Digital Supply Chain Vulnerabilities in Critical Infrastructure: A Systematic Literature Review on Cybersecurity in the Energy Sector

Mari Aarland[a] and Terje Gjøsæter[b]
Department of Information Systems, University of Agder, Kristiansand, Norway

Keywords: Critical Infrastructure, Resilience, Digital Supply Chain, Supply Chain Management, Safety, Energy Sector, Vulnerability, Cybersecurity.

Abstract: The main purpose of this paper is to identify the current state of the art on digital supply chain cybersecurity risks in critical infrastructure and how the term resilience is used in this context. To achieve this objective, the authors applied a systematic literature review method that summarises and analyses the studies relevant for the research topic. In total 33 papers were identified. The results show that limited research is done on supply chain risks in critical infrastructure. Relevant frameworks and methods for resilience of supply chains have also been identified. These frameworks and methods could be very beneficial for a more holistic management of cybersecurity risks in the increasingly complex supply chains within critical infrastructure.

1 INTRODUCTION

Society today is heavily dependent on reliable energy supply to maintain the capabilities that the population demands to feel safe and comfortable. The degree of dependency fluctuates with the degree of digitalisation, and as such, Norway is among those countries that is heavily dependent on its energy supply (Aarland et al., 2020). This dependency creates vulnerabilities, which emphasises the importance of securing a continuous energy supply. However, securing the energy supply is becoming more challenging due to the digitalisation of society. Digitalisation alone poses a threat to the reliability in the energy supply chain (Thakur et al., 2016). In addition, the increasing globalisation that creates linkage across nation borders introduces more vulnerability for the energy supply. Suppliers' dependency on sub-suppliers creates numerous of complex linkages. These linkages may become so interconnected that knowing where one organisation ends and the other begins nearly impossible.

Previous studies on supply chain management illustrates the challenges of maintaining cybersecurity throughout the supply chain following the paradigm shift of digitalisation (Saberi et al., 2019). This requires collaborative management across sectors and between tightly coupled organisations.

Developing resilient framework becomes even more important when multiple stakeholders are involved in the management (Bharadwaj et al., 2012). A resilient framework should be scalable to fit every environment throughout the supply chain. According to Bharadwaj et al. (2012), these environments carry challenges like pervasive connectivity, information abundance, global supply chains, improved price/performance of Information Technology (IT), growth of cloud computing, emergence, and big data.

This field lacks literature on how to transfer this security policy to a more specific field i.e., CI. To determine if resilience can be used as a potential framework for CI, it is necessary to know what research exists on the topic, how resilience is defined in CIs, and which research methods are used to collect empirical data on the topic.

The research questions addressed in this paper:

RQ1: *What research has been conducted on supply chain attacks in CIs?* In which fields are these topics discussed and when did it emerge as a field of

[a] https://orcid.org/0000-0001-5948-3121
[b] https://orcid.org/0000-0002-1688-7377

Aarland, M. and Gjøsæter, T.
Digital Supply Chain Vulnerabilities in Critical Infrastructure: A Systematic Literature Review on Cybersecurity in the Energy Sector.
DOI: 10.5220/0010803800003120
In *Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022)*, pages 326-333
ISBN: 978-989-758-553-1; ISSN: 2184-4356

interest?

RQ2: *How is resilience perceived by stakeholders in the literature in the context of CIs?* To utilise a resilience framework, it is necessary to know how the term resilience is defined and understood today.

RQ3: *What research methods have been applied to study resilience in CI?* For finding out the best research method for mitigating supply chain risks it is useful to determine what methods have been used in previous research.

The rest of this paper is organised as follows. Section 2 presents the research method. Section 3 contains findings from the literature review, while Sections 5 and 6 contain discussion and conclusion.

2 RESEARCH METHOD

Performing a systematic literature review provides foundation necessary to uncover areas in the research field that needs further research. The systematic literature review follows the PRISMA [3] guidelines with predefined inclusion and exclusion criteria. In addition, PRISMA provides a checklist with 27 steps on how to conduct a systematic review. PRISMA is also useful for critical appraisal of published systematic reviews (Page et al., 2021).

