运营商供应链风险应对及智能预警策略研究

Suggestions for Risk Response and Intelligent Warning Strategies in Supply Chain of Operators

宁　丹，彭　雨，敖　迪，付　钰，孔繁怡（中国联通研究院，北京 100048）
Ning Dan，Peng Yu，Ao Di，Fu Yu，Kong Fanyi（China Unicom Research Institute，Beijing 100048，China）

摘　要：
通过分析运营商ICT供应链特点及风险，对标中国移动、中国电信、中国联通、AT&T 4家运营商ICT供应链现状，提出了供应链韧性与安全提升路径建议，一是开展全流程风险应对体系研究，二是开展供应链风险智能监测预警策略研究，三是优化管理流程，强化保障措施，四是推动资源整合，扩大开放合作。

关键词：
运营商ICT供应链；韧性与安全；智能监测预警
doi：10.12045/j.issn.1007-3043.2025.11.008
文章编号：1007-3043（2025）11-0041-05
中图分类号：TN915
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
By analyzing the characteristics and risks of the ICT supply chain of telecom operators，benchmarking the current situation of the ICT supply chain of four telecom operators，China Mobile，China Unicom，and China Unicom，it proposes suggestions for improving supply chain resilience and security. Firstly，the research on the entire process risk response system should be conducted. Secondly，the research on intelligent monitoring and early warning strategies for supply chain risks should be conducted. Thirdly，the management processes should be optimized，and the security measures should be strengthened. Finally，the resource integration should be promoted，and cooperation open should be expanded.

Keywords：
Operator ICT supply chain；Resilience and security；Intelligent monitoring and early warning

引用格式：宁丹，彭雨，敖迪，等. 运营商供应链风险应对及智能预警策略研究[J]. 邮电设计技术，2025（11）：41-45.

1 概述

在ICT供应链全球化背景下，供应链安全事件频发，对企业乃至国家安全、民生造成重大威胁。2020年网络管理软件供应商SolarWinds遭遇国家级APT团伙高度复杂的供应链攻击，2021年Apache Log4j2组件被曝出高危漏洞，2022年电信运营商KDDI遭遇全国性网络故障，2024年苹果M系列芯片被发现存在“Go-Fetch”漏洞，这些安全事件突显了提升供应链韧性与安全的紧迫性[1]。

运营商ICT供应链安全直接关系着关键信息基础设施安全，若运营商面临断供停服等风险，民众生活、企业运行、公共服务将遭受极为严重的影响[2]。在国内各种政策支持下，供应链安全已上升到战略层面。“十四五”规划纲要提出“建立重要资源和产品全球供应链风险预警系统”，二十大报告指出“要着力提升产业链供应链韧性和安全水平”，央企战新产业发展要求中明确提出“要建立供应链安全评估体系”，2025年国资委首次将央企采购提升到供应链战略管理的高度，同时将供应链韧性与安全纳入逐年考核。

收稿日期：2025-10-20

2 运营商ICT供应链特点及风险分析

2.1 运营商ICT供应链特点

运营商ICT供应链具有一些独特的特点，这些特

点对运营商的业务运营至关重要,并对其供应链安全管理提出了特定的要求,具体包括以下3个方面。

a)产品与服务构成复杂。运营商信息系统多,网络覆盖地域广,设备种类及构成组件、零部件繁多且分散,老旧设备参差不齐,部分网络资源、设备资源、资产台账边界不清,归属不明,未知资产仍然存在[3-4]。

b)产业链长,供应商多样且全球分布。运营商ICT产业链是一个由多个上游与下游组织相互连接形成的网链结构,供应商的开发、集成、交付地点遍布全球,且涉及全生命周期。

c)应用软件产品众多、运维服务量大。随着运营商数字化转型,已实现应用系统各专业关键业务场景全覆盖,涉及大量自研、开源、专用软件,更突出了管控源代码安全和漏洞检测等工作的重要性[5]。

