The Relationship between Cyber Risk Management and Digital Transformation. A Bibliometric Analysis

Manuela CATRINA[1]
Alexandru-Mihai GHIGIU[2]

Abstract

Based on the manifold implications of the relationship between cyber risk management and digital transformation, the present paper intends to perform a bibliometric analysis stressing the main topics which have been investigated so far under this overarching research theme. The aim is to conduct a structured examination of cyber risk management in the context of digital transformation, with a focus on management practices. The bibliometric analysis was conducted following the steps in the PRISMA guidelines. 73 sources retrieved from Scopus database were analysed, covering 37 papers presented at conferences, 24 articles published in scientific journals, 8 book chapters and 1 full book together with 2 reviews and 1 conference review. In terms of research areas, the majority of studies came from the disciplines of engineering, computer science and social sciences. By using various approaches to assess cyber risks, the bibliometric analysis provides a solid framework for understanding and managing threats in a systematic and effective way. Moreover, the analyses reflect discrepancies between the perceived level of cybersecurity requirements and the actual level of preparedness and awareness of cyber risks in various industry sectors. This underlines the need for a more comprehensive and proactive approach to cybersecurity management, taking into account not only technologies and protection methods, but also cultural and organisational aspects.

Keywords: *cyber risk management, digital transformation, bibliometric analysis.*

JEL classification: O32; O 33; O39.

DOI: 10.24818/RMCI.2024.1.5

1. Introduction

Global cyber threats are becoming increasingly complex and dangerous, affecting diverse corporations in all industries as well as states and governments. As such, identifying and investing in the right digital technology is critical for firms to survive and thrive in this challenging environment (Fiksel and Fiksel, 2015). Digital risk management is the process by which companies determine which digital risks are most likely to cause the greatest financial loss (Walker,

[1] Manuela Catrina, Doctoral School in Management, National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania, manuela.catrina@gmail.com
[2] Alexandru-Mihai Ghigiu, Department of International Relations, National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania, mihai.ghigiu@dri.snspa.ro

2015). These are followed by the least likely hazards, but which, if they materialise, have the potential to cause significant losses (Hopkin, 2018). The damage in question can be of various types and can be suffered by organisations' networks and IT systems, including those that fall into the category of critical infrastructure targets.

According to Slovic et al. (2016), risk assessment is based on the probability of problems occurring, and this is done in descending order, starting with the most likely. Assessing the impact of risk is a challenging task, especially in the context of digital transformation, where effective risk management becomes crucial for the survival of organisations and their ability to generate revenue (Stark et al., 2014).

Eller et al. (2020) argue that businesses need to progress towards digitisation, which may require considerable effort on their part. Transitioning to digitisation requires additional costs, experienced specialists in the field, staff training, acquisition of new software and technologies, adaptation to them, etc. The transfer of essential firm materials to artificial intelligence or related applications, in particular, takes control from a human employee and transfers it to a software program, an entity with a lower level of trust than a person (Ali et al., 2023). In this context, organizations must manage a variety of emerging risks, including cybersecurity threats, data privacy concerns, and technology disruptions (Paquette et al., 2010; Skopik et al., 2016; Brass and Sowell, 2021).

Based on the manifold implications of the relationship between cyber risk management and digital transformation, the present paper intends to perform a bibliometric analysis stressing the main topics which have been investigated so far under this overarching research theme. To this end, the rest of the will look into the research methodology, the description of the processed data, the analysis of the thematic clusters, the identification of gaps and limitations in the field and will propose several future directions to explore.

2. Research methodology

The aim of this paper is to conduct a bibliometric analysis on cyber risk management in the context of digital transformation, with a focus on management practices. The bibliometric analysis was conducted following the steps in the PRISMA guidelines (Figure 1). The steps are designed to ensure the necessary transparency and rigour in selecting studies for a systematic review or meta-analysis. For this purpose, data were obtained from the Scopus database, founded by Elsevier. Scopus comprises an impressive collection of studies from over 7000 international publishers, totalling over 87 million documents.

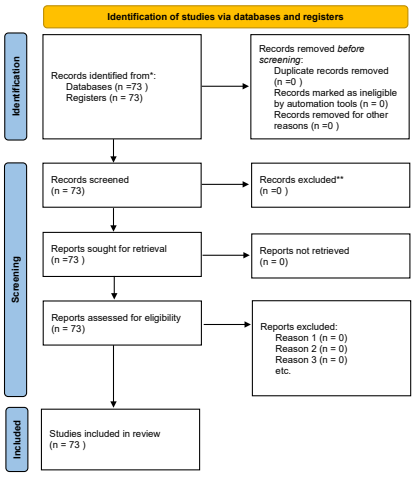

Figure 1. Systematic literature review procedure according to PRISMA guidelines, own processing

Given the limited number of sources available, the search strategy was designed to include all types of documents. Thus, out of the 73 sources analysed, 37 papers presented at conferences, 24 articles published in scientific journals, 8 book chapters and 1 full book were identified, together with 2 reviews and 1 conference review. In terms of research area, the majority of studies came from the disciplines of engineering, computer science and social sciences. Only 4 of these were devoted to the fields of business and management. However, as the subject under investigation is intrinsically cross-disciplinary, no exclusion criteria based on subject area were applied.

As seen in Table 1, the research on the relationship between cyber risks and digital transformation is a relatively new topic. This topic has an annual growth rate of 5.96%, and the papers reviewed have an average age of 2.4 years and an average of 5 citations per paper. In terms of the type of publications, most of the papers published are conference papers, followed by articles and book chapters.

