 DOI: https://doi.org/10.12349/iser.v6i10.7894

Research on software supply chain security governance: From European and American new regulations to China's development path

Wenqiang Lu

Shanghai Digital Security Technology Co., Ltd., Shanghai, 200072, China

Abstract

This paper focuses on software supply chain security governance, analyzing regulatory developments in Europe and the United States. Key references include U.S. executive orders, NIST documents, the Software Bill of Materials (SBOM) initiative, the Open Source Software Act, and multiple EU legislative directives. The study explores how Western practices can inform China's approach, including establishing regulatory bodies, promoting SBOM adoption, and enhancing open-source vetting mechanisms. It outlines China's current applications and future strategic roadmap for critical technologies, encompassing strengthening strategic positioning, improving legal frameworks, advancing standardization, and leveraging emerging technologies to build monitoring systems. These insights aim to provide comprehensive guidance for elevating China's capabilities in software supply chain security governance.

Keywords

software supply chain; security governance; strategic planning

软件供应链安全治理研究：从欧美新规到我国的发展之路

陆文强

上海数字安全科技有限公司，中国 · 上海 200072

摘　要

本文聚焦于软件供应链安全治理，分析了欧美相关法律法规动态，包括美国的行政令、NIST 文件、SBOM 推行、开源软件法案，以及欧盟的多项法案指令。探讨了欧美经验对我国的启发，如构建管理机构、推广 SBOM、强化开源审查等。阐述了我国在关键技术方法上的应用及未来战略布局，包括强化战略地位、完善法律法规、推进标准化、借助新技术构建监控体系等，旨在为我国提升软件供应链安全治理水平提供全面参考。

关键词

软件供应链；安全治理；战略布局

1 引言

随着全球数字化进程加速，软件供应链安全已成为国际网络安全治理的重点议题。软件供应链不仅支撑企业核心业务运行，更是关键信息基础设施安全的基石。然而，全球化背景下的高度互联，使得软件供应链的风险不断显现。近年来的典型案例，如“SolarWinds 事件”“Codecov 供应链攻击”等，暴露了开源组件、第三方库与软件依赖在全球范围内可能引发的连锁安全危机。

针对这一挑战，欧美国家相继出台政策法规并推动技术框架建设，强化软件供应链安全治理。其中，美国通过行政令设立供应链治理机构，发布 NIST 标准框架并强制推广 SBOM；欧盟则出台《网络弹性法案》、实施 NIS2 指令并推动开源软件治理与市场透明化。这些措施不仅提高了供应链透明度和合规性，也为全球软件安全治理提供了参考模型。

我国当前软件供应链治理仍处在快速发展阶段，法律法规、标准体系和技术手段正在逐步完善。借鉴欧美经验，结合我国的产业格局和安全需求，构建适应本土环境的治理体系显得尤为紧迫和必要。

2 欧美软件供应链安全法律法规最新动态

2.1 美国

2.1.1 行政令设立白宫供应链弹性委员会

2024 年 6 月 14 日拜登签署行政令成立该委员会，由国家安全事务助理和经济政策助理共同领导，多部门参与。其使命是提升供应链韧性与安全治理，每四年全面审查供应链安全，首份报告将于 2024 年 12 月 31 日提交，涵盖软件供应链各环节风险评估。

【作者简介】陆文强（1989–），中国上海人，本科，从事网络与数据安全、软件供应链相关研究。

2.1.2 NIST SP 800 - 161r1 的发布

美国国家标准与技术研究院（NIST）发布该框架文件，为企业提供系统的供应链安全管理参考。内容涵盖风险识别、供应商管理与监控等，特别强调对第三方供应商的资质与安全能力进行审查，并建立持续的风险监测机制，从而推动企业由被动防御转向主动治理。

2.1.3 软件物料清单（SBOM）的推行

基于 NIST 框架，美国政府积极推动 SBOM 在联邦政府及关键行业中的应用。美国管理和预算办公室（OMB）和网络安全与基础设施安全局（CISA）发布文件，要求软件供应商在产品交付时提供完整的组件清单，帮助企业在漏洞披露后快速定位风险组件，提升供应链的透明度与可追溯性。

发布《保护开源软件法案》

2023 年，美国出台《保护开源软件法案》，明确要求企业在使用开源软件时对其依赖包进行全面安全评估，限制高风险依赖的使用，并建立漏洞响应机制。该法案凸显了开源软件安全在供应链治理中的特殊地位，推动了企业对开源生态安全性的重视。

2.2 欧盟

2.2.1 《网络弹性法案》（CRA）

2023 年 9 月，欧盟通过《网络弹性法案》，这是欧盟首部针对 ICT 产品安全的强制性法律。法案要求在欧盟市场销售的 ICT 产品（包括软件）必须具备可追溯性，制造商需提供完整的安全信息并保证产品生命周期内的持续安全维护。这一法规不仅对欧盟内部企业具有约束力，也影响所有向欧盟出口 ICT 产品的外国企业。

