Vulnerabilities and Risks Within the Hybrid Knowledge Management Systems that Integrate Human and Artificial Knowledge

Constantin Bratianu
Bucharest University of Economic Studies, Romania

constantin.bratianu@gmail.com

Abstract: The advent of generative artificial intelligence (GenAI) changes the human Knowledge Management Systems (KMS) into Hybrid Knowledge Management Systems (HKMS), composed of humans and computers. The purpose of this paper is to analyse the dynamics of knowledge vulnerabilities and knowledge risks within the HKMS that integrate both human knowledge and artificial knowledge. Knowledge vulnerabilities are the weak elements of a knowledge management system, which are the roots of the knowledge risks. Knowledge vulnerabilities represent a potential, while knowledge risks constitute the probable events with negative consequences for the whole organization. The importance of considering the dynamics between knowledge vulnerabilities and knowledge risks comes from the fact that reducing the number of knowledge vulnerabilities allows managers to reduce the associated knowledge risks and their negative consequences. Generative Artificial Intelligence (GenAI) impacts Knowledge Management (KM) through its generation of artificial knowledge. Using GenAI introduces new knowledge vulnerabilities and knowledge risks that should be known by employees. Our analysis is based on a critical literature evaluation, on the theory of risk management, and on GenAI impact on KM. We introduce in our study tree diagrams to show the dynamic correlations between knowledge vulnerabilities and knowledge risks. The originality of the present research comes from using these tree diagrams and their power to help managers in their decision-making. They offer a better understanding of relationships between knowledge vulnerabilities, knowledge risks, and their probable consequences than a simple classification of these vulnerabilities and risks.

Keywords: Human knowledge, Artificial knowledge, Generative artificial intelligence, Knowledge management systems, Knowledge risks, Knowledge vulnerabilities

1. Introduction

Researchers in Knowledge Management Systems (KMS) have focused so far on *knowledge risks* and their probable consequences on knowledge dynamics in knowledge-intensive organizations (Durst, 2019; Durst & Henshel, 2020; Durst & Zieba, 2019; Durst & Zieba, 2020; Zieba & Durst, 2018). Even so, knowledge risks were defined only for the rational knowledge, although knowledge represents an integration of rational, emotional, and spiritual knowledge fields (Bratianu, 2018; Bratianu & Bejinaru, 2019, 2020). The concept of *knowledge vulnerability* was introduced in the literature relatively recently by Bratianu et al. (2024), and its correlation with knowledge risk is still a research topic. Both of these concepts should be enlarged now to include *artificial knowledge*, a concept that requires more and more attention due to the explosive use of Generative Artificial Intelligence (GenAI) applications (Alavi, Leidner & Mousavi, 2024; Bratianu, 2025; Brusco Pletsch et al., 2026; Sumbal et al., 2024). GenAI changes the human KMS (Alavi & Leidner, 2001; Nonaka & Takeuchi, 1995, 2019) into hybrid human knowledge-artificial knowledge systems. While KMS focus on capturing, transferring, storing, and effectively using knowledge, "GenAI impacts each of these processes, as it can generate novel insights, distribute codified knowledge efficiently, and assist in decision-making and problem-solving" (Alavi, Leidner & Mousavi, 2024, p. 4). In the classical knowledge pyramid, data represents basic facts, information is data with meaning, and knowledge is processed information that reflects human experience and judgment (Alavi & Leidner, 2001; Bratianu & Bejinaru, 2023; Nonaka & Takeuchi, 1995, 2019).

The concept of *vulnerability* is well known in complex research domains such as climate change and natural hazards analysis (Fuchs et al., 2012; McCarthy et al., 2001). It represents a weak part of a system that may generate problems in certain conditions. Vulnerabilities may be considered potential internal threats. In the climate change domain, the concept of vulnerability is defined as "the degree to which a system is susceptible to, or unable to cope with, effects of climate change, including climate variability and extremes" (McCarthy et al., 2001, p. 995). The concept can be transferred to the domain of KMS, where it uncovers the weak elements of the HKMS that can generate knowledge risks under certain conditions (Bratianu et al., 2024). For instance, if a computer is used without protection against viruses, it is vulnerable to any situation in which some viruses can enter the computer software and destroy parts of it. Identifying knowledge vulnerabilities within a HKMS helps knowledge managers to lower the level of knowledge risks and reduce the possible adverse consequences. Also, if data used for training ChatGPT contains errors (i.e., knowledge vulnerabilities), the artificial knowledge presents new risks for decision-making (Alavi, Leidner & Mousavi, 2024; Baker, 2023, 2025; Russell & Norvig, 2023).