2.1 Systematic Literature Review

The search was performed on two databases, Google Scholar and Semantic Scholar. Google Scholar provides a comprehensive amount of data sources. However, limited possibilities for filtering makes the selection process more time-consuming. Semantic Scholar provided peer reviewed articles and allowed for more advanced filtered search (e.g., fields of study, publication type, outlets, most cited, etc.).

Articles published before 2010 were considered as not relevant. Except for three articles (Agrawal and Sambamurthy, 2008; Peppard et al., 2007; Williamson et al., 2004) that contribute foundation knowledge. The initial filtering stage was title relevance. In addition, filters used in Semantic Scholar were 'fields of study': computer science, engineering, and environmental science. Publication type: journals and conference articles. Any duplicates were removed when screening titles.

The search word and results are shown in Table 1. The combination of search words narrowed down the scope of existing literature which was necessary as there exists an overwhelming amount of research on CI. However, some essential articles could potentially be missed because of the narrow search.

Table 1: Search words and results.

Search word	Google	Semantic
Value Chain Attack * Critical Infrastructure * Power Grid * Resilience	**1**	**60**
Value Chain Attack * Critical Infrastructure * Energy Grid * Resilience	**0**	**36**
Supply Chain Attack * Critical Infrastructure * Power Grid * Resilience	**4**	**55**
Supply Chain Attack * Critical Infrastructure* Energy Grid * Resilience	**41**	**81**

Although PRISMA is illustrated in Figure 1 as a waterfall method, the reality was that both the search for papers and selection was more of an iterative process. This included using the backward and forward method from identification of titles to content analysis, which is indicated by the arrows in the *screening* part of Figure 1.

Further selection of relevant papers was conducted by reading abstracts to determine the relevance of each article. At this stage, any papers (including books, thesis, and dissertations) proving not to be peer reviewed was excluded. To answer RQ1 and RQ2, the following criteria were further used to assess the relevance:

1) Articles must reflect on critical infrastructure related to resilience.
2) Articles must include some aspect of supply chain management and related challenges.
3) Literature reviews are excluded but examined for relevant additional sources.
4) Articles only focusing on economic consequences of supply chain attacks are excluded.

As shown in Figure 1, the first 185 articles were excluded because of either being duplicates (31 papers), the title was irrelevant to the research topic (107 papers), not available copy online (19 papers), not published in a peer-review journal or conference (17 papers), or not written in English (11 papers). Next screening stage 56 articles were excluded after reading the abstract, and the last 14 excluded after reading the full article. This eventually resulted in 33 articles included in this systematic literature review. Next, these articles were imported into NVivo 12[4] to

[3] PRISMA 2020 Guidelines, available at: http://www.prisma-statement.org/

[4] https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home

help categorize and extract important data. In addition, NVivo was used to cross-reference the applied research method of each paper for finding out which methods were used to answer the different research problems. This was used to answer RQ3.

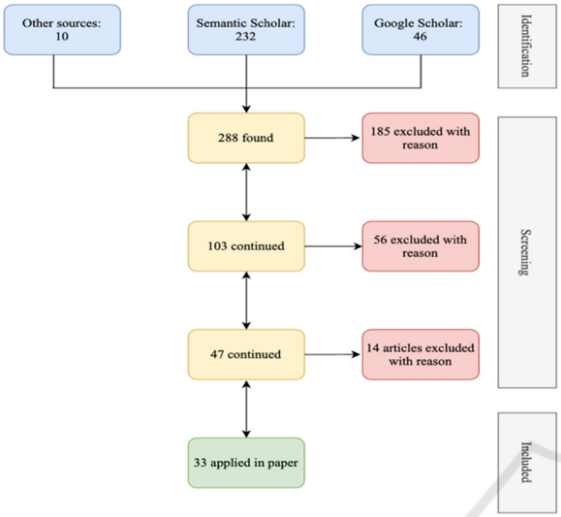

Figure 1: PRISMA selection of papers.

10 additional articles found through other sources was included into the systematic literature review based out of their relevance to the research topic. These articles were either found through snowballing articles on the research topic, or through other sources (e.g., in acknowledged journals like MIS Quarterly).