General information about the extracted records

Table 1

Description	Results
MAIN DATA INFORMATION	
Time interval	2017:2024
Sources (Journals, books, etc.)	65
Documents	73
Annual growth rate % % Annual growth rate	5.96
Average age of the document	2.4
Average citations per doc	5

3. Main Findings

3.1 Identifying Patterns and Impact: Descriptive Scientific Metrics in Cyber Risk and Digital Transformation

Analysing publications and the year-on-year growth of research in cyber risk and digital transformation, Figure 2 highlights the main trends in research interest in this area. As can be seen from the keyword investigation, research peaked on this topic in 2022, with authors producing 21 articles, followed by 2023 with 20 articles, with the overall trend for the period 2017-2024 being one of growth. However, for the period 2017-2020, the scientific output is less relevant as the number of articles produced in this period is the same as the number of articles published in 2021, the difference being 1 article more than the reference year.

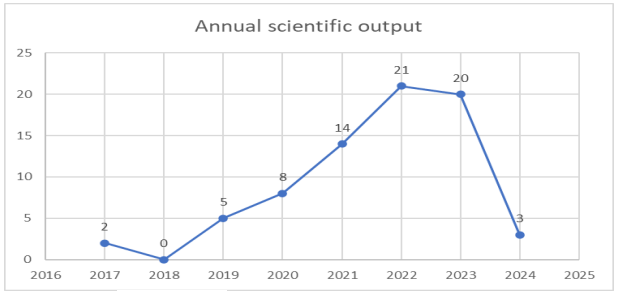

Figure 2. Annual scientific output

Regarding the most used sources in which the papers were published, they are mainly concentrated in 6 sources: 3 journals, totalling 8 articles on the conference website containing 6 papers. In addition, 4 papers were published in *Lecture Notes in Networks and Systems* and all other sources contain 2 papers/articles. The rest of the articles/papers were published in conference proceedings or international journals, with only one article/paper per journal/conference.

Most common sources

Table 2

Source	Document type	Number of articles
Lecture Notes in Networks and Systems	Conference paper	4
Business Horizons	Journal article	2
CEUR Workshop Proceedings	Conference paper	2
European Conference on Information Warfare and Security, ECCWS	Conference paper	2
Proceedings of the International Astronautical Congress, IAC	Conference paper	2
Studies in Systems, Decision and Control	Journal article	2

Most cited articles

Table 3

Authors	Type of publication	Total citations	Average citations/ year
Lee, I. (2021)	Journal	39	9,75
Petratos, P. N. (2021)	Journal	35	8,75
Gunes, B., Kayisoglu, G., & Bolat, P. (2021).	Journal	34	8,50
Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022).	Journal	25	12,50
Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022)	Journal	23	7,67
Teoh, C. S., & Mahmood, A. K. (2017).	Conference paper	23	2,88
Pisoni, G. (2021).	Journal	19	4,75

The relevance of the research is illustrated by analysing the number of citations generated by the Scopus database citation report. Table 3 illustrates the total and average number of citations for articles and papers published by researchers on cybersecurity and digital transformation. The most cited papers with an average of more than 8.5 citations/year were published in 2021 in academic journals and have been cited from 2021 to date by more than 34 other researchers.

Applying Bradford's Law to the findings in Figure 3 and Table 4, it can be concluded that there is a somewhat uniform distribution of fundamental sources among the three identified regions, the first of which has 17 items, while the other two regions each have 24 items. Furthermore, the distribution of the number of items per individual area is uniform, with each area having an average distribution of 33%. Specifically, this implies that the allocation of research resources was balanced, consistent with the pattern predicted by Bradford's Law, reflecting the diversity and balance of academic output.

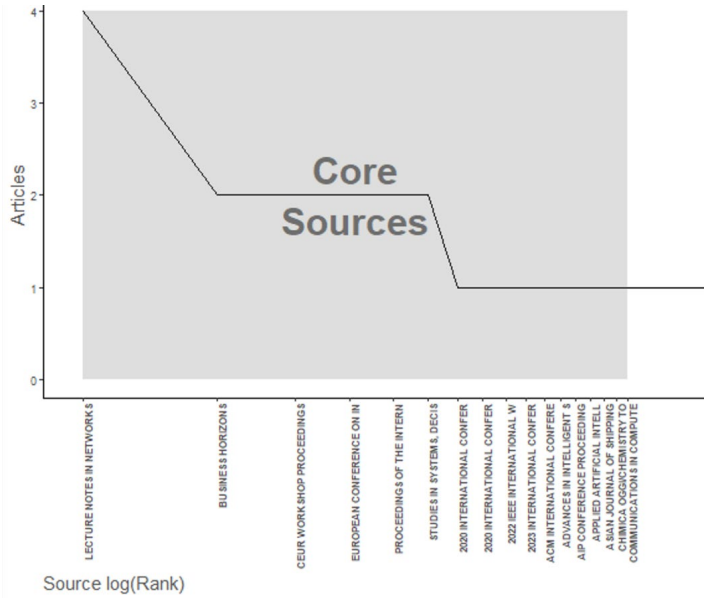

Figure 3. Bradford's Law Grouping of Sources

Distribution of journals by area

Table 4

Zone	Journal	% Journal	Articles	% Articles
1	17	26,15%	25	34,25%
2	24	36,92%	24	32,88%
3	24	36,92%	24	32,88%
Total	65	100%	73	100%

In addition, analysing from the perspective of Lotka's Law, the majority of authors (i.e. 255 authors) address the topic of cybersecurity and digital transformation, while only five authors wrote on adjacent topics, thus indicating a high degree of compliance with Lotka's Law, the results of which are shown in Table 5.

Calculations for Lotka's law

Table 5

Written documents	Number of authors	% of authors
1	255	0,98076923
2	5	0,01923077

In this context, the authors whose contributions are considered most relevant are those who have written at least two reference works, exemplified by people such as Carlo A, Casamassima F, Gkioulos V, Katsikas S and Kavallieratos G, as shown in Figure 4.

