MANAGEMENT - DIGITAL TRANSFORMATION – CYBERSECURITY LINK: AN EMERGING RESEARCH TOPIC?

Ion POPA[1,2], Andreea BREAZU[3]

Abstract. *As our world continues to become more digitally oriented, modern business operations are increasingly reliant on cybersecurity, management, and digital transformation as critical components. This paper aims to investigate the relationship between cybersecurity, management, and digital transformation as reflected in the existing literature. Using bibliometric analysis as the primary methodology, this study examines a variety of academic works to gain a comprehensive understanding of the intersection of these three fields. The main objective is to identify key trends and patterns regarding the ways in which cybersecurity, management, and digital transformation are interconnected. By using the Scopus database, we identified 93 documents that could be analyzed starting with 2016, suggesting that the management – digital transformation – cybersecurity is an emerging topic.*

Keywords: cybersecurity, management, digital transformation, bibliometric analysis.
DOI https://doi.org/10.56082/annalsarscieco.2023.1.20

1. Introduction

In today's increasingly digital world and moving towards information society [1], cybersecurity, management, and digital transformation have become essential aspects of modern business operations. With more and more sensitive information being stored and transmitted online, the need for effective cybersecurity measures has never been greater [2]. At the same time, businesses must be able to manage their digital assets and operations efficiently to remain competitive and responsive to changing market conditions [3]. Finally, as technology continues to advance at a rapid pace, companies must be prepared to adapt and transform their operations to stay ahead of the curve. In short, cybersecurity, management, and digital transformation are critical components of any successful modern business strategy.

The main objective of this paper is to explore the correlation between cybersecurity, management, and digital transformation, with a particular focus on how this connection is reflected in the existing literature. To achieve this goal, we have adopted a quantitative methodology, using bibliometric analysis as our primary approach. By analyzing a diverse range of academic works, we aim to gain a deeper

[1]Prof. PhD, Faculty of Management, Bucharest University of Economic Studies, Bucharest, Romania, (ion.popa@man.ase.ro).
[2]The Academy of Romanian Scientists, 54, Splaiul Independenței, Sector 5, Bucharest, Romania.
[3]PhD Student, Faculty of Management, Bucharest University of Economic Studies, Bucharest, Romania, (andreea.breazu@man.ase.ro).

understanding of the ways in which cybersecurity, management, and digital transformation intersect and to identify key trends and patterns within the field. Through this analysis, we hope to shed new light on the evolving relationship between these critical components of modern business strategy and to provide insights that can inform future research and practice.

Therefore, the structural aspect of this study involves a review of the relevant literature to provide a concise introduction to the field. This is followed by a detailed methodology section, which outlines our chosen data analysis approach and the specific database utilized. Of utmost importance, however, is our analysis of works within the field, with a focus on examining their evolution over time, the types of documents utilized, the most frequently occurring words, and the connections between them, as well as the most highly cited works. By taking a comprehensive approach to our analysis, we aim to provide a nuanced understanding of the key trends and insights within this area of study.

2. Literature review

Modern organizations must rely on a carefully designed strategy that encompasses a wide range of critical components, including but not limited to effective management practices, an internal infrastructure that promotes innovation, robust security measures, and a highly skilled workforce [4]. However, we believe that in recent years, the focus has increasingly shifted toward two key areas: digital transformation and cybersecurity.

Digital transformation refers to the process of integrating digital technologies and solutions into all aspects of business operations, with the goal of improving efficiency, increasing agility, and improving the overall customer experience [5]. This transformation can involve the adoption of new technologies such as artificial intelligence, the Internet of Things (IoT), and cloud computing, among others [6]. By embracing digital transformation, organizations can better position themselves to thrive in today's fast-paced and rapidly evolving business landscape.

At the same time, cybersecurity has become an essential concern for businesses of all sizes and across all sectors [7]. With the increasing amount of sensitive information being stored and transmitted online, organizations must ensure that they have robust security measures in place to protect against cyber threats such as hacking, data breaches, and other types of cyber-attacks. Failure to adequately protect against

these risks can result in significant financial losses, reputational damage, and legal liability [8].

