sciendo

Cybersecurity challenges in the knowledge economy

Vlad-Mihai URSACHE
National University of Political Studies and Public Administration, Bucharest, Romania
vlad.ursache.21@drd.snspa.ro

Abstract. *The paper aims to study cybersecurity correlations with the knowledge economy, focusing on its challenges in this new age of economy. The relevance of the cybersecurity concept is sustained by the academic literature that shows its important role in the business environment, where disruptive changes will become the norm. In the digital age the disruptions are happening frequently which gives organizations less time to manage the change and the fact that they are almost constrained to develop new strategies to answer the challenges of the changing business environment. The knowledge economy has evolved and with that, new concepts began to appear out of necessity and the need to secure the dynamic environment of knowledge management systems. Considering the unprecedented access to information and advancements in conducting academic research, in the present landscape of the knowledge economy and cybersecurity domain, new methods are available to structure and examine a body of literature. The text mining and scientific mapping analysis conducted with VOSviewer software version 1.6.18 is allowing us to identify meaningful insights about the knowledge economy concept, such as the (1) existing research gaps, at least on cybersecurity challenges in the knowledge economy and the (2) the research interests seen for the time period between 2019 and 2021. To achieve this, a database derived from Web of Science's core collection has been used, and the text mining based on term co-occurrence analysis contributed to a deeper understanding of current and future workspace dynamics.*

Keywords: knowledge, knowledge economy, cybersecurity, cybersecurity challenges

Introduction

In a continuous changing and unpredictable time, marked by numerous technological innovations and by a world pandemic that introduced all of us in a new era of digitalization where the information is transferred at a very high speed, the world economy has changed (Lafayette et al., 2019; Massingham, 2020; Nonaka & Takeuchi, 2019). A new chapter begins in human evolution and this is to a new global economy, were knowledge become an essential key component in the evolution process of organizations, societies and as well as for each individual (Bratianu, 2013; Liu, 2020; May & Perry, 2018; O'Dell & Hubert, 2011). Most organizations depend on a combination of technology, knowledge management systems and assimilation of new knowledge to stay competitive, to innovate and to exist in the best possible way in the new economy were digitalization has reached a new stage in his evolution in the new global economy. In the age of analytics and intelligence, nearly 5 billion people and 31 billion devices have access to the internet. The digital world has seen a drastic expansion in the recent time of COVID-19. From MNCs to governments, schools to universities, all are functioning online. Almost all organizations use the internet to transfer data and cloud services to store it. This process increases the concern of all organizations toward the protection of data and communication (Baheti et al., 2020).

The past two years have been very critical for many organizations with respect to their economic needs considering the COVID-19 pandemic events and evolution around the globe. In these turbulent times of a global pandemic, various organizations have suffered losses and others have adapted and created even more wealth than before the pandemic. The pandemic requested a

DOI: 10.2478/picbe-2022-0012

new way of thinking business and emergent knowledge strategies (Bratianu, 2020; Bratianu & Bejinaru, 2021).

In this context of global crises and increasing digitalization, the concern on protecting information come along with the same concern as securing the organizational knowledge. In this times, securing the knowledge in the economy become not only a concern, but a top priority for knowledge organizations (Bech, 2019; Cabaj et al., 2018). One way to secure the knowledge in the digital world, or at least to try it, is via cybersecurity, a new concept through which solutions can be found to this concern. Cybersecurity helps in the protection of this sensitive information and the system used to store the information. With the sudden increase in cybercrimes and cyber-attacks, companies and research organizations are embracing technologies and innovations to tackle them (Baheti et al., 2020).

In this context, the present research aims to perform a systematic bibliometric study and to identify the main cybersecurity challenges to the knowledge economy. Our research question can be formulated as follows:

RQ: What are the cybersecurity challenges in the knowledge economy?

The research is qualitative and interpretive and is performed by using VOSviewer, specialized bibliometric software for massive literature reviews (van Eck & Waltman, 2014; 2020). To best serve the research objectives, the introductory part will be followed by the specific literature reviews with a specific focus on knowledge, knowledge management, knowledge economy and cybersecurity. This will let us visualize the current status of research by observing the existing links between knowledge concept and other important concepts such as cybersecurity and illustrate the most relevant relationships that we have discovered between them. Then, we will analyze the cybersecurity challenges with data sources and the applied methodology that will be presented to conclude with results, study's limitations, and possible future research axes.

