Proceedings of the International Conference on Business Excellence

Knowledge Vulnerabilities Scoring System and the Knowledge Economy

--Manuscript Draft--

Manuscript Number:	ICBE-D-23-00195
Full Title:	Knowledge Vulnerabilities Scoring System and the Knowledge Economy
Article Type:	Original Study
Section/Category:	Knowledge Economy
Keywords:	knowledge; knowledge economy; knowledge vulnerabilities; knowledge vulnerabilities scoring system
Corresponding Author:	Vlad Mihai Ursache, Ph. D. SNSPA: Scoala Nationala de Studii Politice si Administrative Dumbraveni, Sibiu ROMANIA
Corresponding Author Secondary Information:	
Corresponding Author's Institution:	SNSPA: Scoala Nationala de Studii Politice si Administrative
Corresponding Author's Secondary Institution:	
First Author:	Vlad Mihai Ursache, Ph. D.
First Author Secondary Information:	
Order of Authors:	Vlad Mihai Ursache, Ph. D.
Order of Authors Secondary Information:	
Manuscript Region of Origin:	ROMANIA
Abstract:	The paper aims to study knowledge vulnerabilities correlations with the knowledge economy, focusing on identifying knowledge vulnerabilities considering new challenges in the knowledge economy. The purpose is to analyze and understand the knowledge vulnerabilities, focusing our research on identifying some vulnerabilities in the organizational knowledge dynamics. In order to achieve our goal, we propose KVSS method that may be used in the identification and analysis process of knowledge vulnerabilities. The process will be beneficial for a correct analysis of knowledge vulnerabilities and the impact in the knowledge economy, completing the research with some solutions that may reduce negative consequences for organizations that are an active component in the knowledge economy. In today knowledge economy were knowledge has become essential for every organization and 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, identifying knowledge vulnerabilities will increase visibility on organizational knowledge given the opportunity to threat weakness point identified and in the end to achieve the goal to strengthen the organization. The knowledge economy has evolved more that was predicted in a short time period, adding notable value to the knowledge economy. On other side, this fast evolution in the knowledge economy revealed that some components were not fully covered, leaving some gaps that may be exploited. Our research is focused on identifying these gaps in the knowledge economy especially on knowledge vulnerabilities.
Suggested Reviewers:	Constantin Bratianu constantin.bratianu@gmail.com

sciendo

Knowledge Vulnerabilities Scoring System and the Knowledge Economy

Vlad-Mihai URSACHE
National University of Political Studies and Public Administration, Exposition Blvd., No. 30 A, Sector 1, Bucharest, Romania
vlad.ursache.21@drd.snspa.ro

Abstract

The paper aims to study knowledge vulnerabilities correlations with the knowledge economy, focusing on identifying knowledge vulnerabilities considering new challenges in the knowledge economy. The purpose is to analyze and understand the knowledge vulnerabilities, focusing our research on identifying some vulnerabilities in the organizational knowledge dynamics. In order to achieve our goal, we propose KVSS method that may be used in the identification and analysis process of knowledge vulnerabilities. The process will be beneficial for a correct analysis of knowledge vulnerabilities and the impact in the knowledge economy, completing the research with some solutions that may reduce negative consequences for organizations that are an active component in the knowledge economy. In today knowledge economy were knowledge has become essential for every organization and 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, identifying knowledge vulnerabilities will increase visibility on organizational knowledge given the opportunity to threat weakness point identified and in the end to achieve the goal to strengthen the organization. The knowledge economy has evolved more that was predicted in a short time period, adding notable value to the knowledge economy. On other side, this fast evolution in the knowledge economy revealed that some components were not fully covered, leaving some gaps that may be exploited. Our research is focused on identifying these gaps in the knowledge economy especially on knowledge vulnerabilities.

Keywords: knowledge, knowledge economy, knowledge vulnerabilities, knowledge vulnerabilities scoring system, knowledge management

DOI:

Introduction

In a world of continuous change and marked by unpredictability, world pandemic crisis, military tensions between the United States of America and China, Turkiye and Greece, Israeli and Palestinian conflict, insurgencies in Africa and other parts of the world, adding energy crisis, global food crisis, financial crisis, warming climate crisis and cybersecurity war, "we ask how challenging all of this can be to knowledge management especially for knowledge risks management given the fact that organizations have less time to manage all the uncertainties and that they are constrained to continuously develop new strategies to assure healthy management of knowledge risks*"* (Ursache, 2022b).

In a digitalized era where innovative technologies are on a daily basis and information is transferred at a very high speed, the number of research topics in the knowledge economy domain has become more and more diversified challenging researchers to explore unknown's areas and unexploited research fields of interest, leading knowledge economy domain to a larger academic scale than it is now. In this process of continuous change, knowledge has become more critical than ever, becoming the main component in the evolution process of organizations and societies and a key for organizations to achieve their success.

The purpose of the present research is to obtain a more pertinent and objective image of the concepts of knowledge vulnerabilities in the knowledge economy area, starting from the SECI model that describes the dynamics of organizational knowledge elaborated by Ikujiro Nonaka (1994) and refined together with his colleagues, most notably with Hirohata Takeuchi (Nonaka & Takeuchi, 1995). This model contains three main components: the SECI knowledge cycle, the dynamic context Ba, and the knowledge vision (Bratianu, 2015). Nonakian dyad of tacit-explicit knowledge is completed with the research on the triple Helix of knowledge, the triad of cognitive-emotional-spiritual knowledge elaborated by Bratianu (2013a).

Consequently, the research is focused on the three conceptual pillars of our research, presented in Figure 1 below, and presented in two progressive steps. First, the comprehensive literature review findings are thoroughly analyzed under the three conceptual pillars of the research, knowledge vulnerabilities, knowledge risks, and knowledge vulnerabilities scoring systems (KVSS). All three conceptual pillars of the research will be analyzed from the organizational dynamic's perspective. Second, we will focus our research on the proposed method Knowledge Vulnerabilities Scoring System to analyze and identify knowledge vulnerabilities.

