Cybersecurity in Digital Transformation Applications: Analysis of Past Research and Future Directions

Zakariya Belkhamza
Ahmed Bin Mohammed Military College, Doha, Qatar

zbelkhamza@abmmc.edu.qa

Abstract: The term *digital* is often used to indicate the changes occurring in today's world, generally referred to as a cyber-physical system, driven by the rapid adoption of digital technologies, where the cyber and the physical worlds are partly overlapping. Digital transformation refers to the integration of the digital technology of the cyber world into all physical domains. These cyber-physical systems must be secure against the threat of cyberattacks. However, one of the most challenging aspects of cybersecurity is the evolving nature of cyberattack risks, which is highly integrated with digital transformation. Despite a number of published articles, there is little investigation of past literature analysis that presents digital transformation applications and cybersecurity trends. The objective of this paper is to provide an intensive examination of digital transformation applications and cybersecurity research between 2019 and 2022, to detect the most profound research areas, emphasize existing challenges and identify patterns, tendencies or regularities existing in the literature in terms of technological applications. This aims to support scholars with a comprehensive understanding of the past, present and future directions of this research trend. To achieve these objectives, a systematic literature review is utilized. The findings introduce several implications for the present state of the literature, apparent study gaps and several research questions, which can be explored in future research.

Keywords: digital transformation, cybersecurity, systematic literature review, systematic analysis

1. Introduction

Cybersecurity has become a global challenge for digital business activities. Research on cybersecurity in the digital transformation framework has gained significant attention in recent years (Mendhurwar & Mishra, 2021; Sandhu, 2021; Swain et al., 2022). Some research has paid specific attention to the subject of cybersecurity in the post COVID-19 era. For example, Alawida et al. (2022) reviewed and examined the effect of cybersecurity on organizations during the global COVID-19 crisis. Others have focused on various areas of digital transformation, such as cybersecurity in blockchain-based systems (Schlatt et al., 2022), big data analytics (Rawat, Doku & Garuba, 2021), machine learning (Aiyanyo, Samuel & Lim, 2020) and the Internet of things (Rudenko et al., 2022).

Despite these investigations and reviews, and a few recent studies that conducted a literature analysis (Carcary, Doherty & Conway, 2019; Zhu, Ge, & Wang, 2021), a comprehensive analysis of cybersecurity in the digital transformation context still lacks further investigation. Therefore, there is an apparent need for research that provides a comprehensive understanding of the past, present and future of research on cybersecurity in the digital transformation context.

This paper addresses three research questions: 1) what is the current status of cybersecurity research? 2) what are the key areas that interlink cybersecurity and digital transformation applications? and 3) what potential future research avenues can be identified based on existing literature that concern applied technologies of digital transformation? To provide answers to these questions, a systematic review is presented.

2. Research Methodology

To answer the research questions set for this study, a systematic literature review was conducted. Although there are several guidelines for conducting a literature review, this study followed the guidelines published by Kitchenham and Charters (2007). Several studies have successfully used this guideline, for example, Taylor et al. (2020). The following section reports the methodology of this study.

2.1 Inclusion criteria

Since the research article is the unit of analysis, it is important before engaging in a study to set the article inclusion criteria. We used Scopus database as the platform to collect the sample of this research. First, although it was not necessary for the study to directly address the post COVID-19 period, articles published between 2019–2022 were targeted for this research. Second, only articles published in English were considered. Third, articles published in irrelevant research areas, such as law and medicine, were excluded. This refinement process resulted in a total of 67 articles in the Scopus database; after filtering the sample for the database, duplicate articles were excluded, and a final sample of 65 articles was selected.

2.2 Quality assessment

To maintain a quality review for this study, it was important to assess the quality of primary studies as recommended by Kitchenham and Charters (2007). The objective of this stage was to assess the relevance of the papers with regard to the research questions. The following rules were set and each article from the sample had to fulfil these to be included in the study:

Stage 1: **Cybersecurity.** The article had to focus on the use of cybersecurity or the application of cybersecurity technology to a specific problem and be well-commented.

Stage 2: **Digital Transformation.** The article had to focus on digital technology or the various types of digital transformation.

Stage 3: The article had to address the issue of cybersecurity in direct accordance with digital transformation.

Stage 4: The article had to provide sufficient context for the research objectives and findings. This would allow for an accurate interpretation of the research.

Stage 5: The article had to provide sufficient context in the study to enable the findings to be generalized to a larger context in the research field.

Stage 6: Details of how the study was conducted and performed had to be explained and reported in order to determine accuracy.