Literature review

Knowledge economy

Knowledge economy is based on intangible resources which dominate now most of the companies in the well-developed economies. Powell and Snellman (2004, p. 1999) defined knowledge economy as "production and services based on knowledge-intensive activities that contribute to an accelerated pace of technical and scientific advances, as well as a rapid obsolescence". Knowledge has always been used in production and services, but in the knowledge economy knowledge becomes dominant, such that knowledge management emerged as a necessary domain within the classical management (Liu, 2020; Massingham, 2020; Von Krogh et al., 200).

Understanding the knowledge economy means to understand first the concept of knowledge and its specific features. For instance, knowledge does not have a clearly delineated structure because its understanding is bounded by the metaphors used in getting its semantic field (Andriessen, 2004; Andriessen, 2008; Lakeoff & Johnson, 1999). Knowledge is intangible and nonlinear distinguishing this way clearly from the tangible resources like physical objects including monetary resources (Bratianu, 2013; Bratianu & Vasilache, 2009; Nonaka & Takeuchi, 1995). Synthetically, OECD (2006) remarks three basic features of the knowledge assets: "i) they are sources of probable future economic profits; ii) they lack physical substance; iii) to some extent, they can be retained and traded by a firm" (p. 9). Knowledge is created by people and as a

result of the knowledge creating spiral described by Nonaka and Takeuchi (2019), it amplifies and become organizational knowledge contributed significantly to the organization performance. An excellent example of how knowledge powers firms could be the unicorns. They are start-up firms that in very short time reach the value of 1 billion dollars, by far surpassing traditional companies that already have experience in the market. For a unicorn, market experience, tradition and classic business models, doesn't even matter. All that matters is the knowledge they possess, how they used it and how they create value through knowledge in the new economy, where technological innovations and opportunities are everywhere, including risks.

Cybersecurity challenges

Since the COVID-19 pandemic started, we know that there has been a substantial increase in teleworking, self-employed professionals who run their business from home taking advantage of new technologies, organizations having employees in smart working and many businesses they have moved their activities to the online environment (Baldwin & Weder di Mauro, 2020; Zakaria, 2020). Moving in online, in a complex environment and hard to be comprehended, many organizations have experienced many problems with their knowledge systems security due to increased risks in the online working. Thus, companies must understand their new cybersecurity challenges and to find solutions for them. Thus, we have to understand the relationships between knowledge management systems, knowledge economy new conditions, economic crises like COVID-19 and new requests for the firms' cybersecurity systems. The main problems managers face with respect to all these new contextual boundary conditions are the following:

- not understanding the cybersecurity concept and how this may be used to secure the organizational knowledge; because cybersecurity is more than to protect an electronic device or an network, applications, information, operations, disaster-related and business continuity and end-user education; cybersecurity is about protecting an organizational environment;
- as a consequence of the first challenge we add the lack of trainings and awareness for the people that are part of the organization;
- unlimited use of new technologies that are not yet technologically stable and are not sufficiently tested or not properly maintained that may cause easily, leak or stealth of knowledge;
- putting hopes in programs and machines that they will replace human errors;
- a weak controls on information security, inside and outside organization;
- another challenge is not to value the people who are part of the organization, making them vulnerable to other organizations or individuals to leak data thus creating security breaches;
- the fact that business strategies are not being redesigned to meet these cybersecurity challenges.

There are existing technologies for cybersecurity although due to the variations in cyber-attacks, the organizations need better technology for early detection of the attacks. The advancements in technology that we are seeing are blisteringly fast as compared to the past, which increases the number of cyberattacks with new challenging threats. With every passing year, thousands of new threats are created which are getting more and more dynamic which results in hazardous and challenging threats to the organizations (Rajasekharaiah, 2020). Knowledge management systems, like any other systems, are permanently under the pressure of knowledge risks and their possible consequences. Thus, design knowledge management systems should incorporate comprehensive analyses of knowledge risks and cybersecurity specific problems in order to minimize the potential losses of the firms' profits and in reducing their

competitive advantage. Understanding knowledge risk and cybersecurity issue become a challenging task of knowledge managers (Durst, 2019; Durst & Henschel, 2020; Durst & Wilhelm, 2013; Durst & Zieba, 2017; Shekar, 2021).

Methodology

The present paper relies on bibliometric research or statistical bibliography, to answer the research question: *What are the cybersecurity challenges in the knowledge economy?* In this regard, a complementary computer-aided analysis process was conducted, utilizing VOSviewer software. According to the software creators Van Eck and Waltman (2010, 2011, 2020), VOSviewer can be used in academic research projects to define, explore, and visually illustrate network-based scientific maps by employing text mining analysis. Out of the available range of approaches, the author used the term co-occurrence analysis option in the present conceptual exploration. In the present study, the terms or the words represent the unit of analysis. The analysis outcome is an intellectual plan or a knowledge atlas of the studied topic (Iliescu, 2021).

