

Conceptual Framework for The Protection of Critical Information Infrastructure Against Supply Chain Threats

Ozogwu Young¹, Victor Kulugh², Ayaeze Paul¹, Ajishe Oyelola¹, Achimugu Andrew¹, Akiga Jessica¹, Akinremi Soji¹,
Nwokocha Patrick¹, Idris Muhammad¹, Ahiaba Moses¹

¹ Centre for Cyberspace Studies, Nasarawa State University, Keffi (NSUK)

²Department of Cybersecurity, Bingham University, Karu, Nigeria

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.1408000128>

Abstract: The backbone of modern economies relies heavily on Critical Information Infrastructure (CII). It helps to provide critical services in the energy, finance, telecommunications, health, and transportation sectors. This growing dependence on third-party vendors, software applications, and supply chains, has exposed CII to formidable cyber risks. Recent attacks like SolarWinds, NotPetya, and Colonial Pipeline show how damaging supply chain cyber-attacks can be. They threaten both national security and economic stability. This paper hence presents a general conceptual framework that protects CII against supply chain threats. Anchored on the DSR approach, the paper synthesizes some of the literature on prior cybersecurity frameworks, models of supply chain risk, and resilience strategies. The proposed framework integrates three layers: Risk Identification, Governance and Compliance, and Resilience and Response. These layers introduce AI-driven threat detection, ZTA, secure procurement policy, and automated mechanisms for incident response. A comparison of major cybersecurity frameworks such as NIST CSF, ISO/IEC 27001, C-SCRM, and the EU NIS2 Directive shows important gaps in risk assessment, regulation, and resilience strategies. The study therefore contributes to both the academic fraternity and industry practices through the presentation of a structured, adaptive model in mitigating evolving supply chain cyber risks. Future research on empirical validation, cross-border regulatory harmonization, and real-time risk quantification models will be useful in further enhancing global CII resilience.

Keywords: Critical Information Infrastructure (CII), Supply Chain Threat, Cyber Supply Chain Risk Management (C-SCRM), Zero Trust Architecture (ZTA), Threat Intelligence Monitoring

I. Introduction

Background and Context

Critical Information Infrastructure has an ever-growing trend of becoming more vulnerable to hostile cyber-attacks; this trend is happening through the digital supply chain. According to Weiß (2023), CII consists of important systems related to national security, public health, financial services, telecommunications, and critical infrastructure networks. The said infrastructures are using highly complex supply chains that integrate third-party software providers, cloud computing services, and contractors.

While the digitization of supply chains ensures more efficiency, it also generates more vulnerabilities exploited by cybercriminals and state-sponsored hackers. Attackers have breached supply chains through the use of:

- malware-infected software updates,
- stolen third-party vendor credentials,
- unauthorized access to cloud-based infrastructure.

Global incidents from such cyber-attacks are driving up the demand for an organized framework that will defend the supply chain of CII against emerging threats.

Problem Statement

The existing cybersecurity frameworks, which include NIST CSF, ISO/IEC 27001, and the EU NIS2 Directive, have presented risk management but have fallen short, particularly with aspects of supply chain security within CII (Henriksson, 2021). Some of these spheres are;

1. Inadequate Risk visibility, Organizations will not be able to track third-party and fourth-party suppliers (Brucherseifer et al., 2021)
2. Fragmentation of Regulation-this refers to the reality that policies on cross-border cybersecurity are not uniform across multinational supply chains (Henriksson, 2021).
3. Slower incident response - Organizations depend on manual response mechanisms, which make mitigation efforts take longer to happen (Giannopoulos et al., 2023).
4. There is a need to have a comprehensive framework that ties together cybersecurity governance, AI-based risk assessment, and automated resilience strategies (The White House, 2021).

Research Objective

The objective of this research is to develop a structured conceptual framework that enhances the protection of CII against supply chain threats by integrating cyber risk management, governance policies, and resilience mechanisms.

II. Literature Review

Due to growing cyberattacks on global supply chains, security for Critical Information Infrastructure (CII) has gained increased importance. The increasing reliance of businesses on third-party vendors, cloud services, and outsourced software providers due to rapid digital transformation across industries increases the vulnerability of CII to supply chain threats. Cyber adversaries use supply chain weaknesses to launch ransomware, malware injection, data breaches, and nation-state espionage attacks (Weiß, 2023).