2.2 Review Sample

The 33 identified articles in the systematic literature review included journal papers (11 articles), conference proceedings (20 articles), and two in-press works. The distribution of the included articles in their domain-specific outlet is ranging from IT/IS business management (10 articles), computer science (7 articles), engineering (11 articles), social science (4 articles) and manufacturing/production (1 article). Publication outlets included MIS Quarterly, International Journal of CI Protection, IEEE ICC SAC Communication for the Smart Grid, Reliability Engineering and Systems Safety, and International Journal of Information Management.

Regarding the publication year, 67 percent of the identified articles were published after 2019, where the vast majority was published in 2020 with 11 articles, and five was found from 2021, and four in 2019. The remaining 37 percent was published from 2010. This indicates that the research topic has emerged as a major topic just over the last three years.

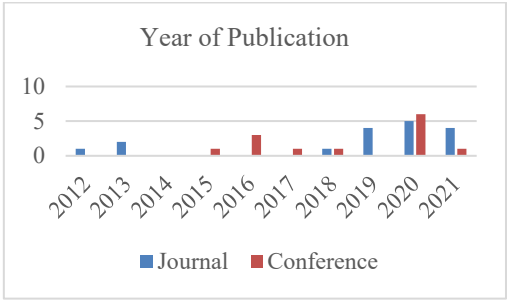

Figure 2: Year of publication.

Based on the systematic literature review, the authors identified five articles as empirical studies with results on how supply chain risks apply in CIs. Furthermore, the authors identified 11 empirical studies with no results on how supply chain risks apply to CIs, three preliminary description of a study or a system, and 14 that were either conceptual or following a framework. Further categorisation of the 16 empirical papers (i.e., studies on how supply chain risks apply in CIs with and without results, and preliminary studies) showed that most of them used a survey as their research method (8), five used case study, two used experiments, one used interview, and one used a mixed-method approach.

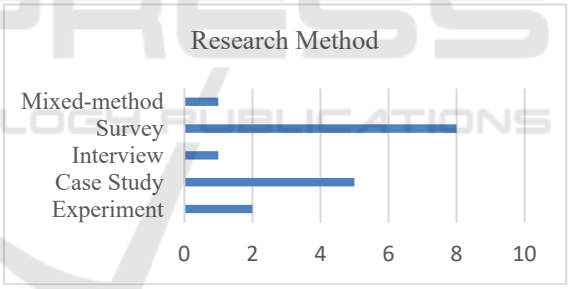

Figure 3: The applied research methods.

3 FINDINGS

In this section, findings from the systematic literature review are used to answer the research questions. To answer RQ1, the scope of the articles is illustrated in Figure 4. This shows that only two articles (Raponi et al., 2021; Desai and Makridis, 2020) discussed supply chain attack in CIs with regards to using resilience or the National Institute of Standard and Technology (NIST) framework for improving critical infrastructure cybersecurity as a framework for mitigating risks for threat exposure.

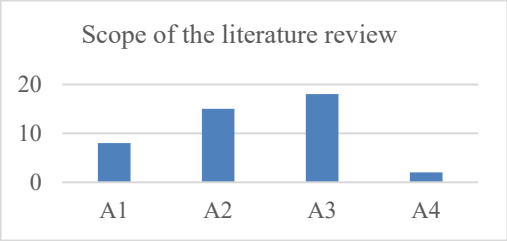

Figure 4: Scope of the literature review.

In Figure 4, A1 shows where resilience in CI is the main scope. A2 is where resilience is partly mentioned, and CI is still the main focus. A3 indicates articles that partly mentioned supply chain in the context of CI. Lastly, A4 shows articles that had supply chain attack as their main topic in CI, where resilience is also mentioned briefly. Articles from category A4 uses the attack against SolarWinds as an example of supply chain attack.

3.1 Conceptual Foundations

In this section, the concepts of critical infrastructure, resilience and supply chain are introduced. The conceptualisation is based on how these concepts are described in the 33 identified papers.