Each article was carefully examined against the above checklist, and articles that failed to meet all the above criteria were removed from the sample. It was found that eight studies did not meet one or more of the checklist items and, therefore, were removed from the sample. Two articles were found to be duplicated, as their findings were published in another article; therefore, these two duplicated articles were excluded. The final sample of the study consisted of 18 papers that passed the quality assessment. Information regarding the articles included in the research is summarized in Table 1.

Table 1: Summary of research articles

Study	Problems of study	Nature of study	Objectives of study	Implications of study
Castelo-Branco et al. (2022)	Inconsistency of available maturity models beyond the manufacturing industry.	Mixed-method approach.	Presented an Industry 4.0 maturity index.	Industry 4.0 implementation to be integrated into a consistent strategic decision framework that went beyond technology adoption and was market oriented.
Haleem et al. (2022)		Literature review analysis.	Identified the major cybersecurity applications for Industry 4.0 and discussed them.	Digital transformation in the industry 4.0 era would increase industrial competitiveness and improve their capacity to make optimum decisions.
Rodrigues et al. (2022)	Issue of artificial intelligence (AI), digital transformation and cybersecurity in the finance and banking sector.	Mixed-method approach.	Developed a realistic decision-support model by combining cognitive mapping and the decision-making trial and evaluation laboratory (DEMATEL) method.	Artificial intelligence, digital transformation and cybersecurity would allow for a better decision-making process in terms of security, efficiency and efficacy in ICT ecosystems.
Malatji, Marnewick and Von Solms (2022)	Interconnectivity between enterprise information technology (IT) and industrial control systems (ICS) environment.	Literature review analysis.	Developed a critical infrastructure cybersecurity capability framework.	Developed a critical infrastructure cybersecurity capability framework comprising 29 capability domains (cybersecurity focus areas).
Reina Quintero et al. (2022)	Existing access control models failed to integrate sophisticated decision-making in security policies.	Design analysis.	Presented a model-based approach to facilitate the definition of complex security policies based on usage control (UCON) in the software development process.	Improved security policies beyond simple access control rules and covered more complex and dynamic scenarios and provided powered decision-making ability.
Muncinelli et al. (2021)	Issue of digital compliance with legal requirements, risks,	Exploratory analysis.	Analysed the primary areas of contribution to the assessment of	Presented the components of the MCP-LGPD capability model (process capability

Study	Problems of study	Nature of study	Objectives of study	Implications of study
	business analysis, good practices and standards efficiently and sustainably.		process capability for digital transformation concerning cybersecurity in the context of personal data protection legislation.	model-Brazil's General Data Protection Law).
Sonkor and De Soto (2021)		Literature review analysis.	Understood the current state of the art and identified gaps to suggest future directions regarding operational technology in construction from the perspective of cybersecurity.	Investigated methods to evaluate security levels on construction sites and countermeasures against cyberattacks.
Petratos (2021)	Insufficient examination of the consequences of misleading information on businesses.	Exploratory analysis.	Offered a primer on misleading information and cyber risks aimed at business executives and leaders across an array of industries, organizations and nations.	Established cybersecurity policies and best practices to manage emerging and multifaceted cyberthreats.
Tarikere, Donner and Woods (2021)	Critical need for cybersecurity in the development of Internet of Medical Things (IoMT) technology, alongside design and utility.	Exploratory analysis.	Examined the market opportunities and risks associated with IoMT.	Implementation of risk management plans would ensure continuity of care that embraced technologies while protecting patient data and information.
Lee (2021)	Rising issues of cyber breaches and the emergence of novel cybersecurity technologies such as machine learning and AI.	Exploratory analysis.	Introduced a cyber risk management framework and illustrated a continuous improvement of cybersecurity performance and cyber investment cost analysis.	Developed a cyber risk management framework in which risk management activities were organized and evaluated in four layers.
Mironeanu et al. (2021)	Increasing number of threats and attack patterns in real-time analytical tools.	Design analysis.	Introduced a novel concept for integrating machine learning and analytical tools into a live intrusion detection and prevention solution.	Proposed the Experimental Cyber Attack Detection Framework (ECAD).
Emer, Unterhofer and Rauch (2021)	Issue of digitalization and connectivity in a digital environment where human–machine collaboration is more flexible and agile.	Exploratory analysis.	Introduced an assessment model of Small & Medium Enterprise cybersecurity for better managerial action and data security.	Concept of an easy-to-use cybersecurity assessment tool would strongly improve the currently difficult introduction of cyber protection solutions in SMEs.
Villegas et al. (2021)		Literature review analysis.	Conducted a literature review of technological pillars to implement Industry 4.0.	Proposed strategies to successfully integrate AI and the technological pillars of Industry 4.0.
Yerina et al. (2021)	Monitoring cyber incidents and anomalies for cybersecurity assessment.	Empirical analysis.	Summarized the international experience of assessing cybersecurity and the effective protection of cyberspace at a national level.	Cybersecurity ratings played the role, to some extent, of an identifier of the relative advantages and vulnerabilities of national cyber strategies and indicated the need for their review to strengthen protection against cyber-attacks.
Mendhurwar and Mishra (2021)	Integration of modern technologies facing key challenges related to information security and privacy.	Exploratory analysis.	Explored interplay and synergetic relationships among technologies and identified key challenges on cybersecurity and privacy.	Identified opportunities related to the integration of social and IoT technologies.
Uddin et al. (2020)	The more banks improve their operational efficiency and quality of service by relying on	Empirical analysis.	Examined whether the law of diminishing marginal returns from overspending on cyber	Established aggressive cyber technology spending could lead to diminishing returns,