Different existing cybersecurity models, such as the NIST Cybersecurity Framework, ISO/IEC 27001, Cyber Supply Chain Risk Management, and Zero Trust Architecture, assure partial security. However, all these models generally aim at broader cybersecurity risk management and hence do not precisely address supply chain-specific security challenges in CII (The White House, 2021). This section will critically analyze various existing cybersecurity frameworks, supply chain security challenges, governance models, and resilience strategies, drawing on the strengths and limitations of each model.

Cybersecurity Models for CII Protection

Several cybersecurity models have been developed for mitigating cyber risks in supply chains regarding CII. Among those mostly in application are the NIST Cybersecurity Framework, ISO/IEC 27001, Cyber Supply Chain Risk Management, and Zero Trust Architecture.

NIST Cybersecurity Framework

The NIST introduced the CSF to organize and manage approaches on risk identification, mitigation, and response. The framework contains five core functions, which are identification, protection, detection, response, and recovery (NIST, 2018). Because of the flexibility, scalability, and a risk-based approach in the application, the framework finds wide applications in many industries.

While the NIST CSF is a great overall tool for cybersecurity management, it does not address the CII supply chain risk. As the Framework states, organizations assume internal control when developing policies related to cyber security; in practice, though, many CII operators rely on outsourcing third-party services with core functions of IT. In the absence of a supply chain risk management module, NIST CSF is inadequate to deal with supply chain-specific threats such as software supply chain attacks, third-party misconfigurations, and supplier credential compromises (Giannopoulos et al., 2023).

ISO/IEC 27001 and Supply Chain Security

The globally recognized standard of ISO/IEC 27001 is for ISMS that emphasizes risk-based cybersecurity governance. This gives an overall set of controls to offer data protection, compliance enforcement, and security audits. As per ISO 2021, the standard covers Annex A.15, which deals with the best practices on supply chain management. This lays down third-party security assessment.

Despite its structured approach, ISO/IEC 27001 has limitations when applied to dynamic, cross-border supply chains in CII. ISO/IEC 27001 is costly, which makes it hard for SMEs and third-party vendors to adopt (Henriksson, 2021). It also lacks real-time monitoring, since it relies on periodic audits that may not keep up with fast-changing cyber threats in CII supply chains (Weiß, 2023).

Cyber Supply Chain Risk Management (C-SCRM)

The C-SCRM model, created by CISA, focuses on assessing third-party risks and securing procurement. It provides best practices for evaluating supplier security policies, enforcing cybersecurity clauses in contracts, and monitoring vendor compliance (CISA, 2020).

C-SCRM is good to apply when it comes to assessing third-party and fourth-party risks, although its implementation remains fragmented across industries. Most CII operators are struggling to enforce the vendor security requirements because many suppliers resist sharing detailed security policies due to their concerns about intellectual property and operational constraints (Mbanaso et al., 2019). Besides, C-SCRM does not incorporate AI-driven risk monitoring or automated incident response, hence limiting its capability to prevent zero-day attacks and real-time cyber threats effectively (Brucherseifer et al., 2021).

Zero Trust Architecture and CII Supply Chain Protection

Zero Trust Architecture is a new model of cybersecurity wherein all implicit trusts within networked environments are revoked. It assumes there is constant authentication, verification, and monitoring of users, devices, and third-party integrations continuously (Giannopoulos et al., 2023). Unlike traditional perimeter-based security, ZTA considers that the network is compromised already and performs strict access controls with multi-factor authentication, least privilege access, and network segmentation.

ZTA is suitable for securing supply chain interactions in CII, from cloud-based services to remote work environments and third-party software dependencies. However, the fully featured implementation of ZTA is expensive and cumbersome, requiring huge IT

infrastructure upgrades and high administrative overheads, as observed by Henriksson (2021). Most CII operators, especially in resource-constrained environments, are struggling with the adoption of ZTA, resulting in partial or incomplete implementations of the same. (Weiß, 2023).

Challenges and Vulnerabilities in CII Supply Chain Security

These strong cybersecurity frameworks nonetheless face several key challenges in the protection of the supply chains within CII.

2.3.1 Insufficient Risk Visibility

One of the most important challenges in CII supply chain security is the lack of visibility into third-party and fourth-party risks. Many CII operators depend on several vendors and subcontractors, and it is hard to track, assess, and monitor security compliance (Brucherseifer et al., 2021). The SolarWinds attack is a good example where malicious code was injected into trusted software updates, thereby compromising thousands of organizations (CISA, 2020).