NIS2 指令的实施

NIS2 指令作为 NIS1 的升级版，强化了企业在开源组件审查与供应商资质管理方面的义务。指令要求企业对所使用的开源组件进行合规审查与风险评估，并定期提交安全合规报告，展示其供应链安全措施与风险控制机制。

2.2.2 开源软件治理与跨国信息共享

欧盟网络安全局（ENISA）推动建立统一的开源软件治理标准，并鼓励跨国信息共享机制，减少因信息不对称造成的供应链风险。这种机制不仅提升了漏洞披露的效率，也加强了跨成员国的风险联动防御。

2.2.3 数字市场法案（DMA）和数字服务法案（DSA）

DMA 和 DSA 要求大型平台企业对其数据安全性和供应链透明度负责，确保供应链中的第三方组件符合合规要求。两部法案共同为欧洲数字市场的安全与合规奠定了基础，也为全球数字治理提供了制度化的范例。

3 欧美供应链安全治理对我国的启发与借鉴

3.1 构建国家级供应链安全管理机构，统筹跨部门协同治理

美国通过设立白宫供应链弹性委员会将供应链治理提升至国家战略高度，而欧盟通过网络安全局（ENISA）在成员国之间推进统一的治理标准和政策。这表明供应链安全治理不仅需要立法支持，还需有效的多部门协作和信息共享。

我国可以在国家层面统筹供应链安全治理，设立供应链安全委员会或领导小组，作为政策制定和协调的核心机构。该机构由网络安全、工业和信息化、商务等多个部门共同参与，负责制定和协调供应链安全的政策、法规和标准，并在应急事件发生时快速调度资源响应，减少信息孤岛，提升系统性和应对效率。

3.2 推动软件物料清单（SBOM）的标准化应用，提升供应链透明度

美国在推动 SBOM 的广泛使用方面取得显著进展，SBOM 不仅提升了软件供应链的透明度，也为快速响应漏洞提供了支持。我国可以将 SBOM 作为供应链透明化管理的重要工具。

通过标准化建设和行业引导，在国内推广 SBOM 的应用。相关监管部门可要求关键基础设施运营商、政府采购和金融机构等行业强制使用 SBOM，以确保供应链的可视化和可追溯性。同时，推动 SBOM 在供应商合规审查中的应用，帮助企业快速识别和排除高风险组件，从而提升企业在国际市场上的竞争力和信誉。

3.3 强化开源软件的安全审查机制，增强自主控制能力

欧美在供应链治理中对开源软件使用提出了严格的安全审查要求。我国可以进一步完善开源软件治理机制，强化对开源软件的安全管理。

建议设立开源软件安全管理和评估机制，结合供应商资质审核、开源代码审查和使用准入制度，确保供应链中开源软件的安全性。通过强制审查关键领域的开源代码，限制高风险开源软件的应用，鼓励本土企业在核心技术上使用自主研发的解决方案，以减少对外部高风险组件的依赖，推动国内软件产业创新。

3.4 建立跨部门情报共享平台，提升供应链动态风险识别能力

欧美高度重视信息共享。欧盟的 NIS2 指令和网络弹性法案鼓励成员国建立信息共享机制，美国的 CISA 设立了威胁情报共享平台，帮助企业应对网络威胁。

我国可在国家层面设立跨部门情报共享平台，整合公安、网信、工信、市场监管等多部门的数据资源，实现供应链中安全情报的实时交换。跨部门情报共享机制不仅能提升风险预警能力，还能在突发事件中提高应对速度，帮助企业迅速获取和共享最新的安全威胁信息，有效降低风险扩散。

3.5 引入零信任架构，增强供应链各环节的动态防护

零信任架构在欧美供应链安全框架中越来越重要，通过多因素认证、动态权限管理等手段，有效防止未经授权的访问，从而保护供应链的各个环节。

我国可以借鉴零信任架构，通过多重验证机制和精细化权限控制，确保各环节安全。特别是在关键基础设施和数字经济的核心供应链中，零信任架构可提供动态、全方位的安全防护，降低供应链安全风险。此外，还能帮助企业实现细粒度的

访问控制和实时监测，使供应链防护更加精准和高效。

4 未来发展方向与我国的战略布局

4.1 强化供应链安全管理的国家战略地位

软件供应链安全是国家数字安全体系的重要组成部分，直接影响我国信息基础设施的安全稳定运行和重要产业链的自主可控能力。今后要在国家层面上确定软件供应链安全的顶层设计和发展目标，在组织上建立跨部门协调的决策机构，构建由国家统领、行业共治、企业主体参与的三级软件供应链安全治理体系，从国家级高度统筹，推进治理政策、监管举措和产业实践三位一体的协同融合。其次，在重大信息基础设施、重点软件系统、重要服务型平台等重要的应用场景中，建设运行软件供应链动态安全评估与响应体系，做到对可能存在的安全风险和威胁能及时发现、及时报告与处置，确保整个安全工作的前瞻性与准确性。