3.1.1 The Criticality Aspect

Infrastructures are categorised as critical when the disruption impacts the wellbeing for the population in the society (Abedi et al., 2019). In the United States, sixteen sectors are recognised as CI "*whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof*" (Raponi et al., 2021).

Examples of CI are energy, banking, distribution of water and gas. According to Filippini and Silva (2015), these are modern infrastructures that surpass traditional systems found in organisational complexity. However, they focus more on operational interdependencies of CI which is called "systems-of-systems" (SOS) (Abedi et al., 2019).

How digitalisation creates closer interconnections between CIs is emphasised by several articles (e.g., Raponi et al., 2021). Abedi et al. (2019) describe a scenario in a gas network were an action leads to shutdown of generators supplied by gas, and eventually impacts the energy sector. This is also a concern in Nguyen et al. (2020b), where population growth and dependency on a reliable energy supply, combined with energy grid vulnerability increases the potential impact of an attack.

Self-healing mechanisms are mentioned as methods for networks to detect abnormalities in real-time and adjust to unforeseen events so downtime is reduced as much as possible (Skopik and Langer, 2013; Djenna et al., 2021). Encryption, message authentication codes and digital signatures are all cryptographic tools that reduce the chance for eavesdropping and replay attacks substantially (Gunduz and Das, 2020). Nevertheless, cryptography alone has its limitations for mitigating supply chain risks according to Skopik and Langer (2013). Several articles mention that traditional risk assessment methods and vulnerability analysis are no longer applicable for current cyberthreats emerging for more complex and interconnected CIs (e.g., Jung et al., 2016). Nystad et al. (2020) emphasise the importance of human capabilities for acquiring more knowledge.

3.1.2 The Concept of Resilience

Skopik and Langer (2013) point out that resilience is both necessary and essential for the CI of energy grids for designing security architectures to protect against cyberattacks. A resilient evaluation tool is proposed by Jung et al. (2016) to assess effectiveness of responses where the objective is to obtain more detailed information about the interconnected infrastructures which can help with decision-making.

Resilience definitions vary between disciplines, e.g., psychology, ecology, engineering, and sociology (Woltjer et al., 2018), and will continuously change (Das et al., 2020). Woltjer et al. (2018) describe resilience as a property used to understand a system's ability to respond and recover from extreme events, which is relevant for all disciplines mentioned.

While these definitions describe the traits of the term, other argue that they do not cover the whole aspect of resilience. Das et al. (2020) suggest in their article that resilience should be divided into what they call resilience measures. The three measures *avoidance by prevention*, *absorption* and *recover*, are relevant for different phases of the crisis, and may contribute the resilience framework. Avoidance by prevention are actions before any events, while absorptions referred to the time during an event occurs, and recovery after the initial phase is done. Another important aspect of resilience in CI is the capability to guarantee that the level of service is acceptable while still enduring any hazards exposed to the infrastructure (Das et al., 2020).

From the study of resilience of energy grids, two themes are prominent in the field according to

Woltjer et al. (2018). These are development of qualitative frameworks, and development of metrics. Qualitative frameworks are developed as guidelines to identify potential policies that help to improve current resilience levels. Developing metrics helps to quantify the actual resilience level of the energy grid (Woltjer et al., 2018). Another method for ensuring resilience in CI proposed by Das et al. (2020) is to conduct a resilience analysis of the behaviour of the infrastructure upon the failure of its constituent elements. The infrastructure's response to the disruptions is analysed by using forward inductive reasoning and characterised by their response time to recover from the events.

Nguyen et al. (2020a) describe an approach to CIP as a "*defence-in-depth*" reaching from prevention, preparation, response, to recovery. Requirements for securing resilience levels in CI are enforced by accurate threat detection, continuously monitoring of infrastructure vulnerability, and prompt action for response and recovery. The defence-in-depth consists of *technical, operational*, and *human measures* to ensure the entire system capable for managing future hazards. The literature describes some technical measures for ensuring resilience in the energy grid e.g., grid hardening through redundancy, reinforcement, maintenance of technical equipment, but also for critical assets (Nguyen et al., 2020a).