Figure 1. The pillars of the research program

(Author's research)

The subject chosen to be researched, in this case, "Knowledge Vulnerabilities Scoring System and the Knowledge Economy", generates a complex set of future research directions, which may be clearly defined and specified in future research. The research objective is identifying, analyzing and proposing solutions that may be applied in the knowledge economy, which may reduce negative consequences within an organization increasing their knowledge in the economy area.

The expected results are to understand the primary sources of vulnerabilities and risks that may be generated for a knowledge economy system and to identify solutions that may be used to treat vulnerabilities and assess the risks in the knowledge economy.

Although there are some excellent papers focusing on knowledge (Nonaka and Takeuchi (2019); Bratianu, 2013; Bratianu & Vasilache, 2009; Bratianu, 2015) on knowledge risks (Bratianu, Nestian, Tita, Voda, & Guta, 2020; Durst, 2019; Durst & Wilhelm, 2013; Durst & Zieba, 2017; Durst & Henschel, 2020), there is no paper analyzing the vulnerabilities on knowledge economy from a dynamic organizational perspective. There are only very few papers on vulnerabilities (Mehri, Arlos & Casalicchio, 2022; Timmerman, 1981; Shitangsu, 2013; Turner, 2003; Bejinaru, 2022; Bratianu & Bejinaru, 2022), but none of them analyze or identify and treat vulnerabilities purely from a knowledge perspective and only marginally about their relationship with the management domain from different perspectives.

Thus, there is a critical knowledge gap in the literature dedicated to analyzing, identifying, and

understanding knowledge vulnerabilities in the knowledge economy, not to mention a method dedicated to scoring and metrics of knowledge vulnerabilities. The gap identified in the knowledge domain is critical for future improvements in knowledge economy research and organizational knowledge dynamics.

The present research aims to perform a systematic bibliometric study to identify some correlations of knowledge vulnerabilities with knowledge economy. Our research question can be formulated as follows:

RQ: Are knowledge vulnerabilities treated in the knowledge economy domain?

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 economy, knowledge vulnerabilities and knowledge risks. This will let us visualize the current status of research by observing the existing links between knowledge economy concept and other important concepts such as knowledge vulnerabilities and illustrate the most relevant relationships that we have discovered between them. Then, we will analyze the knowledge vulnerabilities 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

From most famous work in the economy of Adam Smith (1723-1790), Wealth of Nations, published by Smith's in 1776 and considered the founding document of modern economics were it analyzes the division of labor, the role of self-interest in market economies, and the benefits of free trade and specialization to the Theory of Moral Sentiments, were Smith's earlier work on ethics and human behavior, published in 1759, explores the idea that people are naturally sympathetic to one another and that this empathy drives social cooperation.

Continued to the Principles of Economics of Alfred Marshall (1842-1924), considered to be a seminal work in the field of neoclassical economics. It introduced the concept of marginal utility and popularized the idea that supply and demand determine prices in markets. Marshall also developed the concept of consumer surplus and producer surplus, which are still used today to measure the welfare gains from trade. To John Maynard Keynes (1883-1946) and the General Theory of Employment, Interest and Money, published in 1936, Keynes' book fundamentally challenged classical economic theory by arguing that market economies can experience prolonged periods of high unemployment and that government intervention can help to address this problem. Keynes being also known for his contributions to macroeconomics, including the idea of the "paradox of thrift" and the importance of aggregate demand in determining economic growth.

Reaching to Milton Friedman (1912-2006) and to the famous research, A Monetary History of the United States. This 1963 book, co-authored with Anna Schwartz, argues that monetary policy played a central role in the Great Depression and subsequent periods of inflation

and deflation. It also advocates for a monetary rule to stabilize the economy. Friedman is known for his advocacy of monetarism, the idea that the money supply should be controlled to achieve stable economic growth, and for his support of free-market policies and deregulation.

To current research in the economy area were we have different needs and gaps, paying due attention to the knowledge vulnerabilities, will do nothing but finding solutions to various challenges and bringing that added value necessary for a better functioning of any organization and the economy.

It is worth noting that a knowledge-based economy has existed since the dawn of human civilization and its evolution has been based on its ever greater accumulation of knowledge over time. Societies benefited from knowledge in the form of the goods and services that were produced and made available to meet socioeconomic needs. Knowledge was incorporated into the production function in the form of human capital. In the early economic literature, there were no specific references to the importance of knowledge. Economists began to realize its importance in the late 19th century as Alfred Marshall suggested that "knowledge is our most powerful engine of production" and the organization facilitates the growth of knowledge. In early 20th century, Schumpeter considered the "new combination of knowledge" as an important element for innovation and entrepreneurship (Cader, 2008).

In a positive economy, we discover that economics as a positive science is a body of tentatively accepted generalizations about economic phenomena that can be used to predict the consequences of changes in circumstances. Progress in expanding this body of generalizations, strengthening our confidence in their validity, and improving the accuracy of the predictions they yield is hindered not only by the limitations of human ability that impede all search for knowledge but also by obstacles that are especially important for the social sciences in general and economics in particular, though by no means peculiar to them (Friedman, 1953).

In economies, the functions of knowledge are characterized by four important features: (a) knowledge ages rapidly and new knowledge is constantly replacing the old; (b) scientific (including social scientific) knowledge is highly valued, and the scale and economic penetration of scientific knowledge increases through subsequent economic development phases; (c) knowledge economies are especially characterized by the exploitation of new knowledge in order to create more new knowledge; and (d) knowledge is used in the production of goods and services, and to enhance the social welfare of its citizens (Cader, 2008).

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., 2020).

The characterization and identification of knowledge is a complex process. There are kinds of know-ledge (know-what, know-why, know-how and know-who) which are important for knowledge-based economies (OECD, 1996). The stock or knowledge of these „kinds of knowledge" could vary from economy to economy, firm to firm, or region to region, and there is no clear understanding of what constitutes different kinds of knowledge (Cader, 2008).

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 (Ursache, 2022a).

Another example will be on blockchain technologies and on crypto currencies, were the knowledge has reached an unimaginable well-being that is in a continuous growth, and research in these fields being almost non-existent.