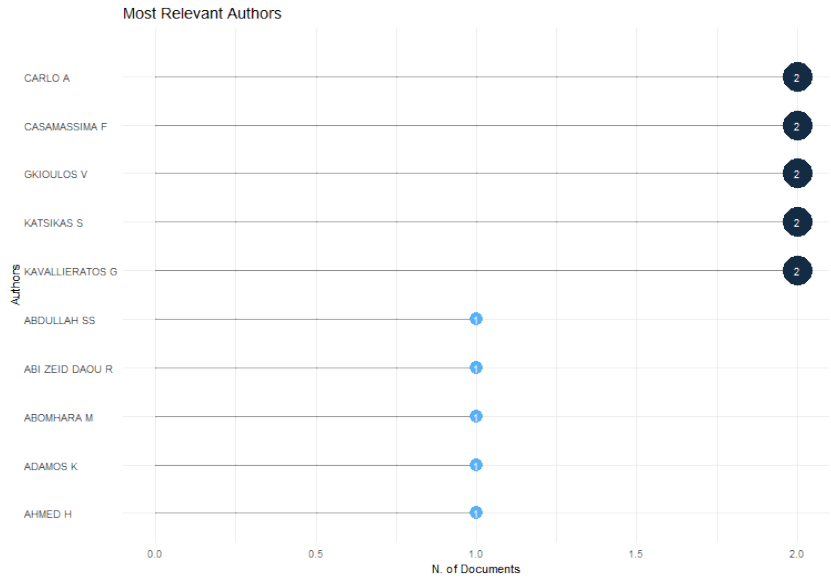

Figure 4. Most relevant authors

In the first phase, when analysing preliminary data, the descriptive analysis of the link between cybersecurity and digital transformation led to the conclusion that it is still in its infancy, and this connection was poorly researched by the authors, indicating a low number of citations and articles. On the other hand, it is to be appreciated that there are efforts made by researchers in this direction, as well as an increased interest, with the majority of papers published in the last 5 years, with an upward publishing trend.

3.2 Clustering in the Academic Literature: an In-Depth Examination

In order to identify and explore the existence of different building themes on the relationship between cybersecurity and digital transformations, Figure 6 shows a map of the main themes addressed, as well as the clusters formed (Table 6), generated using the "Bibliometrix" software. As can be seen in Figure 6, 12 clusters have been identified on accident prevention, big data, critical infrastructures, cyber threats, cyber vulnerabilities, electricity, transport networks, industry 4.0, manufacturing, personal computing, risk assessment, risk management and data security, with each cluster named by the keywords described.

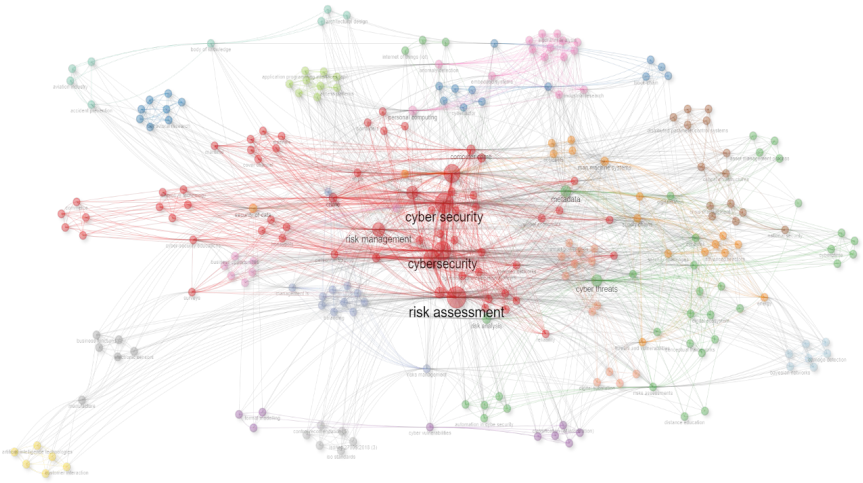

Figure 6. Thematic map

Continuing the analysis, the generated clusters were grouped into 12 main themes based on the relationship with centrality and density indicators, as shown in Figure 7 and Table 6. Keywords related to the two main themes are shown in Table 7.

Table 6 provides a detailed overview of relevant clusters and themes in the field of cyber security and risk management. Clusters such as "Risk assessment", "Cyber threats" and "Security of data" are fundamental to the discussion of cyber security, reflecting significant levels of centrality and density. They suggest an increased concern for assessing and managing risks associated with data security and cyber threats.

On the other hand, clusters associated with emerging themes such as "Big data" and "Cyber vulnerabilities" suggest an increasing focus on risk management in the context of big data and cyber vulnerabilities. These clusters may be less central and dense, but point to an important direction for cyber security research and practice.

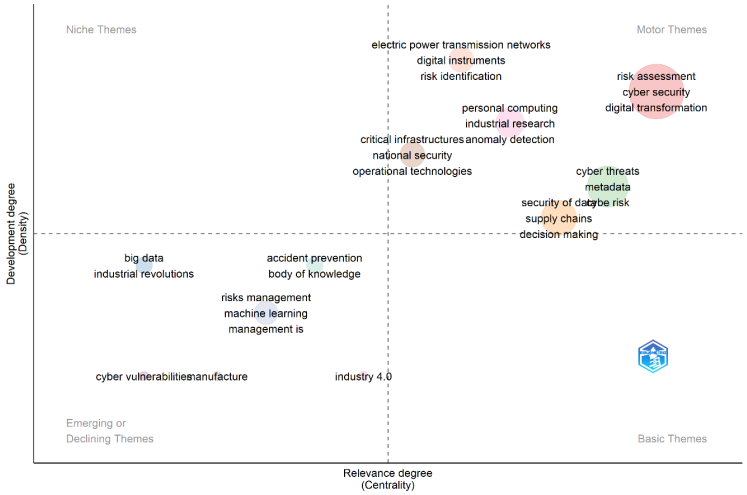

Figure 7. Thematic evolution

At the same time, the cluster and theme analysis provides a comprehensive perspective on various aspects of cybersecurity and risk management, highlighting areas of interest and priorities for organisations and researchers in this evolving field.