Fragmented Regulatory Landscape

Cybersecurity regulations remain very different among geographical regions and industries, leading to gaps in cross-border supply chain security. Whereas the NIS2 EU Directive makes for strict cybersecurity requirements in critical sectors, other parts of the world lack the means of enforcement authority. Giannopoulos et al. (2023) explained that regulatory misalignment inhibits the harmonization of security standards across multinational supply chains. Mbanaso et al. (2019).

Limited Real-Time Threat Detection

Most of the existing supply chain security frameworks rely on static risk assessments and periodic audits, which are insufficient to detect and mitigate cyber threats in real time. AI-driven threat intelligence and machine learning-based anomaly detection have not yet been widely adopted in CII supply chain security practices Henriksson, 2021.

Summary of Key Gaps in Existing Research

1. Limited use of real-time AI driven monitoring within supply chain security models.
2. Inconsistencies in regulations around global CII supply chains.
3. Poor third-party and fourth-party risk visibility.
4. High cost and complexity to implement Zero Trust Architecture.

The research gaps clearly indicate a dire need for an overall conceptual framework that integrates AI-driven advanced threat detection, Zero Trust principles, and automated risk response for enhancing security in CII supply chains.

FRAMEWORK	FOCUS AREA	LIMITATIONS
NIST Cybersecurity Framework (CSF)	Structured risk management through Identify, Protect, Detect, Respond, Recover phases	Limited focus on third-party supply chain risks (NIST, 2018).
ISO/IEC 27001	Establishes Information Security Management Systems (ISMS) for supply chain security	High cost of compliance, making adoption difficult for SMEs (ISO, 2021).
Cyber Supply Chain Risk Management (C-SCRM)	Focuses on vendor risk assessment and secure procurement	Lacks real-time threat intelligence capabilities (CISA, 2020).
Zero Trust Architecture (ZTA)	Limits assumed trust in supply chain access	Difficult implementation across large-scale infrastructures (Giannopoulos et al., 2023).

Table 1: Summary of Existing Cybersecurity Frameworks for CII Protection

III. Methodology

This study uses qualitative methods to build a framework for protecting Critical Information Infrastructure (CII). The research design has five steps: a literature review, case study analysis, comparative analysis, framework development, and validation.

We reviewed key cybersecurity frameworks and new technologies. We looked at frameworks like: NIST CSF, C-SCRM, and the EU NIS2 Directive. We also studied past cyber incidents like: SolarWinds and MOVEit to understand their weaknesses.

- We analyzed the SolarWinds and Colonial Pipeline attacks. We chose these cases because they show how attackers exploit weaknesses in supply chains and where controls need to be better.
- We compared our proposed framework to global standards and local approaches, including Nigeria's official gazette. This helped us find the strengths and weaknesses of current supply chain security practices.

- We used the findings from our analysis to create a three-layer framework. This framework brings together governance, risk management, and new technologies like AI and blockchain.
- We did an early validation of the framework. We used case study mapping and expert reviews. Section 6 explains how we applied the framework to the SolarWinds and Colonial Pipeline attacks. Future work will include simulations for measurable results.

Proposed Conceptual Framework

As underlined in the Literature Review, current cybersecurity frameworks only provide general principles of security and cannot catch all the peculiarities of supply chain threats to CII. Contemporary models, including but not limited to NIST CSF, ISO/IEC 27001, C-SCRM, and ZTA, contribute to offering a fragmented solution without real-time threat intelligence, automated mitigation strategies, and holistic regulatory alignment (Weiß, 2023; Giannopoulos et al., 2023).

It will bridge these gaps by proposing an overall conceptual framework for securing the supply chains of CII. The framework provides an integrated structure in three layers that incorporates mechanisms for identifying cyber risks, governance, AI-driven security automation, and resilience. Each layer targets a particular theme in supply chain security to ensure that in real time, risks are identified, managed, and mitigated.

