Neutrosophic Systems with Applications, Vol. 12, 2023
https://doi.org/10.61356/j.nswa.2023.98

Evaluation of Cyber Insecurities of the Cyber Physical System Supply Chains Using α-Discounting MCDM

Rehab Mohamed [1,*] **and Mahmoud M. Ismail** [1]

[1] Decision support department, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Sharqiyah, Egypt.
Emails: rehab_argawy@zu.edu.eg; mmsabe@zu.edu.eg.

* Correspondence: rehab_argawy@zu.edu.eg.

Abstract: Recently, supply chains (SCs) are applying information technology to enable data sharing among suppliers, instant access to information, and complete tracking of products. With more Cybersecurity risks present, such as theft of information, service interruptions, and financial resources risks, the vulnerability of systems is increased. The management of supply chain Cybersecurity, which encompasses information systems, software, and infrastructure, is the emphasis of the supply chain's safety measure. There are several serious danger that attack supply chain systems. Most SC Cybersecurity procedures are used to reduce the threats posed by vulnerabilities to those processes. Researchers have mostly concentrated on supply chain-related cyber physical system (CPS) issues. This study makes attempts to classify and evaluates the Cybersecurity insecurities of supply chains. In addition, this work provides an update of the analytic hierarchy process (AHP) method called α-discounting multi-criteria decision-making (α-D MCDM), which enables a more uniform assessment of supply chain cyber insecurities. This paper suggests using the α-D MCDM in various ways to address various supply chain evaluation problems.

Keywords: Supply Chain; Cybersecurity Risks; Cyber Physical System; α-D MCDM.

1. Introduction

A supply chain (SC), which is a combination of various entities that coordinate their procedures, targets and some system elements with those of suppliers, customers, and other external organizations. A SC consists of all operations associated with the movement of products, services, and information from suppliers to consumers [1]. Supply chain management (SCM) aims to deliver the appropriate item to the appropriate customer at the optimal cost, at the correct place, and at the optimal time. In order to increase process effectiveness as well as cost enhancement, businesses are now utilizing information technologies (IT) in their processes [2]. According to Singh et al. [3], the efficient use of IT tools guarantees an ongoing development of supply chains.

Cyber-physical systems (CPS) are systems made up of physical ingredients, network infrastructures, embedded hardware, software, and connections between devices and sensors for transferring data. The development of CPS with SC operations has changed how supply chains operate in numerous ways over time [4]. An organization's information systems and information technologies, which improves supply chain productivity, may also be the source of security risks as well as weaknesses. The organization and business relationships through every phase of the supply chain is required for efficient and achievable supply chain management (SCM). Integrating technology into corporate operations improves overall productivity and even costs optimizing. Cyber threats are one of the difficulties brought on by utilizing CPS in supply chain processes [5].

Modern industrial demands, such as decentralization and systems connectivity cannot be satisfied by the conventional supply chain architecture. In contrast, the utilization of CPS and the internet of things (IoT) leads to the production system being intelligently connected, which improves manufacturing, efficiency, and productivity increases [6]. Data authenticity, consistency, and security are some of the issues that come with growing connection, the volume of data, and their sensitive nature. Due to several factors, including software flaws and vulnerabilities discovered in any supply chain through data transfer, cyber-attacks could have consequences on supply chain processes [7].

In this paper, the objective is to categorize the cyber insecurities of cyber SC regarding to supply, operation, and customer. Firstly, cyber supply chain definitions are discussed and how it may improve the SCs performance and efficiency. Secondly, we describe the expansion of analytic hierarchy process (AHP), which, by addressing AHP's imperfections in order to evaluate the categories of the cyber insecurities that may attack supply chain. Thirdly, we put forth the concept of a multi-criteria decision-making (MCDM) framework that supports management in assessing supply chain cyber vulnerabilities by combining the α-discounting (α-D) with various MCDM techniques.

This research is structured as follows: Section 2 reviews earlier papers on the cyber supply chain and cyber-attacks that could target the SC phases. In Section 3, discussion of cyber supply chain insecurities is presented. The suggested concept of evaluating cyber supply chain vulnerabilities based on α-D MCDM with various MCDM is presented in Section 4. The conclusion and future directions are made clear in Section 5.

2. Literature Reviews

Supply chains are now integrated with organizations through digital communication channels as a result of digitalization. In supply chains, all members become as powerful due to shared knowledge and security mechanisms along the supply chain, as stated by Pandey et al. [8]. An organization can achieve its strategic goals by utilizing the secure network infrastructure that supply chain Cybersecurity offers. While the way that organizations and industries function has changed significantly, as a result of the application of CPS in the field of SCs. However, CPS supply networks also brought forth a number of difficulties, including a lack of security measures and risk management [9].