3.1.3 The Supply Chain Concept

Raponi et al. (2021, p. 6) define a supply chain as a "*network of all the individuals, resources, organizations, and activities involved in the creation and distribution of specific products to the final buyer*." Supply chains create a global network consisting of network distribution and transport systems, which makes supply chains transnational i.e., crossing national boarders (Aarland et al., 2020). Gajek et al. (2020) conclude in their research that integration of transnational supply chains leads to more vulnerabilities since risks no longer can be contained.

Typically, the supply chain consists of three distinct phases, i.e., *procurement, production*, and *distribution*. In the CIs of energy grids, it is becoming a new normal to procure services from other businesses to keep up with the demand for digitalisation. This collaboration and outsourcing of services transform the supply chain management (Saberi et al., 2018).

Kieras et al. (2021) mention integrity as one of the key concerns in supply chains. Another key concern mentioned by Xu et al. (2019) is when untrusted parties are involved in the three phases of the supply chain. Along with other concerns (e.g., human error, natural hazards, technological disruptions) supply chain risks arise. What differentiates supply chain risks from other forms of risk is the attack surface. Kieras et al. (2021) describe the supply chain risk as coextensive with the entire CI system and that supply chain threats are robust and of the type "unknown unknown". An important aspect of assessing the vulnerability of the supply chain risk is to ask questions about the jurisdictions and regulatory policies (Kieras et al., 2021).

SolarWinds is an American IT organisation that sells software for managing IT systems (Raponi et al., 2021). The monitoring and management software Orion has 33,000 customers all over the world (Desai and Makridis, 2021; Raponi et al., 2021). On the 13th of December 2020, FireEye published a report about the breach in the SolarWinds Orion Software. The breach also known as Sunburst was allegedly part of a Russian espionage campaign (Raponi et al., 2021). In FireEye's report, they announced the breach as a supply chain attack on SolarWinds Orion Software carried out by a sophisticated group known as "Cozy-bear" or "ATP29" (FireEye, 2020).

The Cybersecurity and Infrastructure Security Agency (CISA, 2021, p. 2) describe software supply chain attack as occurring "*when a cyber threat actor infiltrates a software vendor's network and employs a malicious code to compromise the software before the vendor sends it to their customers*." Threat actors exploit the trust between the organisation and the third-party suppliers (Raponi et al., 2021), as well as the well-established machine-to-machine communication channels. For the case of SolarWinds the software updates were exploited (FireEye, 2020), hence why it was so difficult to identify (Raponi et al., 2021). CISA (2021) also emphasises that the initial infection vector is not limited to the Orion platform exclusively, i.e., another software might also be a way into the firm's system.

3.1.4 Theoretical Perspectives

Several different theoretical perspectives were identified as the variation of publication outlets indicates. In addition, there is also a variation in the frameworks applied in the core literature. Whilst some articles used several theoretical perspectives and frameworks, others used none. Some of the theoretical aspects were game-theoretic, cyber-physical systems (CPS), enterprise architecture (EA),

systems of systems (SoS), and Technology Organization and Environment (TOE). Perspectives related to technology, business management, and software development were also identified.

Figure 5: Resilience word cloud.

To answer RQ2, Figure 5 visualises keywords detected from definitions found in the literature. To use resilience frameworks for mitigating supply chain risks, consensus on the term is necessary for achieving common situational awareness throughout the supply chain. Key words acknowledged in the literature on CIs as resilience's main traits are recover, ability, response, absorb, and change.

4 DISCUSSION

After conducting the systematic literature review, the analysis revealed gaps in existing literature regarding RQ1, *what research had been done on supply chain attack in CIs using resilience as a potential framework*. This highlights the need for more research on the topic as more attacks against the CIs supply chain is emerging as a concern for the future. Nevertheless, the concept of resilience is increasingly more used in papers discussing CIP. As stated in the introduction, traditional CIP is no longer a sufficient approach for meeting threats that the supply chain risks experience. A possible method, provided by Kieras et al. (2021), which is used to interpret suppliers' trust and how to assess their dependency, could be applied to a more general case of assessing supply chain risks in general. However, while resilience is more frequently applied in the CI context, different definitions are found in the existing literature, making it more difficult to contribute with a common consensus on the meaning of the term.