Knowledge vulnerabilities

Knowledge vulnerabilities is a new research field for the knowledge economy and this research area has become essential for any organization to understand how internal and external forces influence each other, how the organizational balance works, how important is the identification process of knowledge vulnerabilities to an organization, and how this process can make the difference between success and failure for an organization.

Aware that we live in an increasingly turbulent environment where uncertainty dominates, it is the knowledge of the world that one possesses. The capability to learn can make a difference (Bratianu & Bolisani, 2017, p. 234).

Considering the fact that knowledge is intangible and nonlinear, distinguishing this way clearly from tangible resources like physical objects, including monetary resources (Bratianu, 2013; Bratianu & Vasilache, 2009; Nonaka & Takeuchi, 1995).

Synthetically, OECD (2006) remarks three essential 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).

People create knowledge, and as a result of the knowledge-creating spiral described by Nonaka and Takeuchi (2019), it amplifies and becomes organizational knowledge that contributes significantly to the organization's performance.

Academic research on knowledge domain has been conducted in various fields, including management, economy, philosophy, and psychology, sociology, and computer science, but none of researches focus on knowledge vulnerabilities in the knowledge economy domain.

In academic research, vulnerabilities have been treated in disaster management, geography, climate change, economics, information security, and, more recently, cybersecurity. However, research has yet to be made so far in the knowledge domain, identifying and analyzing, in particular, the subject of knowledge vulnerabilities.

Having its roots in the Latin word *vulnus* and later on evolved into *vulnerabilis* and recently in *vulnerability*, the terminology has been used for centuries and from the beginning of its use until now, the same idea has been stated in numerous definitions. According to some studies, being vulnerable means having a weakness. However, it is incomplete because an organization may have some vulnerabilities, and as long as they are not exploitable, the organization does not have a weakness.

Our research is grounded on thoroughly examining the literature to comprehend what has been explored about vulnerabilities. The aim is to identify different vulnerability classifications and analyze them to accommodate additional risks. Table 1 below outlines various vulnerability perspectives available in the literature. It will detail the definition, year, authors' name, journal name, and main findings.

Table 1: Vulnerabilities definition available in the literature

Definition	Year	Author
Vulnerability is the degree to which a person, system or unit is likely to experience harm due to exposure to perturbations or stress	2002	Kasperson, R. & Kasperson, J. & Dow, K.
Vulnerability is defined as the extent to which a natural or social system is susceptible to sustaining damage from climate change. Vulnerability is a function of the sensitivity of a system to changes in climate and the ability to adapt to systems to changes in climate. Under this framework, a higly vulnerable system would be one that is highly sensitive to modest changes in climate	1996	Intergovernmental Panel on Climate Change (PCC). World Meteorological Organisation.
Vulnerability is conceived as both a biophysical risk as well as a social response, but within a specific areal or geographic domain. This can be geographic space, where vulnerable people and places are located, or social space who in those is most vulnerable.	1996	Cutter, S.
By vulnerability we mean the characteristics of a person or group in terms of their capacity to anticipate, cope with, resist and recover from the impact of a natural hazard. It involves a combination of factors that determine the degree to which someone's life and livelihood are put at risk by a discrete and identifiable event in nature or in society.	1994	Blaikie, P. & Cannon & Davis, L. & Wisner, B.

Vulnerability is defined in terms of exposure, capacity and potentiality. Accordingly, the prescriptive and normative response to vulnerability is to reduce exposure, enhance coping capacity, strengthen recovery potential and bolster damage control (i.e., minimize destructive consequences) via private and public means.	1993	Watts, M.J., & Bohle, H.
Vulnerability is the differential capacity of groups and individuals to deal with hazards based on their positions within physical and social worlds.	1992	Dow, K.
Vulnerability is operationally defined as the inability to take effective measures to insure against losses. When applied to individual's vulnerability is a consequence of the impossibility or improbability of effective mitigation and is a function of our ability to detect the hazards.	1989	Bogard, W.
Vulnerability is the potential for loss	1989	Chambers, R.
Vulnerability is the degree of loss to a given element or set of elements at risk resulting from the occurrence of a natural phenomenon of a given magnitude.	1982	United Nations Disaster Relief Organization (UNDRO).
Vulnerability is the degree to which a system acts adversely to the occurrence of a hazardous event. The degree and quality of the adverse reaction are conditioned by a system's resilience (a measure of the system's capacity to absorb and recover from the event).	1981	Timmerman, P.
Vulnerability is the threat (to hazardous materials) to which people are exposed (including chemical agents and the ecological situations of the communities and their level of emergency preparedness). Vulnerability is the risk context.	1980	Gabor, T., & Griffitch, T.

Source: Authors' own research.

On ISO 27005, we find vulnerability being defined as: *a weakness of an asset or group of assets that can be exploited by one or more threats, where an asset is anything that has value to the organization, its business operations, and their continuity, including information resources that support the organization's mission;* and on ISO/IEC 29147:2018(en) Information technology, security techniques, vulnerability disclosure, define that a *vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence*.

We agree more on the shape of the definitions given by the mentioned standards, at least for the mention *that can be exploited by one or more threats, where an asset is anything that has value to the organization* and *allows a security impact or consequence.*

From the above definitions, the term's weakness, threats, exposure, impact and consequence caught our attention for a deep analysis. Analyze-it together, each term can be associated with a process. Each process is part of a management system where vulnerabilities can be analyzed, identified, treated, and monitored and are directly connected with risks. Weakness, threats and exposure will not have sense without impact and consequence and vice-versa.

In all the process of vulnerabilities identification and analysis, an important component is the risks calculation. The National Institute of Standards and Technology, NIST, defines risk as the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. The formula traditionally represents risk:

*R (risk) = P (probability of occurrence) * C (consequence of occurrence either represented by some value or by a loss function)*

Risk management is the process of identifying risk, assessing risk, and taking steps to manage risk by reducing risks to an acceptable level (Stoneburner et al., 2001). Additionally, Smith et al. (2001) and Aubert et al. (1998) agree that IS managers and researchers traditionally define risk in terms of negative consequences describing risk as the possibility of loss or damage and the possibility of suffering harm or loss. An alternative view by Billington (1997) points out that, when examined closely, 'risk' can actually lead to both positive and/or negative consequences.