2.2 运营商ICT供应链风险

运营商的ICT供应链风险主要涉及断供停服风险、攻击风险、漏洞风险、知识产权风险4类[6-7]。断供停服风险是指核心材料、高端设备与关键技术存在短板,对国外产品和供应链依赖程度较高,通信运营企业普遍面临采购量不足、甚至断供停服的风险[8]。攻击风险是指在供应链整个过程中植入恶意程序或代码,以及在制造过程中植入恶意芯片、硬件后门,导致设备被攻击或控制,整个供应链停止运行或受到严重影响。漏洞风险是指在软硬件设计或实现中存在错误或缺陷、开源漏洞等导致敏感信息泄露、系统被入侵、服务中断等后果,而对供应链产生严重负面影响[9]。知识产权风险是指违反许可协议,侵犯专利或软件著作权等。

3 主要运营商ICT供应链风险应对措施

中国移动针对5G、传输、IT、基础软件等关键领域,梳理技术卡点图谱,并建立全面风险信息库和常态化供应链安全分析跟踪机制,覆盖供应链管理各主要环节;定期收集分析上游供应链信息,持续开展风险识别与动态评估;根据产品特点和供应风险实际情况,主动防范各类供应风险;建立常态化供应链安全分析跟踪机制,做好分析研判;定期开展供应链安全专题分析,预警相关产品供应风险并制定有效措施。

中国电信围绕构建新发展格局,深化创新链、产业链、供应链“三链”融合发展,建立供应链风险分析平台,大力推进供应链数字化转型;对风险事件及相关供应链信息实时动态风险评估;根据评估模型来判定产品的供应风险等级,制定具体的应对策略;强化软件供应链管理,建立SBOM态势分析平台,实时监测软件;建立关键产品供应链风险综合评估预警机制,完善供应链应急响应机制。

中国联通利用AI、大数据、物联网等技术,推进供应链全环节智慧化提升,建立采购与供应链内控风险管理体系,对内控风险进行识别;构建“集团+分子公司”两级供应链风险评估机制;定期组织各专业线开展风险分析,针对突发事件开展风险研判和策略调整;对内控风险偏高等行为进行实时监督、预警与管控,依托平台开展在线检查;建立在线预警中心,对内控风险进行预警并制定对应措施。

美国AT&T采用全面的风险管理框架,涵盖供应链风险的识别、评估和应对;具有完善的风险评估机制和实践,确保供应链安全可靠;制定详细的应急预案,缓解各种风险;利用AI和机器学习技术监控和管理供应链风险,快速识别和响应潜在威胁;使用先进技术分析供应链数据,预警潜在风险。

综上,通过对4家运营商对标分析发现,供应链风险应对和监测预警是关注重点,国内运营商在全流程风险应对和智能监测预警方面存在薄弱环节,需要进一步提升。

4 运营商ICT供应链韧性与安全提升路径建议

针对国内运营商ICT供应链薄弱环节,提出供应链韧性与安全提升路径建议,一是开展全流程风险应对体系研究;二是开展供应链风险智能监测预警策略研究;三是优化管理流程,强化保障措施;四是推动资源整合,扩大开放合作。

4.1 开展全流程风险应对体系研究

4.1.1 风险识别

开展风险识别,首先进行资产识别,梳理ICT供应链中的所有资产,形成资产库,其次厘清ICT供应链全生命周期的各个风险点,构建风险库,最后构建硬件产业链供应链图谱和软件构成图谱,并精确关联资产库和风险库,增强供应链的可追溯性、可审计性[10]。

a)资产识别。通过利用数字化、智能化手段,面向业务和场景,将软硬件产品拆分成各个部件、组件,系统性梳理ICT供应链中的所有资产,形成资产库,包括硬件设备、软件应用、数据资源、服务等,每项资产收集详尽的信息,如型号、版本、供应商信息、采购日