The data was retrieved, from the Web of Science (WoS) Core Collection and the retrieval model was through an advanced search function, while the retrieval period was: 2020-2022. The default values provided by WoS were used on all the rest of the retrieval settings, besides selecting publications that have titles and abstracts in English. In terms of the document type, we have selected the knowledge domain, economic, technological and business.

In the preparation phase and extract of data from Web of Science, we have implemented settings for the data search, filtering, and extraction, to get the most conclusive results. In the first place, we have defined a topic category, and we have focused our study on titles, abstracts, author keywords and keywords plus field. In this way we consider more relevant to gather more accurate findings for our term co-occurrence analysis. In the second phase, we set the search structure on "knowledge" to identify relevant publications for this concept. Other set concepts were knowledge economy and cybersecurity. In our study's case, the "knowledge economy" search returned all publications including terms like "knowledge", "economy" or "strategy". Furthermore, quotation marks have been used to ensure correct results and avoid lemmatization.

Searching primarily concepts as knowledge, knowledge economy, cybersecurity, and cybersecurity challenges, results showed that from 25254 terms, 509 meet the threshold and setting a minimum occurrences of a term to 15, for each of 509 terms, has been calculated a score. Based on this score, the most relevant terms were selected and the default choice selected by 60% for the most relevant terms. Applying this settings, were selected 331 terms and among most relevant terms were selected those with relevance more than 1.72 and occurrences more than 39. The result after clearing and filtering the data resulted 199 terms identified, 53 unique relevant items and 4 clusters were considered for VOSviewer mapping.

Results and discussions

In this section, we will discuss in detail the connections established between the knowledge domain (cluster 1) and the cybersecurity domain (cluster 2). As illustrated in this section, the two clusters are gaining relevant meaning only in the context of the cybersecurity challenges in the knowledge economy, and this will also reflect in the discussions below.

Table 1. VOSviewer cluster 1 analysis

Term	Cluster	Occurrences	Links	Link strength
Knowledge	1 - Knowledge	272	34	756
Economy		182	29	511
Strategy		125	34	445
Change		99	34	340
Understanding		89	33	314
Value		91	31	290

Source: Authors' own research.

In Table 1, we present the first cluster, "Knowledge", the term assigned by VOSviewer under this cluster, as well as the occurrences, links, and link strength value for each of the terms. The "Knowledge" term registers the most substantial values for all three parameters: throughout all analyzed publications and after performing the methodological data cleaning, the "Knowledge" term appears 272 times, and this value has been obtained by implementing the full counting analysis option. As the link's value is 34, this represents is that the term "Knowledge" is directly linked with each of the other terms in our database (a total of 16).

This indicates a direct relationship between the subject of the research and the rest of the identified term co-occurrence analysis items. The link strength represents a parameter that always takes a positive numerical value, and it is flexible, depending on the incidence of a given term through analyzed documents. The value 756 indicates that the first and most popular term of the first cluster has the highest incidence across the identified documents, compared with all other terms, regardless of the cluster. The link strength values are also helping us to identify the peak points in our analysis; concepts most related to the knowledge concept in the literature: "economy" (182) with a link strength 511, "strategy" (125) with a link strength 445, and "change" (99) with a link strength 340. At the same time, "understanding" (89) with link strength 314 and the term "value" (91) with the link strength 290, have the lowest incidence values of the first cluster.

From our first cluster it should be noted the interconnection of "knowledge", "economy" and "strategy" concepts and the link strength between terms, revealing the interdependencies and influence which may have on each other. In Table 2, we illustrate the terms associated with the second cluster, "Cybersecurity". The term also gives the name of the cluster. It is the second most encountered term across all analyzed documents, having an occurrence value of 189, generating in turn relevant connections with "attack", "network", "threat", "security" and "solution".

Table 2. VOSviewer cluster 2 analysis

Term	Cluster	Occurrences	Links	Link strength
Cybersecurity	2 - Cybersecurity	189	33	774
Attack		162	32	768
Network		168	33	707
Threat		155	33	700
Security		158	33	678
Solution		140	34	549

Source: Authors' own research.