Knowledge risk can be defined as "the measure of the probability and severity of adverse effects of any activities engaging or related somehow to the knowledge that can affect the functioning of an organization on any level" (Zieba & Durst, 2018, p. 256). Knowledge vulnerabilities can be considered as the roots of knowledge risks, and knowledge risks as triggers of some events with adverse consequences for organizations. Knowledge risks manifest only in conditions of uncertainty. For an ideal situation of certainty, there are no knowledge risks. The most frequently encountered knowledge risks are the following: knowledge loss, knowledge leakage, knowledge spillover, knowledge outsourcing, knowledge gaps, and obsolete knowledge (DeLong, 2004; Durst & Zieba, 2020; Zieba & Durst, 2018). Due to the scarcity of papers on knowledge vulnerabilities and their correlations with knowledge risk (Bratianu, Bejinaru & Ursache, 2014), as well as considering the potential risks of using artificial knowledge (Baker, 2023, 2025), we formulate the following research question for the present research:

RQ: What are the correlations between knowledge vulnerabilities and knowledge risks in the hybrid knowledge management systems, and how can we analyze them using the tree diagrams?

We try to answer this question by performing a critical literature review and by using the tree diagrams for identifying possible correlations between the main constructs. The paper has the following structure: after this Introduction, we present the Literature review, Methodology, Results and discussions, Conclusions and References.

2. Literature Review

Most of the papers published in this domain of *knowledge risk* considered only rational knowledge (Durst, 2019; Durst & Henshel, 2020; Durst & Zieba, 2020). However, the concept of *knowledge* integrates three fields: the rational, emotional, and spiritual knowledge fields (Bratianu & Bejinaru, 2019, 2020). Therefore, the concept of knowledge risk should contain rational, emotional, and spiritual components that influence managerial decision (Baron, 2000; Blake, 2008; Kahneman, 2011). For instance, the risk generated by the fear of being fired is mostly an emotional risk, and the risk of being punished for breaking a behavior code is mostly a spiritual one. Therefore, we should have a holistic approach to knowledge risks. "Having an extended framework, knowledge risks appear in their complexity of influencing all the aspects of the managerial decision-making, from reflective to intuitive processes" (Bratianu, 2018, p. 602). The emergence of GenAI and of artificial knowledge induces new types of vulnerabilities and risks within the knowledge management systems (Alavi, Leidner & Mousavi, 2024; Baker, 2023, 2025; Russell & Norvig, 2023).

Knowledge loss is the most important and studied knowledge risk, due to the ageing problem in Europe and USA. Also, knowledge loss has an important impact on the competitive advantage of a company (DeLong, 2004; Durst & Zieba, 2020; Joe et al., 2013). Knowledge loss changes the knowledge balance of the company and decreases its knowledge entropy. It appears when there is a significant percentage of workers with a high level of experience who leave the company almost in the same time. A classic example can be the huge knowledge loss at NASA after a policy of downsizing its workforce. "In an era of cost-cutting and downsizing, the engineers who designed the huge Saturn 5 rocket used to launch the lunar landing craft were encouraged to take early retirement from the space program. With them went years of experience and expertise about the design trade-offs that had been made in building the Saturn rockets" (DeLong, 2004, p. 11). Knowledge loss can be reduced through strategies of knowledge retention and intergenerational learning (Bratianu et al., 2010).

Knowledge leakage is the risk of having critical knowledge escape through different mechanisms to competitors. That knowledge can be used against the owner company in the market competition (Mohamed et al., 2017). This risk is only for rational knowledge, but not for emotional and spiritual knowledge. Also, it is related to business intelligence where the focus is on extracting critical knowledge from a certain KMS. *Knowledge spillover* is a metaphor for the knowledge that spills over the boundary of a company towards other companies (Durst and Zieba, 2020).

Emotional risks are generated by fear of losing the job or even a certain position within the organization when there are managerial changes or external economic crises. Emotional risks are related to organizational climate and managerial style. For instance, changing the managerial style from democratic to autocratic or transformational will induce these kinds of risks (Bratianu & Anagnoste, 2011). In the case of implementing GenAI, emotional knowledge risk may be generated by the fear of losing the job, being replaced by AI (Kurtzweil, 2024). *Spiritual knowledge risks* are related to changes in a company's value system, resulting from mergers and acquisitions or simply a change in leadership. For instance, think about the change induced in the Apple company after Steve Jobs was forced to step down as the CEO. As Keeny remarks, "Values are what we care about. As such, values should be the driving force of our decision-making" (Keeny, 1992, p. 3). GenAI may induce such a risk in decision-making as a biased database or some possible hallucinations (Baker, 2023, 2025).