期、保修期限、安全特性、软件许可证状态等。资产识别是供应链透明度和效率的基础，有助于提高运营效率、降低成本、增强风险管理能力，并支持更好的战略决策[11]。

b）构建风险库。通过多维度数据交叉分析，厘清ICT供应链全生命周期的各个风险点，形成风险库，并定期对风险库进行更新，涉及规划设计阶段、生产供应阶段、仓储物流阶段、运维退服阶段的风险，并且按照供应商风险、技术风险、漏洞风险、攻击风险、许可证风险等不同类别构建风险库。风险库可以帮助运营商更好地管理供应链中的不确定性和潜在威胁，降低潜在风险对企业运营的影响[12]。

c）构建图谱。在梳理现有资产台账和风险库的基础上，构建硬件产业链供应链图谱，并针对软件产品构建软件构成图谱。通过构建图谱可以清晰地展示整个供应链中各个环节和参与者之间的关系和依赖，并且随着市场环境变化，定期更新图谱。

硬件产业链供应链图谱是面向重点业务重点品类的产业链多级供应关联图谱，包括传输/承载网、无线网、核心网、云计算、网络设备、光通信、服务器/计算机等产业链，涉及一二三级供应商，并将资产库和风险库精确关联，增强供应链的可追溯性（见图1）。

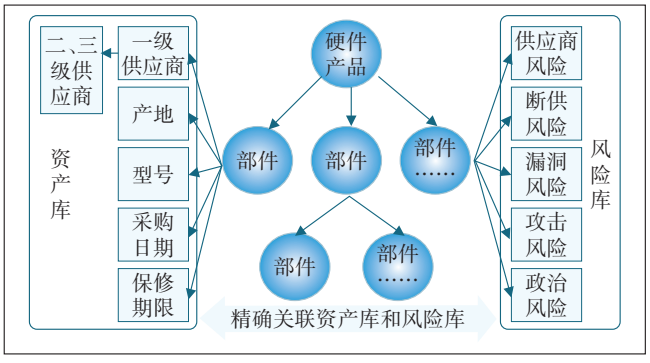

图1　硬件产业链供应链图谱

软件构成图谱是利用软件成分分析SCA技术和SBOM资产分析技术形成的图谱，包括物料清单信息、软件信息、组件信息等，并且依赖漏洞知识库、许可证知识库来识别开源组件的漏洞和许可证风险，将识别出的风险和组件精确关联，实现风险溯源（见图2）。

4.1.2　风险评估

风险评估分为2个部分，一是对风险库中的风险点进行评估，从风险发生概率和风险发生后造成的影响2个维度来评估供应链风险，构建风险三色矩阵；二是基于产品评估模型对软硬件产品进行评估，评估出

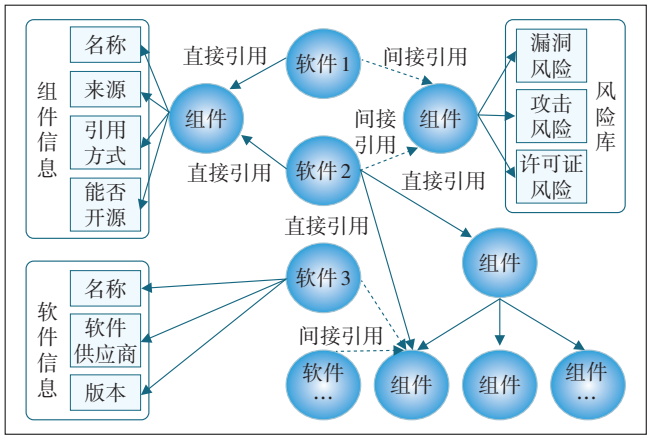

图2　软件构成图谱

五级风险产品，形成风险产品分级目录[12]。

评估风险点首先要进行风险概率分析，通过演绎分析，识别危险事件的成因，根据统计分析、德尔菲法（Delphi Method）等方法以及专家判断，预测危险事件的频率；然后进行风险影响评估，识别所有由危险事件引起的潜在后果，综合考虑多维度因素，找出所有可能的最终结果；最后结合供应链风险概率和风险影响评估结果，对风险进行高中低排序，构建风险矩阵。