Works on topics of interest

Table 6

Thematic	Centrality	Density	Centrality level	Density level	Theme frequency	Main Theme
Risk assessment	11,15	93,37	12	11	171	**Driving theme**: cyber security
Cyber threats	7,01	78,10	11	8	45	**Driving theme:** cyber security
Data security	4,76	74,31	10	7	25	**Driving theme**: cyber security
Critical infrastructures	1,06	79,17	7	9	9	**Driving theme:** cyber security
Personal computers	2,30	81,67	9	10	13	**Driving theme:** cyber security
Electricity transmission networks	1,39	95,83	8	12	9	**Driving theme:** cyber security
Big data	0,00	62,50	1,5	5,5	4	**Emerging theme**: risk management
Cyber vulnerabilities	0,00	50,00	1,5	2	2	**Emerging theme:** risk management
Manufacture	0,25	50,00	3	2	2	**Emerging theme:** risk management
Accident prevention	0,50	62,50	5	5,5	4	**Emerging theme:** risk management
Risk management	0,46	58,33	4	4	8	**Emerging theme:** risk management
Industry 4.0	0,75	50,00	6	2	2	**Emerging theme**: risk management

Table 7 presents the analysis of themes and keywords associated with cyber security and risk management. The main themes, such as "Risk assessment", "Cyber security" and "Digital transformation", are highlighted by their high number of occurrences and high values of centrality measures. These are considered central to the discussion of cyber security. In contrast, keywords in emerging themes, such as 'Big data' and 'Cyber vulnerabilities', have lower centrality values, suggesting less importance or more recent relevance within the field.

The main themes resulted from grouping the clusters into themes

Table 7

Theme	Keywords	Appearances	Btw centrality	Close centrality	Centrality page rank
Driving theme: cyber security	Risk assessment	23	4.449,94674	0,00239234	0,03905053
	Cyber security	20	3.073,58912	0,00242718	0,0352365
	Digital transformation	18	2.779,53005	0,00234742	0,02902044
	Network security	15	2.926,13935	0,00235849	0,02876693
	Risk management	10	2.054,14476	0,00226757	0,01884125
	Cyber attacks	9	792,632121	0,0021097	0,01761961
	Cyber threats	9	1.152,12534	0,00217865	0,01554324
	Risk perception	7	830,891983	0,00205761	0,01325352
	Metadata	7	1.173,77146	0,00217391	0,01327256
	Cybercrime	6	525,608995	0,0021645	0,01125582
	Crime	6	332,705756	0,00199601	0,01099077
	Internet of Things	6	395,301019	0,00196464	0,00959101
	Data security	6	1.140,27619	0,00215517	0,00936171
	Systems security	4	248,501024	0,00205761	0,00882826
	Cyber risks	4	303,761837	0,00200401	0,00718288
	Digitisation	4	325,214155	0,0020284	0,00740118
Emerging theme Risk management	Big data	2	134,467617	0,00204499	0,00400421
	Industrial Revolutions	2	118,509314	0,00203252	0,00340971
	Cyber vulnerabilities	2	77,3125152	0,00193424	0,00346415
	Manufacture	2	103,517894	0,00172712	0,00396167
	Accident prevention	2	40,4975126	0,00193798	0,00266808
	Body of knowledge	2	57,2886765	0,00201613	0,00315769
	Risk management	4	347,021321	0,00206186	0,00743196
	Machine learning	2	219,434332	0,00212314	0,00519352
	Management	2	170,319102	0,00210526	0,00491708
	Industry 4.0	2	160,463201	0,00207469	0,00424324

Theme 1 - Cyber Security

The rapid development of the Internet and the software industry has led to the emergence of vulnerabilities in the market, especially in the cyber system (Sun et al., 2018), thus affecting the physical infrastructure of companies, the economy and even society, each of us is exposed to such risks, society is exposed to an exponential increase in access to information, being able to access information for which the degree of truth is less identifiable (Kaur and Ramkumar, 2022).

When we talk about cybersecurity, we focus primarily on ensuring the integrity, confidentiality and availability of data belonging to one organization or connecting to another organization's network (Ahmad et al., 2020). On the other hand, the threats we may be exposed to are diverse (cryptographic attack, access attack, malware attack, etc.) and can greatly influence human behavior (Aslan et al., 2023). Moreover, technological developments have led to the economy being a knowledge economy, resulting in their actions in innovative services and products based on the digital process (Garcia-Perez et al., 2023). By this, business digitization refers to the updating of companies' current processes with new technologies (Saeed et al., 2023). As digitization plays a key role in an organization's success, cybersecurity should be a key factor in risk management (Lee, 2021).

In order to manage cybersecurity threats, it is necessary to implement a risk management system that manages and defends the infrastructure against the dangers that may arise (Gain et al., 2020). Thus, it is necessary to manage the risks to which organisations are exposed, with risk management having the role of ensuring data integrity and confidentiality through effective security systems (Metin et al., 2024).

Based on the arguments presented above, the most relevant studies analysing the relationship between cyber security and digital transformation are presented in Table 8.

Studies on the impact of cyber security and digital transformation

Table 8

Study	Type of work	Research method
Gunes et al. (2021)	Article	Cyber risk assessment method
Ashraf et al. (2022)	Article	Cybersecurity survey and testing
Teoh and Mahmood (2017)	Conference paper	Case study
Kechagias et al. (2022)	Article	Case study
Kessler et al. (2022)	Article	Case study
Omerovic et al. (2019)	Conference paper	Model-based risk analysis
Franke et al. (2020)	Conference paper	Case study

The study proposed by Gunes et al. (2021) explores the cybersecurity risk assessment for seaports using a container port as a case study. Ports are key components of maritime transport systems and have undergone a digital transformation in the context of Industry 3.0 and 4.0, becoming part of intelligent transport systems. The study proposes the application of an integrated cyber risk assessment method for a container port with a cyber-physical perspective by analysing four exemplary cyber attack scenarios. For each cyber attack scenario, a risk assessment methodology was applied using an integrated cyber security management approach, taking into account the cyber-physical assets of the container port. The results indicate that, for the specified cyber threats, the risks were assessed as unacceptable. Mitigation strategies were also briefly presented in the conclusion.

