数智供应链的网络安全风险传导抑制机制

胡慕海，范家乐，张 良

（武汉纺织大学管理学院，武汉 430200）

摘要：在数智化背景下，供应链主体面临着多重网络安全风险，易通过节点关联形成连锁传导，对国家利益、企业经营及个人权益构成威胁。现有研究多聚焦单一风险、定性分析，缺乏对风险传导动态机制的系统探讨，难以应对数智技术赋能下的供应链运营复杂情境。基于文献梳理，选取高质量专业文献为语料，运用文本因果关系挖掘与模糊认知图建模方法，构建数智供应链网络安全多重风险的复杂系统模型，开展风险传导路径识别与抑制策略仿真分析。揭示了多重核心风险的传导机制及其关键影响因子，构建具针对性的传导抑制策略，为实现风险传导精准防控提供决策支持与理论依据。

关键词：数智供应链；网络安全风险；风险传导；系统仿真

中图分类号：C931.2 **文献标志码：**A **文章编号：**1671－1807(2026)04－0121－10

数智供应链是数字化技术与智能化决策的深度融合，强调通过数据驱动实现供应链全链路协同[1]，物联网、区块链、数字孪生等技术集群的成熟，使得供应链具备神经网络的智能特性。数智供应链的发展，其本质是为满足生产、仓储、运输和交付等各流通环节对高效率、低成本的现实需求，意味着其既具有数字化的特征，又具有智慧化的效能[2]。数智供应链的核心特征在于能够应用人工智能自主分析复杂数据、生成预测性洞察，并在最小化人工干预的情况下执行决策[3]。但数智技术的规模化应用使供应链网络安全风险防控压力陡增，《Verizon 2024 数据泄露调查报告》指出，有15%的数据泄露涉及供应链攻击，较前一年增长68%[4]。对此，各国政府已积极出台应对举措：美国网络安全与基础设施安全局（CISA）专门成立供应链风险管理工作组，中国则将《中华人民共和国网络安全审查办法》《关键信息基础设施安全保护条例》等纳入供应链安全核心保护范畴。这些行动充分表明，提升数智供应链的风险防控能力已成为亟待解决的现实需求。

1 文献回顾

相关研究涉及数智供应链网络安全风险的界定、影响因素以及模糊认知图在风险演化复杂系统中的应用。Carnovale 和 Sengun[5]认为其是供应链网络环境内外部漏洞导致的、可能影响信息和运营技术并造成业务中断及经济损失的负面事件；Herburger[6]指出其是与网络空间活动相关的运营和物理风险，会损害供应链资产、信息等的完整性、可用性和保密性。风险分类方面，杨昕然和黄玉杰[7]认为在当今全球化和日益动荡的环境中，供应链主体主要面临信息中断的风险；Ghadge 等[8]将供应链管理中的网络风险分为物理威胁、故障、间接和直接攻击以及内部威胁。在数智化技术深度应用背景下，传统供应链系统的网络安全风险已难以全面反映供应链数智化后多源异构、高频交互、跨域协同带来的复杂多变的网络安全风险[9]。为适应这一变化，Melnyk 等[10]、Creazza 等[11]结合数智供应链情境，提出如数字供应链运营风险、供应链第三方网络安全风险以及供应链数据泄露等新的风险类型，但目前缺乏针对这些风险的系统性量化研究。

数智供应链网络安全风险的影响因素大致涵盖如下类别视角：技术应用视角，众多学者认为供应链数智化管理为黑客创造机会，供应链信息化系统则面临更多更频繁的网络攻击风险[12-14]；组织管理视角，供应链主体内部员工有意或无意的行为、薄弱的内部监管机制都可能造成敏感信息泄露、重要数据资产被转移、系统访问权限被滥用等风险，从而给供应链主体造成非常严重的损失[15-16]；外部

收稿日期：2025-08-16

基金项目：湖北省教育厅哲学社会科学研究一般项目（24Y096）；国家社会科学基金一般项目（22BGL139）

作者简介：胡慕海（1976—），男，湖北武汉人，博士，副教授，硕士研究生导师，研究方向为供应链管理；范家乐（2001—），男，湖北荆州人，硕士研究生，研究方向为数智供应链安全；张良（1998—），男，湖北陆安人，硕士研究生，研究方向为网络安全。

环境视角，自然灾害和社会事件可能会对供应链造成影响，这可能会导致供应链中断的风险[17]。总体而言，现有研究多聚焦单一风险或有限因素的定性分析，缺乏对多重风险动态关联的系统性探究，难以适配复杂数智化情境。

2　研究设计

如图 1 所示，分三个阶段展开研究。

2.1　数智供应链网络安全风险、影响因素识别及关系挖掘

（1）采集相关文献文本语料，以句子为单位切分语料，通过因果触发词组建匹配句式，并设定关系模板，将句子切割为因果两类短文本，作为语料库。

（2）参考李方正等[18]、陆振昇和马超[19]的做法，基于主题聚类提炼相关概念，首先基于核心文献组织语料，提炼数智供应链当前存在的主要网络安全风险类型 R_1，R_2，…，R_n，进而基于前期构建的语料库语料划分为特定风险类语料库和影响因素类语料；进一步引入主题聚类完成非风险类语料文本的主题挖掘，结合文献总结，提炼出风险影响因素的概念。

（3）为反映各风险的聚合效应，将风险类型 R_1，R_2，…，R_n 建立单向等强度因果关系。以数据安全风险 R_1，R_2，R_3，…，R_n，以及影响因素为概念节点，基于语料中挖掘的因果对按概念聚合因果关系，构建各类风险和影响因素为节点的因果关联有向网络图，即构建数智供应链的网络安全风险传导网络。节点间关系权重计算公式为

$$W(e_i \rightarrow e_j) = \frac{\mathrm{count}(e_i \rightarrow e_j)}{\sum_k \mathrm{count}(e_i \rightarrow e_k)} \tag{1}$$

式中：$W(e_i \rightarrow e_j)$ 为由概念节点 e_i 指向 e_j 的关系权重；$\mathrm{count}(e_i \rightarrow e_j)$ 为以 e_i 作为原因节点、e_j 作为结果节点的关系频数；k 为总的概念节点数。