The COVID-19 pandemic has greatly accelerated the pace of digital transformation in multiple industries, prompting many organizations to adopt new technologies and digital processes at an unprecedented rate [9]. Although this digital shift can bring significant benefits, such as increased efficiency, productivity, and agility, it also exposes organizations to new and complex cybersecurity risks [8]. Today, there is a growing emphasis in studies on the correlation between management, digital transformation, and cybersecurity.

Given that research on the intersection of cybersecurity, management, and digital transformation is still emerging, our next step is to perform a thorough bibliometric analysis. This will involve examining the volume and impact of the existing literature on the subject to gain a deeper understanding of the current state of research. By taking this approach, we aim to contribute to the ongoing development of this important and rapidly evolving field.

3. Methodology

The goal of this paper is to investigate the correlation between cybersecurity and management in the context of digital transformation, based on existing literature. To accomplish this objective, the study uses a bibliometric approach considering previous studies conducted in this field [10-12], to discover and scrutinize patterns and links between these three concepts. Research involves creating an inventory of relevant academic work and identifying key factors such as keyword usage, changes over time, document type, distribution across subject areas, and other related aspects. By examining the current literature, this article aims to deepen our understanding of the relationship between cybersecurity, management, and digital transformation, while also identifying gaps and opportunities for further research in this area.

To determine the best data collection method and identify the appropriate database for the academic paper collection, two keyword searches were conducted in two of the largest databases, Web of Science and Scopus. The objective was to determine which database offered the most comprehensive information on the topic. The process involved performing thorough keyword searches in both databases, followed by a comparative analysis of the results obtained, as can be seen in Table 1. This allowed an accurate evaluation of the relevance and comprehensiveness of the academic papers found in each database. After analyzing the results, we determined

that the Scopus database provided more detailed and relevant information compared to the Web of Science. This allowed the most suitable database to be selected for data collection purposes, ensuring the highest quality and accuracy of the data collected.

Table 1. Information from the two databases on the relationship between the keywords cybersecurity, management, and digital transformation

Database:	Scopus	Web of Science
Result	93 scientific papers	41 scientific papers
	Period: 2016-2023	Period: 2018-2023

Source: authors

Therefore, the next step in our investigation was to thoroughly analyze the data collected from the Scopus database. After identifying the academic papers that included the three keywords of interest for our study (namely, cybersecurity, management, and digital transformation) in their title, abstract, or keywords, we decided to download the database for further processing. To analyze and visualize the data, we employ a range of advanced tools and techniques. One such tool was the VOSviewer software [13], which allowed us to process and visualize the data in an efficient and organized manner. Additionally, we utilized other online tools such as RAWGraphs [14], Data wrapper [15], and Microsoft Excel to create graphics and gain further insights into the data.

4. Data analysis and discussion

4.1. The evolution of the research over time and document types

Analyzing the evolution of scientific research trends over time is a reliable method to assess the level of interest in various topics, in our case cybersecurity, management, and digital transformation. This approach helps us to determine the timeline of when a particular research trend began, whether it is a new or old field, and what the current trend is. By examining the growth and development of research in these areas, we can also gain insight into the emerging issues and future directions of these fields. Therefore, the evolution of research trends can serve as a valuable indicator of the level of interest in a particular scientific topic.

As mentioned above, Figure 1 provides insights into the time development of studies that investigate the interplay between keyword cybersecurity, management,

and digital transformation. The data in the table reveal that this field is relatively new in the specialized literature, with the first papers appearing in 2016. Another paper was published in 2017, and from 2018 onward, the field experienced a noticeable upward trend, with six papers published in that year alone. The field's research output has seen a significant increase in recent years, with 2020, 2021, and 2022 being the glory years of research in this area. In 2020, 16 studies were published, followed by 27 in 2021 and 31 in 2022. This trend indicates that the field is gaining prominence among researchers, and there is a growing interest in investigating the relationship between cybersecurity, management, and digital transformation. The reason for this may be that the pandemic has disrupted the equilibrium state of organizations, leading to a state of unrest. Many organizations have had to undergo significant digitization efforts to keep their customers engaged from a distance. Considering the fact that the research was carried out at the beginning of 2023, there is no complete situation for this activity, it can only be mentioned that up to the time of the analysis, 2 scientific papers have been published.