Viewing risk as something more than a hazard is highly applicable to risk management in KM. This is consistent with the NIST risk definition so the NIST risk algorithm will be used as the basis for determining knowledge loss risk (Murray, 2009).

Nowadays, we find at least one detailed definition of vulnerability in each discipline and field of research. For the knowledge field we did not find an explicit definition, but starting from the fact that being vulnerable means to have a weakness, we may say that vulnerability is an abstract idea that encompasses the inner state of an internal environment of an individual or system that when interact with an unfriendly external environment losses may result and the internal environment may be affected.

Researchers from the global environmental risk area as Kasperson, R., Kasperson, J. & Dow, K. (2001) defined vulnerability as the degree to which a person, system or unit is likely to experience harm due to exposure to perturbations or stresses.

According to environmental change researcher W. Neil Adger (2006), the concept of vulnerability has been a powerful analytical tool for describing states of susceptibility to harm, powerlessness, and marginality of both physical and social systems, and for guiding normative analysis of actions to enhance well-being through reduction of risk.

The key point when we discuss it further on vulnerabilities is that we have to analyze it according to their exposure and exploitation. In case the exploitation of vulnerabilities is not possible, we have to consider only a possible vulnerability that may occur in the near future and

only when the actual action of exploitation takes place, an action that we may call it "0 Zero time", only starting from that moment we may consider to be indeed a vulnerability to the organization.

Starting from our above understanding of the essence of vulnerabilities, from the time when a possible vulnerability is identified, considered to be a weakness and to generate a treat, to the exposure and the exploitation process that will change a possibility into certainty, the whole process will be at the basis of our future research on knowledge vulnerabilities.

Vulnerabilities can be analyzed and identified separately from risks. Up to a certain point, this process is helpful for any organization, but if this process ends here and needs to be followed by an analysis, identification and risk assessment, will not only be complete, it will become a cost in the end for the organization.

On the other hand, risk analysis, risk identification, and risk assessment can be made without identifying vulnerabilities, but this approach can also have some shortages. A more practical method in correctly identifying knowledge risks, is to include even the analysis of knowledge vulnerabilities.

The identification process of knowledge vulnerabilities it is not easy at all and involves a very good understanding of knowledge concepts, risks, knowledge management, and many other constructs. Considering that *vulnerabilities are essentially the weaknesses that allow threats to exploit an organization* (Winkler & Treu Gomes & Shackleford, 2017, p. 164) and *vulnerabilities enable risks,* our research will analyze vulnerabilities, including the risks as also.

Observing that knowledge risks have been treated in various research and already have been identified by researchers some of the knowledge risks, we will continue our research analysis on knowledge vulnerabilities having for reference the existing studies.

Our research is grounded on a thorough examination of the literature to comprehend what risks have been identified in the research on knowledge risk and knowledge risk management so far. The aim is to identify knowledge vulnerabilities considering some identification of knowledge risks and to correlate risks with vulnerabilities, understanding the reason behind any risks and outlining from our perspective the knowledge vulnerabilities identified. It will detail the authors' name, journal name, identified knowledge risks and identified possible knowledge vulnerabilities.

The calculation part for each vulnerability identified through the knowledge Vulnerability Scoring System (KVSS), exposure part, and the exploitation point of each vulnerability will be treated in future research.

Table 2: Knowledge vulnerabilities identified

Authors	Year	Knowledge Risks	Knowledge Vulnerabilities
Jamieson & Loeng	2003	➢ Lack of effective knowledge base maintenance ➢ Knowledge stealing ➢ Risk of declining organizational creativity and innovation ➢ Ineffective management	➢ Lack of effective knowledge base maintenance vulnerabilities ➢ Knowledge stealing vulnerabilities ➢ Declining organizational creativity and innovation vulnerabilities ➢ Ineffective management vulnerabilities
Bayer &Maier	2006	➢ Knowledge transfer risks *are concentrated at the level of operational business practices.*	➢ Knowledge transfer vulnerabilities
Perrot	2007	➢ Knowledge gap risk, *which may hinder the company in fulfilling its objectives.*	➢ Knowledge gap vulnerabilities
Lambe	2013	➢ Knowledge articulation risks ➢ Knowledge outsourcing risks ➢ Knowledge acquisition risks ➢ Knowledge continuity risks	➢ Knowledge articulation vulnerabilities ➢ Knowledge outsourcing vulnerabilities ➢ Knowledge acquisition vulnerabilities ➢ Knowledge continuity vulnerabilities
Durst & Zieba	2017	➢ Knowledge risks due to unlearning ➢ Knowledge risks due to forgetting	➢ Unlearning knowledge vulnerabilities ➢ Forgetting knowledge vulnerabilities
Brătianu	2018	➢ Knowledge waste risk ➢ Knowledge hoarding risk ➢ Knowledge hiding risk ➢ Knowledge attrition risk ➢ Knowledge obsolescence risk	➢ Knowledge waste vulnerabilities ➢ Knowledge hoarding vulnerabilities ➢ Knowledge hiding vulnerabilities ➢ Knowledge attrition vulnerabilities ➢ Knowledge obsolescence vulnerabilities

Source: Authors' own research.

Knowledge vulnerability scoring system (KVSS)

Being an intangible resource, because knowledge is not a tangible physical object and does not have a certain form and mass, it can be represented by a field (Cegarra-Navarro et all., 2023); knowledge is hard to quantify, measuring it and associate a value for this type of resource, not to mention giving it a score. Indeed is hard, but it is not impossible.

Our research opens a new ways in the research of knowledge vulnerabilities proposing an ambitious goal to set a system through which it can be analyzed, monitor and capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. The scoring formula and principles will be treated in future research. In present research paper, we propose a method that may be used in a very challenging and complex area, on the knowledge domain.

We know that 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.