2.1 Cyber Supply Chain

The quality of services provided in the field of SC has steadily improved due to technological applications. Cheung et al. [10] investigated the Cybersecurity measures in SCM. Several major findings and relevant research initiatives related to Cybersecurity in logistics and SCM are discussed [10]. The research of Yeboah-Ofori et al. [11] tries to analyze and predict risks in order to improve Cybersecurity in the field of SCs. They used Cyber Threat Intelligence (CTI) to investigate and anticipate attacks based on CTI features [11].

Luo and Choi [12] focused their research on how firms make investments in Cybersecurity at a high cost. Because cyber-attacks pose a threat to e-commerce supply chains and its participants. Customers who buy things online run the danger of having their personal information hacked [12]. Pandey et al. [8] attempt to classify the Cybersecurity threats that arise as a result of supply chains working in cyber physical systems. The research provides a framework comprised of various cyber-attacks spanning information flows in global supply chains [8].

2.2 Cybersecurity and Supply Chain Risk

In order to evaluate the influence of Cybersecurity on digital operations in the UAE pharmaceutical business, the research of Del Giorgio Solfa [13] examined empirical data. The results confirmed the strong positive association between supply chain risk and Cybersecurity in relation to digital operations [13]. The main goal of Melnyk et al.'s study from 2022 is to create a foundation for future research on supply chain Cybersecurity [14]. A need for greater research on Cybersecurity throughout the supply chain is made in the paper's conclusion. An exploratory research technique was used, which drew on a number of sources to construct the research framework [14].

In order to investigate how supply chain managers view the components of cyber supply chain risk management and the degree to which this is aligned with increased cyber supply chain resilience, Creazza et al. [15] studied the subject of supply chain security. In order to better respond to cyber threats, this study revealed that Logistics Service Providers can play a significant role as administrators of the Cybersecurity process. The study also emphasizes how crucial it is to prioritize humans while enhancing supply chain cyber resilience. Using a data fusion technique, Hossain et al. [16] established a paradigm that takes into account supply chains' resilience, sustainability, and Cybersecurity to determine how effectively they operate without interruption. A healthcare supply chain is used to verify the suggested framework [16]. In cyber supply chain risk analysis, SC weaknesses are frequently disregarded. To help with risk assessment and to investigate the intricate problems related to the demands for protecting hardware, firmware, software, and system data over the whole SC lifecycle, a novel SC cyber-attack framework is presented [17].

3. Cybersecurity Risks in Supply Chains

3.1 Cyber Physical System Supply Chains

Factors that make it difficult to model CPS effectively include the variety of systems and programming, the absence of representation of real-time operating systems, and timing-related system responsiveness [18]. The foundation of CPS is the fusion of both traditional and technological procedures. CPS encompass machines, structures, vehicles, and other means of transportation as well as logistical, management procedures, and internet-based services [19]. While devices are used to respond to industrial or organisational changes and connect with other components, sensors help CPS gather, organise, and analyse data. CPS can be employed to handle a variety of concerns, including manufacturing, logistics, quality control, planning, and scheduling operations within the supply chain [20].

3.2 Cybersecurity Risks Categories Occurring along Supply Chains

Cyber supply chain systems based on CPS are frequently vulnerable to cyber-attacks notwithstanding their advantages in terms of safety and dependability. At a time, there are more and more advanced cyber-attacks that have a variety of negative effects on al supply chain operations and businesses. Attacks against emerging CPS can also have a negative effect, particularly on those that function in the logistics and SCM sectors [21]. Supply, operations, and demand are the three key supply chain stages that can be used to categorise cyber supply chain insecurities as shown in Table 1.

Table 1. Cybersecurity risks of cyber supply chains and their categorization.

Risks categories	Risk types
Supply risks	Lack of availability of providers
	Vendor credentials hacked
	Vulnerability of the supplier's connection
	Malware-induced source code alteration
	Provision of tainted software
Operations risks	Disruption of the manufacturing facility
	Unexpected breakdown of the manufacturing's operations
	Missing coding errors
	Invalid product specifications
	Information leakage
Demand risks	Theft of inventions
	Altering information
	Access of Client information without permission
	Deceptive communication
	Data destruction
	Unlicensed payment processors

- *Supply Insecurities*

Supply risks are the incident related to incoming supplies that could lead to supplier failures. The firm's difficulties to satisfy client demand is the result of these failings. Prior to the final manufacturing, suppliers frequently give the companies with the necessary parts. Therefore, it's essential to effectively manage the supply chain of Cybersecurity products in accordance with the requirements of the Cybersecurity strategy [22].