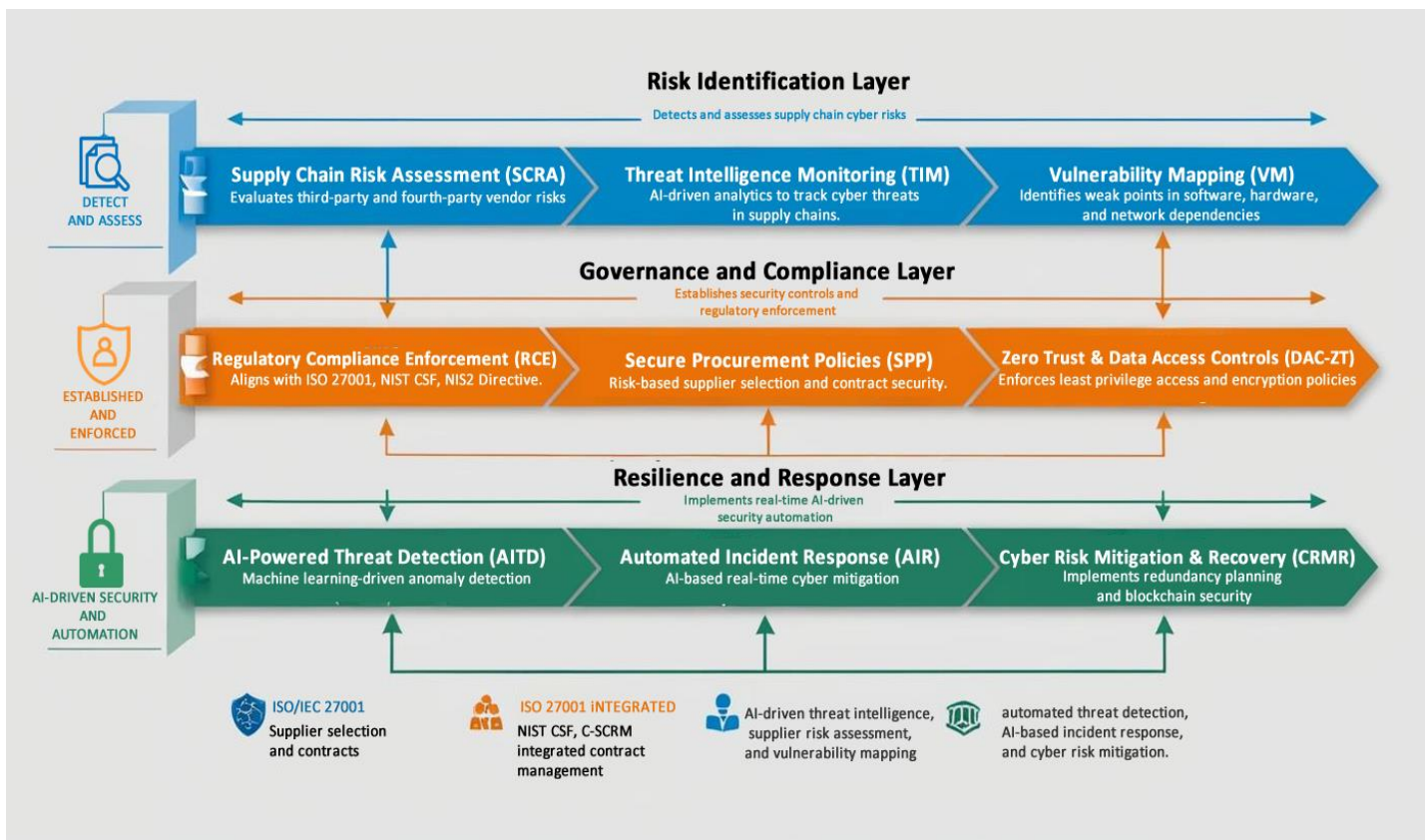


Figure 1: Diagrammatic representation of the proposed framework

Overview of Conceptual Framework

The proposed Conceptual Framework for Protecting CII Against Supply Chain Threats is made up of three interdependent layers, namely:

1. **Risk Identification Layer:** This focuses on supply chain risk assessment, threat intelligence monitoring, and vulnerability detection.
2. **Governance and Compliance Layer:** This establishes cybersecurity policies, supplier security standards, and regulatory compliance mechanisms.
3. **Resilience and Response Layer:** In practice, this is implemented through AI-powered threat detection, Zero Trust security models, and automated incident response systems.

These layers are meant to operate interactively and iteratively through dynamic and continuous feedback, which reinforces CII protection against supply chain cyber threats.

Layer 1: Risk Identification Layer**Purpose**

It does this through the proactive identification and investigation of cybersecurity threats emanating from third-party suppliers, software dependencies, and digital infrastructure. Recent attacks such as SolarWinds, NotPetya, and Kaseya have shown just how destructive software supply chains can be when those chains contain unseen weaknesses. Real-time threat intelligence has become an operational necessity in response (CISA, 2020).

Key Components

1. Supply Chain Risk Assessment
 - It assesses vendor security maturity using risk scoring models.
 - It assesses third-party cybersecurity policy compliance.
 - It determines potential risks from subcontractors of suppliers.
2. Threat Intelligence Monitoring
 - It use AI analytics to track cyber-attacks in supply chains.
 - It connects to global threat feeds to discover new attack trends.
 - It studies past attacks to improve risk forecasts.
3. Vulnerability Mapping (VM)
 - It shows how CII depends on third-party vendors.
 - It finds single points of failure in the supply chain.
 - It runs penetration tests and red-team exercises to simulate attacks.