With a high link strength between terms, almost in the same strength line, cybersecurity term is immediately succeeded by the term “attack”. This indicate a new trend in the cybersecurity concept, were attacks are treated, meaning that a dynamic exist, including in defining the challenges in the knowledge economy, due to the multitude of research and diversification. Therefore, we have four concepts that have very high link strength values, which again suggest researchers' interest in cybersecurity-attack, cybersecurity-network and cybersecurity-threat correlations.

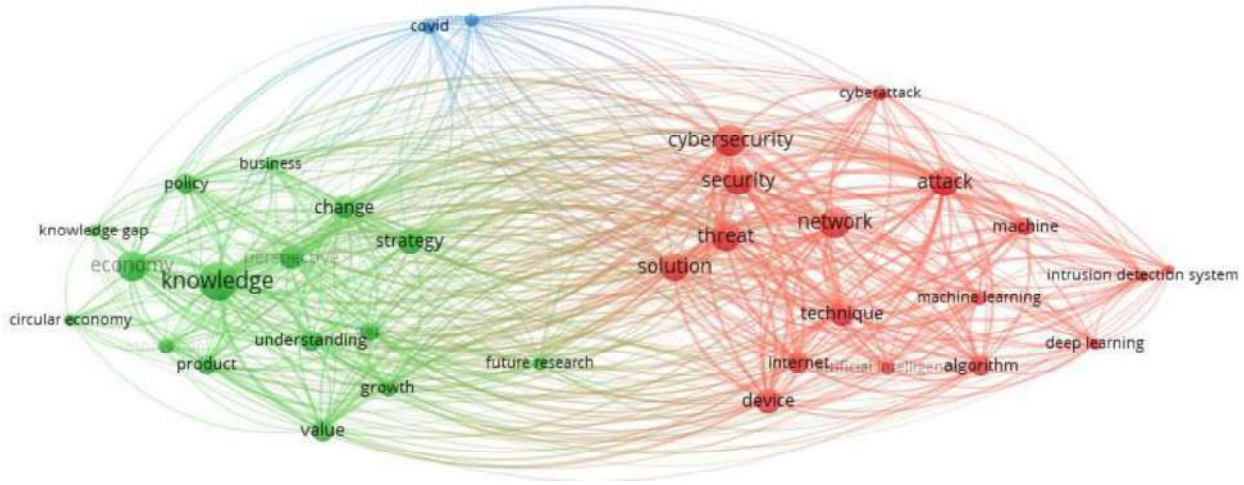

Figure 1. Network clusters visualization by VOSviewer software version 1.6.18

Source: Author’s research.

In Figure 1, we are presenting the network visualization of the four clusters, of which only two are relevant: cluster 1 “Knowledge” in green and cluster 2 “Cybersecurity” in red. Each term sphere size and distance are visual representations of their connection strength values given in the tables, according to Van Eck and Waltman (2010). In the cluster 1, the term “Knowledge” is positioned in the relative center of the network, sharing a similar position with the “Economy” term, as they are both located on the contour of an imaginary center of the network. This means that there is not one predominant concept in our analysis, but a set of essential ones defining the meaning of the knowledge economy idea. Another exciting network aspect relates to the fact that, even though directly connected specific items, cluster 1 “Knowledge” and cluster 2 “Cybersecurity” seem to be separated but still with strong connections between them. Understanding the insights gained through the systematic literature review, this visual distribution can be explained as follows: knowledge is a fundamental concept for the economy and associated with cybersecurity this should be understood as a new challenge for future research.