如图3所示，评估产品要首先构建产品评估模型，依托资产库确定评估指标的范围，包括供应商、产品研发情况、知识产权、设计服务商、生产服务商、封测服务商等；其次对评估指标进行分级设计，包括一级评估指标、二级评估指标，在一级评估指标基础上进行细化，并分档设计指标数值和权重，计算出软硬件产品风险数值，量化产品供应风险。

最后依据产品评估模型，按照M1、M2、M3、M4、M5共5个等级对产品进行分级，形成风险产品分级目录，帮助运营商更好地管理其产品组合中的风险水平，从而提高整体的风险管理能力（见表1）。

4.1.3　风险应对

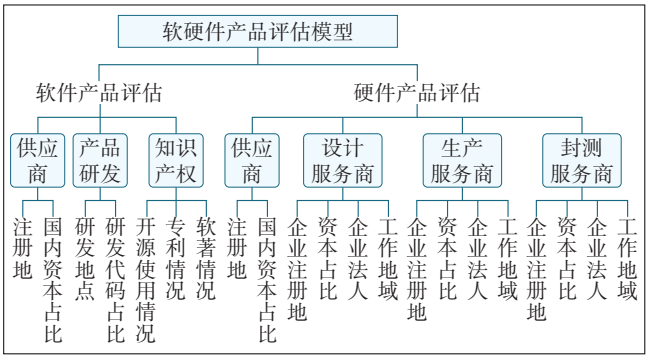

图3　软硬件产品评估模型

表1　风险产品分级目录

风险分级	硬件产品	软件产品
高	硬件1	软件1
中	硬件2	软件2
低	硬件……	软件……

风险矩阵中将风险分为高中低3类,针对低风险,无需采取额外控制措施,持续监视使风险水平得以维持现状;针对中风险,需要尽快采取控制整改措施,对风险进行控制,努力降低风险发生概率和影响;针对高风险,必须制定措施进行重点控制管理,积极调度各种资源,协同制定风险应对措施。

基于风险矩阵制定应对策略,采取的风险应对策略包括:风险规避策略,通过彻底改变供应链的某些方面来避免风险的发生,建立多供应商体系,避免与高风险供应商合作;风险转移策略,通过合同协议或保险解决方案将风险从一方转移到另一方;风险减轻策略,通过提高库存水平作为应对供应中断的预防策略;风险接受策略,对于低风险或可接受的风险不采取额外措施。

风险产品分级目录中M5、M4级风险产品容易出现技术故障,或者依赖单一供应商、依赖政治经济不稳定地区的供应商,断供风险很高;M3、M2级风险产品的供应链存在一定程度的不确定性,供应商较为集中或市场波动较大;M1级风险产品,供应商多元化,供应链相对稳定。

基于风险产品分级目录制定应对策略,针对M5~M2级风险产品,采取分级分类战略储备,确保极限情况下的关键产品和服务供应稳定,保障基础通信服务。同时针对软件产品建立安全态势分析平台,通过平台实时监控软件供应链,检测异常活动和潜在威胁,及时处理发现的漏洞和安全问题,减少潜在的供应链攻击和数据泄露风险,从源头上控制,避免安全风险。运营商还需要持续提高国产化设备采购占比,促进本土技术创新和产业发展,增强自主可控能力。

4.2 供应链风险智能监测预警策略研究

深入研究供应链风险智能监测预警策略,整合企业内部数据和外部数据,实时监测ICT供应链各个环节,应用人工智能算法模型,实现智能预警风险,同时进一步分析预警风险在图谱上的影响路径,实现供应链的智能风险溯源,最后进行预警反馈,形成风险监测预警闭环机制。