- *Operational Insecurities*

Operations risk is defined as the potential for an occurrence that has an impact on the firm's capability to provide goods and services, productivity, and its financial performance. These risks arise from a major breakdown in the access restrictions on supply chain operations, which gives the attacker the ability to interrupt business [23].

- *Demand Insecurities*

Demand risk is defined as the potential of a situation involving outgoing transactions that could change the possibility of clients placing orders with the business. Demand risk results from the unanticipated change in markets and business breakdown. The public's opinions are impacted by the supply risks in CPS, and the associated demand also creates the demand risks [24].

4. Application of α-D MCDM to evaluate Cybersecurity Risks of Supply Chain

4.1 *α-D MCDM Definitions*

In this research, we examine a novel method that extends Saaty's AHP and is known as the α-D MCDM. This method can be applied to any set of preferences that can be transformed into a set of homogeneous linear equations [25]. It is helpful not only for preferences that are pairwise comparisons of criteria as AHP does, but also for preferences of any n-wise (with n ≥ 2) assessments of criteria that can be expressed as linear homogeneous formulas.

The overall aim of α-D MCDM is to change the null-solution of linear homogeneous system, into a non-null solution system, by reduce or raise the coefficients in the right-hand side [26].

Additionally, this approach has an edge in that it can convert those MCDM issues that the AHP has categorized as inconsistent into a consistent form. Taking a decision among the options available to a decision maker is not an easy task since most often, numerous criteria with diverse orientations are used in place of a single criterion with a single direction in the decision-making process. That's why, α-D MCDM is a good choice in such evaluation problems.

4.2 Application of α-D MCDM

The MCDM techniques in the literature have benefits and drawbacks. AHP is constrained in the way some issues are structured. The most beneficial advantage of the α-D MCDM that is not limited by the number of comparisons of criteria. By decreasing or increasing the linear evaluation equation coefficients at/to specific amounts, α-D MCDM can solve the problem of converts an inconsistency of the problem. The following are the procedure steps for α-D MCDM [27]:

1. Let $X = \{X_1, X_2, X_3, \dots, X_n\}$,$n \geq 2$, be a problem structure components. The group of preferences is $R = \{R_1, R_2, R_3, \dots, R_m\}$, $m \geq 1$. Each preference R_m represent the relationship to a certain criteria X_n as follows$R_m = f_i(X_1, X_2, X_3, \dots, X_n)$. Let us build a basic belief assignment (bba) for the weights of the problem components. $m: X \to [0, 1]$, where $m(X_i) = x_i$,$0 < x_i < 1$.
$$\sum_{i=1}^{n} m(X_i) = \sum_{i=1}^{n} x_i = 1$$
2. In order to get the variable x_i in accordance with preferences R, build $m \times n$ linear homogeneous matrix $A = (a_{ij})$ as follows
$$\begin{Bmatrix} x_{1,1}w_1 + x_{1,2}w_2 + \cdots + x_{1,n}w_n = 0 \\ \cdots \\ x_{m,1}w_1 + x_{m,2}w_2 + \cdots + x_{m,n}w_n = 0 \end{Bmatrix}$$
$$A = \begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \cdots & \cdots & \cdots \\ x_{m,1} & \cdots & x_{m,n} \end{bmatrix}$$
3. Calculate the determinant $\det(A)$ of the matrix A. If $\det(A) = 0$, then the system is consistent. Otherwise, it's inconsistent.
4. After examine the problem consistency, if the problem is inconsistent, then do the following steps of α discounting:
   - Introduce a new matrix called A(α) by increasing or decreasing the right hand side with α, then compute α that makes the determinant equal 0 using the Fairness principle (equalize all parameters). Then, solve the system.
   - Substitute the secondary variables by 1 and then, normalize the result.

4.3 α-D MCDM in the Evaluation of Cyber Insecurities Categories of Cyber Supply Chains

α-D MCDM outperforms AHP in the evaluation of n-wise comparisons. According to the literature, we used the α-D MCDM in this study to quantify the cyber insecurities of cyber SCs. In order to use this approach, we consult with a SCM specialist who can provide us with advice on the relative importance of each category of supply chain cyber threats.