In the process of assess and prioritize the knowledge vulnerabilities, we propose a method by which several factors will be considered in the analysis process of a knowledge vulnerabilities.

KVSS will be composed of three metric groups: Base, Temporal, and Environmental. A referral system for our method will be the mechanisms conceived by Forum of Incident Response and Security Teams. In this system, the Base will reflect the severity of a vulnerability according to its intrinsic characteristics which are constant over time and assumes the reasonable worst case impact across different deployed environments. The Temporal metrics will adjust the Base severity of a vulnerability based on factors that change over time, such as the availability of exploitation, considering the exposure surface. The Environmental metrics will adjust the Base and Temporal severities to a specific environment. Factors such as the presence of mitigations in that environment will be considered. Exposure, exploitation and threats will be among the indicators that may be used to achieve a qualitative representation of the vulnerabilities impact and further, a score will be used to prioritize vulnerability.

In the KVSS method, a part mentioned indicators, the assessment and prioritization of knowledge vulnerabilities we should include a risk analysis and risks calculation, focusing first on principal characteristics of knowledge and thus using the KVSS method we will be able to identify correctly the existing vulnerabilities in the knowledge domain. In the knowledge economy or other related area of knowledge.

Method to establish a Knowledge Vulnerabilities Scoring System (KVSS) will use the notion of severity, which is common among indicators used in the cybersecurity field. We will use the severity measure based on a metric that will produce a score ranging from 0 to 10, with 0

being the lowest and 10 being the highest severity. The metrics will be divided in groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. The scores will be computed in sequence in such a way that the Base Score will be used to calculate the Temporal Score and the Temporal Score will be used to calculate the Environmental Score. Metrics, impact metrics, and equations will be detailed in future research.

A KVSS method will also be represented as a vector string, a compressed textual representation of the values used to derive the score. Two common uses of KVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of knowledge vulnerabilities remediation activities.

KVSS method will not be a measure of risk, will be a method that may be used to supply a qualitative measure of severity of knowledge vulnerabilities that may be a very useful as measurement system for any type of organization, and to prepare them to anticipate threats and to calculate better the risks. In all this process the goal will be to help organizations to properly assess and prioritize the knowledge vulnerabilities in the knowledge management system and finally making the organization stronger, anticipating and preventing the exposure vulnerabilities faster, improving even the treatment process.

Methodology

Knowledge vulnerabilities in an unexplored area, and finding no research that analyze and identify knowledge vulnerabilities, on our research we have performed a systematic bibliometric study to identify the main correlations of the existing vulnerabilities studies from various fields with the knowledge economy.

The present paper relies on bibliometric research or statistical bibliography, to answer the research question: *Are knowledge vulnerabilities treated in the knowledge economy domain?*

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 researches, the introductory part will be followed by the specific literature reviews with a specific focus on vulnerabilities, threats, exposure, exploitation, knowledge risks and knowledge management.

This will let us visualize the main correlations of the vulnerabilities research from various fields with the knowledge domain, observing the existing links between vulnerabilities research from various fields with the knowledge domain. In the next stage, we will analyze the vulnerabilities research with data sources and the applied methodology that will be presented to conclude with results, study's limitations, and possible future research axes.

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 Scopus and the retrieval model was through an advanced search function, and our search was within *article title*, *abstract* and *keywords*, the term *vulnerability*, while the retrieval period was: 2015-2024.

We have selected starting from 2015, considering that almost 10 years will reveal notable results for our study. The same advanced set of data will be used for the terms *threats, exposure, exploitation, knowledge risks* and *knowledge management*. Subject area, was selected Business Management and Accounting. Other available subject areas were considered not directly connected to the knowledge management.

In the preparation phase and extract of data from Scopus, 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 this regard, we divided our study in two parts.

In the first part, we set the search structure on "vulnerability" to identify relevant publications for this concept to view the connection with other relevant concepts and the connection strength with other concepts. In our study's case, the "vulnerability" search initially returned 231,283 research and after applying the filter on subject area Scopus returned 7,118 results meet the threshold and setting a minimum occurrence of a term to 5, for each of 7,118 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 setting, of the 10,190 keywords, 502 meet the threshold. For each 502 keywords, the total strength of the co-occurrence links with other keywords was calculated. The keywords with the greatest total link strength was selected, from 502 keywords. The result after clearing and filtering the data resulted 480 terms identified, and 6 clusters were considered relevant for our study, where the term vulnerability was found in the same cluster with terms such as risk, management.

Results and discussions

In this section, we will discuss in detail the connections established between the vulnerability and COVID-19 (cluster 2), network security (cluster 1), risk assessment and climate change (cluster 3). As illustrated in this section, the three clusters are gaining relevant meaning in the context of vulnerability correlation with other research fields, and this will also reflect in the discussions below.

Table 3. Scopus cluster 2 analysis

Term	Cluster	Occurrences	Links	Link strength

Vulnerability	2 - Vulnerability & COVID-19	324	390	1352
COVID-19		196	228	590
Human		30	98	201
Pandemic		33	93	153
Public Health		17	58	84
COVID-19 Pandemic		24	40	45
Financial vulnerability		22	26	28

Source: Authors' own research.

In Table 3, we present the second cluster, considered relevant for our research, "Vulnerability & COVID-19".The term assigned by VOSviewer under this cluster, as well as the occurrences, links, and link strength value for each of the terms. The "Vulnerability" term registers the most substantial values for all three parameters: throughout all analyzed publications and after performing the methodological data cleaning, the "Vulnerability" term appears 324 times, and this value has been obtained by implementing the full counting analysis option. As the link's value is 390, representing that the term "Vulnerability" is linked with terms that are in all our clusters.

This indicates a direct relationship between the subject of the research and the rest of the identified term co-occurrence analysis items, including financial vulnerabilities. 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 1352 of link strength 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: "COVID-19" (196) with a link strength 590, "Human" (30) with a link strength 201, and "Pandemic" (33) with a link strength 153. At the same time, "Public Health" (17) with link strength 84, "COVID-19 Pandemic" (24) with the link strength 45 and "Financial vulnerability" (22) with link strength 28. From incidence of terms and connection, we may see that "Vulnerability" has a notable link strength and has been used in various research fields of interest.

