形态，例如网络威胁告警和威胁情报等。随着信息技术的快速发展，网络安全工作所产生海量的数据要素成为网络安全治理的核心要素之一。这些安全数据的收集、存储、传输与处理在协助提供网络安全决策支持的同时，也带来了巨大的安全隐患。从数据要素的安全角度出发，分析网络安全数据汇聚过程中面临的主要安全威胁，提出相关的保护措施和技术方案，旨在为网络安全治理提供实践指导。

关键词：数据要素；网络安全大模型；大数据；网络检测
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 10. 009
引用格式：唐珂，宋崴，张文瑾，等. 网络安全视角下数据要素安全治理研究［J］. 网络安全与数据治理，2025，44（10）：54 - 58.

Research on data element security governance from a cybersecurity perspective

Tang Ke，Song Wei，Zhang Wenjin，Liu Bilan，Shi Xiaoli
（Unit 96941 of the Chinese People's Liberation Army，Beijing 100085，China）

Abstract：Data elements are the core resources driving the development of the digital economy. Their essence lies in the integration，processing，and circulation of data resources to unlock data value and empower business decision-making，social governance，and economic growth. In the field of cybersecurity，data elements are not merely "raw data"，but take the form of data resources that can directly deliver cybersecurity value through processes such as collection，integration，processing，circulation，and application—for example，network threat alerts and threat intelligence. With the rapid development of information technology，the massive data generated in cybersecurity operations has become a key component of cybersecurity governance. While the collection，storage，transmission，and processing of these security data support cybersecurity decision-making，they also introduce significant security risks. This paper examines the security of data elements from a cybersecurity perspective，analyzes the major security threats encountered during the aggregation of cybersecurity data，and proposes corresponding protection measures and technical solutions，aiming to provide practical guidance for cybersecurity governance.

Key words：data elements；cybersecurity large model；big data；network detection

0　引言

当前，网络安全治理正面临数据规模与处理效能的双重挑战。互联网、物联网及云计算技术的普及催生了海量异构安全数据，如网络流量、系统日志、攻击行为等结构化与非结构化信息。这些数据的采集、存储与分析因实时性要求高、复杂度大而面临瓶颈，传统技术难以支撑高效治理。与此同时，安全威胁持续演进，从传统病毒攻击升级为 APT 攻击、零日漏洞利用等高级威胁，防御难度显著提升。确保安全数据的保密性、完整性和可用性，已成为构建网络安全治理体系的关键环节。

然而，现有研究多聚焦于单一环节的防护措施（如加密存储、访问控制等），缺乏覆盖数据全生命周期的系统化与智能化安全治理方案。同时，尚未充分发挥安全大模型在语义理解、威胁溯源和响应决策方面的潜能，导致安全数据价值未能有效转化为智能防御能力。为此，

本文提出基于安全大模型的全生命周期安全治理框架，通过多模态融合与攻击链动态建模实现智能化风险识别与响应，为网络安全治理提供新的技术路径。

1 网络安全领域数据要素安全的特殊性

网络安全数据是指在防护、监控、检测和响应等网络安全活动中所生成的各类安全相关数据集合。这些数据来源广泛，包括网络监控设备、传感器、日志系统、入侵检测/防御系统（IDS/IPS）、漏洞扫描工具、防病毒软件等，涵盖了网络流量、系统日志、攻击行为记录、漏洞信息、恶意软件样本等。随着网络架构的复杂性持续提升，网络安全数据的规模和种类不断扩展，其分析和治理正成为网络安全管理的关键支撑。网络安全大数据具有以下几个显著特性：

（1）数据量庞大

在物联网、云计算和移动互联网高度普及的背景下，网络设备和终端数量急剧增加，所产生的安全数据呈指数级增长。2023 年，全球物联网终端数量已超过 20 亿[1]，移动互联网月度接入流量达 2 384 亿 GB，户均月流量达 17.12 GB[2]。与此同时，安全事件频发，网络告警等数据生成速率高，对系统的实时处理能力提出严峻挑战，传统的数据存储与分析架构难以胜任。

（2）数据类型多样

网络安全数据涵盖结构化数据（如 IP 地址、端口、网络流量等）、半结构化数据（如配置文件、系统调用记录）以及非结构化数据（如日志文件、邮件正文、攻击报文等）。这些数据维度广泛，关联性强，涉及网络通信、应用行为、设备状态、用户活动等多个层面，对数据融合与关联分析技术提出更高要求。