Let's propose that supply risks is x, operations risks is y, and demand risk is z. The following is the expert's preference:

i. Supply risks is as important as 2 times of operations risks plus 3 times of demand risks.
ii. Operations demand is 4 times as important as supply risks.
iii. Demand risks is 5 times as important as supply risks.

$$\begin{cases} x = 2y + 3z \\ y = 4x \\ z = 5x \end{cases} \qquad A = \begin{bmatrix} 1 & -2 & -3 \\ -4 & 1 & 0 \\ -5 & 0 & 1 \end{bmatrix}$$

As det ≠ 0, so right-side coefficient must be parameterized.

$$\begin{cases} x = 2\alpha_1 y + 3\alpha_2 z \\ y = 4\alpha_3 x \quad ;\text{ where } \alpha_{1,}\ \alpha_{2,}\alpha_{3,}\alpha_{4,}\alpha_{5,}\alpha_6 > 0\ . \\ z = 5\alpha_4 x \end{cases}$$

The α-D MCDM outperforms AHP in the evaluation of n-wise comparisons. According to the literature, we used the α-D MCDM in this study to quantify the cyber insecurities of cyber SCs. In order to use this approach, we consult with a SCM specialist who can provide us with advice on the relative importance of each category of supply chain cyber threats.

Then, we will solve the system:

$x = 2\alpha_1(4\alpha_3 x) + 3\alpha_2(5\alpha_4 x)$

$1 = 8\alpha_1\alpha_3 + 15\alpha_2\alpha_4$ Set 1 to the secondary variable

Let $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = \alpha > 0$

$1 = 8\alpha^2 + 15\alpha^2$ (Parametric equation)

$\alpha = \sqrt{23/23}$

$S = [1 \quad 4\alpha_3 \quad 5\alpha_4\,]$ (Priority vector)

$S = \left[1 \quad \frac{4\sqrt{23}}{23} \quad \frac{5\sqrt{23}}{23}\right]$

Normalized priority vector to find the weight of each cyber insecurities category.

$W = [0.3476, \quad 0.2899, \quad 0.3625]$

The α-D MCDM method was used to evaluate the three cyber insecurities of supply chains, and based on expert preferences, demand risks were found to be the superior element with a weight of 0.3625. The supply risks and operation risks are ranked second and third, with weights of 0.3476 and 0.2899, respectively as presented in Figure 1.

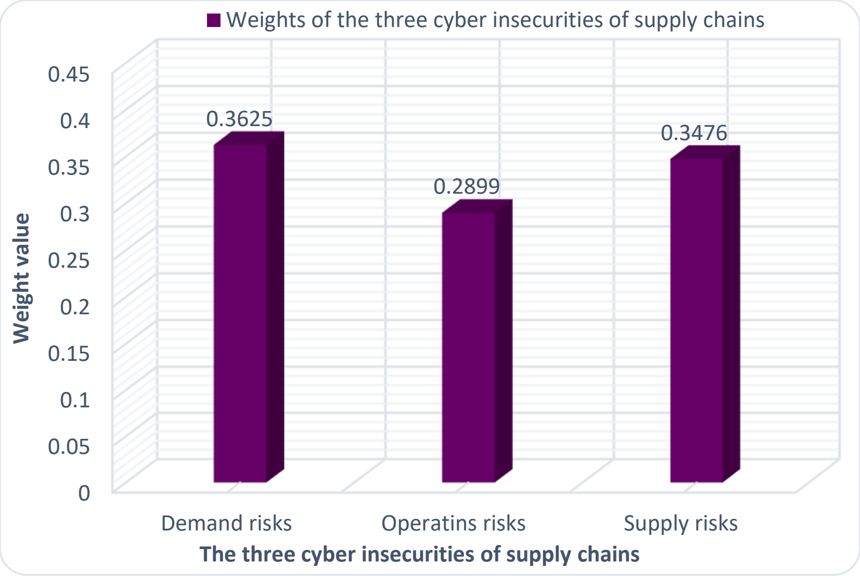

Figure 1. Weights of the three cyber insecurities of supply chains.

5. Conclusion and Future Works

Managing cyber insecurities in SCs is a significant concern for organizations seeking to remain competitive in today's market. The digital transformation of the supply chain has resulted in a platform with fewer silos. Risks that attacks data are higher than ever. While new technologies have provided up new supply chain management opportunities, they have also produced potential security holes that cybercriminals may exploit. Thus, in this study the cyber insecurities that facing the cyber supply chains have been highlighted. According to the literature, the cyber supply chain insecurities are categorized into three types: supply risks, operational risks, and demand risks. Also, the α-D MCDM method was discussed and applied to evaluate the three categories of cyber supply chain insecurities in sufficient manner.