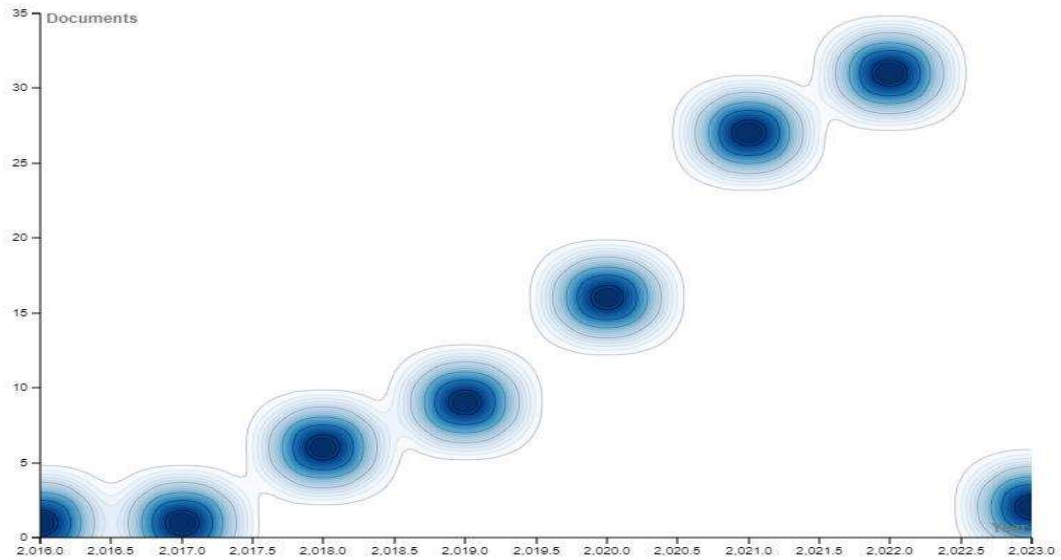

Fig. 1. Evolution over time of research that analyzes the relationship between cybersecurity, management, and digital transformation.

Source: authors with RAWGraphs

Analyzing document types is an essential aspect of bibliometric analysis because it provides a deeper understanding of the research landscape and the different types of

sources that contribute to it [16]. In addition, the distribution of document types can reflect the state of research in a particular field or subfield. According to [16], if many of the analyzed documents are conference procedures, it may indicate that the field is still in its early stages. In contrast, if a large part of the analyzed documents are journal articles, it can indicate a more mature area, with consecrated research and academic networks.

Thus, we observe in the case of our analysis and according to Figure 2, that most documents are conference papers (41.9 % out of a total of 93 research). As previously mentioned, it is apparent from the document type of the field that it is still in its early stages of research. Trend analysis supports this observation, indicating that there is still much to explore and discover in this area. Analyzing the scientific papers and their typology, we notice that 26.9% of the total are articles published in specialized journals and 12.9% of the total, are reviews of conference papers, the rest of the documents being: book chapters (9.7%), reviews (6.5%) and books (2.2.%).