As Figure 5 indicates, there are some main traits recognized by CIs as resilience features. Nevertheless, the word cloud also illustrates several other features to describe and define resilience. To use resilience as a framework, it would need consensus on the definition for the supply chain to achieve common situational awareness for suppliers. Interestingly there were few articles that mentioned the organisational aspect of resilience with human factors (e.g., knowledge, training, awareness, decision-making). Although CIs is related to engineering it is also within a social system that features the interrelationship between suppliers. Utilising Nguyen's et al. (2020a) approach which stems from CIP as the "*defence-in-depth*" could be interesting for developing the resilience framework, whereas human, technology and organization is seen as an interconnected system. This system consists of components that needs equal attention to create the defence in depth that a supply chain should embody. The well-known saying "a chain is only as strong as its weakest link" enlightens that only focusing on one of these components is not sufficient.

The topics that emerged from the analysis were related to how CI adjusted to digital transformation, cascading failures, interdependency amongst CI, vulnerability analysis, risk assessment, supply chain management, and supply chain risks. However, some articles did not fit perfectly into any single category but has aspects of multiple categories. For example, one of the articles covered both CI and digital transformation. The three topics were:

Developing a new framework for risk assessment for the purpose of improving CI against future attacks, particularly in energy grids. Several papers mention the need for a new framework for conducting risk assessment to manage interconnections between CIs.

Using quantitative (game-theoretic, algorithm, and discrete models) approaches to contribute with empirical data on critical systems reliability and robustness with cascading failures.

Using a resilience approach as a way of reducing downtime, to enable response, and to achieve the holistic approach for cyberattacks. Scenarios are used to describe how potentially resilience could be implemented as framework for a changing system.

For future work, existing attention towards hardware and software hardening for mitigating supply chain risks must be supplemented with a focus on the human aspect to enforce the organisational component to mitigate supply chain risks. More multidisciplinary research is needed to fill the knowledge gap on how supply chain attack in CI can be managed properly with several suppliers involved. In addition, CI need a resilience framework for suppliers for managing supply chain risks as there are no such frameworks available today. This framework

should be flexible and applicable to each supplier in the supply chain for CI.

An approach which could help develop more empirical knowledge on supply chain risks in CI is the recent study of implementing digital twins in the energy grid sector (Meske et al., 2021). More research into this approach would be interesting for future work. An advantage of digital twins is that it allows monitoring of real-time data which is essential for an energy grid that is vulnerable for downtime.

5 CONCLUSION

The goal of this paper was to conduct a systematic literature review to investigate supply chain risks in critical infrastructures. 33 relevant papers were identified which covered the topic in various degree. Only two papers explicitly discussed the topic of supply chain attacks in critical infrastructure. This indicates the need the need for more research on supply chain attack in critical infrastructure. However, the papers proposed relevant frameworks and methods applicable to manage supply chain attacks. These methods and approaches can be used for developing a resilience framework. In addition, more organisational understanding of the complex phenomenon is needed to properly manage the supply chain in critical infrastructure.

REFERENCES

Aarland, M., Gjøsæter, T., & Radianti, J. (2020). Cyber-Security in Digital Metering Value Chain for Mountain Landslide Warning. *International Conference on Information Technology in Disaster Risk Reduction (ITDRR),* pp. 170-182.

Abedi, A., Gaudard, L., & Romerio, F. (2019). Review of major approaches to analyze vulnerability in power system. *Reliability Engineering and System Safety.* Vol. 183, pp. 153-172.

Agrawal, S. R., & Sambamurthy, V. (2008). Principles and Models for Organizing the IT Function. *MIS Quarterly Executive*, Vol. 1, Issue 1, Article 6, pp. 1-16.

Bai, Z., Jain, N., Kurdyukov, R., Walton, J., Wang, Y., & Wasson, T., et al. (2019). Conduction Systematic Literature Reviews in Information Systems: An Analysis of Guidelines. *Issues in Information Systems,* Vol. 20, Issue 3, pp. 83-93.