Our future plan is to apply an integrated MCDM framework to evaluate the overall cyber insecurities that face the cyber supply chains as a result of the noticeable trend towards fourth and fifth generation technologies for industry. The integrated framework that suggested in the future studies is recommended to be as integration between α discounting method and other MCDM method to evaluate the main insecurities and its corresponding risks.

Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Data availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflict of interest

The authors declare that there is no conflict of interest in the research.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Boyens, J., Paulsen, C., Moorthy, R., Bartol, N., & Shankles, S. A. (2015). Supply chain risk management practices for federal information systems and organizations. NIST Special publication, 800(161), 32.
2. Mangan, J., & Lalwani, C. (2016). Global logistics and supply chain management. John Wiley & Sons.
3. Singh, R. K., Kumar, P., & Chand, M. (2019). Evaluation of supply chain coordination index in context to Industry 4.0 environment. Benchmarking: An International Journal, 28(5), 1622-1637.
4. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802-1831.
5. Latif, M. N. A., Aziz, N. A. A., Hussin, N. S. N., & Aziz, Z. A. (2021). Cyber security in supply chain management: A systematic review. LogForum, 17(1), 49-57.
6. Wiesner, S., & Thoben, K. D. (2017). Cyber-physical product-service systems. Multi-Disciplinary Engineering for Cyber-Physical Production Systems: Data Models and Software Solutions for Handling Complex Engineering Projects, 63-88.
7. Chhetri, S. R., Faezi, S., Rashid, N., & Al Faruque, M. A. (2018). Manufacturing supply chain and product lifecycle security in the era of industry 4.0. Journal of Hardware and Systems Security, 2, 51-68.
8. Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1), 103-128.
9. Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. Future internet, 11(3), 63.
10. Cheung, K. F., Bell, M. G., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. Transportation Research Part E: Logistics and Transportation Review, 146, 102217.
11. Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. IEEE Access, 9, 94318-94337.

12. Luo, S., & Choi, T. M. (2022). E-commerce supply chains with considerations of cyber-security: Should governments play a role?. Production and Operations Management, 31(5), 2107-2126.
13. Del Giorgio Solfa, F. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. International Journal of Technology, Innovation and Management (IJTIM), 2.
14. Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162-183.
15. Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. Supply Chain Management: An International Journal, 27(1), 30-53.
16. Hossain, N. U. I., Rahman, S., & Liza, S. A. (2023). Cyber-susiliency index: A comprehensive resiliency-sustainability-cybersecurity index for healthcare supply chain networks. Decision Analytics Journal, 100319.
17. Eggers, S. (2021). A novel approach for analyzing the nuclear supply chain cyber-attack surface. Nuclear Engineering and Technology, 53(3), 879-887.
18. Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics, 9(11), 1864.
19. Klötzer, C., & Pflaum, A. (2015, October). Cyber-physical systems as the technical foundation for problem solutions in manufacturing, logistics and supply chain management. In 2015 5th International Conference on the Internet of Things (IOT) (pp. 12-19). IEEE.
20. Revetria, R., Tonelli, F., Damiani, L., Demartini, M., Bisio, F., & Peruzzo, N. (2019, April). A real-time mechanical structures monitoring system based on digital twin, iot and augmented reality. In 2019 Spring Simulation Conference (SpringSim) (pp. 1-10). IEEE.
21. Babu, B., Ijyas, T., Muneer, P., & Varghese, J. (2017, March). Security issues in SCADA based industrial control systems. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 47-51). IEEE.
22. Inserra, D., & Bucci, S. P. (2014). Cyber supply chain security: A crucial step toward US security, prosperity, and freedom in cyberspace. The Heritage Foundation, 273-284.
23. Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of risk management implementation for Industry 4.0. Procedia manufacturing, 11, 1223-1230.
24. Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. Technology Innovation Management Review, 5(4), 28.
25. Smarandache, F. (2010, July). α-discounting method for multi-criteria decision making (α-d MCDM). In 2010 13th International Conference on Information Fusion (pp. 1-7). IEEE.
26. Smarandache, F. (2015). α-Discounting method for multi-criteria decision making (α-D MCDM). Infinite Study.
27. Karaman, A., & Dagdeviren, M. (2015). Fuzzy α-discounting method for multi-criteria decision-making. Journal of the Chinese Institute of Engineers, 38(7), 855-865.

Received: 15 Jul 2023, **Revised:** 30 Oct 2023,

Accepted: 05 Nov 2023, **Available online:** 23 Nov 2023.