首先,整合企业内部数据(如ERP企业资源计划、SCM供应链管理系统、图谱平台数据等)和外部数据(如市场动态、供应商情况、交通情况、地缘政治事件等),利用大数据分析技术和物联网技术,实时监测ICT供应链各个环节,持续跟踪供应链中的关键指标和事件。

然后,结合区块链技术和大模型AI技术等,在产业链供应链图谱上应用人工智能算法模型,结合历史数据和实时数据进行预测和模拟分析,及时发现异常情况和潜在风险,实现智能预警;预测风险事件的发生概率和影响,设定高中低不同的预警等级,根据风险的紧迫性和严重程度采取相应的应对措施。

其次,利用风险规则、图计算等方法进一步分析预警风险在图谱上的影响路径,确定图谱中受影响的节点或产品,实现供应链的智能风险溯源,并对事件引起的风险进行分析,有效提升产业链供应链的自主性、可持续性和韧性。

最后,收集和分析风险事件以及预警反馈,评估预警系统的准确性和有效性,不断改进模型和策略,形成风险监测预警闭环机制[7]。

4.3 优化管理流程,强化保障措施

4.3.1 完善组织架构

为了全面加强供应链安全风险管理工作,首先需要组建一级供应链安全联合管理机构,构建以公司总经理为主导,采购供应链部门、需求部门、财务部门等多部门联动的组织架构,全面加强供应链安全风险管理工作,从公司层面建立统一高效的风险管理组织体系,组织协调风险管理日常工作;然后组建二级供应链安全管理小组和分子公司二级组织,负责日常供应链安全风险的监测和管理,及时上报重大风险;此外还应组建供应链安全智库研究团队,依托公司研究机构建立供应链安全研究团队,紧跟党中央在供应链方面的决策部署与公司发展战略,持续推动供应链战略规划编制、评估与调整,开展专项技术攻关和课题研究。

4.3.2 推动闭环管理

为推动供应链战略规划闭环管理,应紧跟党中央在供应链方面的决策部署与公司发展战略,制定公司的供应链战略,确保与国家战略和政策相一致。同时,要持续推动供应链战略规划实施、评估与调整,将供应链战略规划转化为具体的行动计划。此外,还需按照供应链成熟度模型评估企业供应链安全成熟度,衡量企业在供应链安全管理方面的发展水平和能力[3]

（见图4）。

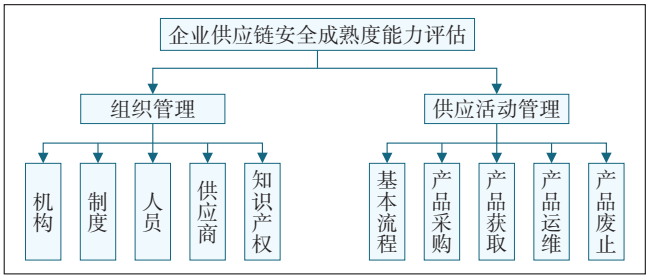

图4　企业供应链成熟度评估模型

4.4 推动资源整合，扩大开放合作

在当今全球化的背景下，推动资源整合和扩大开放合作是运营商提升供应链安全的重要举措。通过采用多元备选采购策略，分散安全风险，适当增加ICT产品备选芯片方案，从源头出发，从网络结构设计阶段出发，提升网络结构和ICT产品之间的耦合性；坚持供应商多元化策略，通过推进工厂的多地区分布，缓解限电、疫情、自然灾害等突发情况导致的无法生产和供应的风险，减少独家供应商和生产基地单一的供应商，根据市场形势可增加中标供应商数量，构建和健全关键产品多元供应商体系，持续提升供应链的连续性和稳定性[10]。