Furthermore, Ashraf et al. (2022) analyzed the impact of cyber threats on the maritime industry, focusing on maritime security, privacy, integrity and availability. Using risk assessment methods, potential threats are analyzed and cyber risk mitigation schemes and frameworks are proposed. The results highlight the need to implement effective security policies to protect maritime assets and suggest countermeasures to mitigate the impact of future cybersecurity challenges. On the other hand, Teoh and Mahmood (2017) investigated the relationship between the development of the National Cyber Security Strategy (NCSS), the success of a nation's digital economy, and the methodology involved in analyzing the NCSS of 9 countries by digital economy success. They find that the country with the largest digital economy launched its most recent NCSS in 2016. The conclusion that NCSS is not a necessity to initiate the digital economy, but is essential to its growth and success continues.

Kechagias et al. (2022) set out to connect research and practice in maritime industry cybersecurity by presenting a detailed case study analysis as a methodology. The authors focus on a real-world company's systemic approach to cybersecurity, referring to procedures and policies in order to assess its current state, gather evidence, objectively determine security gaps and reduce cyber risk. The results of the case study and audit study demonstrate that the company has successfully identified security gaps and implemented appropriate measures to mitigate cyber risk, providing valuable information for continuous improvement and future proactive measures.

Kessler et al. (2022) explored the relationship between Industry 4.0 technologies and supply chain risks using a methodology comprising 300 case studies of industrial practice in Germany and 53 interviews with relevant managers and experts. The results indicate that while digital technologies are being adopted to address existing supply chain risks, they also introduce new sources of risk, such as cyber risks. Building on *Normal Accident Theory*, a framework for elucidating the determinants and unforeseen factors of these new risks is proposed, with practical recommendations provided for supply chain managers based on the technology life cycle.

An interesting analysis by Omerovic et al. (2019) who proposed and validated a custom four-step approach for identifying and modeling cybersecurity risks in smart energy grids. This approach aims to address the challenges arising from the interdisciplinary nature of risk analysis in this context, encompassing digital security, energy domains, energy networks, control systems and human factors. Methodologically, the study applies components of the "CORAS" method for model-based risk analysis. Empirically, the paper reports results and experiences derived from the application of this approach to a realistic industrial case involving a distribution system operator (DSO) responsible for hosting a pilot plant with self-healing functionality within an electricity distribution network. The evaluation of the approach demonstrates its feasibility in identifying cybersecurity risks in a practical setting. In addition, the experiences from the case study highlight the suitability of the proposed approach for its intended purpose, although it also points to areas requiring further refinement and evaluation.

In a research effort, Franke et al. (2020) analyzed the complexity of cybersecurity protocols in the context of Swedish manufacturing firms amidst the disruptive wave of Industry 4.0. Using a methodological framework based on an industry survey conducted in collaboration with the renowned *Swedish Association of Engineering Industries*, the authors' analysis reveals a discernible dissonance. Despite the pervasive adoption of digitization within these manufacturing entities, our findings suggest a palpable disconnect between the perceived demand for cybersecurity measures and the commensurate level of concern about the associated risks.

Theme 2 - Risk management and digital transformation

One of the biggest drivers of change in the digital age is the digital transformation of business processes, products and services (Rogers, 2016). Digital transformation can create value, innovation, and competitive advantage, but it can also introduce new risks, such as cyberattacks, data breaches, security breaches, regulatory compliance, and disruption to various services. To effectively manage these risks, it is necessary to align risk strategy with digital strategy and adopt a proactive, agile and integrated approach (Banciu et al., 2023; Mizark, 2023). Digital tools and platforms, such as cloud computing, artificial intelligence and analytics, should also be used to improve risk capabilities, visibility and resilience (Radanliev et al., 2020; Dubey et al., 2022; Gupta et al., 2022; Aljohani, 2023).

The goal of risk management is to limit potential negative effects and increase positive ones through a continuous, methodical process of risk discovery, assessment and control. The primary objectives of risk management are to predict, evaluate and control events that may impact an organization's or an individual's objectives and operations (Borghesi and Gaudenzi, 2012). In other words, risk management is a process that consists of identifying risks, qualitative and quantitative assessment, and responding with an appropriate method of treatment and control (Taofeed et al., 2019). Banaitiene and Banaitis (2012) found that expertise and existing knowledge in the field of the many forms of risk are as

important as having an appropriate and systematic methodology when it is necessary to carry out risk management in an effective way.

As technology becomes central to business models, decision makers are increasingly challenged to maintain operational excellence while accelerating digital strategy (Brenner, 2018; Martínez-Peláez et al., 2023). However, C-suite (top managers) and front-line representatives know that it is often the operational requirements of technology that consume the most resources (Andriole and Barsky, 2022). Ultimately, strategic competitiveness will not be determined by how well or poorly companies modernise their 'systems', but by how well they reimagine their digital future (Williamson , 2017; Ross et al., 2019).

Therefore, to remain competitive, executives need to focus on the urgency of digital strategy imperatives rather than the status of cloud-distributed IT projects. Three meaningful questions and three actionable steps can significantly support the development of digital strategies that work (Debauche et al., 2022; Zeb et al., 2023; Bazi et al., 2022).

Looking at these issues, some of the most relevant studies addressing the relationship between risk management and digital transformation are presented in Table 9.

Studies on the impact of risk management and digital transformation

Table 9

Study	Type of work	Research method
Ifthikar et al. (2022)	Article	Case study
Assante et al. (2023)	Conference paper	Case study
Safitri and Kabetta, 2023	Conference paper	Case study
Kang (2023)	Article	Case study
Petrenko et al. (2021)	Conference paper	Content analysis of standards
El-Hajal et al. (2021)	Conference paper	Case study

According to Ifthikar et al. (2022), the rise of digital transformation has brought more cyber risks, especially in terms of *RESTful APIs*, which act as a main channel connecting countless users, companies and data. As organisations increasingly rely on APIs for their operations, hackers are targeting them more often. Traditional methods are used to detect these attacks due to the unique nature of API access patterns. To address this challenge, the authors set out to use a new way of doing things, this combining anomaly detection and classification using Artificial Intelligence. This system monitors API traffic, learns its patterns and alerts administrators to any suspicious activity, ensuring cyber security. The results of the experiment confirm the effectiveness of this system in accurately detecting API attacks.