Berkeley, R. A., & Wallace, M. (2010). A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council. *National Infrastructure Advisory Council,* pp. 1-83.

Bharadwaj, A., El Sawy, A. O., Pavlou, A. P., & Venkatraman, N. (2013). Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly.* Vol. 37, No. 2, pp. 471-482.

Bie, Z., Lin, Y., Li, G., & Li, F. (2017). Battling the Extreme: A Study on the Power System Resilience. *Proceedings of the IEEE*, Vol. 105, No. 7, pp. 1253-1266.

Bie, Z., Lin, Y., & Qiu, A. (2015). Concept and research prospects of power system resilience. *Automation in Electronic Power Systems,* Vol. 39, No. 22, pp. 1-9.

Camachi, M. E. B., Ichim, L., & Popescu, D. (2018). Cyber Security of Smart Grid Infrastructure. *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI),* pp. 000303-000308.

Chen, H., Chiang, H. L. R., & Storey, C. V. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly,* Vol 36, No. 4, pp. 1165-1188.

CISA, (2021). Defending Against Software Supply Attack. *NIST*. Available at: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

Collier, A. Z., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research,* Vol. 59, No. 11, pp. 3430-3445.

Crosignani, M., Macchiavelli, M., & Silva, F. A. (2021). Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains. *Federal Reserve Bank of New York Staff Reports*. No. 937, pp. 1-42.

Das, L., Munikoti, S., Balasubramaniam, N., & Srinivasan, B. (2020). Measuring smart grid resilience: Methods, challenges, and opportunities. *Renewable and Sustainable Energy Reviews.* Vol. 130, pp. 1-16.

Desai, R. D., & Makridis, A. C. (2020). Identifying Critical Infrastructure in a World with Supply Chain and Network Cybersecurity Risk. *Georgia Tech Scheller College of Business Research Paper,* pp. 1-20.

Djenna, A., Harous, S., & Saidouni, E. D. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Applied Science*, Vol. 11, No. 4580, pp. 1-30.

Eggers, S. (2020). A novel approach for analyzing the nuclear supply chain cyber-attack surface. *Nuclear Engineering and Technology*, pp. 879-887.

Filippini, R., & Silva, A. (2015). I®ML: An Infrastructure Resilience-Oriented Modeling Language. *IEEE Transactions on systems, man, and cybernetics: systems,* Vol 45, No. 1, pp. 157-169.

FireEye. (2020). Threat Research Blog: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor. Available at: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Gajek, S., Lees, M., & Jansen, C. (2020). IIoT and cyber-resilience: Could blockchain have thwarted the Stuxnet attack? *AI & Society,* pp. 1-11.

Gunduz, Z. M., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks,* Vol. 169, No. 14, pp. 1-14.

Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International Journal of Production Research,* Vol. 58, No. 10, pp. 2904-2915.

Jung, O., Vasenev, A., Ceccarelli, A., & Clarke, T. (2016). Towards a Collaborative Framework to Improve Urban Grid Resilience. *IEEE International Energy Conference (ENERGYCON)*, pp. 1-6.

Kieras, T., Farooq, J M., & Zhu, Q. (2020). RIoTS: Risk Analysis of IoT Supply Chain Threats. *IEEE 6th World Forum on Internet of Things (WF-IoT)*, pp. 1-6.

Kieras, T., Farooq, J M., & Zhu, Q. (2021). I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions. *IEEE Access*, Vol. 9, pp. 29827-29840.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection,* Vol. 25, pp. 36-49.

Lenk, S., Arnoldt, A., Rösch, D., & Bretschneider, P. (2020). Hardware/Software architecture to investigate resilience in energy management for smart grids. *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe),* pp. 51-55.

McLaughlin, D. M., & Gogan, J. (2018). Challenges and Best Practices in Information Security Management. *MIS Quarterly Executive*. Vol. 17, Issue 3, Article 6, pp. 237-262.

Meske, C., Osmundsen, S. K., & Junglas, I. (2021). Designing and Implementing Digital Twins in the Energy Grid Sector. *MIS Quarterly Executive,* Vol. 20, Issue 3, Article 3, pp. 183-198.