2.2　数智供应链的网络安全风险模糊认知图系统建模

（1）模糊认知图（fuzzy cognitive map，FCM）由一系列存在因果关联的概念构成，可支持知识表达、机器学习、因果推理及复杂系统研究[20]。因此以网络安全风险传导网络为输入，构建 FCM 概念模型。因果关联图可转换为以概念节点为行、列要素的邻接矩阵 $\boldsymbol{W}$。其中，W_{ij} 表示 i 节点对 j 节点的影响强弱，如果两个节点间不存在联系，则 $W_{ij}=0$。

（2）初始状态矩阵是概念节点初始状态的集合：$C=(C_1, C_2, \cdots, C_n)$。其中，$C_i$ 为系统中第 i 个概念节点的初始状态值。节点处于激活状态则初始状态值设置为 0，反之设置为零。

（3）节点的状态值转换函数为

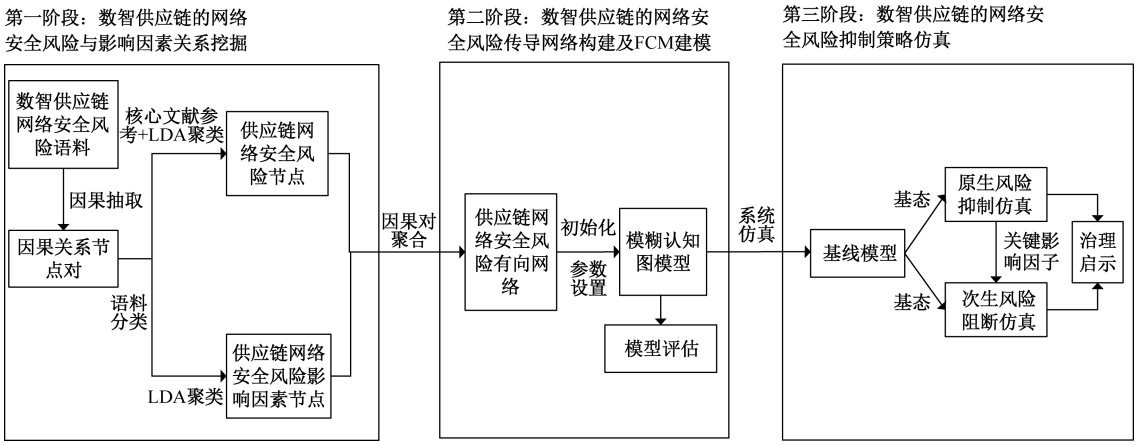
$$A_i(t+1) = f\left[A_i(t) + \sum_{j=1, j\neq i}^{n} w_{ji} A_j(t)\right] \tag{2}$$

式中：t 为迭代步长；$A_i(t)$、$A_j(t)$ 为概念 C_i、C_j 在时间 t 的值；$A_i(t+1)$ 为概念 C_i 在 $t+1$ 时的值；w_{ji} 为概念 C_j 到概念 C_i 的连接权重；$f(\cdot)$ 为阈值函数，当节点初始状态区间为［0，1］时，通常使用 sigmoid 函数。

$$f(x)=\frac{1}{1+\mathrm{e}^{-cx}},\ c>0 \tag{3}$$

2.3　数智供应链的网络安全风险系统仿真

设定模型运算迭代时的容忍值 r，当最终各节点的当前状态值与上一次迭代状态值的差异小于 r 时，则系统视为达到稳定状态。进行模型评估后展开系统仿真，观测系统稳态时节点状态值的变化，



LDA：latent Dirichlet allocation

图 1　技术路线

识别系统关键要素。在此基础上,提出基于单个影响因素,多个因素组合的供应链网络安全风险管理策略,采用系统仿真,观测风险抑制效应,形成治理建议。

3 实证研究

3.1 数智供应链的网络安全风险与影响因素关系挖掘

3.1.1 语料准备

以供应链数智化管理中与网络安全风险主题高度相关的文献作为语料文本数据,选择中国知网以及 Web of Science 核心合集作为文献筛选的主要检索数据库;构建了("digital technology" OR "Industry 4.0" OR "blockchain" OR "artificial intelligence" OR "cloud computing" OR "Internet of Things (IoT)" OR "the zero trust") AND "supply chain"AND ("cyber security risk" OR "cyber risk" OR "cyber security")的英文检索词以及相对应的中文检索词的基本正则检索关系,设置多种搜索范围和条件进行广泛检索,并辅以人工阅读筛选,确保语料数据的相关性。筛选后得到的文献发表时间主要集中在近五年(截至 2025 年 6 月),与研究主题高相关性的文献 143 篇作为语料文本数据,最终合计形成 18 万余字、86 392 句语料。

3.1.2 因果关系抽取

文本因果关系可基于规则和模板抽取,以句子为单位切分网络安全风险初始语料文本[21],参考北京大学现代汉语语料库的因果句法分类,通过因果触发词组建匹配句式,并设计关系模板将句子切割为因果两类短文本,作为基本语料单位。去除语义匮乏的节点 508 个,最终抽取到因果关系文本短句共 3 076 个,将这些短句形成因果短句库作为因果节点展开后续研究。

3.1.3 供应链网络安全风险识别及分类

根据期刊分区、影响因子、引文指标和被引次数四个指标梳理出供应链网络安全领域的核心综述类文献 4 篇[8,10-12],提炼出其中对网络安全风险定义及分类的描述性语句 32 句,将其与其他语料进行相似度比较,高相似语料(相似度大于 0.8)作为网络安全风险类语料,剩余语料作为影响因素类语料。最后筛选出共计 332 个因果短句作为全部风险类语料,并把除开风险类语料之外 2 744 句因果节点短句作为风险影响因素类语料。之后通过 LDA 分析风险类语料主题,综合考虑主题一致性和主题空间分布两个指标确定最优聚类主题数量。当主题数为 3 时,主题一致性指标为 0.541 6 到达第一次峰值,此时各主题的空间分布较离散,说明此时主题聚类效果较好,形成的主题词和主题分布(表 1)。

结合文献和 LDA 分析,本文界定了数智供应链中高发的三种网络安全风险:供应链主体数据资产泄露风险:由供应链主体内部人员造成的敏感数据资产丢失、泄露和滥用的风险;供应链业务信息流中断风险:供应链成员间的业务信息在合作授权过程中可能因访问权限、不当行为操作或合规性问题导致中断的风险;供应链通信基础设施损坏风险:软件信息系统崩溃、设备故障以及基础设施遭受物理攻击被损坏的风险。进一步基于语料的最高主题隶属度,将风险类语料细分为三个子风险类语料(表 2)。