同时，要持续提升战略储备管理机制：对战略物资储备存储数量、轮换周期、资金保障、预警分析、统计报告等方面进一步优化升级；根据安全、应急形势及物资生产、流通能力的变化，应及时调整实物储备的品种、规模、布局；充分考虑物资的供应时效、需求强度、市场容量等因素，合理确定具体储备方式；加强对储备物资的计划、采购、仓储、轮换等环节的管理，及时调整品种、类别以及储备方式，以确保随时发挥应有的作用。

此外，应打造长期深度合作的战略伙伴，积极主导供应链生态：以长期稳定的协同关系取代短期利益，发挥供应链一体化的效率优势和成本优势。运营商还应发挥“链长”作用，促进产业升级：利用通信企业在产业链、供应链中的特殊地位，发挥好“链长”作用，充分发挥“链长”企业在供应链、产业链中强大的带动能力和整合能力，引领促进上下游中小企业协同共荣发展。

5 结论

在ICT供应链安全管理的新时代背景下，运营商作为国家关键信息基础设施的守护者，必须采取前瞻性、系统性、创新性的策略来应对日益增长的供应链风险，通过开展全流程风险应对体系研究和供应链风险智能监测预警策略研究，优化管理流程以及推动资源整合这4个方面的实施强化，提升供应链的安全性和韧性，确保国家通信安全，确保社会公共利益得到坚实保障。

参考文献：

[1] SOLDANI D. 5G and the future of security in ICT[C]//2019 29th International Telecommunication Networks and Applications Conference (ITNAC). Auckland:IEEE,2019:1-8.

[2] LU T B,GUO X B,YAO P X,et al. A framework for standardization of ICT supply chain security[C]//ZHANG R T,ZHANG Z J,LIU K C,et al. LISS 2013. Berlin:Springer,2015:1121-1126.

[3] MIN S H,SON K H. Comparative analysis on ICT supply chain security standards and framework[J]. Journal of the Korea Institute of Information Security & Cryptology,2020,30(6):1189-1206.

[4] NORRIS W,RODGERS J B,BLAZEK C,et al. A market-oriented approach to supply chain security[J]. Security Challenges,2020,16(4):65-81.

[5] 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术 ICT供应链安全风险管理指南：GB/T 36637-2018[S]. 北京：中国标准出版社，2018.

[6] GURTU A,JOHNY J. Supply chain risk management:literature review[J]. Risks,2021,9(1):1-16.

[7] TUMMALA R,SCHOENHERR T. Assessing and managing risks using the supply chain risk management process (SCRMP)[J]. Supply Chain Management,2011,16(6):474-483.

[8] 王佳硕，程建宁，朱敏，等. 通信运营企业ICT供应链安全风险预防及应对策略研究[J]. 供应链管理，2023，4(7)：25-36.

[9] 韩晓露，段伟伦，吕欣，等. 5G供应链安全风险分析与对策研究[J]. 信息安全研究，2021，7(12)：1178-1183.

[10] 李璐，倪平，何昊坤，等. ICT供应链安全风险及典型事件分析[J]. 国防科技工业，2019(9)：24-26.

[11] 徐绪松，曾学工，郑小京. 供应链风险管理研究综述--风险识别[J]. 技术经济，2013，32(5)：78-86，120.

[12] 姚小华，薛富国. 通信运营商ICT一体化供应链建设与创新应用[J]. 中国市场，2024(2)：171-174.

作者简介：
宁丹，毕业于西安电子科技大学，工程师，硕士，主要从事信创生态及供应链风险应对研究等工作；彭雨，毕业于北京邮电大学，高级工程师，硕士，主要从事信创生态及供应链风险应对研究等工作；敖迪，毕业于北京邮电大学，工程师，硕士，主要从事信创生态研究、数据治理等工作；付钰，毕业于北京工业大学，工程师，硕士，主要从事信创生态研究、数据治理等工作；孔繁怡，毕业于英国布里斯托大学，工程师，硕士，主要从事信创生态及供应链风险应对研究等工作。