（3）处理时效性要求高

网络攻击呈现出快速传播和隐蔽并存的特征，尤其是 DDoS 攻击、勒索病毒等类型，若不能在第一时间发现并响应，将可能导致系统瘫痪、数据泄漏或业务中断。因此，安全数据处理体系需具备低延迟、高吞吐的处理能力，实现对潜在威胁的实时监测与快速处置。

（4）数据流通频繁

网络安全数据往往来自分布式的异构系统，如防火墙、IDS/IPS、端点安全设备、云平台等。这些数据在多个安全控制层级之间流通与共享，是实现协同防御与全局态势感知的重要基础。然而，频繁的数据流动也带来了更大的数据安全风险，对数据传输安全与使用边界提出更高要求。

2 网络安全数据面临的安全挑战

基于以上网络安全数据的特殊性，在安全数据的广泛应用背景下，保障其在隐私保护、完整性、访问控制和共享管理方面的安全性成为关键[3]。当前网络安全数据面临的核心安全挑战主要包括以下四点：

（1）海量数据的实时监控与分析困难

随着网络安全体系接入的终端设备、业务系统和安全探针数量不断增加，网络安全平台面临的安全数据规模达到亿级甚至百亿级别，涉及日志、流量、行为事件等多种格式。这种数据不仅体量庞大，而且更新频率极高，往往以秒级甚至毫秒级不断涌入，传统的批处理分析方式难以满足响应需求。

（2）数据完整性与一致性问题

安全数据在采集、传输、存储及处理过程中，容易遭遇篡改、丢失、重复等问题，严重时会干扰风险评估与防御决策。例如，攻击者若篡改攻击日志，可掩盖攻击行为，延迟响应。保障数据完整性需引入如哈希校验、区块链等抗篡改机制，并建立数据全生命周期审计体系。

（3）数据访问控制问题

安全数据通常权限等级敏感，不同部门或用户对数据有不同访问需求。传统的基于角色的访问控制（Role-Based Access Control，RBAC）模式在面对大规模、动态化的数据使用需求时存在局限性。为此，需引入更细粒度的访问控制模型或基于上下文动态控制策略，确保敏感数据仅对合规用户和系统开放。

（4）数据跨域共享问题

为提升整体防御能力，安全数据常需要在不同组织、平台之间实现共享，构建联合防护机制。但不同组织之间存在安全等级、政策、技术标准不一致的问题，容易在共享过程中引发数据泄露、误用等风险。安全数据共享体系需通过数据脱敏、传输加密、访问审计与合规评估等机制保障数据的安全跨域流转。

图 1 给出了网络安全数据要素全生命周期面临的安全挑战分布。在四大安全挑战中，“海量数据实时监控与分析困难”是当前网络安全数据治理的核心瓶颈。若无法在海量数据流中实现快速、精准的威胁识别与处置，其他安全措施如数据完整性保护、访问控制优化及安全共享机制都将缺乏实时响应基础，难以发挥应有效能。面对秒级乃至毫秒级的安全事件增长趋势，传统检测体系已难以支撑动态威胁环境的防御需求。因此，本文将重点聚焦该核心问题，提出一种基于安全大模型的实时监测与分析解决方案，通过语义解析、多模态数据融合和攻击链建模，实现对安全数据的智能关联与即时响应，为构建高效、可持续的网络安全防护体系提供新的技术路径。

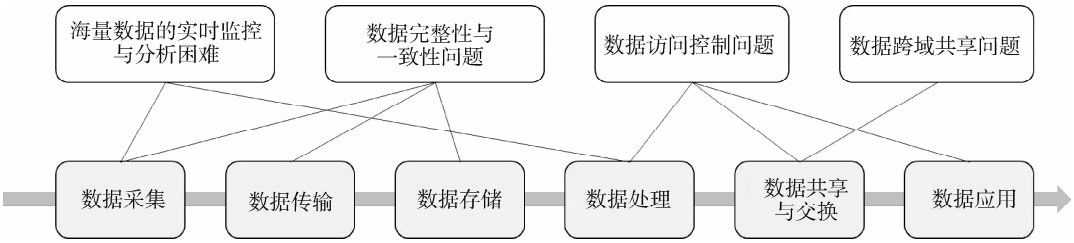

图 1　网络安全数据要素全生命周期安全挑战分布图

3　基于安全大模型的网络安全数据实时监控技术研究

以安全大模型技术为依托，赋能安全数据实时监控，为网络安全领域的实时监控提供了新的突破口。本文聚焦于“基于安全大模型的网络安全实时监控”技术路径，系统阐述其核心架构、关键能力和典型应用。