3.1.4 供应链网络安全风险影响因素挖掘

影响因素类语料主题聚类分析在主题数为 6 时第一次达到峰值 0.621 7,如图 2 所示,从主题分布来看,当主题数为 6 时,主题间不存在重合,如图 3 所示;在主题数为 10、15 时,随主题数增加,主题重合程度越来越高,如图 4 和图 5 所示,不利于影响因素概念的明显区分。综合考虑,确定聚类最优主题数量为 6,并结合相关文献调研总结提炼出 6 个数智供应链的网络安全风险影响因素 C_0~C_5,如表 3 所示。

3.2 数智供应链的网络安全风险传导网络构建及 FCM 建模

3.2.1 多重网络安全风险传导网络构建及 FCM 建模

根据式(1)可以确定概念节点间边权重,完成网

表 1 网络安全风险主题-主题词-隶属占比

主题号	主题高隶属度关键词	隶属文本量	隶属文本百分比
0	0.011×"数据泄露"+0.011×"员工"+0.007×"资产"+0.004×"丢失"+0.004×"泄露"+0.004×"内部"+0.004×"滥用"+0.003×"敏感数据"+0.003×"内部人员"	116	0.349 4
1	0.014×"供应商"+0.011×"未经授权"+0.010×"信息"+0.008×"访问"+0.007×"服务"+0.007×"第三方"+0.006×"中断"+0.006×"操作"+0.003×"合作伙伴"+0.003×"合规"	107	0.322 3
2	0.011×"软件"+0.009×"信息"+0.009×"设备"+0.004×"基础设施"+0.004×"崩溃"+0.004×"物理攻击"+0.004×"故障"+0.004×"损坏"+0.004×"信息系统"	109	0.328 3

表 2　节点短文本分类(部分)

语料 ID	节点因果类型	短文本语料内容	语料类别
11436	Cause 因节点	因此在供应链中增加数据交换	影响因素
11436	Effect 果节点	包括信息优势的丧失因不公平行为而受到惩罚的威胁分销渠道的泄露议价能力的削弱以及跳过供应链的风险	供应链主体数据资产泄露风险
11885	Cause 因节点	当资源共享分配发生变化时	影响因素
11885	Effect 果节点	可能会通过数据残留破坏和泄露信息	供应链业务信息流中断风险
13289	Cause 因节点	使恶意行为者能够部署更多的恶意软件	影响因素
13289	Effect 果节点	随后该病毒在客户的信息技术基础设施中建立了一个秘密接入点	供应链通信基础设施损坏风险
…	…	…	…

表 3　网络安全风险因素关键词-主题-主题概念

主题号	主题高隶属度关键词	影响因素	概念内涵
0	0.015×“来源”+0.012×“设备”+0.011×“韧性”+0.010×“服务”+0.008×“完整性”+0.003×“检测”+0.003×“潜在”+0.004×“隔离”+0.004×“缓解”+0.004×“信息系统”+0.004×“限制+0.003×“协调”+0.003×“可追溯”+0.003×“实时”+0.003×“快速”+0.003×“间接”+0.003×“可用性”	供应链网络安全系统韧性不足(C_0)	供应链网络安全系统因韧性不足,难以快速检测追溯风险及协调资源限制隔离风险,进而影响设备可用性与服务完整性
1	0.012×“恶意”+0.010×“整个”+0.008×“基础设施”+0.005×“勒索”+0.005×“脆弱性”+0.005×“设备”+0.004×“攻击者”+0.004×“破坏”+0.004×“持续”+0.003×“严重破坏”+0.003×“关键基础设施”+0.003×“易受攻击”+0.003×“接口”+0.003×“安全漏洞”	面向供应链基础设施的网络攻击(C_1)	恶意攻击者针对供应链基础设施发动病毒、勒索等攻击,利用系统安全漏洞破坏设备接口,影响核心设施正常运转,使供应链基础设施在持续外部攻击下呈现脆弱性
2	0.015×“客户”+0.006×“信息”+0.006×“入侵”+0.006×“感知”+0.004×“可追溯”+0.004×“成员”+0.004×“黑客”+0.004×“培训”+0.004×“缺乏”+0.004×“供应商”+0.003×“参与者”+0.003×“未经授权”+0.003×“合作伙伴”+0.003×“弱点”+0.003×“下游”+0.003×“攻击者”+0.004×“损害”+0.003×“犯罪”	供应链相关方风险感知能力弱(C_2)	供应链中的客户、合作伙伴及供应商等相关方,由于缺乏风险感知培训,难以辨别黑客伪装的未经授权访问,自身风险感知能力较弱,容易成为攻击目标,进而给供应链带来安全风险
3	0.011×“第三方”+0.011×“泄露”+0.010×“供应商”+0.008×“信任”+0.006×“攻击者”+0.005×“资源”+0.005×“缺乏”+0.005×“共享”+0.005×“客户”+0.004×“资产”+0.003×“合作伙伴”+0.003×“入侵”+0.003×“通信”+0.003×“相互”+0.003×“数据交换”+0.002×“信息安全”	供应链主体互信共享机制不健全(C_3)	供应链主体之间缺乏互信共享标准,在数据交换和资源共享过程中,容易遭受攻击者以虚拟身份窃取数据,导致资产泄露等安全问题
4	0.015×“技术”+0.007×“物理”+0.007×“数字”+0.006×“功能”+0.006×“缺陷”+0.006×“故障”+0.005×“设备”+0.004×“标准”+0.004×“灾难性”+0.004×“系统故障”+0.003×“区块链”+0.003×“服务器”+0.003×“端口”+0.003×“硬件”	供应链网络安防技术存在缺陷(C_4)	数智化管理中区块链等技术缺乏安防保障,攻击者利用技术缺陷污染端口致系统故障、设备功能异常
5	0.014×“评估”+0.011×“意识”+0.009×“缺乏”+0.008×“安全漏洞”+0.006×“操作”+0.006×“合作伙伴”+0.005×“内部”+0.005×“业务”+0.004×“培训”+0.004×“安全措施”+0.004×“供应商”+0.003×“标准”+0.003×“敏感数据”+0.003×“共享”	供应链主体缺乏安全意识和审计(C_5)	供应链主体因安全意识不足缺乏系统安全评估,难发现内部漏洞且安全措施单一,缺乏对相关方业务审计易致违规操作