From our study results, we may see that "knowledge vulnerabilities" is not treated directly, there are no studies so far, but the importance of the term "Vulnerability" in other research is quite notable. As may be seen from *Figure 2*, the term "Vulnerability" not only that is has connection with other terms such as "Risk assessment", "Resilience", "Sustainable development", "Climate change", "Network security", "Cybersecurity" and many others, but is has occurrence of 324, confirming us one more time the importance of our study in the knowledge vulnerabilities and risks area.

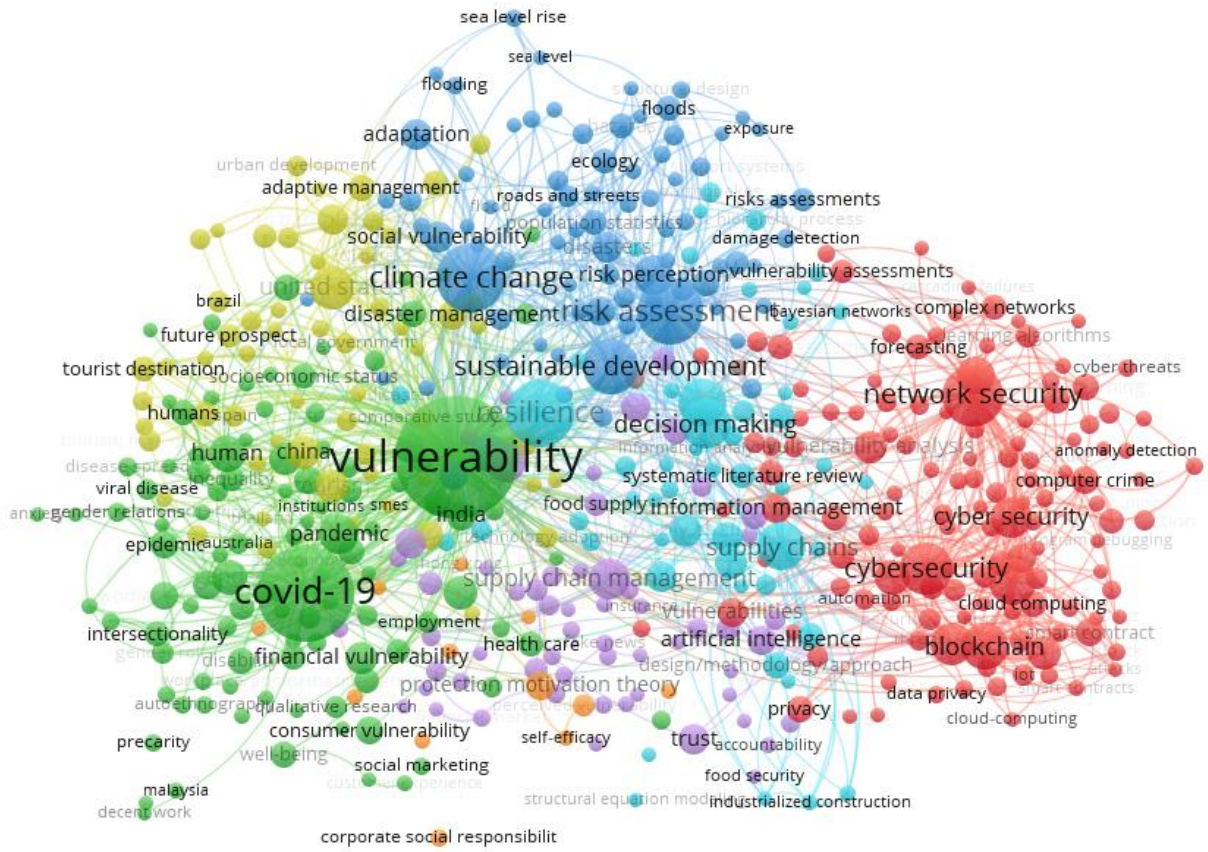

Figure 2. Network clusters visualization by VOSviewer software version 1.6.18

Source: Authors' own research.

In Figure 2, we are presenting the network visualization of all clusters, of which only three are relevant: Vulnerability & COVID-19 (cluster 2), network security (cluster 1), risk assessment and climate change (cluster 3). 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 2, the term "Vulnerability" is more visible in the network together with the term COVID-19, and other terms as network security (cluster 1), risk assessment and climate change (cluster 3), as they have a notable presence in the network. This means that there is one predominant concept in our analysis and this is the "Vulnerability" concept, an essential term with strong connections in various fields. Another exciting network aspect relates to the fact that, even though directly connected specific items, cluster 2 "Vulnerability & COVID-19" and cluster 3 "risk assessment and climate change" and cluster 1 "network security", 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: vulnerability is a fundamental concept for the knowledge economy and associated with risks this should be understood as a new challenge for our future research.