3.1　安全大模型的基本定义与体系架构

所谓“安全大模型”，是指在网络安全场景中基于大规模安全数据进行预训练和微调的深度学习模型，其训练目标是理解、识别和预测复杂网络攻击行为与安全事件。其核心思想是以丰富的安全语义信息（包括网络日志、攻击路径、系统配置、告警上下文、威胁情报等）为基础，构建统一的信息表征空间，提升威胁感知与响应的智能化水平。如图 2 所示，典型的安全大模型架构包含数据采集与接入层、多模态数据处理层、安全大模型训练与推理层、安全任务适配与微调层以及可视化呈现与处置响应层。

当前主流安全大模型在应用层面仍存在一定局限性。例如，360 SLM[4] 主要聚焦于威胁情报的语义关联与知识图谱推理，在攻击行为逻辑的动态演化建模方面相对薄弱；奇安信 Q-GPT[5] 则侧重于日志解析与安全事件语义理解，在多源异构数据融合与跨阶段攻击链分析上存在局限。这些模型多以单一模态输入（文本或结构化日志）为主，缺乏对网络流量、系统行为、威胁情报等多模态数据的联合理解与推理能力，难以实现从“检测“到“溯源”再到“响应”的全链条智能支撑。

本文提出的技术方案以“多模态融合 + 攻击链动态建模”为核心创新，通过融合日志、流量、威胁情报、资产画像等多维数据，构建统一的安全语义空间，实现攻击阶段、行为模式和意图目标的动态建模。该方法不仅提升了模型在复杂攻击场景下的理解与关联推理能力，还可自动生成溯源路径与响应处置建议，真正实现从安全监测到智能响应的全流程支撑，突破了现有安全大模型在单模态和静态分析层面的局限。

3.2　核心技术能力分析

（1）多模态融合与语义建模

网络安全数据具有高度异构性，例如系统日志是非结构化文本，网络流量是二进制报文，用户行为是时序事件。安全大模型通过 Embedding 机制对不同模态数据进

图 2　基于安全大模型的网络安全实时监控平台逻辑结构

行统一编码[5]，并在注意力机制的引导下学习其语义关系。例如，针对某次攻击行为，模型可以将日志中“failed login”、网络中“port scan”以及端点检测与响应（Endpoint Detection and Response，EDR）中“malware execution”整合为同一攻击上下文，实现跨模态的威胁识别。

（2）上下文建模与攻击链分析

传统方法往往关注单点异常，难以揭示攻击链条的全过程。大模型通过长上下文建模能力（例如使用 Transformer 或 Memory 机制），可以理解多跳攻击路径，识别攻击生命周期（如 MITRE ATT&CK 阶段中的初始访问、执行、持久化、横向移动等）。例如，模型可以识别出某 IP 在登录失败数次后，在其他主机上尝试远程桌面协议（Remote Desktop Protocol，RDP）连接，进而推断为横向渗透[4]。

（3）自监督学习与零样本识别

在安全领域，新的攻击手法不断涌现，标签数据稀缺且滞后。安全大模型可通过自监督学习，如“掩码语言建模”“事件预测”或“图结构重构”等方式，从海量未标注日志中学习通用表示，从而具备一定的“零样本识别”能力。例如模型可识别从未见过的恶意进程行为模式。

（4）智能网络攻击溯源[6]

大模型在网络攻击溯源中主要通过攻击路径重建、攻击者画像、恶意基础设施追踪三个环节发挥作用。包括利用日志、防火墙记录等多源数据恢复攻击链，从初始突破点到权限提升与内部横向扩散的全过程。采用综合攻击方式、IP/域名/邮箱等线索，推测攻击者的组织归属、技术水平与偏好特征。

3.3 典型应用场景

目前，基于安全大模型的实时检测已在多个网络安全场景中展现出良好的效果。本文以高级持续性威胁（Advanced Persistent Threat，APT）攻击检测为例，阐述安全大模型在网络安全实时检测中的原理和作用[7]。