络安全风险传导网络建模,其中包含三类供应链网络安全风险节点(R_1～R_3)和 6 个风险影响因素节点(C_0～C_5),形成节点间聚合的因果关系权重矩阵,如表 4 所示。进一步地,将三类供应链网络安全子风险视为系统全局响应变量,影响因素节点视为系统控制变量,基于挖掘的网络安全风险传导网络,引入式(2),用 sigmoid 函数式(3)作为阈值函数,容忍值 R 设置为 0.001 构建 FCM 系统模型,如图 6 所示。

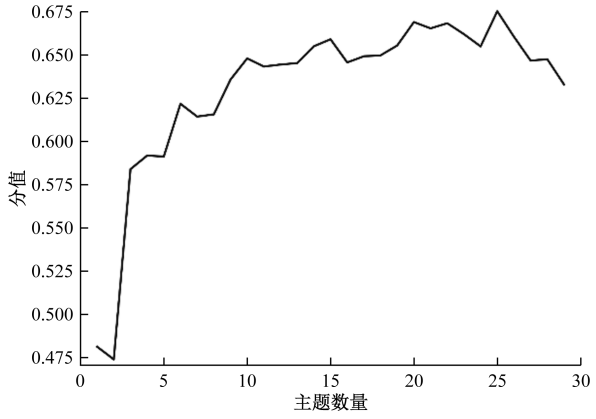


图 2　主题一致性

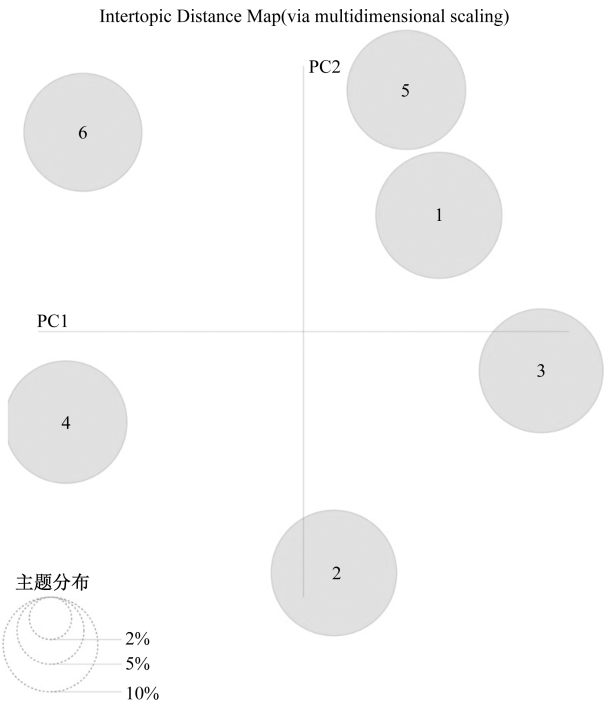


图 3　主题分布(topic=6)

表 4　节点间因果关系权重矩阵

节点	C_0	C_1	C_2	C_3	C_4	C_5	R_1	R_2	R_3
C_0	0	0.13	0.13	0.09	0.14	0.12	0.02	0.03	0.03
C_1	0.32	0	0.17	0.10	0.12	0.08	0.03	0.03	0.04
C_2	0.36	0.11	0	0.08	0.12	0.11	0.04	0.03	0.04
C_3	0.33	0.12	0.06	0	0.08	0.13	0.04	0.04	0.02
C_4	0.34	0.13	0.12	0.11	0	0.07	0.04	0.02	0.03
C_5	0.29	0.13	0.14	0.12	0.13	0	0.02	0.03	0.04
R_1	0.33	0.17	0.12	0.09	0.14	0.06	0	0.00	0.03
R_2	0.35	0.08	0.11	0.09	0.15	0.17	0.02	0	0.03
R_3	0.30	0.15	0.11	0.08	0.15	0.13	0.03	0.02	0

3.2.2　FCM 系统模型评估

生成 100 组随机初始值进行迭代,当实验次数逐渐增多时,各影响因素及风险的稳态均值基于序列[0.966 2,0.852 7,0.849 5,0.832 2,0.860 2,

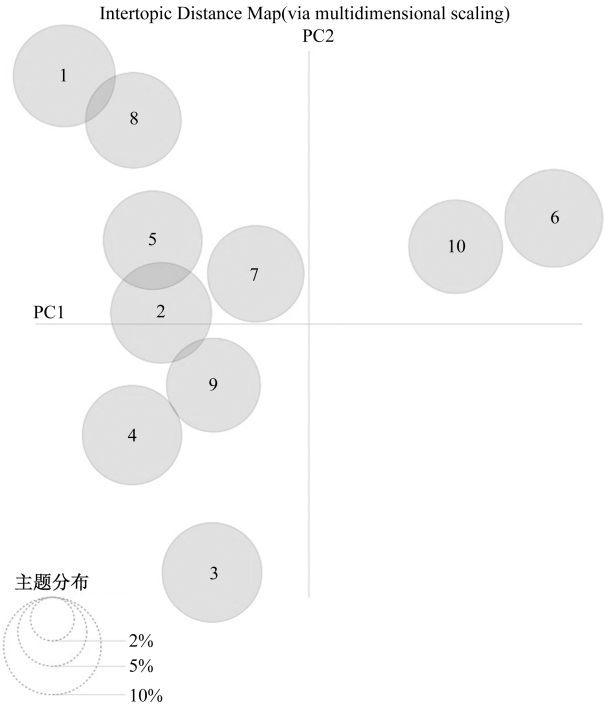


图 4　主题分布(topic=10)

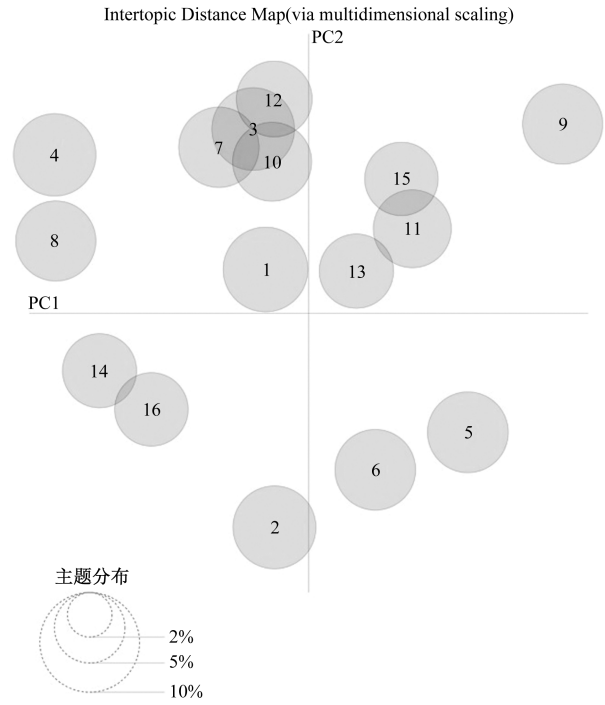


图 5　主题分布(topic=15)