Expected Outcomes

- There is a clearer understanding of supply chain cyber risks.
- Weaknesses can be detected earlier before they are exploited.
- There is more ability to predict and prevent threats.

Layer 2: Governance and Compliance Layer**Purpose**

This layer ensures that the right policies, security controls, and risk management rules to all third-party suppliers, vendors, and contractors follow cybersecurity best practices. To prevent supply chain cyber incidents from happening, strong compliance is very key. (Giannopoulos et al., 2023).

Key Components

1. Regulatory Compliance Enforcement
 - It aligns CII security policies with ISO 27001, NIST CSF, and the EU NIS2 Directive.
 - It requires mandatory cybersecurity audits for vendors.
 - It ensures compliance with data protection laws like GDPR and CCPA.
2. Secure Procurement Policy
 - It uses risk-based criteria when selecting suppliers.
 - It adds cybersecurity clauses to vendor contracts.
 - It applies blockchain tracking to verify supplier integrity.
3. Data Access Controls and Zero Trust Security
 - Implementation of principles of Zero Trust Architecture (ZTA) to supply chain access control.
 - Applies MFA and encryption protocols for sensitive data exchanges.

- Incorporates least privilege access policies to prevent unauthorized access by vendors.

Anticipated Outputs

- There will be increased third-party risk governance.
- There will be better regulatory alignment and security enforcement.
- There will be enhanced protection against insider threats and unauthorized access.

Layer 3: Resilience and Response Layer**Purpose**

The Resilience and Response Layer aims at real-time detection of cyber threats, automatic security response, and quick recovery in case of supply chain incidents. Due to the rise in ransomware attacks and data breaches, proactive mitigation strategies need to be put in place by an organization (Weiß, 2023).

Main Components

1. AI-Powered Threat Detection (AITD)
 - It deploys machine learning algorithms to detect suspicious activity in supply chains.
 - Behavioral analytics identify anomalous patterns in network traffic.
 - Integrate your solution into SIEM for automated incident notification
2. Automated Incident Response - AIR
 - Deploys pre-set playbooks to mitigate adverse cyber incidents in real time.
 - Utilizes AI-driven security orchestration in isolating malware and neutralizing the threat.
 - Offers automated security patching to reduce attack surfaces.
3. Cyber Risk Mitigation and Recovery Strategy - CRMR
 - Redundancy and backup systems planning for supply chain continuity
 - Block-chain Security for tracking integrity in supply chains
 - Resilience testing-table top exercising and simulated cyber-drills.

Expected Outcomes

- Faster incident detection and mitigation.
- Reduced downtime following cyber disruptions.
- Improved overall resilience of CII supply chains.

Empirical Validation and Case Study Application

This section provides early validation of the proposed framework. The aim is to show how it works when applied to real-world supply chain cyber incidents. By using case studies and practical illustrations, the framework becomes more than theory. It demonstrates how its three layers, risk identification, governance and resilience could prevent or reduce actual attacks.

Case Study: SolarWinds Attack

The proposed framework could have helped prevent the malicious software update that led to the SolarWinds breach in 2020 that compromised thousands of organizations (Centre for Cyber Security [CFCS], 2021). It could have helped in the following specific ways.

1. The Risk Identification Layer could have flagged the unusual update behavior earlier, through its vendor risk scoring and continuous threat intelligence monitoring
2. The Governance Layer might have prevented tampered updates from being trusted through its blockchain verification of software integrity and stronger procurement policies.
3. The Resilience Layer on the other hand would have reduced detection time and system exposure through its automated incident response and AI-based anomaly detection.

This case study shows that the framework adds value because it brings prevention, governance, and quick response together in a single approach

Case Study: Colonial Pipeline Ransomware

The 2021 Colonial Pipeline attack incident that disrupted critical fuel supply across the United States, has its main weakness due to poor incident response and vendor credential compromise (Giannopoulos et al., 2023). The framework provides improvements:

- **Risk Identification Layer** could have flagged weak credential policies.
- **Governance Layer** would enforce Zero Trust principles, limiting lateral movement inside networks (NIST, 2021).
- **Resilience Layer** ensures automated backups and response, reducing downtime.

The case shows that resilience strategies in the framework directly address downtime challenges.