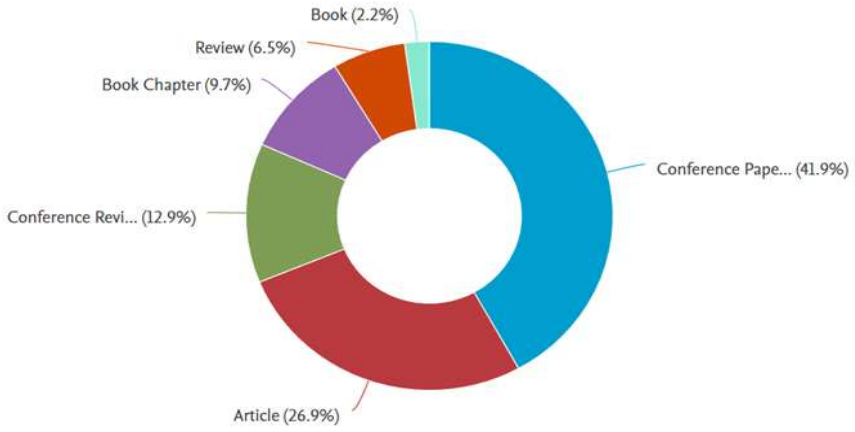

Fig. 2. The types of documents that analyze the relationship between cybersecurity, management, and digital transformation.

Source: Scopus (2023)

4.2. Most used keywords and keyword analysis

Conducting a keyword analysis in bibliometric research is important for identifying research trends, improving literature searches, understanding research collaborations, and evaluating the impact of research. In Figure 3, the frequency of

occurrence of the most used keywords in our results is depicted. It can be seen that 'cybersecurity' was the most common keyword among researchers, appearing in 71 of 93 research articles. The 'digital transformation' was second with 49 occurrences, while 'risk management' appeared third with 30 occurrences. Researchers have also explored other keywords related to the main topics of interest, such as 'networking security', 'artificial intelligence', and 'automation'. There may be correlations between these keywords and the top keywords, indicating potential areas of overlap or convergence in research.

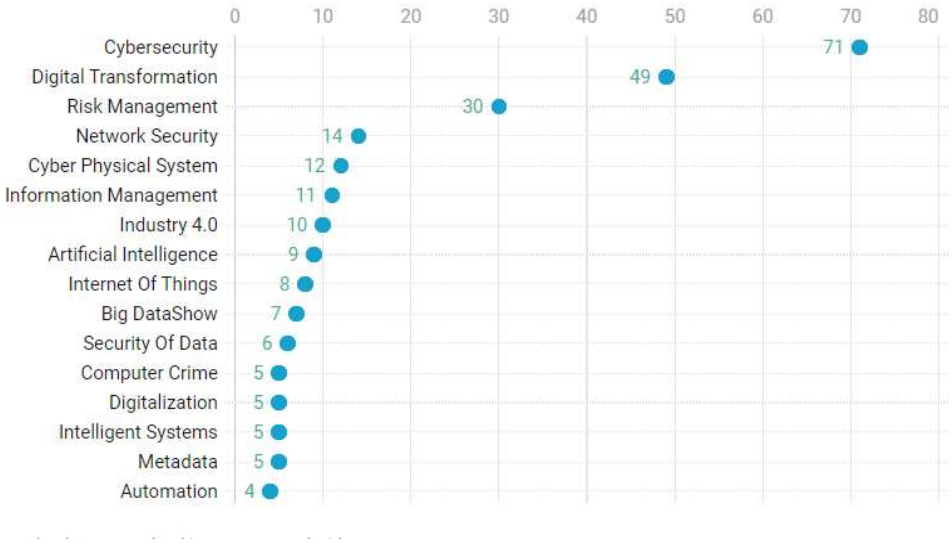

Fig. 3. The number of occurrences of the keywords

Source: authors with Data wrapper

Further, we used Vosviewer [13] to generate a keyword map that explores the connections between keywords relevant to the topics of cybersecurity, management, and digital transformation. In total, 736 keywords were found to be relevant, but only 163 were selected for analysis, based on the selection criterion (2 minimum number of occurrences of the keywords). Figure 4 shows the resulting keyword map. This approach allowed us to comprehensively examine the relationships between the selected keywords.