0.838 1,0.723 4,0.706 4,0.721 6]中对应各值上下略微波动,影响因素 C_0 的均值标准偏差稳定在 0.000 02 附近,其余影响因素和风险的均值标准偏差稳定在 0.000 05 附近,C_0、C_1 稳态均值及均值标准偏差如图 7 和图 8 所示。因此该模型的稳态均值波动极小,说明模型具有较好的稳定性;稳态均值

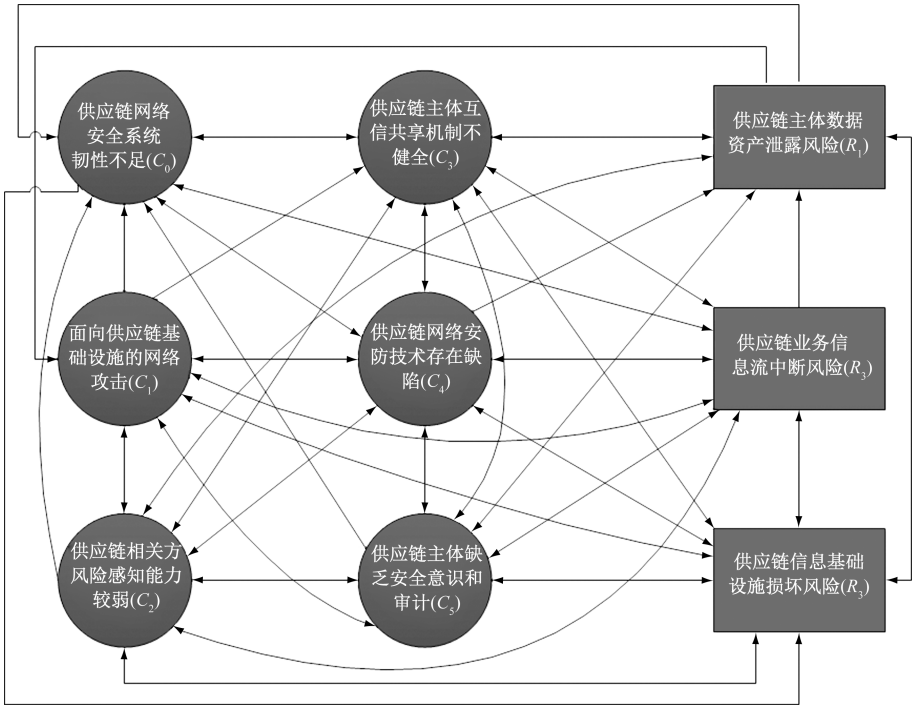


图 6　FCM 系统结构

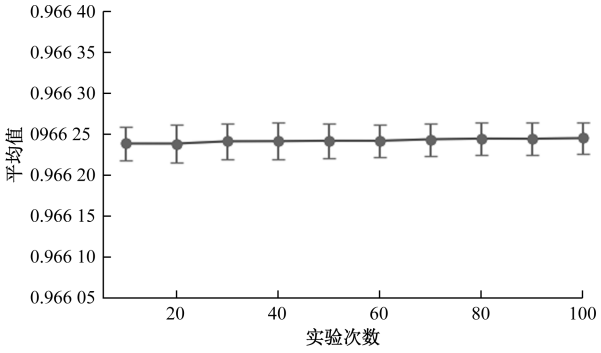


图 7　C_0 稳态均值及均值标准偏差

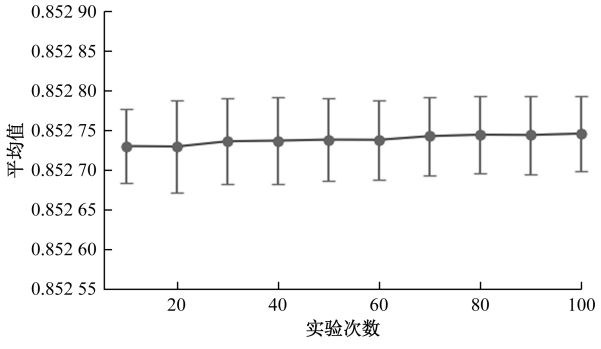


图 8　C_1 稳态均值及均值标准偏差

标准偏差变化范围较小，也验证了该模型具有较好的鲁棒性。

3.3　数智供应链的网络安全风险抑制策略仿真

3.3.1　基线构建

将各影响因素的初始状态值设置为 1，各风险的初始状态值设置为 0，根据模型参数设置[22-23]，得到初始矩阵(1,1,1,1,1,1,0,0,0)，即各因素处于完全激活状态，构建基线模型，模拟由各影响因素相互作用而形成供应链网络安全风险的过程。最终各因素及风险的稳态值序列为[0.966 3,0.852 8,0.849 5,0.832 2,0.860 2,0.838 1,0.723 4,0.706 4,0.721 5](依次对应 C_0～C_5、R_1～R_3)，系统迭代过程如图 9 所示。

3.3.2　原生风险抑制仿真

1)各风险稳态变化

将全部影响因素初始值相对于基线模型的初始值 1 分别下调 25%、50%、75%、100%，以模拟对各因素进行不同程度管控的效果，计算对因素进行调控后的稳态值相对于基线模型稳态值的变化量及变化均值，结果将排序前三的因素视为关键影响因素，如表 5～表 7 所示。