Expert Validation

In addition to case study mapping, expert input is key. Structured interviews with cybersecurity practitioners can test the framework's feasibility. For example, Henriksson (2021) highlights how supply chain operators often lack visibility into third-party risks. Experts can confirm whether the framework's layered structure improves that visibility in practice.

Simulation Approach

Future validation can include pilot simulations. For instance, AI-based threat detection models, such as anomaly detection with machine learning, can be tested on synthetic supply chain traffic. Blockchain-based procurement tracking can also be trialed in a lab environment. These tests will provide measurable results and highlight areas for refinement.

Conclusion and Future Work

This paper set out to improve the protection of Critical Information Infrastructure (CII) against supply chain threats. It reviewed existing frameworks, identified their gaps, and proposed a new three-layer model. The framework combines risk identification, governance, and resilience. It uses tools such as AI threat detection, Zero Trust security, and blockchain tracking. Early validation shows that the framework can work in practice. Case studies like SolarWinds and Colonial Pipeline show how it could have reduced risk or limited damage. Expert review also supports its value. These steps move the work beyond theory and show practical relevance.

More work is still needed. Future research should test the framework in live environments through pilot projects and simulations. For example, AI-based monitoring tools should be tested on real supply chain data. Blockchain-based procurement tracking should also be deployed in controlled settings. Another area is regulation. Since supply chains cross borders, there is a need to study how rules in different countries can be harmonized. Future studies can also develop quantitative models to measure supplier risk using machine learning. These steps will provide deeper validation, improve accuracy, and make the framework easier to adopt across industries.

References

1. Ahlqvist, O., Dewitz, J., & Raines, G. (2019). Multi-level governance models for securing critical infrastructure supply chains. *Journal of Cybersecurity and Infrastructure Security*, **15**(3), 110-129.
2. Brucherseifer, J., Müller, K., & Lang, R. (2021). Digital twin conceptual framework for improving cyber resilience in supply chain security. *Computers & Security*, **105**, 102178. <https://doi.org/10.1016/j.cose.2021.102178>
3. Centre for Cyber Security. (2021). Supply chain attack against SolarWinds Orion Platform [Report]. Danish Defence Intelligence Service, Centre for Cyber Security. <https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/CFCS-solarwinds-report-EN.pdf>
4. CISA (Cybersecurity and Infrastructure Security Agency). (2020). Cyber Supply Chain Risk Management Practices for Federal Agencies and Critical Infrastructure. U.S. Department of Homeland Security. Retrieved from <https://www.cisa.gov/c-scrm>
5. European Union Agency for Cybersecurity (ENISA). (2023). NIS2 Directive: Strengthening Cyber Resilience for Critical Infrastructure in Europe. Retrieved from <https://www.enisa.europa.eu/publications/nis2-directive>
6. Giannopoulos, G., Jungwirth, R., & Hadjisavvas, C. (2023). Fortifying Defense: Strengthening Critical Energy Infrastructure Against Hybrid Threats. *EU Cybersecurity Journal*, **19**(1), 45-63.
7. Henriksson, L. (2021). Cyber supply chain vulnerabilities: A strategic analysis of third-party risks in the ICT sector. *Journal of Strategic Information Security*, **14**(2), 89-105.
8. ISO (International Organization for Standardization). (2021). ISO/IEC 27001: Information Security Management Systems. Retrieved from <https://www.iso.org/isoiec-27001-information-security.html>
9. Jenks, M. (2015). Risk-based procurement frameworks for securing critical supply chains: A comparative study of public and private sector practices. *Security Journal*, **28**(4), 378-395.

10. Mbanaso, U., Cooper, G., & Gordon, P. (2019). ICT Dependency Index (IDI): Measuring cyber risk exposure in critical supply chains. *International Journal of Cybersecurity Policy*, 7(1), 58-72.
11. NIST (National Institute of Standards and Technology). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce. Retrieved from <https://www.nist.gov/cyberframework>
12. NIST (National Institute of Standards and Technology). (2021). Zero Trust Architecture: Implementing Continuous Authentication in Critical Infrastructure. U.S. Department of Commerce. Retrieved from <https://www.nist.gov/publications/zero-trust-architecture>
13. The White House. (2021, May 17). Executive Order 14028: Improving the nation's cybersecurity. *Federal Register*, 86(93), 26633–26647. <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>
14. Weiß, M. (2023). Cyber supply chain security: Addressing third-party risks in critical infrastructure operations. *International Journal of Cybersecurity Research*, 22(4), 199-218.