On the other hand, digital transformation has brought both opportunities and risks to business. Cybersecurity is a pressing concern, especially for Small and Medium-sized Enterprises (SMEs), which are particularly vulnerable. SMEs often lack in-house IT expertise, leaving them unprepared to tackle cyber threats. There is therefore a critical need to raise awareness among SME management of the importance of implementing robust IT security policies and providing adequate training to staff. The Erasmus+ InCyT (Interdisciplinary Cyber Training) project aims to address this gap by providing tailored training to SME staff lacking IT skills. The project identifies and addresses the training needs of both managers and employees through two separate training courses.

Digital transformation, which continues in both the government and private sectors, has improved the quality of services, but has also increased cyber threats. In order to address risks to organisational assets, effective cyber risk management planning is crucial. The ABC organization, an IT-focused entity, has no prior risk management planning for its assets, leaving them vulnerable to recurring risks. This study aims to develop a cyber risk plan for ABC's ICT unit using three security standards: the NIST CSF v1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5. The research identified 105 risk scenarios within the ICT unit, resulting in 64 accepted risks and 43 mitigated risks, along with 86 control recommendations tailored to the organization's specific risks, aiming to effectively control cyber risks (Safitri and Kabetta, 2023).

However, risk management is crucial for organisations, allowing them to navigate potential financial losses and make informed decisions. In the digital realm, effective risk management involves identifying and mitigating cyber threats to protect data integrity and reputation. For example, the rapidly advancing technology sector is increasingly vulnerable to cyber risks, including data breaches. Kang (2023) proposed the integration of explainable machine learning (exML) techniques in large-scale agriculture to improve cyber risk analysis and mitigate threats. The framework includes statistical analytical modeling and a multi-criteria objective function to balance investment value and cost. By leveraging exML and addressing key motivations such as cyber security, data protection and economic sustainability, the method provides a comprehensive approach to cyber risk analysis in large-scale agriculture with the goal of effectively adapting to evolving technology landscapes.

In another vein, Petrenko et al. (2021) analyzed the complexity of cyber risks and the identification of their components, such as threats and vulnerabilities, based on the level of detail required. The research method involves examining the requirements for detailing cyber risks at different levels of organizational maturity, focusing in particular on the base level where specific requirements may be lacking. For example, the German BSI standard provides a typical cyber threat catalogue for component information infrastructure, providing a level of completeness but at the same time leading to some challenges in assessing risk levels and countermeasure effectiveness. The results highlight the advantages and disadvantages of using standard lists of cyber risk classes, highlighting the need for

more specific risk assessments to accurately assess cyber risk levels and design effective countermeasures.

At the same time, El-Hajal et al. (2021) addressed the increasing frequency of cyber incidents exacerbated by the COVID-19 pandemic-induced digital transformation in enterprises. As cyber threats expand, representatives of top leadership recognize the criticality of cybersecurity in their transformation efforts, especially in the context of balancing the situation with limited resources at hand. In order to prioritize actions effectively, the research develops a procedure to calculate risk scores (RS) for detected cyber threats and to obtain priority scores (PS) needed to rank threats. This approach helps businesses to identify and prioritise actions needed to ensure data integrity, confidentiality and availability, enabling informed decision-making in mitigating cyber risks.

4. Gaps in the Studies Carried Out and Limitations of Scientific Research

As a result of our scientific research on the relationship between cyber risk management and digital transformation, we have identified a number of issues of interest that have not been addressed in studies conducted to date by other researchers. These are novel and the results of their approach could be of interest for both Romanian and EU authorities.

In this context, we mention Emerging and Disruptive Technologies (*EDT*), which have the potential to radically change the way industry or society operates, as well as create new business and development opportunities. Some emerging disruptive technologies in IT could be the following.

1. Web 3.0 represents a major next generation and revolution of the internet, smarter and more connected to cyberspace than previous versions, which will offer new opportunities for users and radically change the way we connect and interact with the digital world. Web 3.0 is likely to integrate technologies such as the internet of things and artificial intelligence and be better able to process and understand structured and unstructured data so that it can provide more relevant and personalised results to users' searches. Some experts believe that Web 3.0 will be more focused on connecting users to apps and services through smart devices, such as voice assistants and other smart home devices. Either way, Web 3.0 is expected to be an important evolution of the Internet.

2. Quantum computing is a branch of computer science that focuses on using quantum phenomena to process information. Quantum computers can solve certain types of highly complex problems (route optimisation or data encryption) in a much shorter time than would be possible for traditional computers.

3. Quantum as a Service (QaaS) is a form of cloud computing that provides access to quantum computing services over the internet. This means that users can access and use quantum computing power through a cloud computing platform

4. Artificial Intelligence (AI) has the potential to radically change the way many industries operate, including cybersecurity, risk management, financial services, healthcare, retail, transport services, etc.

5. The Internet of Things (IoT) can revolutionise the way industrial devices and processes are monitored and controlled, with the potential to offer new opportunities for efficiency and automation. On the other hand, internet-connected devices, controlled by an attacker without the owners' knowledge, can be used to launch various types of cyber attacks. These present a real danger given the multitude of active IoT devices, many of which are poorly secured and have many vulnerabilities.

6. Virtual and augmented reality (VR and AR) technologies enable the creation of "immersive digital environments" that can be used to provide new and unique learning or entertainment experiences. They can also provide new business opportunities and radically change the way entertainment and training is delivered.