分别对各影响因素进行不同程度的下调管控，由表 5 中变化均值的大小可知，管控 C_3、C_4、C_2 能够最大程度地抑制 R_1。

根据表 6 中变化均值的结果，进行管控后对 R_2 起到显著抑制效果的影响因素先后为 C_3、C_5、C_1。

表 7 中变化均值可以初步判断，对于抑制 R_3 而言，风险管控排序前三的因素 C_5、C_1、C_2。

2)关键管控因子识别的案例验证

通过调控 6 个影响因素的初始值，识别出抑制

三类原生风险的关键因子:管控 C_3 对 R_1、R_2 抑制效果最优(稳态值降低幅度最大);管控 C_5 对 R_3 抑制效果最显著。2023 年,宁德时代因与上游锂矿供应商数据共享缺乏加密机制,3 次发生原材料采购数据泄露,导致采购成本抬高、直接损失 2 100 万元;2024 年投入 800 万元构建“区块链+权限分级”管理体系,全年未再发生数据泄露,还因采购数据透明化减少溢价支出 1 500 万元。引入投资回报率概念(return on investment,ROI),ROI=(投资净收益÷投资总成本)×100%;此时 ROI=(1 500−800)/800=0.87,达到了良好的投资回报率。案例中“数据共享加密机制缺失”对应了供应链主体互信共享机制不健全(C_3),“采购数据泄露”属于供应链主体数据资产泄露风险(R_1),管控 C_3 后 R_1 得到有效抑制的结果,宁德时代的该案例表明管控 C_3 确实对抑制 R_1 效果显著。

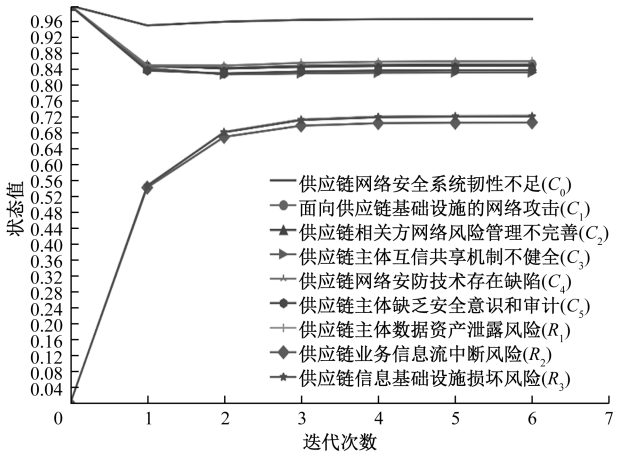


图 9　基线模型系统迭代

3.3.3　次生风险传导抑制仿真

在某种网络安全风险一定发生并促成次生风险增加的情况下,通过对风险影响因素分别进行不同程度的模拟管控仿真,从而得到针对抑制次生风险增加的相应策略。选取对供应链网络安全原生风险抑制效果总体最好的 3 个影响因素作为管控对象,即 C_3、C_1、C_5,将这些影响因素初始值相对于基线模型的初始值 1 分别下调 25%、50%、75%、100%,以模拟进行不同程度管控后的各风险稳态值变化情况。

1)供应链主体数据资产泄露风险发生(R_1 发生)

假定在 R_1 发生的情况下(该风险初始值为 1),对 C_1、C_3、C_5 分别进行不同程度的管控,通过计算可得到管控后另外两种风险的稳态值相对于基线模型稳态值的变化量及变化均值,结果如表 8 和表 9 所示。

辨识表 8 和表 9 中变化均值最大的因子,可知当 R_1 发生时,抑制 R_2 的最优策略是管控 C_3 因素,抑制 R_3 的最优策略是管控 C_5 因素。

2)供应链业务信息流中断风险发生(R_2 发生)

假定在 R_2 发生的情况下(该风险初始值为 1),对 C_1、C_3、C_5 分别进行不同程度的管控,通过计算可得到管控后另外两种风险的稳态值相对于基线模型稳态值的变化量及变化均值,结果如表 10 和表 11 所示。

表 5　供应链主体数据资产泄露风险 R_1 的稳态变化情况

影响因素	基线模型	−25%	−50%	−75%	−100%	排序
C_0	0.723 433 1	0.723 429 5	0.723 425 6	0.723 421 2	0.723 416 4	6
C_1	0.723 433 1	0.723 426 6	0.723 419 3	0.723 411 2	0.723 402 2	4
C_2	0.723 433 1	0.723 426 6	0.723 419 2	0.723 411 0	0.723 401 9	3
C_3	0.723 433 1	0.723 426 2	0.723 418 4	0.723 409 5	0.723 399 7	1
C_4	0.723 433 1	0.723 426 4	0.723 418 9	0.723 410 4	0.723 401 1	2
C_5	0.723 433 1	0.723 427 5	0.723 421 2	0.723 414 1	0.723 406 4	5

表 6　供应链业务信息流中断风险 R_2 的稳态变化情况

影响因素	基线模型	−25%	−50%	−75%	−100%	排序
C_0	0.706 358 5	0.706 355 1	0.706 351 3	0.706 347 1	0.706 342 5	6
C_1	0.706 358 5	0.706 353 1	0.706 347 1	0.706 340 4	0.706 333 0	3
C_2	0.706 358 5	0.706 353 4	0.706 347 7	0.706 341 3	0.706 334 2	4
C_3	0.706 358 5	0.706 351 8	0.706 344 2	0.706 335 5	0.706 325 9	1
C_4	0.706 358 5	0.706 354 2	0.706 349 4	0.706 344 0	0.706 338 0	5
C_5	0.706 358 5	0.706 352 9	0.706 346 6	0.706 339 5	0.706 331 7	2

辨识表 10 和表 11 中变化均值最大的因子，当 R_2 发生时，抑制 R_1 的最优单策略是管控 C_3 因素，由于 C_5 因素及 C_1 因素对风险的稳态变化均值近乎是相同的，均可以作为抑制 R_3 效果较好的单策略。

3）供应链通信基础设施损坏风险发生（R_3 发生）

假定在 R_3 发生的情况下（该风险初始值为 1），对 C_1、C_3、C_5 分别进行不同程度的管控，通过计算可得到管控后另外两种风险的稳态值相对于基线模型稳态值的变化量及变化均值，结果如表 12 和表 13 所示。

表 7　供应链通信基础设施损坏风险 R_3 的稳态变化情况

影响因素	基线模型	−25%	−50%	−75%	−100%	排序
C_0	0.721 539 0	0.721 535 2	0.721 531 1	0.721 526 5	0.721 521 4	6
C_1	0.721 539 0	0.721 532 4	0.721 525 0	0.721 516 8	0.721 507 8	2
C_2	0.721 539 0	0.721 532 6	0.721 525 4	0.721 517 3	0.721 508 4	3
C_3	0.721 539 0	0.721 533 1	0.721 526 5	0.721 519 1	0.721 510 8	4
C_4	0.721 539 0	0.721 533 5	0.721 527 2	0.721 520 3	0.721 512 6	5
C_5	0.721 539 0	0.721 532 2	0.721 524 5	0.721 515 9	0.721 506 4	1