A key determinant of the knowledge risks is *uncertainty*, a state of incomplete knowledge about events and phenomena. Uncertainty is related mostly to the future. Thinking about the future of the company requires switching from deterministic thinking to probabilistic thinking. Events are not certain but probable (Massingham, 2020; Spender, 2014). Uncertainty is not an objective feature of a certain context. It is a subjective interpretation of the relationship between a person and his context at a given time. The level of uncertainty differs from person to person, within the same context. Lindley posits that "it is not *the* uncertainty but *your* uncertainty" (Lindley, 2006, p. 1). Therefore, there is a difference between the objective probability, that is a mathematical construct, and the subjective probability, that is a human perception of it. This dual meaning is transferred to the construct of risk, respectively, knowledge risk. The mathematical value can be computed by multiplying the probability of a certain event happening by the magnitude of the negative consequences of that event. The subjective value is given by the intensity of risk perception. Taleb (2007) showed that our human nature is risk-averse, and we have an inability to think of the highly improbable events. The same happens with thinking of vulnerabilities.

The emergence of GenAI opened the discussion of the nature and quality of the outputs of GenAI applications, like ChatGPT. These humanlike outputs constitute the result of a machine learning process powered by mathematical algorithms (Baker, 2023, 2025; Kurzweil, 2024; Russell & Norvig, 2023). Because we consider that human knowledge is a result of the human learning process, we may consider that the result of the machine learning process is *artificial knowledge* (Bratianu, 2025; Di Vaio et al., 2024; Harfouche et al., 2017). Artificial knowledge has its roots in human data, information, and knowledge, but as a result of an artificial process (Simon, 1996), it is different from human knowledge. Knowledge-intensive organizations that use GenAI applications transformed their human Knowledge Management Systems (KMS) into Hybrid Knowledge Management Systems (HKMS). The main role of these HKMS is to integrate human and artificial knowledge and to manage its distribution and dynamics throughout the organization. Within HKMS, managers should be able to identify knowledge vulnerabilities for both components, human and GenAI, and make correlations with possible knowledge risks and their negative consequences.

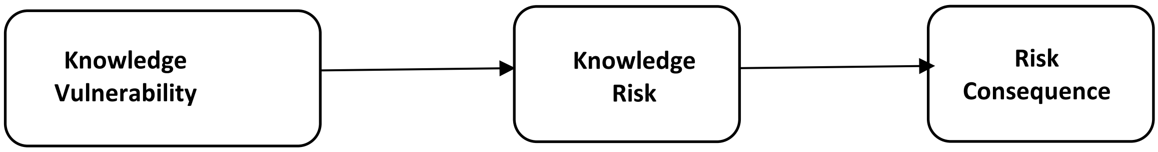
3. Methodology

The first stage of our research is a critical literature review and the identification of the knowledge gap. This stage is supported by the basic theories of knowledge fields and knowledge dynamics (Bratianu & Bejinaru, 2019, 2020), and the risk management theory (Krajewsky et al., 2007; Massingham, 2020). This is a conceptual paper. It analyzes the correlations between knowledge vulnerabilities and knowledge risks within HKMS, and uses tree diagrams to represent them. The method of tree diagrams is taken from risk management analysis and nuclear safety (Massingham, 2020; Krajewski, I.J., Ritzman, L.P., & Malhorta, M.K., 2007). They illustrate the links between knowledge vulnerabilities, knowledge risks, and their possible consequences. It is for the first time that such tree diagrams are used for studying these kinds of correlations. The tree diagrams can help managers to understand much better the complex correlations between knowledge vulnerabilities, knowledge risks, and possible negative consequences (Bratianu, Bejinaru & Ursache, 2024).