Applying the keyword clustering selection criterion to identify terms that appeared in more than two publications resulted in the detection of 127 nodes, with each keyword representing a node whose size is proportional to its frequency of

occurrence [10,17]. The 127 keywords were classified into nine distinct clusters, which were highlighted in different colors in Figure 4. The largest cluster, consisting of 24 nodes, was marked in red, followed by the green cluster with 19 nodes, the blue cluster with 16 nodes, the yellow and purple clusters with 14 nodes each, the orange cluster with 10 nodes, the brown cluster with 9 nodes, and the pink cluster with 8 nodes. The classification of the keywords into clusters provides a visual representation of the relationships and connections between them.

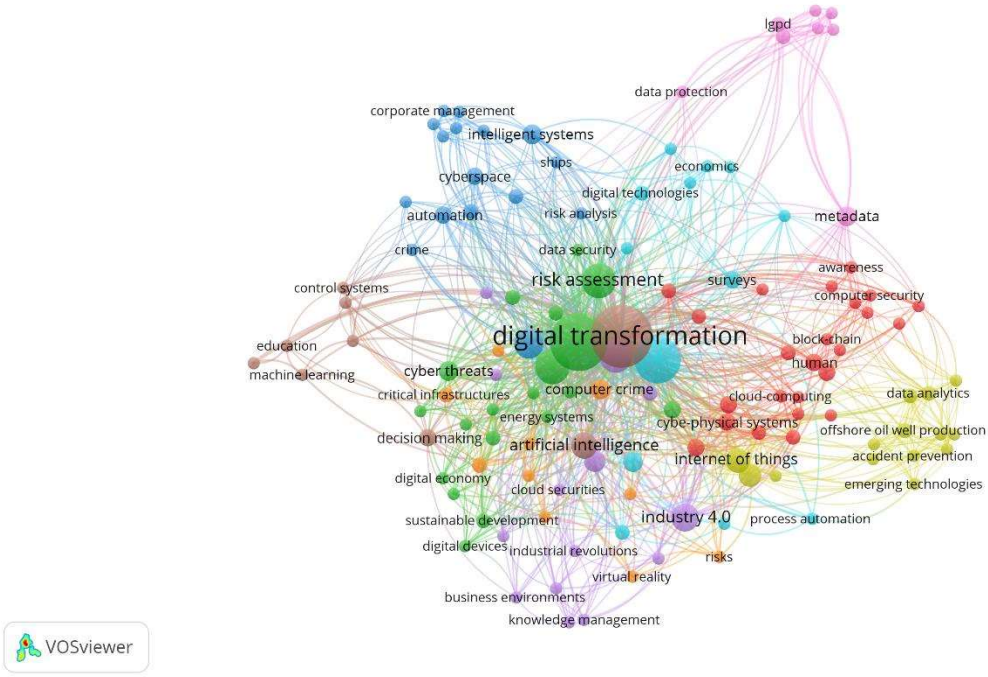

Fig. 4. Keyword map

Source: authors with VOSviewer (Van Eck & Waltman, 2010)

4.3. Analysis of the most important clusters

We marked the largest cluster in red, which contained 24 nodes. Within this cluster, we observed the occurrence of the following words: ‘access control’, ‘artificial intelligence’, ‘blockchain’, ‘cloud computing’, ‘computer security’, ‘cryptography’,

‘cyber-physical systems’, ‘digital maturity’, ‘pandemic’, ‘security, ‘technology’, etc. Thus, identified nodes have a common theme with information security and technology, and we made the following correlations.

Access control and computer security - Access control is a fundamental aspect of computer security, which focuses on protecting computer systems and networks from unauthorized access, theft, and damage.

Artificial intelligence and cyber-physical systems - Artificial intelligence (AI) has become increasingly important in the development of cyber-physical systems, which are systems that integrate physical and computational components. AI can enhance the performance of cyber-physical systems by providing better decision-making capabilities, faster processing, and improved reliability [18].

Digital maturity and technology - Digital maturity refers to an organization's ability to leverage technology to improve its operations, processes, and customer experience [19]. Technology plays a crucial role in digital maturity by providing the tools and platforms needed to achieve digital transformation.

Pandemic and security - The COVID-19 pandemic has highlighted the importance of security, particularly in the context of remote work and online collaboration. The pandemic has also accelerated the adoption of digital technologies, making security even more critical [9].