Study	Problems of study	Nature of study	Objectives of study	Implications of study
	cyber technology the more they become vulnerable to cybersecurity.		technology affected bank stability.	which adversely affected stability of banks.
Chatfield and Reddick (2019)	Strategic use of the IoT is still in the early stages of development in governments across the globe (Meyers et al., 2015) and the IoT adoption rate remains low.	Literature review analysis.	Developed a new framework for IoT-enabled smart government.	Addressed knowledge gap in the literature on smart government, from a dynamic capabilities theory perspective.
Yuan et al. (2022)	Impact of various power application services on the security situation still requires further investigation.	Design analysis.	Proposed a method for quantifying the information security of the power network based on the evolutionary neural network.	Improved the quantification accuracy of the information security of the power network to a certain extent.

3. Results and Discussion

It is significant to observe how digital transformation is introduced and presented in the literature. Most studies failed to consider defining the operationalization of digital transformation in the context of the study. Various articles presented digital transformation as a process, which is a synonym of the so-called Industry 4.0 (Castelo-Branco et al., 2022). Other studies investigated elements of digital transformation, such as IoT (Chatfield & Reddick, 2019; Mendhurwar & Mishra, 2021; Villegas et al., 2021), cyber-physical systems (Sonkor & De Soto, 2021) and risk management (Lee, 2021; Uddin, Mollah, & Ali, 2020).

Rodrigues et al. (2022), for instance, differentiated between artificial intelligence and digital transformation, and adopted Kaplan & Haenlein (2019)'s definition as *'a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation'*. However, they defined digital transformation simply as the use of digital technology in new ways to solve traditional problems.

Unlike digital transformation, cybersecurity is well-defined in the literature; for instance, Lee (2021) defined cybersecurity as the preservation of the confidentiality, integrity and availability of information in complex environments resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it. Several studies investigated components of cybersecurity such as cyber threat, cyberattack, cybercrime and cyber risk.

Table 2: Types of methodology of articles

Methodology of articles	Number of articles	%
Exploratory analysis	6	34%
Literature review analysis	5	28%
Design analysis	3	16%
Mixed-method analysis	2	11%
Exploratory analysis	2	11%
Total	18	100%

From a methodological perspective, the articles may be broadly grouped into five categories: the first group used exploratory analysis and consisted of six articles; the second group used literature review analysis and consisted of five articles; the third group used design analysis and consisted of three articles; and two groups consisted of two articles each, and used mixed-method analysis and empirical analysis, respectively. Table 2 summarizes these findings.

In terms of the nature of research, the sample can be grouped into two groups equally with nine articles each; the first group of articles proposed model/framework development, and the second represented conceptual investigation.

Further insight into the first group of articles revealed that five articles developed some interesting frameworks that could be used in different scenarios in cybersecurity. These frameworks are: the Industry 4.0 maturity framework (Castelo-Branco et al., 2022), the critical infrastructure cybersecurity capability framework (Malatji, Marnewick & Von Solms, 2022), the cyber risk management framework (Lee, 2021), the experimental

cyberattack detection framework (Mironeanu et al., 2021) and the IoT enabled smart government framework (Chatfield & Reddick, 2019). In addition to these frameworks, two models were proposed: the realistic-decision support model (Rodrigues et al., 2022) and the SME cybersecurity assessment model (Emer, Unterhofer & Rauch, 2021), and a model for quantifying the information security of the power network (Yuan et al., 2022).