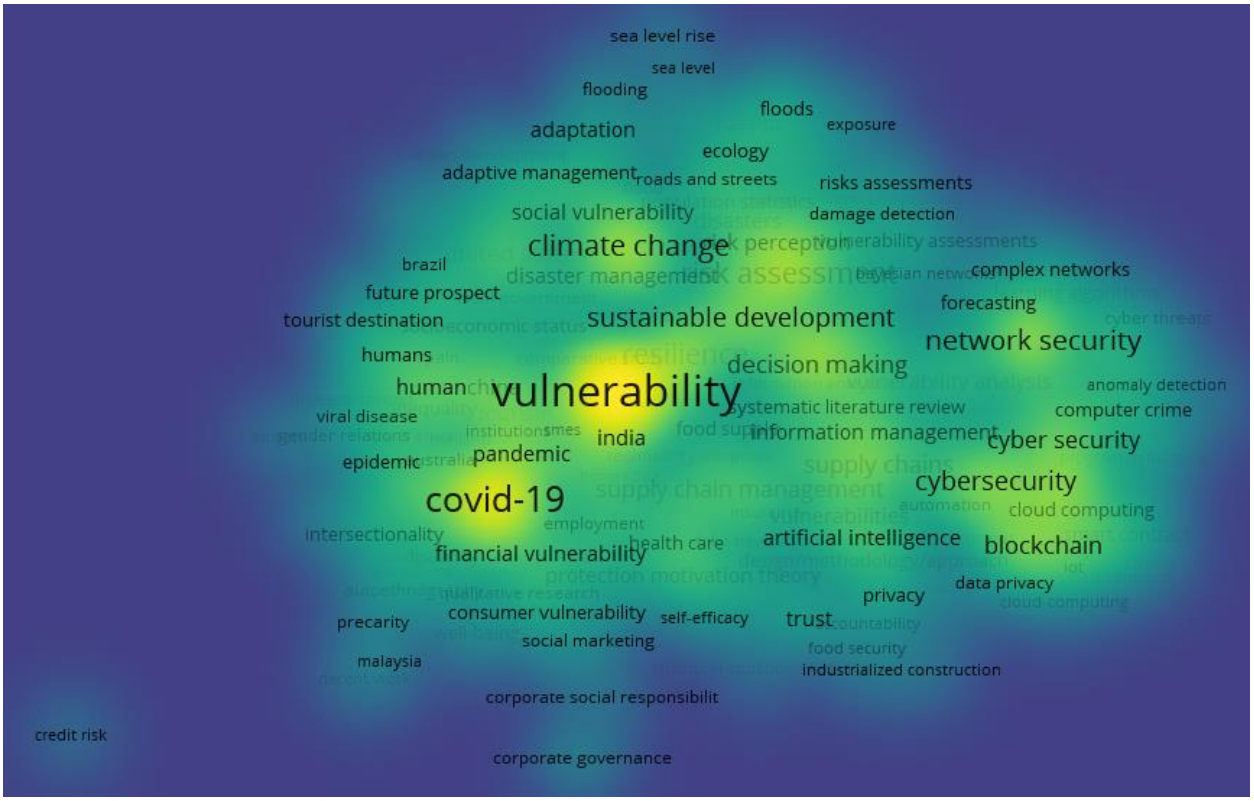

Figure 3. Network density visualization by VOSviewer software version 1.6.18

Source: Authors' own research.

In Figure 3, we can observe the representation of the density overview of the clusters, broadcasting the most visited concepts in the literature, correlated with the vulnerability concept. According to Van Eck and Waltman (2010), each term has an associated sphere with a specific dimension and density of color. In Figure 3, 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, "vulnerability", "COVID-19", "sustainable development", "climate change", "network security", and "cybersecurity" 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 the fact that on the one hand, "vulnerability" concept appears to be in closer relationship with "COVID-19", and on the other, "network security" is in a close relationship with "cybersecurity". 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 vulnerability and risks is more than obvious.

Conclusions and limits of the study

The purpose of this study was to analyze the knowledge vulnerabilities, focusing our research on identifying some vulnerabilities in the organizational knowledge dynamics with some impacts in the knowledge economy. Through our research we register notable progress, particularly in the knowledge vulnerabilities area where some knowledge vulnerabilities were identified, which has not been done so far in previous research and more than that in our research we conceived and proposed a new method for further research, named Knowledge Vulnerabilities Scoring System (KVSS).

The process will be beneficial for a correct analysis of knowledge vulnerabilities and the impact in the knowledge economy, completing the research with some solutions that may reduce negative consequences for organizations that are an active component in the knowledge economy. This was achieved by initially implementing a comprehensive literature review, followed by a text mining analysis with VOSviewer software. While we successfully identified a set of research interests in knowledge management associated with the knowledge risk concept, we have also found that bureaucratic system holds specific knowledge gaps, and research area in this field would require increased scientific attention, especially in the bureaucratic system analyzed as a risk generator for knowledge domain.

Not being a subject deeply analyzed, knowledge vulnerabilities has a high importance for the knowledge domain. Even if we didn't find specific research on the knowledge vulnerabilities in the knowledge economy, from the current research we identified that indeed there are gaps in the literature and researches are more than needed to fulfill this need. Research on this area will reveal much more conclusive results that will become a real support for further identification of vulnerabilities, comprehend in more details KVSS in a further research paper, finally identifying solutions to treat knowledge vulnerabilities.

In today knowledge economy were knowledge has become essential for every organization and 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, identifying knowledge vulnerabilities will increase visibility on organizational knowledge given the opportunity to threat weakness point identified and in the end to achieve the goal to strengthen the organization. The knowledge economy has evolved more that was predicted in a short time period, adding notable value to the knowledge economy. On other side, this fast evolution in the knowledge economy revealed that some components were not fully covered, leaving some gaps that may be exploited. Our research identify some of gaps in the knowledge economy especially on knowledge vulnerabilities. Considering the unwitnessed access to information and advancements in conducting academic research, in the present landscape of the knowledge economy, knowledge vulnerabilities will have an increasingly role, and new methods will be available to assess and prioritize the knowledge vulnerabilities.

References

Adger, W. (2006). Vulnerability. *Global Environmental Change*. 16. 268-281. 10.1016/j.gloenvcha.2006.02.006.

Aubert, B. & Patry, M. & Rivard, S. (2001). Managing IT Outsourcing Risk: Lessons Learned. 10.1007/978-3-662-04754-5_7.

Bayer, F., & Maier, R. (2006). Knowledge risks in inter-organizational knowledge transfer. Proceedings of I-KNOW '06 Graz, Austria, 200-208.

Blaikie, P. & Cannon & Davis, L. & Wisner, B. (1994). *At Risk: Natural Hazards*, *People's Vulnerability and Disasters*, Routledge, London.

Bolisani, E. & Bratianu, C. (2017). Knowledge strategy planning: an integrated approach to manage uncertainty, turbulence, and dynamics. *Journal of Knowledge Management*. 21. 233253. 10.1108/JKM-02-2016-0071.

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

Bratianu, C. (2015). *Organizational Knowledge Dynamics: Managing Knowledge Creation, Acquisition, Sharing, and Transformation.* IGI Global. 10.4018/978-1-4666-8318-1.