Upon analyzing the green cluster, which comprises 19 nodes, we found that the term “cybersecurity” was the word most frequently used. Furthermore, this term is closely associated with other important terms such as ‘risk management’, ‘data security’, ‘digitization’, ‘digitized economy’, ‘energy’, ‘power’, ‘risk manager’, ‘robots’, and “sustainable development”. The presence of these words suggests that the green cluster is focused on the intersection of cybersecurity and various other domains such as risk management, data security, energy, and sustainable development. The emphasis on digitization and the digitized economy further highlights the growing importance of cybersecurity in today's digital landscape. Furthermore, the inclusion of terms such as ‘power’ and “robots” suggests that the group may also have connections to the fields of robotics and energy. Overall, the green cluster represents a rich and interconnected network of ideas related to cybersecurity and its diverse applications in modern society.

Cluster number 8 has a strong association with the term “digital transformation”, which is linked to a variety of other words within and outside the cluster. Some of

these words include ‘artificial intelligence’, ‘education’, ‘control systems’, and “decision systems”. This suggests that digital transformation is a crucial concept that intersects with many other areas. On the other hand, the other clusters have a more limited set of connections. They tend to focus on digital terms, risk, and management. This may indicate that these clusters are more specialized and less broad in scope than cluster number 8. However, they are still important and offer unique insight into specific aspects of digital technology.

4.4. Top 5 most cited papers

Identifying the most cited papers in a bibliometric analysis is important because highly cited papers are often considered influential and impactful within their respective fields. They can provide a good indication of the key developments and trends that have shaped the field over time. By examining these papers, researchers can gain a deeper understanding of the evolution of the field and the major contributions that have been made. Table 2 presents the most cited papers that analyzed the relationship between cybersecurity, management, and digital transformation.

As shown in Table 2, the field is still in its early stages as even the most highly referenced paper has not received an exceptionally large number of citations. The top-ranked publication is a paper by Kappelman et al. [20] with 41 citations, while the bottom-ranked publication is a book by Brunet-Thornton and Martinez [21] from 2018 with 14 citations. Furthermore, the variety of materials presented, including articles, conference proceedings, and books, further illustrates the nascent state of the field. For more information on the individual works, please see Table 2, which includes a brief overview of each study.

Table 2. The most cited research

Top	*Authors*	*Scope*	*Method*	*Findings*	*Number of citations*
1	Kappelman et al. [20]	The objective of this paper is to investigate how employee salaries and expenditures on cloud services impact IT management practices, as well as to identify other significant	The research uses a quantitative method, specifically, a questionnaire addressed to	Compared to the previous year (2018), IT spending increased by almost 5% and accounted for approximately 7% of corporate revenues on average.	41

		findings and their implications. This analysis includes a comparison with US-based organizations for additional information.	European IT managers	Most companies have seen an increase in IT headcount, salaries, and spending on cloud services.	
2	Barreto & Amaral [22]	This paper aims to bring attention to some considerations concerning the security obstacles encountered by Smart Farming systems.	The research uses an empirical methodology	Smart farming faces various challenges, particularly in the technological and cybersecurity realms.	37
3	Andriole [23]	The article investigates the difficulties and prospects that digital transformation brings and how it affects the workforce, along with its consequences for education and training.	Literature review	The findings suggest that digital transformation is creating a demand for a new set of skills and competencies in the workforce.	23
4	Carrero et al. [24]	The objective of the articles is to investigate the advancement of recruitment and selection practices that are inclusive of people with disabilities in the workplace.	The study used a qualitative approach (semi-structured interview)	Individuals who took part in the DXC program expressed favorable opinions regarding the program's practices that promote the inclusivity of people with disabilities.	15
5	Brunet - Thornton & Martinez [21]	The scope of the paper is to examine the impact of Industry 4.0 on modern business environments.	Literature review	The results of the research article indicate that Industry 4.0 is exerting a notable influence on contemporary business environments.	14

Source: authors

Conclusions

The literature has shown a great deal of interest in digital transformation, yet there remains a lack of understanding about the complex interplay between cybersecurity, management, and digital transformation. Although much of the current research focuses on risk management, we argue that it is equally important to explore the managerial perspective in more detail.