Finally, these studies suggested that the most technological applications were IoT (Chatfield & Reddick, 2019; Mendhurwar & Mishra, 2021; Tarikere, Donner & Woods, 2021; Villegas et al., 2021), AI (Mendhurwar & Mishra, 2021; Rodrigues et al., 2022; Villegas et al., 2021), robotics and virtual reality (Villegas et al., 2021).

4. Future Research Directions

This article reports on the cybersecurity in digital transformation applications. Based on the results of this study, some research directions concerning cybersecurity are presented. Cybersecurity is well positioned in the literature, and various aspects of it have been investigated in various applications of technology. However, a clear framework of cybersecurity in the digital transformation process is still required, and most of the literature investigated few aspects of digital transformation, while an inclusive framework of digital transformation was not observed. Thus, future research needs to develop comprehensive and quantifiable guidelines to fill this gap in the literature. Moreover, the findings from this study are subject to the inherent limitations of a small sample. The sample of the study was limited to journal articles in English from the Scopus database, and this might not provide an adequate generalizability of the findings. Future studies may address these limitations by exploring different databases, including book chapters and conference proceedings, and may also include documents in other languages. Finally, this study only focused on articles published between 2019–2022, a period that might not actually represent the current research in the domain. Further studies may expand the period included to afford a better insight. From this systematic review, it is concluded that a collaborative and standardized approach for the application of various digital transformation manifestations on cybersecurity attacks is required to collectively strengthen organizations against increasing cyber threats.

References

Aiyanyo, I. D., Samuel, H., and Lim, H. (2020)."A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning", *Applied Sciences (Switzerland)*, Vol. 10, No. 17. https://doi.org/10.3390/app10175811

Alawida, M., Omolara, A. E., Abiodun, O. I., and Al-Rajab, M. (2022)."A Deeper Look into Cybersecurity Issues in the Wake of Covid-19: A Survey", *Journal of King Saud University – Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2022.08.003

Carcary, M., Doherty, E., and Conway, G. (2019)."A Framework for Managing Cybersecurity Effectiveness in the Digital Context", *European Conference on Information Warfare and Security, ECCWS*, *2019-July*, pp 78–86.

Castelo-Branco, I., Oliveira, T., Simões-Coelho, P., Portugal, J., and Filipe, I. (2022)."Measuring the Fourth Industrial Revolution Through the Industry 4.0 Lens: The Relevance of Resources, Capabilities and the Value Chain", *Computers in Industry*, Vol. 138. https://doi.org/10.1016/j.compind.2022.103639

Chatfield, A.T., and Reddick, C. G. (2019)."A Framework for Internet of Things-Enabled Smart Government: A Case of IoT Cybersecurity Policies and Use Cases in U.S. Federal Government", *Government Information Quarterly*, Vol. 36, No. 2, pp 346–357. https://doi.org/10.1016/j.giq.2018.09.007

Emer, A., Unterhofer, M., and Rauch, E. (2021)."A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises", *IEEE Engineering Management Review*, Vol. 49, No. 2, pp 98–109. https://doi.org/10.1109/EMR.2021.3078077

Haleem, A., Javaid, M., Singh, R. P., Rab, S., and Suman, R. (2022)."Perspectives of Cybersecurity for Ameliorative Industry 4.0 Era: A Review-Based Framework", *Industrial Robot*, Vol. 49, No. 3, pp 582–597. https://doi.org/10.1108/IR-10-2021-0243

Kaplan, A., and Haenlein, M. (2019)."Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence", *Business Horizons*, Vol. 62, No. 1, pp 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Kitchenham, B. and Charters, S. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report EBSE 2007-001, Keele University and Durham University Joint Report

Lee, I. (2021)."Cybersecurity: Risk Management Framework and Investment Cost Analysis", *Business Horizons*, Vol. 64, No. 5, pp 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Malatji, M., Marnewick, A. L., and Von Solms, S. (2022)."Cybersecurity Capabilities for Critical Infrastructure Resilience", *Information and Computer Security*, Vol. 30, No. 2, pp 255–279. https://doi.org/10.1108/ICS-06-2021-0091

Mendhurwar, S., and Mishra, R. (2021)."Integration of Social and IoT Technologies: Architectural Framework for Digital Transformation and Cyber Security Challenges", *Enterprise Information Systems*, Vol. 15, No. 4, pp 565–584. https://doi.org/10.1080/17517575.2019.1600041

Mironeanu, C., Archip, A., Amarandei, C.-M., and Craus, M. (2021)."Experimental Cyber Attack Detection Framework. *Electronics (Switzerland)*, Vol. 10, No. 14. https://doi.org/10.3390/electronics10141682