4. Results and Discussions

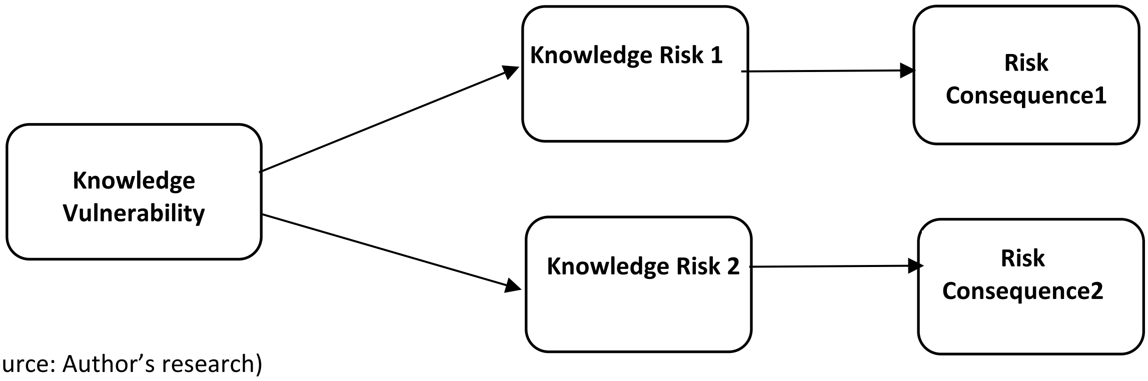
We will consider three basic concepts: knowledge vulnerabilities (KV), knowledge risks (KR), and risk consequences (RC). Knowledge vulnerabilities represent the roots of the causal chain, and risk consequences constitute its end. Knowledge vulnerabilities, knowledge risks and risk consequences are specific to each organization. Therefore, we cannot design diagrams valid for any organization, but we can show how these tree diagrams can be designed and used. The following are only qualitative examples, but they can be used to establish quantitative information for each organization. The links between the basic constructs can be measured based on statistical procedures to show their strength and chances to occur. The usefulness of these diagrams comes from the multiple connections they can show between knowledge vulnerabilities, knowledge risks and risk consequences. Understanding these connections, managers can find ways to decrease the number of knowledge vulnerabilities and of knowledge risks.

Figures 1-3 show three possible correlations between knowledge vulnerabilities (KV), knowledge risks (KR), and risk consequences (RQ). Figure 1 illustrates the simplest case when there is a chain of single events. Figure 2 illustrates the case when one KV can influence several probable KR, each of them with a specific RC. Figure 3 shows the case when several KV contribute to generate a KR that may have several RC.



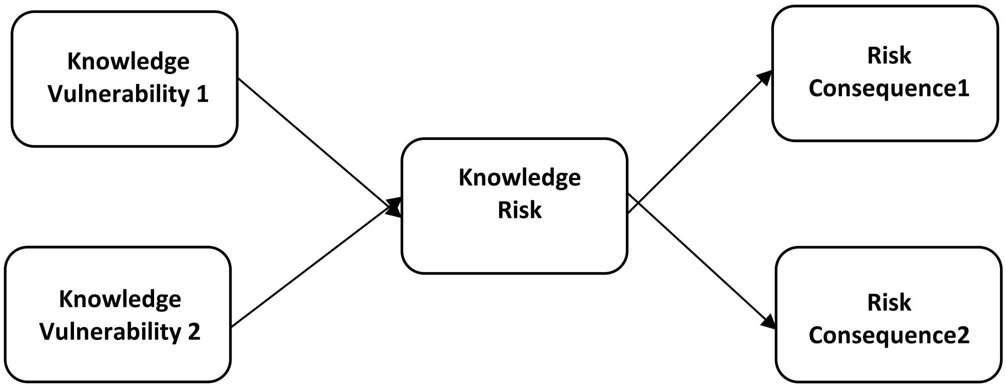
(Source: Author's research)

Figure 1: A simple causal chain



(Source: Author's research)