Although several studies analyze the implications of digital transformation [5,9,25] and the role of cybersecurity in organizations [7,26], none of the studies identified in our analysis address the broader relationship between these topics and management. By exploring this relationship from a managerial perspective, we can develop more nuanced and effective strategies to manage digital transformation while minimizing cybersecurity risks. This, in turn, can lead to improved organizational performance and a competitive advantage in today's fast-paced and rapidly evolving business environment.

Our study focused on bibliometric analysis, and we discovered that the intersection of cybersecurity, management, and digital transformation is a relatively new field, with research on the topic only beginning to emerge in 2016. In addition, according to [16], a significant proportion of the literature in this field includes conference proceedings, suggesting that the area is still in its nascent stages of development. Our analysis supports this finding, with most of the documents we reviewed also being categorized as conference proceedings. Although this indicates that there is still much work to be done in terms of developing a more robust understanding of the intersection of cybersecurity, management, and digital transformation, it also highlights the potential for exciting new insights and discoveries in this rapidly evolving field. As more research is conducted and the body of knowledge expands, we can expect to see new and innovative strategies emerge to manage the risks and opportunities associated with digital transformation. Also, the relationship between the keywords made within the keyword link map is a multidisciplinary one, until now researchers analyzed the field from several perspectives.

We anticipate that our paper will have significant implications for the existing literature on cybersecurity, management, and digital transformation. Ultimately, we hope that our paper will stimulate further research in this area and help in the direction of future research. In the future, if we were to prioritize research, we would concentrate on exploring the relationship among cybersecurity, digital transformation, and the

involvement of managers. The paper, however, has some limits, specific to the bibliometric analysis, in terms of the impact or the quality of the analyzed documents.

R E F E R E N C E S

[1] Banciu, D., Rădoi, M., Belloiu, Ș. Information Security Awareness in Romanian, Public Administration: An Exploratory Case Study, *Studies in Informatics and Control, 29*(1), 121-129, https://doi.org/10.24846/v29i1y202012, (2020).

[2] Möller, D. *Cybersecurity in digital transformation: Scope and applications*. Berlin/Heidelberg, Germany: Springer, (2020).

[3] Ebert, C., & Duarte, C. H. C. Digital transformation. *IEEE Software, 35*(4), 16-21, (2018).

[4] Teece, D. J. Business models and dynamic capabilities. *Long range planning, 51*(1), 40-49. https://doi.org/10.1016/j.lrp.2017.06.007, (2018).

[5] Gong, C., & Ribiere, V. Developing a unified definition of digital transformation. *Technovation, 102*, 102217. https://doi.org/10.1016/j.technovation.2020.102217, (2021).

[6] Heilig, L., Lalla-Ruiz, E., & Voß, S. Digital Transformation in maritime ports: analysis and a Game-Theoretic Framework. Netnomics: Economic Research and electronic networking, 18(2-3), 227-254. https://doi.org/10.1007/s11066-017-9122-x, (2017).

[7] Craigen, D., Diakun-Thibault, N., & Purse, R. Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. http://doi.org/10.22215/timreview/835, (2014).

[8] Cybersecurity, C. I. Framework to improve cybersecurity of critical infrastructure. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018, (2018).

[9] Gabryelczyk, R. Has COVID-19 accelerated digital transformation? Initial lessons learned for public administrations. *Information Systems Management, 37*(4), 303-309. https://doi.org/10.1080/10580530.2020.1820633, (2020).

[10] Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research, 133*, 285-296. https://doi.org/10.1016/j.jbusres.2021.04.070, (2021).