Bratianu, C. (2016). Knowledge Dynamics. *Management Dynamics in the Knowledge Economy*. 4. 323-337.

Bratianu, C. (2018). A holistic approach to knowledge risk. *Management Dynamics in the Knowledge Economy*, 6 (4), 593-607.

Bratianu, C. & Bejinaru, R. (2022). Exploring vulnerabilities and risks related to knowledge management systems.

Bratianu, C. & Nestian, A.S. & Tita, S.M. & Voda, A.I. & Guta, A.L. (2020). The Impact of Knowledge Risk on Sustainability Firms. *Amfiteatru Economic*, 22(55), pp. 639-652. DOI: 10.24818/EA/2020/55/639

Bogard, W. (1989). Bringing social theory to hazards research conditions and consequences of the mitigation of environmental hazards. *Sociological Perspective*, 31, 147-168.

Cader, H. (2008). The Evolution of the Knowledge Economy. Journal of Regional Analysis and Policy. 38.

Cegarra-Navarro, J.G., Bratianu, C., Martinez-Martinez, A., Vatamanescu, E.M. & Dabija, D.C. (2023). Creating civic and public engagement by a proper balance between emotional, rational, and spiritual knowledge. *Journal of Knowledge Management*. 10.1108/JKM-07-2022-0532.

Chambers, R. (1989). Editorial Introduction: Vulnerability, Coping and Policy. *IDS Bulletin* 20(2).

Cutter, S. (1996). Vulnerability to environmental hazards. *Progress in Human Geography* 20(4): 529-539

Dow, K. (1992). *Exploring differences in our common future(s): the meaning of vulnerability to global environmental change*. Geoforum 23, 417-436.

Durst, S. & Henschel, T. (2020). *Knowledge Risk Management From Theory to Praxis: From Theory to Praxis*. 10.1007/978-3-030-35121-2.

Durst, S. & Zieba, M. (2017). Knowledge risks - Towards a taxonomy. *International Journal of Business Environment*. 9. 51. 10.1504/IJBE.2017.084705.

Durst, S. & Wilhelm, S. (2013). Do you know your knowledge at risk?. *Measuring Business Excellence.* Vol. 17 No. 3. pp. 28-39. https://doi.org/10.1108/MBE-08-2012-0042

Friedman, M. (1953). The Methodology of Positive Economics. The Philosophy of Economics: An Anthology. 10.1017/CBO9780511819025.010.

Friedman, M. (1963). A monetary history of the United States, 1867-1960. Princeton University Press,

Gabor, T., & Griffitch, T. (1980). The Assessment of Community Vulnerability to Acute Hazardous Materials Incident. DOI:10.101/0304-3894(80)80004-5

Iliescu, A. (2021). The Emergence of Knowmads from the Knowledge Workers. *Management Dynamics in the Knowledge Economy*. 9. 94-106. 10.2478/mdke-2021-0007.

Intergovernmental Panel on Climate Change (PCC). (1996). Climate Change 1995: *Impacts, Adaptations and Mitigation of Climate Change: Summary for Policy Makers*. World Meteorological Organisation, Geneva.

Jamieson, R., & Loeng, D. (2003). *An exploratory study of risks and issues in knowledge management.* 14th Australasian Conference on Information Systems, Perth, Western Australia.

Kasperson, R.E. & Kasperson, J.X. & Dow, K. (2001). *Global environmental risk and society*. Global Environmental Risk, Tokyo. 1-48.

Kasperson, R.E. & Kasperson, J.X. & Dow, K. (2001). *Vulnerability, equity, and global environmental change, In: Global Environmental Risk*. United Nations University Press and Eartscan: 247-272.

Keynes, J. M. (2017). *The general theory of employment, interest and money*. Wordsworth Editions.

Lambe, P. (2013). *Four types of knowledge risk*, 1-3 [online]. Retrieved from www.greenchameleon.com/uploads/Four_Types_of_Knowledge_Risk.pdf.

Marshall, A. (1920). Principles of Economics. 8th Edition, Macmillan, London.

Massingham, P. (2010). Knowledge risk management: a framework. *Journal of Knowledge Management,* VOL. 14 NO. 3 2010, pp. 464-485, Q Emerald Group Publishing Limited, ISSN 1367-3270 DOI 10.1108/13673271011050166

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

Nonaka, I. & Takeuchi, H. (2019). *The wise company. How companies create Continuous innovation*. Oxford: Oxford University Press. Organization for Economic Co-operation and Development (OECD) (2006). *Creating value from intellectual assets*. Retrieved from http://www.oecd.org/science/inno/36701575.pdf.

Perrot, B. E. (2007). A strategic risk approach to knowledge management. *Business Horizons*, 50, 523-533.

Schumpeter, J.A. (1934), *The Theory of Economic Development*, Harvard University Press, Cambridge, MA (Oxford University Press, New York, NY, 1961) (first published in German, 1912).

Smith, Adam. (2012). *Wealth of Nations*. Wordsworth Classics of World Literature. Ware, England: Wordsworth Editions.

Timmerman, P. (1981). *Vulnerability, Resilience, and the Collapse of Society*. Environmental Monograph No. 1. Institute of Environmental Studies.

Turner II, B.L. & Kasperson, R. & Matson, P. & Mccarthy, J. & Corell, R. & Christensen, L. & Selin, N. & Kasperson, J. & Luers, A. & Martello, M. & Polsky, C. & Pulsipher, A. & Schiller, A. (2003). *A framework for vulnerability analysis in sustainability science*. Proceedings of the National Academy of Sciences of the United States of America. 100. 8074-9. 10.1073/pnas.1231335100.

United Nations Disaster Relief Organization (UNDRO). (1982). *Natural disasters and vulnerability analysis*. Geneva: Office of the United Nations Disaster Relief Co-ordinator.

Ursache, V.M. (2022a). *Cybersecurity challenges in the knowledge economy*. Proceedings of the International Conference on Business Excellence. 16. 121-129. 10.2478/picbe-2022-0012.