4.2 完善法律法规，提升合规性

针对当前我国软件供应链安全管理体系中存在的法规碎片化与责任边界模糊问题，应当利用《网络安全法》《数据安全法》确立的法律体系框架建立覆盖全流程、全主体的法律体系。并针对我国相关实践经验，在参考欧盟《网络韧性法案》和美国《国家供应链安全战略》的基础上，进一步明确软件开发、测试、分发以及运维等各环节的具体安全标准和合规要求，加强重点环节监管和安全审计。此外，鼓励企业健全合规自评和外部评估双重机制，实现可溯源、可量化的安全责任追责链路。以法治之手压实政府监管、行业组织、企业主体三个方面的安全责任，使安全标准有法必依、违法必究，杜绝隐患滋生，是完善供应链安全治理体系的关键。

4.3 推进供应链标准化，构建全球竞争力

达成供应链安全的标准统一有助于打造国外互信、技术互通的基础条件，这就要求加快健全符合我国本土产业生态的安全标准体系，包括代码审查，漏洞响应、版本控制和开源软件管控在内的各方面标准。一方面深度参与 ISO/NIST 等国际组织规则制定，把国内标准向 ISO/IEC/NIST 等国际组织推动和争取互认互通，提高中国在全球软件安全治理格局当中的影响。另一方面利用国家级重点实验室或产业联盟搭建起软件供应链安全评估认证体系，促进技术创新与标准体系建设协同发展。以标准化治理帮助企业获得国际市场上的安全信誉优势、竞争地位，形成本领更强的以标准为引路、技术为驱动的安全生态优势。

4.4 借助 AI 和大数据技术构建智能化监控体系

4.4.1 数据采集与整合层面

软件供应链各个环节部署采集终端，对代码开发、依赖管理、版本更新、组件调用以及运行日志等数据进行采集并实现实时同步，利用统一的数据采集平台构建跨平台的数据采集框架，形成本地源代码库 - 构建环境 - 部署节点 - 使用端的全链路数据流，把采集来的代码文件、依赖关系、版本管理信息等信息转化成结构化、非结构化数据。并利用图数据库形成一张供应链的数据图谱，明确各个节点的依赖关系、数据流向，为后续安全分析与风险判定提供可视化参考。

4.4.2 风险评估与预警层面

基于深度学习和关联分析的方法，建立了考虑组件来源可信度、漏洞传播路径、版本依赖性风险及代码完整性风险等多方面的风险量化评估模型。并且引入时间序列分析及异常检测机制，依据模型检测结果设置风险阈值，实现了风险态势自适应变化。同时，模型检测到异常波动或者风险聚集信号后可直接触发分等级预警，将详细的危险信息及关联指标通过多渠道反馈给用户。

4.4.3 智能决策支持层面

根据预警结果、风险模型以及运用人工智能的算法对于不同的应对策略进行了仿真与多场景的推演，并对措施的实施可能产生的效果以及耗费资源等进行计算分析，自动形成优化建议并与已有预案库对比后，选择最优策略快速匹配执行。在突发事件发生时，系统能够进行自动化的决策辅助工作，通过可视化指令链完成跨部门的联动响应，缩减决策时间。通过对数据不断回溯与场景模拟不断地优化改进，从而不断完善系统自身的动态响应能力，形成具有高度扩展性的智能化应急体系。

4.4.4 协同管理与优化层面

借助云架构建立供应链安全协同管理平台，拆解部门之间、企业之间以及不同区域之间的信息障碍，同步安全事件、数据分析结果及应急处理方式，并且根据 AI 算法优化引擎，持续优化供应链各节点的运行效率、安全防护等级、数据流路径，形成资源调度和风险防范相结合的联动机制。并且根据大数据分析技术挖掘出企业的管理短板和流程冗余，为软件采购、代码更新和组件维护等工作提供改进建议。

5 结语

在全球化数字经济环境下，软件供应链安全不仅关乎企业运营与产业竞争，更直接关系到国家安全与战略自主。欧美在法律法规、治理模式和技术框架上的探索，为我国提供了宝贵经验。我国应立足本土需求，结合国际经验，逐步构建透明化、合规化、智能化的软件供应链安全体系。通过制度、标准与技术的协同发展，实现“全链路可视、全过程可控、全生态可信”，在有效防范风险的同时，为数字经济的持续健康发展提供坚实的安全保障。

参考文献

[1] 余建利,姜荣霞,卢蓉.电信运营商开源软件供应链安全治理探讨[J].网络安全与数据治理,2023,42(01):67-71+85.DOI:10.19358/j.issn.2097-1788.2023.01.009.

[2] 苏俐竹,徐雷,郭新海,等.国内外软件供应链安全现状分析与对策建议[J].邮电设计技术,2022,(09):24-26.DOI:CNKI:SUN:YDSJ.0.2022-09-006.

[3] 张小梅,苏俐竹.基于DevSecOps的软件供应链安全治理技术简析[J].邮电设计技术,2022,(09):13-18.DOI:CNKI:SUN:YDSJ.0.2022-09-004.

[4] 董国伟.从美行政令看软件供应链安全标准体系的构建[J].中国信息安全,2022,(02):84-87.DOI:CNKI:SUN:CINS.0.2022-02-012.