APT 攻击通常具有高度隐蔽性、长期潜伏性和多阶段攻击链的特征，往往由具备组织化背景的攻击者实施。传统的基于规则或特征码的检测方法，更多依赖已知攻击特征库，难以及时发现新型或变种的 APT 攻击行为。而安全大模型凭借其对海量安全数据的深度语义建模与上下文理解能力，正逐步成为网络安全实时监控的核心引擎，能够在第一时间发现异常并作出响应。

首先，大模型具备强大的日志语义解析与多源数据关联能力。在实际环境中，安全运营中心（Security Operations Center，SOC）会接收来自防火墙、终端安全软件、邮件网关、EDR 等不同系统的大量日志，这些日志既包含结构化的告警信息，也包含非结构化或半结构化的事件记录。大模型通过自然语言处理与深度语义建模技术，可以自动抽取日志中的关键要素，对用户行为、系统进程、网络流量、邮件内容等进行语义理解和事件建模。例如，当攻击者通过鱼叉式钓鱼邮件诱导用户点击后门文件后，系统日志可能仅表现为一次“邮件附件下载”与“进程启动”。大模型能够进一步结合后续的“异常端口通信”“横向登录尝试”等事件，将这些零散的日志信息串联成完整的攻击链条，从而识别出攻击行为的真实意图[8]。

其次，大模型在知识融合方面具有显著优势。通过引入攻击知识图谱与 APT 攻击行为模板，结合 MITRE ATT&CK 知识库，大模型可以对检测到的行为进行自动分类和上下文标注。例如，当系统监测到使用 PowerShell 下载远程脚本的行为，大模型不仅能识别该命令行行为的恶意意图，还能进一步判断其属于攻击链中的执行阶段；当检测到内网大规模端口扫描或 RDP 登录暴力破解尝试时，大模型能够将其标注为“横向移动”或“持久化”阶段行为，并判断其与已知 APT 组织的攻击模式高度相似。这样一来，安全人员可以在攻击者完成数据渗漏或持久控制之前，提前获取告警并开展阻断。例如，在某单位网络环境中，基于安全大模型的 APT 攻击检测准确率达 85%，较传统规则检测提升 20% ~30%。

第三，大模型还能够结合实时威胁情报与历史攻击案例，实现动态学习与持续优化。不同于传统检测依赖静态规则，大模型可以不断吸收最新的威胁情报信息，对攻击工具、攻击域名、恶意 IP 等进行语义化扩展和关联推理。例如，当发现某一异常 C2（Command and Control）通信特征时，大模型可结合全球威胁情报，推断其与某 APT 组织近期活动相关，从而帮助安全团队快速锁定攻击源头，提升检测的时效性和准确性。

最后，安全大模型在实时检测中还具备辅助响应的价值。借助对攻击链的自动还原与行为预测能力，大模型不仅能够告警，还能提供响应建议，如立即隔离受感染终端、阻断特定 IP 通信、加强关键账户多因素认证等。这使得安全运营从“发现 - 分析 - 处置“的链条大幅缩短，提高了企业网络安全防护的自动化和智能化水平。安全大模型通过语义解析、多源数据关联、知识图谱融合以及威胁情报驱动，在 APT 攻击检测场景中展现出强大的实时监控与响应能力。它不仅解决了传统方法对未知威胁检测不足的问题，也为未来网络安全体系构建提供了新的技术范式。