[11] Marinaș, C. V., Goia, S. I., Gora, A. A., Igreț, R. Ș., Roman, M., & Ștefan, S. C. A Bibliometric Analysis of the Relationship Internship–Skills–Employ-Ability. In I. Popa, C. Dobrin, C.N., Ciocoiu (eds), *Proceedings of the 15th International Management Conference - Managing People and Organizations in a Global Crisis*, Bucharest, Romania, (pp. 669-681), (2021).

[12] Breazu, A. & Ștefan, S. C. A Bibliometric Analysis of The Effects of The COVID-19 Pandemic on Students. In I. Popa, C. Dobrin, C.N., Ciocoiu (eds), *Proceedings of the 16th International Management Conference "Management and resilience strategies for a post-pandemic future"*, Bucharest, Romania, (pp. 260-271), (2022).

[13] Van Eck, N., & Waltman, L. Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics, 84*(2), 523-538. https://doi.org/10.1007/s11192-009-0146-3, (2010).

[14] Mauri, M., Elli, T., Caviglia, G., Uboldi, G., & Azzi, M. RAWGraphs: a visualisation platform to create open outputs. In *Proceedings of the 12th Biannual Conference on Italian SIGCHI Chapter*, 27, 1-5. https://doi.org/10.1145/3125571.3125585, (2017).

[15] Data wrapper. Enrich your stories with charts, maps, and tables. Retrieved from: https://www.datawrapper.de/ (Accessed on 21 02ed 2023), (2023).

[16] de Oliveira, O. J., da Silva, F. F., Juliani, F., Barbosa, L. C. F. M., & Nunhes, T. V. *Bibliometric method for mapping the state-of-the-art and identifying research gaps and trends in literature: An essential instrument to support the development of scientific projects.* In Scientometrics recent advances. IntechOpen, (2019).

[17] Corboș, R. A., Bunea, O. I., & Breazu, A. A Bibliometric Analysis Of Scientific Production Concerning Online Consumer Reviews And The Sale Of Home Appliances. Management and Marketing Journal, 20(2), 249-262. https://doi.org/10.52846/MNMK.20.2.10, (2022).
[18] Radanliev, P., De Roure, D., Van Kleek, M., Santos, O., & Ani, U. Artificial intelligence in cyber physical systems. *AI & Society, 36*, 783-796. https://doi.org/10.1007/s00146-020-01049-0, (2021).
[19] Teichert, R. Digital transformation maturity: A systematic review of literature. *Acta Universitatis Agriculturae Et Silviculturae Mendelianae Brunensis. 67* (6), 1673-1687, https://doi.org/10.11118/actaun201967061673, (2019).
[20] Kappelman, L., Johnson, V., Torres, R., Maurer, C., & McLean, E. A study of information systems issues, practices, and leadership in Europe. *European Journal of Information Systems, 28*(1), 26-42. https://doi.org/10.1080/0960085X.2018.1497929, (2019).
[21] Brunet-Thornton, R., & Martinez, F. (Eds.). Analyzing the impacts of industry 4.0 in modern business environments. *IGI Global*. https://doi.org/10.4018/978-1-5225-3468-6, (2018).
[22] Barreto, L., & Amaral, A. Smart farming: Cyber security challenges. In *9th International Conference on Intelligent System 2018 Proceedings. Theory, Research, and Innovation in Applications*, Funchal, Portugal, pp. 870 – 876. https://doi.org/10.1109/IS.2018.8710531, (2018).
[23] Andriole, S. J. Skills and competencies for digital transformation. *IT Professional, 20*(6), 78-81. https://doi.org/10.1109/MITP.2018.2876926, (2018).
[24] Carrero, J., Krzeminska, A., & Härtel, C. E. The DXC technology work experience program: disability-inclusive recruitment and selection in action. Journal of management & organization, 25(4), 535-542. https://doAA Mi.org/10.1017/jmo.2019.23, (2019).
[25] Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. V. Digital business strategy: toward a next generation of insights. *MIS Quarterly, 37*(2), 471-482, (2013).
[26] Dash, B., & Ansari, M. F. An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *International Research Journal of Engineering and Technology, 9*(4), 1-6, (2022).

.