7. Big data refers to large sets of data that are collected by companies, governments and other organisations to be analysed and used to improve services or decision-making. Big data analytics is the process of processing and analyzing large amounts of data to identify trends and patterns in the data, make recommendations and predictions, improve efficiency and productivity, make informed decisions, etc.

8. Datafication is the process of transforming unstructured information into structured data that can be processed and analysed by computer systems. Datafication can be used to improve efficiency and productivity, informed decision-making, to make predictions and recommendations and for other specific purposes.

EDTs are increasingly present in our lives, touching multiple aspects of the modern world, which is why it is important to consider the balance between innovation and security. On the one hand, emerging technologies will bring multiple benefits to mankind, but on the other hand they will generate various challenges, as they can also be used for malicious purposes, cyber attacks, disinformation, deep fakes, etc. While there is currently no guarantee that all of these technologies will truly revolutionise industries or society, it is important that ITC experts are prepared to face new and increasingly complex cyber risks and attacks in order to protect critical information infrastructures, networks and information systems, citizens and the digital single market.

As for the limitations of research, these are related to the complexity and rapid evolution of emerging technologies, which can emerge unexpectedly and cause significant shocks to companies and the market, while having the potential to change the entire structure of the industry or market and create new categories of products or services that rapidly replace existing ones. In this context, we believe that problems may arise in identifying an adequate amount of topical data that is available or reliable to be properly analysed in this paper in order to obtain realistic results. Also, the researcher's inability to have access to certain documents or limited access to certain people for interviews in order to obtain relevant

information can be limitations of scientific research. At the same time, issues related to data measurement and analysis may be limitations of the research. Ethical limitations can be considered in terms of the fact that the research must respect certain ethical principles, such as issues of confidentiality of participants or their rights, and the type of information obtained. On the other hand, some data or sources of information may be inaccessible or limited.

However, aspects that are currently limitations of the present scientific work may constitute new research directions, which can be addressed at a later stage to extend the study.

5. Final Considerations

By analysing the relationship between cybersecurity and digital transformation, we have identified a detailed perspective on the importance of cybersecurity in a variety of areas, including for the maritime industry and in the context of digital transformation. Through the bibliometric analysis, we have identified the considerable risks associated with cyber threats, such as attacks on critical infrastructure and important assets. In addition, it highlighted the urgent need to develop and implement effective policies and strategies to counter these risks and to protect information systems and networks as well as sensitive data.

By using various approaches and methods to assess cyber risks, bibliometric analysis provides a solid framework for understanding and managing threats in a systematic and effective way. They also provide practical solutions and recommendations for mitigating risks and building resilience to cyber attacks. Moreover, the analyses reflect discrepancies between the perceived level of cybersecurity requirements and the actual level of preparedness and awareness of cyber risks in various industry sectors. This underlines the need for a more comprehensive and proactive approach to cybersecurity management, taking into account not only technologies and protection methods, but also cultural and organisational aspects.

In conclusion, risk management is fundamental to any organisation, enabling it to manage potential negative impacts and capitalise on opportunities. It is a continuous and methodical process that involves identifying, assessing and controlling risks to prevent or minimise their impact on the organisation's objectives and operations. The studies reviewed highlight the importance of risk management in the context of digital transformation and increasing cyber threats. Developing appropriate plans and procedures, as well as using emerging technologies such as explainable machine learning, can help make addressing cyber risks more efficient. It is essential for organisations to be proactive in managing risks and to allocate adequate resources to ensure security and data protection in an ever-changing and increasingly complex environment.

References

1. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020) How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology, 71*(8), 939-953.
2. Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J. M., Confalonieri, R., ... & Herrera, F. (2023). Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. *Information Fusion, 99*, 101805.
3. Aljohani, A. (2023). Predictive analytics and machine learning for real-time supply chain risk mitigation and agility. *Sustainability, 15*(20), 15088.
4. Andriole, S. J., & Barsky, N. P. (2022) Why Digital Strategy & Operational Technology Must Remain Perfect Strangers. California Management Review Insights.
5. Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in IoT - enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2677-2690.
6. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333.
7. Assante, D., Fornaro, C., Hamburg, I., Gokdemir, A., Kieseberg, P., Oz, F., ... & Vladut, G. (2023, March). Cybersecurity Education for SMEs. In *International Conference on Remote Engineering and Virtual Instrumentation* (pp. 569-576). Cham: Springer Nature Switzerland.
8. Banaitiene N, Banaitis A. 2012. *Risk management in construction projects*. Rijeka (Croatia): INTECH Open Access Publisher.
9. Banciu, D., Vevera, A. V., & Ion, P. O. P. A. (2023). Digital Transformation Impact on Organization Management and Several Necessary Protective Actions. *Studies in Informatics and Control, 32*(1), 49-56.
10. Borghesi, A., & Gaudenzi, B. (2012) *Risk management: How to assess, transfer and communicate critical risks* (Vol. 5). Springer Science & Business Media.
11. Brass, I., & Sowell, J. H. (2021). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance, 15*(4), 1092-1110.
12. Brenner, B. (2018) Transformative sustainable business models in the light of the digital imperative-A global business economics perspective. *Sustainability, 10*(12), 4428.
13. Bzai, J., Alam, F., Dhafer, A., Bojović, M., Altowaijri, S. M., Niazi, I. K., & Mehmood, R. (2022). Machine Learning-Enabled Internet of Things (IoT): Data, Applications, and Industry Perspective. *Electronics, 11*(17), 2676.
14. Debauche, O., Mahmoudi, S., Manneback, P., & Lebeau, F. (2022). Cloud and distributed architectures for data management in agriculture 4.0: Review and future trends. *Journal of King Saud University-Computer and Information Sciences, 34*(9), 7494-7514.
15. Dionne, G. (2013). risk management: history, definition, and critique. *Risk Management and Insurance Review, 16*(2), 147-166.
16. Dubey, R., Bryde, D. J., Dwivedi, Y. K., Graham, G., & Foropon, C. (2022) Impact of artificial intelligence-driven big data analytics culture on agility and resilience in humanitarian supply chain: A practice-based view. *International Journal of Production Economics, 250*, 108618.