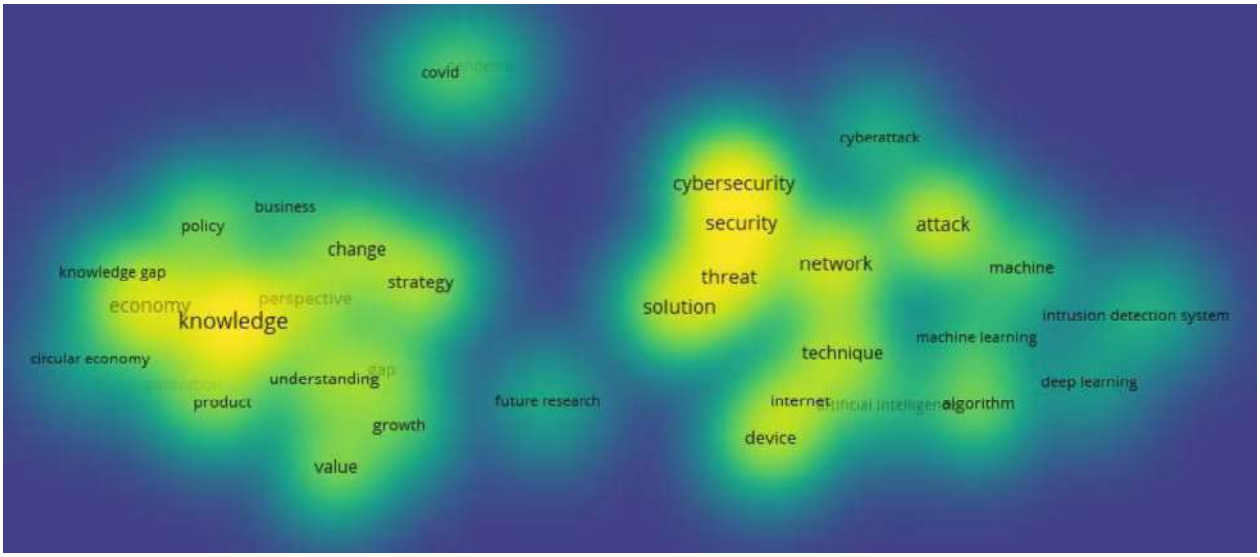

Figure 2. Network density visualization by VOSviewer software version 1.6.18
Source: Author's research.

In Figure 2, we can observe the representation of the density overview of the clusters, broadcasting the most visited concepts in the literature, correlated with the knowledge concept. According to Van Eck and Waltman (2010), each term has an associated sphere with a specific dimension and density of color. In Figure 2, as can been seen, is a specific distance between each sphere. These five parameters are directly linked to each item's values reflected in the cluster tables. For instance, "knowledge", "economy", "cybersecurity", "security" and "threat" have the most visible hallows on the map, and this is in alignment with their leading clusters positions and highest values in their cluster when it comes to the occurrences. An interesting aspect is a fact that on the one hand, "knowledge" concept appears to be in closer relationship with "economy", and on the other, "cybersecurity" is in a close relationship with "security", "threat" and "solution". This visual effect can be caused by the fact that closer items on the density map are part of the same article. It is also interesting to note the appropriation between items belonging to different clusters. The evident interest in knowledge and the economy influence on the knowledge economy are two examples of spikes of the knowledge literature.

The knowledge economy is not separate from the global economic system, but is part of that system – actively produced and reproduced to enable globalisation, economic liberalisation and the movement of financial capital. The key shift is the movement from knowledge about the economy to knowledge for the economy as part of a broader set of processes designed to reify all possible resources as objects amenable to commodification and control (May & Perry, 2018). The research also points out the direct correlation between cybersecurity – attacks and considering available research papers, this field will open new perspectives in further research on cybersecurity challenges which can be correlated with knowledge economy.

Conclusion and limitations

The purpose of this study was to evidence a connection between knowledge economy and cybersecurity concepts and to build a visual atlas of the interconnections. This was achieved by implementing a comprehensive literature review initially, followed by a text mining analysis with

VOSviewer software. While we successfully identified a set of research interests in cybersecurity associated with the knowledge economy concept, we have also found that each of them holds specific knowledge gaps and research areas that would require increased scientific attention, especially in cybersecurity area.

The main semantic clusters obtained by using VOSviewer are those of "Knowledge" and "Cybersecurity". The first cluster identifies the necessary links between the concepts of "knowledge", "economy", "strategy", "change", and "value". It is interesting to see how strategic thinking and business strategies become so important in the knowledge economy and how they are linked with knowledge management risks and their security. From the second cluster we get the connections between "cybersecurity", threat", "attack", and "security". Thus, it becomes obvious the need to study the vulnerabilities and risks embedded in the knowledge management systems and to anticipate possible threats and attacks from the external business environment and how to create emergent knowledge strategies to counteract them. So, together with many important advantages brought by digitalization in the knowledge economy, we have to be aware of the increased knowledge risks and cyber-attacks coming from the external business environment and to take adequate measures to mitigate their happening.

Regarding the limits of the study, for the present research paper, we have analyzed only papers from WoS, although papers on this topic were also published in some journals which are not indexed in WoS, including reports on cybersecurity from state Agencies and Governments.

References

Alavi M. & Leidner D. E. (2001). Knowledge management and knowledge management systems: conceptual foundations and research issues. *Management Information Systems Quarterly*, 25(1), 107. 10.2307/3250961.

Andriessen, D. (2004). *Making sense of intellectual capital: design a method for valuation of intangibles*. Amsterdam: Elsevier.