Muncinelli, G., De Lima, E. P., Cestari, J. M. A. P., Deschamps, F., and Da Costa, S. E. G. (2021)."Developing a conceptual model for process capability in the brazilian data protection regulation context". *Journal of Industrial Integration and Management*, Vol. 6, No. 4, pp 407–427. https://doi.org/10.1142/S2424862221400017

Petratos, P. N. (2021)."Misinformation, disinformation, and fake news: Cyber risks to business". *Business Horizons*, Vol. 64, No. 6, pp 763–774. https://doi.org/10.1016/j.bushor.2021.07.012

Rawat, D. B., Doku, R., and Garuba, M. (2021)."Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security", *IEEE Transactions on Services Computing*, Vol. 14, No. 6, pp 2055–2072. https://doi.org/10.1109/TSC.2019.2907247

Reina Quintero, A. M., Pérez, S. M., Varela-Vaca, Á. J., López, M. T. G., and Cabot, J. (2022)."A domain-specific language for the specification of UCON policies". *Journal of Information Security and Applications*, Vol. *64*. https://doi.org/10.1016/j.jisa.2021.103006

Rodrigues, A. R. D., Ferreira, F. A. F., Teixeira, F. J. C. S. N., and Zopounidis, C. (2022). "Artificial Intelligence, Digital Transformation and Cybersecurity in the Banking Sector: A Multi-Stakeholder Cognition-Driven Framework", *Research in International Business and Finance*, Vol. 60. https://doi.org/10.1016/j.ribaf.2022.101616

Rudenko, R., Pires, I. M., Oliveira, P., Barroso, J., and Reis, A. (2022)."A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity", *Electronics (Switzerland)*, Vol. 11, No. 11. https://doi.org/10.3390/electronics11111742

Sandhu, K. (2021)."Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges", *Handbook of Research on Advancing Cybersecurity for Digital Transformation*, pp 1–17. https://doi.org/10.4018/978-1-7998-6975-7.ch001

Schlatt, V., Guggenberger, T., Schmid, J., and Urbach, N. (2022)."Attacking the Trust Machine: Developing an Information Systems Research Agenda for Blockchain Cybersecurity", *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2022.102470

Sonkor, M. S., and García De Soto, B. (2021)."Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective", *Journal of Construction Engineering and Management*, Vol. 147, No. 12. https://doi.org/10.1061/(ASCE)CO.1943-7862.0002193

Swain, A., Swain, K. P., Pattnaik, S. K., Samal, S. R., and Das, J. K. (2022)."Cybersecurity in Digital Transformations", *Lecture Notes in Networks and Systems*, Vol. 430, 247–252. https://doi.org/10.1007/978-981-19-0825-5_26

Tarikere, S., Donner, I., and Woods, D. (2021)."Diagnosing a Healthcare Cybersecurity Crisis: The Impact of IoMT Advancements and 5G", *Business Horizons*, Vol. 64, No. 6, pp 799–807. https://doi.org/10.1016/j.bushor.2021.07.015

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., and Choo, K. K. R. (2020)."A systematic literature review of blockchain cyber security". *Digital Communications and Networks*, Vol. 6, No. 2, pp 147–156. https://doi.org/10.1016/j.dcan.2019.01.005

Uddin, M. H. M. H., Mollah, S., and Ali, M. H. M. H. (2020). "Does Cyber Tech Spending Matter for Bank Stability?" *International Review of Financial Analysis*, Vol. 72. https://doi.org/10.1016/j.irfa.2020.101587

Villegas, O. O. V., Nandayapa, M., Azuela, J. H. S., Franco, E. G. C., and Linares, G. T. R. (2021). ”Artificial Intelligence for Industry 4.0 in Iberoamerica", *Computacion y Sistemas*, Vol. 25, No. 4, pp 761–773. https://doi.org/10.13053/CyS-25-4-4056

Yerina, A. M., Honchar, I. A., and Zaiets, S. V. (2021)."Statistical indicators of cybersecurity development in the context of digital transformation of economy and society". *Science and Innovation*, Vol. *17*, No. 3, pp 3–13. https://doi.org/10.15407/scine17.03.003

Yuan, Q., Pi, Y., Kou, L., Zhang, F., and Ye, B. (2022)."Quantitative Method for Security Situation of the Power Information Network Based on the Evolutionary Neural Network. *Frontiers in Energy Research*, Vol. 10. https://doi.org/10.3389/fenrg.2022.885351

Zhu, X., Ge, S., and Wang, N. (2021)."Digital Transformation: A Systematic Literature Review", *Computers and Industrial Engineering*, Vol. 162. https://doi.org/10.1016/j.cie.2021.107774