表 8　供应链业务信息流中断风险 R_2 的稳态变化情况（R_1 发生）

影响因素	R_2 稳态基线	−25%	−50%	−75%	−100%	变化均值
C_1	0.706 376 8	0.706 372 1	0.706 366 8	0.706 360 9	0.706 354 3	0.000 013 3
C_3	0.706 376 8	0.706 370 7	0.706 363 7	0.706 355 7	0.706 346 8	0.000 017 6
C_5	0.706 376 8	0.706 371 7	0.706 365 8	0.706 359 3	0.706 352 0	0.000 014 6

表 9　供应链信息通信设施损坏风险 R_3 的稳态变化情况（R_1 发生）

影响因素	R3 基线	−25%	−50%	−75%	−100%	变化均值
C_1	0.721 575 7	0.721 570 0	0.721 563 6	0.721 556 3	0.721 548 3	0.000 016 2
C_3	0.721 575 7	0.721 570 5	0.721 564 6	0.721 557 8	0.721 550 3	0.000 014 9
C_5	0.721 575 7	0.721 569 5	0.721 562 4	0.721 554 5	0.721 545 7	0.000 017 7

表 10　供应链主体数据资产泄露风险的稳态变化情况（R_2 发生）

影响因素	R_1 基线	−25%	−50%	−75%	−100%	变化均值
C_1	0.723 463 9	0.723 457 9	0.723 451 3	0.723 443 8	0.723 435 6	0.000 016 7
C_3	0.723 463 9	0.723 457 7	0.723 450 5	0.723 442 5	0.723 433 4	0.000 017 9
C_5	0.723 463 9	0.723 459 0	0.723 453 4	0.723 447 2	0.723 440 3	0.000 013 9

表 11　供应链通信基础设施损坏风险的稳态变化情况（R_2 发生）

影响因素	R_3 基线	−25%	−50%	−75%	−100%	变化均值
C_1	0.721 577 0	0.721 571 1	0.721 564 4	0.721 556 9	0.721 546 8	0.000 016 8
C_3	0.721 577 0	0.721 571 9	0.721 565 9	0.721 559 3	0.721 551 8	0.000 014 8
C_5	0.721 577 0	0.721 571 1	0.721 564 4	0.721 556 8	0.721 548 3	0.000 016 9

表 12　供应链主体数据资产泄露风险的稳态变化情况（R_3 发生）

影响因素	R_1 基线	−25%	−50%	−75%	−100%	变化均值
C_1	0.723 473 9	0.723 468 2	0.723 461 8	0.723 454 7	0.723 446 7	0.000 016 1
C_3	0.723 473 9	0.723 467 7	0.723 460 5	0.723 452 4	0.723 443 4	0.000 017 9
C_5	0.723 473 9	0.723 469 0	0.723 463 5	0.723 457 3	0.723 450 4	0.000 013 9

表 13　供应链业务信息流中断风险的稳态变化情况（R_3 发生）

影响因素	R_1 基线	−25%	−50%	−75%	−100%	变化均值
C_1	0.706 386 7	0.706 382 0	0.706 373 7	0.706 370 7	0.706 364 1	0.000 013 3
C_3	0.706 386 7	0.706 380 6	0.706 373 6	0.706 365 6	0.706 356 7	0.000 017 6
C_5	0.706 386 7	0.706 381 7	0.706 376 1	0.706 369 8	0.706 362 8	0.000 014 0

由表12和表13中变化均值可知,在R_3发生的情况下,抑制另外两种供应链网络安全风险的最优单策略均为管控C_3因素。

4)核心传导因子阻断的案例验证

以R_1、R_2、R_3分别作为初始发生的原生风险,验证出C_3与C_5是阻断次生风险传导的核心控制点:当R_1发生时,管控C_3对R_2抑制效果最优;当R_2发生时,管控C_5对R_3抑制效果最显著。2023年京东物流区域仓储中心POS系统信息流中断,未及时发现漏洞引发黑客入侵,导致分拣设备瘫痪,3天内订单履约延误损失860万元;2024年其投入320万元建立"信息流中断-设备巡检"联动流程,全年此类设备瘫痪事件降至1次(损失50万元内),还因履约稳定新增客户留存收益600万元,综合收益650万元(对比2023年减少损失810万元)。按公式计算ROI=(650−320)/320≈1.03,投资回报显著。该案例中"信息流中断"可对应R_2、"设备瘫痪"对应R_3、"联动流程"对应C_5管控,京东的改善策略表明管控C_5阻断R_2向R_3传导确实具有良好实际效果。

4 数智供应链网络安全风险传导防控治理启示

4.1 优化防控资源配置,精准抑制原生风险

三类原生风险(数据资产泄露、信息流中断、通信设施损坏)的诱因不同,需聚焦关键因子精准管控。其中,健全互信共享机制对抑制数据资产泄露与信息流中断最为有效,有助于降低因外部服务方介入或通信环境不安全导致的信息风险;加强安全意识和审计对通信设施损坏的抑制作用最强,通过定期评估、及时修复漏洞可有效防范攻击引发的瘫痪。优先聚焦上述核心因子,有助于提升原生风险治理效能与防控资源配置效率。

4.2 阻断风险传导路径,聚焦次生风险关键节点

互信共享机制与安全意识和审计同样是风险链中关键控制点。在不同初始风险情境中,优化前者可显著抑制数据泄露引发的信息流中断及其他次生风险,提升后者则能从全流程审计层面降低通信设施损坏的次生影响。二者作为高频传导中枢,通过干预其引发机制,可在多场景下实现高效的风险阻断,构建全链条控制闭环。

4.3 差异化精准治理,应对多重次生风险演化

原生风险往往同步诱发多个次生风险,治理策略需兼顾多重风险间的差异性与互动性。部分治理因子虽对多个次生风险具一定抑制效果,但影响程度存在显著差异,需避免"顾此失彼"。如提升安全意识与审计虽能强力抑制信息流中断,但对其他风险控制效应有限。因此应优先选取对多个风险具高抑制效力的因子,并结合风险严重度与演化趋势,动态调整干预重心,实现实时精准治理。

4.4 构建协同治理体系,强化风险全链条防控

面对风险多路径、多节点、跨层级的传导特征,单点治理难以应对复杂情境,需建立"原生风险优先+次生风险协同"机制。以互信机制建设、安全审计能力与基础设施防护为核心抓手,根据风险类型动态调整治理重心;通过因子组合策略覆盖风险诱发、扩散、传导全过程;构建风险传导监测机制,推动从静态防御向动态、主动、智能阻断转型,全面提升数智供应链的抗风险韧性与治理效能。

5 结论

本文基于文本因果关系挖掘、LDA与FCM方法,构建数了智供应链网络安全风险的复杂系统模型,识别出数据资产泄露、信息流中断、通信设施损坏三类核心风险及关键影响因素,提出原生与次生风险抑制策略,为供应链数智化管理提供了量化治理路径。但是,本文研究尚存在样本多样性不足与FCM结构优化不足等局限,后续将进一步完善。

参考文献

[1] 宋华. 人工智能数智供应链的理论探索与展望[J]. 中国流通经济, 2024, 38(1): 44-54.