17. El-Hajal, G., Abi Zeid Daou, R., & Ducq, Y. (2021). A novel approach to classify vulnerabilities based on authenticated measurements In *IT Convergence and Security: Proceedings of ICITCS 2021* (pp. 91-98) Springer Singapore.
18. Eller, R., Alford, P., Kallmünzer, A., & Peters, M. (2020). Antecedents, consequences, and challenges of small and medium-sized enterprise digitalization. *Journal of Business Research, 112*, 119-127.
19. Fiksel, J., & Fiksel, J. R. (2015). *Resilient by design: Creating businesses that adapt and flourish in a changing world*. Island Press.
20. Franke, U., & Wernberg, J. (2020). A survey of cyber security in the Swedish manufacturing industry. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (CyberSA) (pp. 1-8). IEEE.
21. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis, 40*(1), 183-199.
22. Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation*. Technovation, 121*, 102583.
23. Glette-Iversen, I., Flage, R., & Aven, T. (2023). Extending and improving current frameworks for risk management and decision-making: A new approach for incorporating dynamic aspects of risk and uncertainty. *Safety Science, 168*, 106317.
24. Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security, 103*, 102196.
25. Gupta, S., Modgil, S., Kumar, A., Sivarajah, U., & Irani, Z. (2022). Artificial intelligence and cloud-based Collaborative Platforms for Managing Disaster, extreme weather and emergency operations. *International Journal of Production Economics, 254*, 108642.
26. Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.
27. Ifthikar, A., Thennakoon, N., Malalgoda, S., Moraliyage, H. K., Jayawickrama, T., Madushanka, T., & Hettiarachchi, S. (2022). A Novel Anomaly Detection Approach to Secure APIs from Cyberattacks.
28. Kang, Y. (2023). Development of Large-Scale Farming Based on Explainable Machine Learning for a Sustainable Rural Economy: The Case of Cyber Risk Analysis to Prevent Costly Data Breaches. *Applied Artificial Intelligence, 37(*1), 2223862.
29. Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. Journal of King Saud University-Computer and Information *Sciences, 34*(8), 5766-5781.
30. Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure *Protection, 37*, 100526.
31. Kessler, M., Arlinghaus, J. C., Rosca, E., & Zimmermann, M. (2022). Curse or Blessing? Exploring risk factors of digital technologies in industrial operations. *International Journal of Production Economics, 243*, 108323.
32. Kobrin, S. J. (2022). *Managing political risk assessment: Strategic response to environmental change*. Univ of California Press.
33. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons, 64*(5), 659-671.

34. Martínez-Peláez, R., Ochoa-Brust, A., Rivera, S., Félix, V. G., Ostos, R., Brito, H., ... & Mena, L. J. (2023) Role of digital transformation for achieving sustainability: mediated role of stakeholders, key capabilities, and technology. *Sustainability, 15*(14), 11221.
35. Metin, B., Duran, S., Telli, E., Mutlutürk, M., & Wynn, M. (2024). IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation that Engenders a Security Culture. *Information, 15*(1), 55.
36. Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management, 10*(3), 98-108.
37. Omerovic, A., Vefsnmo, H., Erdogan, G., Gjerde, O., Gramme, E., & Simonsen, S. (2019). A feasibility study of a method for identification and modelling of cybersecurity risks in the context of smart power grid. In *COMPLEXIS 2019-Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk 2019*. SciTePress.
38. Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010) Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly, 27*(3), 245-253.
39. Petrenko, A. A., Petrenko, S. A., Makoveichuk, K. A., & Olifirov, A. A. (2021). Methodological recommendations for the cyber risks management. In CEUR Workshop Proceedings (Vol. 2914, pp. 234-247). CEUR.
40. Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., ... & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity, 3*(1), 1-21.
41. Rogers, D. L. (2016). *The digital transformation playbook: Rethink your business for the digital age*. Columbia University Press.
42. Ross, J. W., Beath, C. M., & Mocker, M. (2019). *Designed for digital: How to architect your business for sustained success*. MIT Press.
43. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), 6666.
44. Safitri, E. H. N., & Kabetta, H. (2023, August). Cyber-Risk Management Planning Using NIST CSF V1. 1, ISO/IEC 27005: 2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization). In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 332-338). IEEE.
45. Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., & García-Muiña, F. E. (2021). Flexibility and resilience in corporate decision making: a new sustainability-based risk management system in uncertain times. *Global Journal of Flexible Systems Management, 22*(Suppl 2), 107-132.
46. Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security, 60*, 154-176.
47. Slovic, P., Fischhoff, B., & Lichtenstein, S. (2016). Facts and fears: Understanding perceived risk. In *The perception of risk* (pp. 137-153). Routledge.
48. Stark, A., McConnell, A., & Drennan, L. T. (2014). *Risk and crisis management in the public sector*. Routledge.

49. Sun, C.C., Hahn Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: state-of-the-art. *International Journal of Electrical Power & Energy Systems, 99*, 45-56.
50. Taofeed DM, Adekele AQ, Hassan AK. 2019. Factors affecting contractor's risk attitude from Malaysia construction industry perspective. *Soc Sci Hum Journal, 3*(6), 1281-1298.
51. Teoh, C. S., & Mahmood, A. K. (2017, July). National cyber security strategies for digital economy. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.
52. Walker, R. (2015). The increasing importance of operational risk in enterprise risk management. *The Journal of Enterprise Risk Management, 1*(1), 82-96.
53. Williamson, B. (2017). Big data in education: The digital future of learning, policy and practice. *Big Data in Education*, 1-256.
54. Zeb, S., Mahmood, A., Khowaja, S. A., Dev, K., Hassan, S. A., Gidlund, M., & Bellavista, P. (2023). Towards defining industry 5.0 vision with intelligent and softwarized wireless network architectures and services: A survey. *Journal of Network and Computer Applications*, 103796.