Mingers, J., Murch, A., & Willcocks, L. (2013). Critical Realism in Information Systems Research. *MIS Quarterly,* Vol. 37, No. 3, pp. 795-802.

Nguyen, N. T., Liu, B., Nguyen, P. N., & Chou, J. (2020b). Cyber Security of Smart Grid: Attacks and Defenses. *ICC 2020- 2020 IEEE International Conference on Communications (ICC),* pp. 1-6.

Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., & Dehghanian, P. (2020a). Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access*, Vol. 8, pp. 87592-87608.

Nystad, E., Katta, V., Simensen, E. J., Jørgensen, A. P., Sechi, F., Toppe, L. A., & Nihlwing, C. (2020). What happens in a control room during a cybersecurity attack? *2020 IEEE/ACM 42nd International Conference on Software Engineering Workshops (ICSEW),* pp. 270-275.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems*, Vol. 10, No. 26, pp. 1-49.

Page, J. M., Moher, D., Bossuyt, M. P., Boutron, I., Hoffmann, C. T., Mulrow, D. C., et al. (2021). PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. *British Medical Journal (BMJ): Research Methods and Reporting,* Vol. 372, No. 160, pp. 1-36.

Peppard, J., Ward, J., & Daniel, E. (2007). Managing the Realization of Business Benefits from IT Investments. *MIS Quarterly Executive*, pp. 1-22.

Rao, V. S. N., Ma, T. Y. C., Hausken, K., He, F., & Zhuang, J. (2016). Defense Strategies for Infrastructures with Multiple Systems of Components. *2016 19th International Conference on Information Fusion (FUSION),* pp. 270-277.

Raponi, S., Caprolu, M., & Di Pietro, R. (2021). Beyond SolarWinds. *The Italian Conference on Cybersecurity (ITASEC 2021)*, pp. 1-11.

Saberi, S., Kochuzadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, Vol. 57, No. 7, pp. 2117-2135.

Skopik, F., & Langer, L. (2013). Cyber Security Challenges in Heterogeneous ICT Infrastructures of Smart Grids. *Journal of Communication.* Vol. 8, No. 8, pp. 463-472.

Sobb, T., Turnball, B., & Moustafa, N. (2020). Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. Electronics, Vol. 9, No. 1864, pp. 1-32.

Standish, J. R., Hobbs, J. R., Mayfield, M. M., Bestelmeyer, T. B., Suding, N. K., Battaglia, L. L., et al. (2014). Resilience in ecology: Abstraction, distraction, or where the action is? *Biological Conservation,* Vol. 177, pp. 43-51.

Thakur, K., Ali, L. M., Jiang, N., & Qiu, M. (2016). Impact Of Cyber-Attacks On Critical Infrastructure. *2016 IEEE 2nd International Conference on Big Data Security on Cloud,* pp. 183-186.

Wei, M., Lu, Z., & Wang, W. (2016). Dominoes with Communications: On Characterizing the Progress of Cascading Failures in Smart Grid. *IEEE International Conference on Communications*, pp. 1-6.

Weil, T., & Murugesan, S. (2020). IT Risk and Resilience – Cybersecurity Response to Covid-19. *IEEE Computer Society,* Vol. 22, No. 3, pp. 12-18.

Williamson, A. E., Harrison, K. D., & Jordan, M. (2004). Information systems development within supply chain management. *International Journal of Information Management*. Vol. 24, pp. 375-385.

Woltjer, R., Hermelin, J., Nilsson, S., Oskarsson, A. P., & Hallberg, N. (2018). Using Requirements Engineering in the Development of Resilience Guidelines for Critical Infrastructure. *2018 13th Annual Conference on System of Systems Engineering (SoSE),* pp. 615-622.

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research,* Vol. 39, Issue 1, pp. 93-112.

Xu, X., Rahman, F., Shakya, B., Vassilev, A., Forte, D., & Tehranipoor, M. (2019). Electronics Supply Chain Integrity Enabled by Blockchain. *ACM Transactions on Design Automation of Electronic Systems,* Vol. 24, No. 3, Article 31, pp. 1-25.