[2] 聂昀秋, 马晓君, 肖潇. 中国数智供应链发展评价研究——基于CRITIC-G1法和Bonferroni算子[J]. 物流研究, 2024(2): 15-28.

[3] POURNADER M, GHADERI H, HASSANZADEGAN A, et al. Artificial intelligence applications in supplychain management[J]. International Journal of Production Economics, 2021, 241: 108250.

[4] VERIZON BUSINESS. 2024 Data Breach Investigations Report[R/OL]. [2025-08-01]. https://www.verizon.com/business/resources/reports/dbir/2024/summary-of-findings/.

[5] CARNOVALE S, SENGUN Y. Cyber security and supply chain management: risks, challenges and solutions [M]. Hackensack, USA: World Scientific, 2021.

[6] HERBURGER M. Supply chain resilience-a concept for coping with cyber risks[D]. Copenhagen: Copenhagen Business School, 2022.

[7] 杨昕然, 黄玉杰. 大数据分析能力对供应链弹性的影响——双元创新能力的中介作用[J]. 科技和产业, 2023, 23(9): 109-115.

[8] GHADGE A, WEIβ M, CALDWELL N D, et al. Managing cyber risk in supply chains: a review and re-

search agenda[J]. Supply Chain Management: An International Journal, 2020, 25(2): 223-240.
[9] MOTUNRAYO O I, DAVID O O. Cybersecurity in supply chains: addressing emerging threats with strategic measures [J]. International Journal of Management, 2024, 6(6): 2024-2047.
[10] MELNYK S A, SCHOENHERR T, SPEIER-PERO C, et al. New challenges in supply chain management: cybersecurity across the supply chain [J]. International Journal of Production Research, 2022, 60(1): 162-183.
[11] CREAZZA A, COLICCHIA C, SPIEZIA S, et al. Who cares? supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era[J]. Supply Chain Management: An International Journal, 2022, 27(1): 30-53.
[12] CHEUNG K F, BELL M G H, BHATTACHARJYA J. Cybersecurity in logistics and supply chain management: an overview and future research directions [J]. Transportation Research Part E: Logistics and Transportation Review, 2021, 146: 102217.
[13] 陈剑, 刘运辉. 数智化使能运营管理变革: 从供应链到供应链生态系统[J]. 管理世界, 2021, 37(11): 227-240.
[14] ETEMADI N, VAN GELDER P, STROZZI F. An ism modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity[J]. Sustainability, 2021, 13(9): 4672.
[15] BOYENS J, PAULSEN C, BARTOL N, et al. Key practices in cyber supply chain risk management: observations from industry [R]. Gaithersburg, Maryland, USA: National Institute of Standards and Technology, 2021.
[16] COLLIER Z A, SARKIS J. The zero trust supply chain: managing supply chain risk in the absence of trust[J]. International Journal of Production Research, 2021, 59(11): 3430-3445.
[17] PANDEY S, SINGH R K, GUNASEKARAN A. Supply chain risks in Industry 4.0 environment: review and analysis framework[J]. Production Planning & Control, 2023, 34(13): 1275-1302.
[18] 李方正, 虢毅, 陈佩璇, 等. 基于LDA的"人工智能鸿沟"多维主题分析[J]. 科技和产业, 2025, 25(12): 36-43.
[19] 陆振昇, 马超. 基于LDA模型的专利文本主题分析——以国内元宇宙领域为例[J]. 科技和产业, 2023, 23(11): 85-88.
[20] HAN H, YANG Y, ZHANG R, et al. FCM-based P2P network lending platform credit risk dynamic assessment [J]. IEEE Access, 2020, 8: 195664-195674.
[21] 高靖超, 彭丽徽, 张艳丰, 等. 在线医疗社区健康焦虑用户画像模型构建及实证研究[J]. 图书情报工作, 2023, 67(16): 124-134.
[22] PENG Z, LIU W, OH S K. AFS-FCM with Memory: a model for air quality multi-dimensional prediction with interpretability[J]. IEEE Transactions on Big Data, 2025, 11(2): 810-820.
[23] 牛衍亮, 李思远, 汪钏, 等. 基于模糊认知图的高铁企业国际声誉形成机制仿真分析[J]. 系统管理学报, 2024, 33(2): 536-546.

Inhibition Mechanism of Cybersecurity Risk Transmission in Digital-Intelligent Supply Chains

HU Muhai, FAN Jiale, ZHANG Liang
(School of Management, Wuhan Textile University, Wuhan 430200, China)

Abstract: Against the backdrop of digital and intelligent transformation, entities in the supply chain are confronted with multiple cybersecurity risks. These risks are prone to forming a cascading transmission effect through node connections, posing threats to national interests, enterprise operations, and individual rights and interests. Existing studies largely focus on single risks and qualitative analyses, lacking systematic exploration of dynamic risk propagation mechanisms, making them inadequate for addressing the complexities of supply chain operations empowered by intelligent technologies. Grounded in a thorough literature review, high-quality academic sources were selected as textual data and textual causal relationship was integtated mining with fuzzy cognitive map (FCM) modeling to construct a complex system model of cybersecurity risks in intelligent supply chains. Simulation analyses were conducted to identify risk transmission paths and evaluate suppression strategies. The results uncover the propagation mechanisms and key influencing factors of multiple core risks, and establish targeted risk suppression strategies. Both theoretical insights and decision-making support are provided for achieving precise prevention and control of cybersecurity risk propagation in intelligent supply chains.

Keywords: digital-intelligent supply chain; cybersecurity risk; risk propagation; system simulation