Andriessen, D. (2008). Stuff or love? How metaphors direct our efforts to manage knowledge in organizations. *Knowledge Management Research & Practice*, 6(1), 5-12.

Baheti, S., Tiwari, N., Parikh, R., Dandekar, P., Chandak, R. & Raipurkar, A.R. (2020). Challenges and innovations in cybersecurity, *Bioscience Biotechnology Research Communications,* 13(14), 227-230.

Baldwin, R. & Weder di Mauro, B. (2020). *Mitigating the COVID economic crisis: act fast and do whatever it takes.* London: CEPR Press.

Bech, M. (2019).Cyber-security and cyber-resilience, *The Eurofi Magazine*, 118-121

Bratianu, C. (2013). Nonlinear integrators of the organizational intellectual capital. In: Fathi, M. (Ed.). *Integration of practice-oriented knowledge technology. Trends and perspectives* (pp.3-16). Berlin: Springer-Verlag.

Bratianu, C. (2013). Exploring knowledge entropy in organization. *Management Dynamics in the Knowledge Economy,* 7(3), 353-366. DOI: 10.25019/MDKE/7.3.05.

Bratianu, C. (2020). Toward understanding the complexity of the COVID-19 crisis: a grounded theory approach. *Management & Marketing. Challenges for the Knowledge Society*. 15(S1), 410-423. DOI: 10.2478/mmcks-2020-0024.

Bratianu, C. & Bejinaru, R. (2021). COVID-19 induced emergent knowledge strategies. Knowledge and Process Management, 28(1), 11-17.

Bratianu, C. & Vasilache, S. (2009). Evaluating linear-nonlinear thinking style for knowledge management education. *Management & Marketing*, 4(3), 3-18.

Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. *Eurasip Journal on Information Security*, doi.org/10.1186/s13635-018-0080-0, 1-3.

Durst, S. (2019). How far have we come with the study of knowledge risk? *VINE Journal of Information and Knowledge Management Systems*, 49(1), 21-34.

Durst, S. & Henschel, T. (2020). *Knowledge risk management. From theory to praxis*. Cham: Springer Nature.

Durst, S. & Wilhelm, S. (2013). Do you know your knowledge at risk?, *Measuring Business Excellence*, 17(3) 28-39.

Durst, S. & Zieba, M. (2017). Knowledge risks – towards a taxonomy. *International Journal of Business Environment*, 9(1), 51-63.

Lafayette, B., Curtis, W., Bedford, D. & Iyer, S. (2019). *Knowledge economies and knowledge work.* Bingley: Emerald Publishing.

Lakeoff, G. & Johnson, M. (1999). *Philosophy in the flesh. The embodied mind and its challenge to western thought*. New York, NY: Basic Books.

Liu, S. (2020). *Knowledge management. An interdisciplinary approach for business decisions.* London: Kogan Page.

May, T., & Perry, B. (2018). *Cities and the knowledge economy. Promise, politics and possibilities*. London: Routledge.

Massingham, P. (2020). *Knowledge management. Theory in practice*. Lso Angeles, CA: SAGE.

Nonaka, I. & Takeuchi, H. (1995). *The knowledge-creating company. How Japanese companies create the dynamics of innovation*. Oxford: Oxford University press.

Nonaka, I. & Takeuchi, H. (2019). *The wise company. How companies create continuous innovation*. Oxford: Oxford University Press.

O'Dell, C. & Hubert, C. (2011). *The new edge in knowledge. How knowledge management is changing the way we do business*. New York, NY: John Wiley & Sons.

Organization for Economic Co-operation and Development (OECD) (2006). *Creating value from intellectual assets.* Retrieved from http://www.oecd.org/science/inno/36701575.pdf.

Powell, W.W. & Snellman, K. (2004). The knowledge economy. *Annual Review of Sociology*, 30, 199-220. Doi: 10.1146/annurev.soc.29.010202.100037.

Rajasekharaiah, K. M. (2020). Cyber security challenges and its emerging trends on latest technologies. *IOP Conference Series: Materials Science and Engineering*, 1-8.

Shekar, S. (2021). *Design knowledge management system. A practical guide for implementing ISO30401 KMS standard*. Delhi: Penman Books.

Von Krogh G., Ichijo K., Nonaka I. (2000). *Enabling knowledge creation: how to unlock the mystery of implicit knowledge and release the power of innovation*. Oxford: Oxford University Press.

Zakaria, F. (2020). *Ten lessons for a post-pandemic world*. London: Penguin Books.