图 3 展示了安全大模型在 APT 攻击检测中的具体流程。

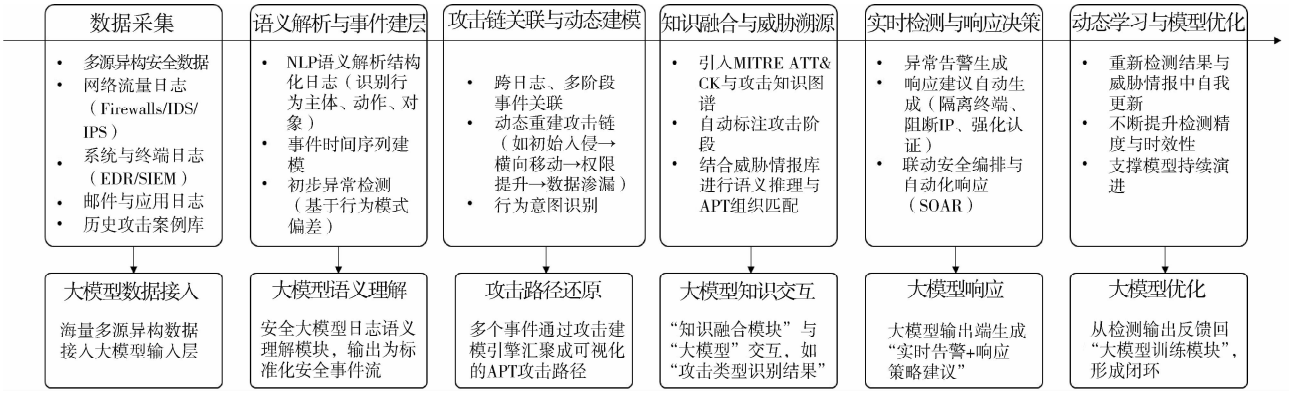

图 3　APT 攻击检测流程图

4　结论

随着数字经济和网络空间的快速发展，数据已成为核心生产要素，而网络安全数据在保障国家、企业和个人信息安全中扮演着重要角色。本文从网络安全视角对数据要素安全治理进行了系统研究。首先，分析了网络安全领域数据要素的特殊性，包括数据量大、类型多样、处理时效要求高等，这些特性决定了数据治理必须兼顾高性能处理能力与安全保障能力。其次，本文梳理了网络安全数据面临的主要安全挑战，如海量数据实时监控与分析难度大、数据完整性与一致性难以保障、访问控制和权限管理复杂、跨域共享存在风险等，这些问题直接制约了数据要素在安全环境下的高效流通与价值释放。

针对上述挑战，本文进一步探讨了基于安全大模型的网络安全数据实时监控技术。通过引入大模型的语义理解、上下文关联、多源数据融合和攻击链分析能力，可以显著提升对复杂威胁、异常行为及高级持续性威胁攻击的检测和响应效率。本文详细分析了安全大模型的核心技术，包括日志语义解析、溯源链条重建、攻击知识图谱构建及多阶段威胁识别等，并结合典型应用场景说明了其在网络安全实时检测、告警预测和辅助决策等方面的实际价值。研究表明，安全大模型能够实现从海量数据中高效提取威胁特征，增强网络安全防护的智能化和自动化水平，为数据要素安全提供了新的技术支撑。

网络安全视角下的数据要素安全治理需要在保障数据安全性、完整性与可用性的基础上，引入智能化技术手段。安全大模型为网络安全数据实时监控提供了有效路径，不仅能够应对海量、多样化数据带来的监控压力，还能够对复杂攻击行为实现早期识别与预测，从而支撑数据要素的安全流通与价值释放。未来，随着大模型技术的不断发展和优化，其在网络安全治理、数据合规性保障及跨域数据共享中的应用潜力将进一步扩大，为构建安全、可信、可持续的数据要素生态提供重要支撑。

参考文献

[1] 中国互联网络信息中心（CNNIC）. 中国互联网络发展状况统计报告（第 52 次）[R]. 北京. 中国互联网络信息中心，2023.

[2] 工业和信息化部. 2023 年 1－10 月通信业经济运行情况 [EB/OL]. (2023－11－22) [2025－08－01]. https://www.miit.gov.cn/gxsj/tjfx/txy/art/2023/art_f124b65c5e17464a93ae4ae3aa4b0b08.html.

[3] 美国国家标准与技术研究院. NIST Special Publication 800－150：Guide to Cyber Threat Information Sharing [S]. 2016.

[4] 三六零集团. 360 安全大模型（360SLM）白皮书 [Z]. 北京：360 安全研究院，2023.

[5] 奇安信科技集团. 奇安信 Q－GPT 安全机器人系统技术白皮书 [Z]. 北京：奇安信安全研究院，2024.

[6] 阿里云，中国信通院. 大模型安全研究报告（2024 年）[R]. 2024.

[7] 虎嵩林，李涓子，秦兵，等. 亦正亦邪大模型——大模型与安全专题导读 [J]. 计算机研究与发展，2024，61（5）：1085－1093.

[8] 冯云，刘宝旭，张金莉，等. 基于主机事件的攻击发现技术研究综述 [J]. 信息安全学报，2023，8（4）：31－45.

（收稿日期：2025－09－08）

作者简介：

唐珂（1984－），男，硕士，工程师，主要研究方向：网络安全。

宋崴（1986－），男，博士，工程师，主要研究方向：网络安全。

张文瑾（1970－），女，硕士，正高级工程师，主要研究方向：网络安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部