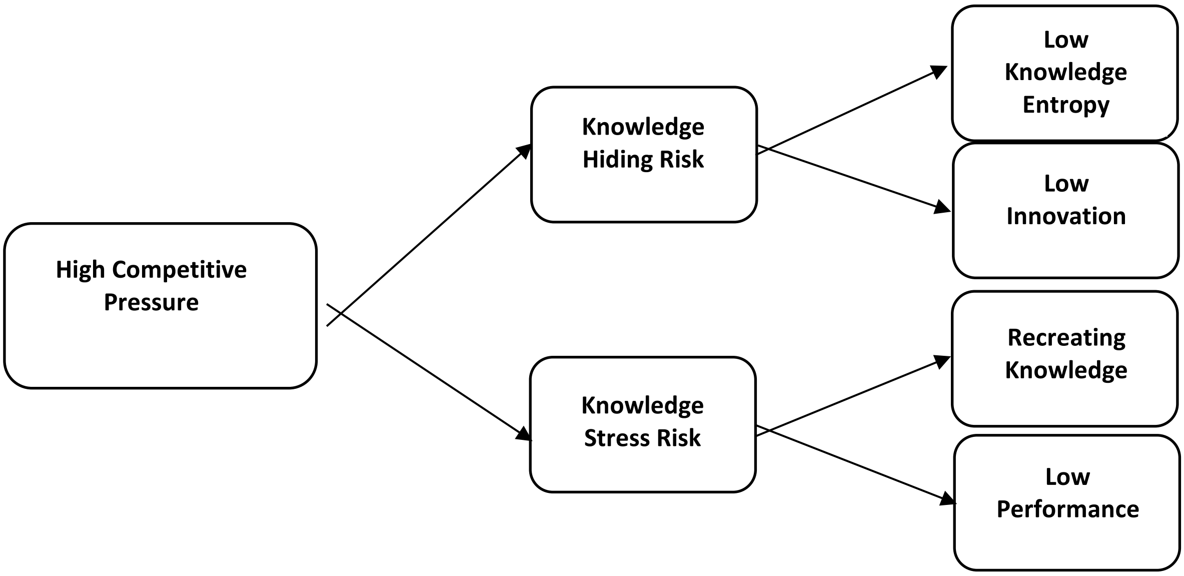
Figure 2: Multiple knowledge risks are generated by one knowledge vulnerability



(Source: Author's research)

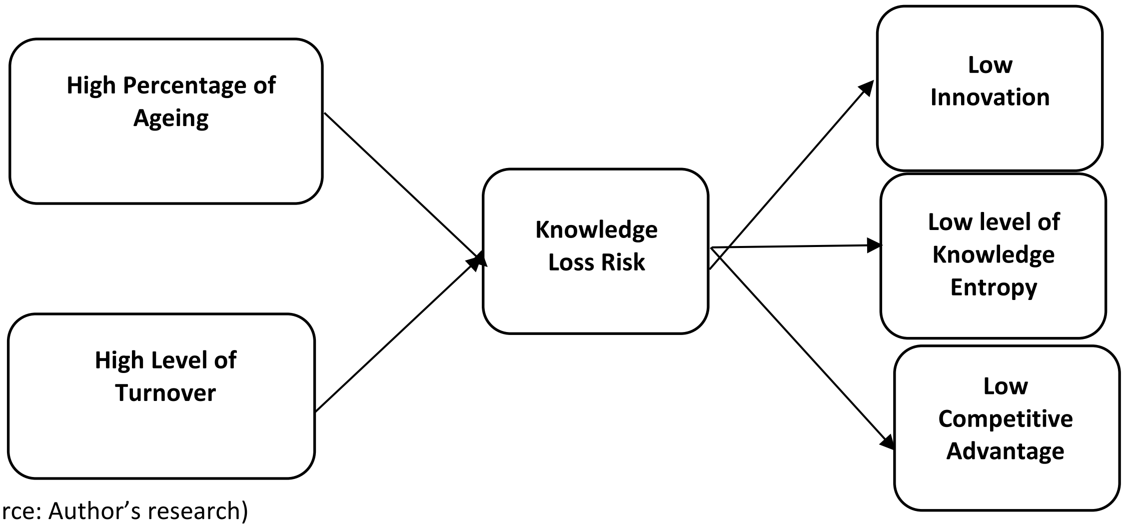
Figure 3: Multiple knowledge vulnerabilities generate one knowledge risk

In the next figures, we illustrate some concrete cases of correlations between knowledge vulnerabilities, knowledge risks, and risk consequences. Figure 4 shows the case of a company where there is a high level of competition among employees, as in some American companies. That high competition implies that knowledge becomes real power for each employee, and there is a tendency to hide it instead of sharing it. The high competition pressure is a knowledge vulnerability that generates two probable knowledge risks: hiding knowledge and knowledge stress. Knowledge hiding may have direct consequences: a low level of knowledge entropy and a low level of innovation. The knowledge stress risk will impact the knowledge recreation and the low performance of the company. Knowledge recreation is the phenomenon of searching and creating new knowledge by some employees, although that knowledge might exist within the organization, but it is not shared.



(Source: Author's research)

Figure 4: Tree diagram for the vulnerability chain of high competition pressure



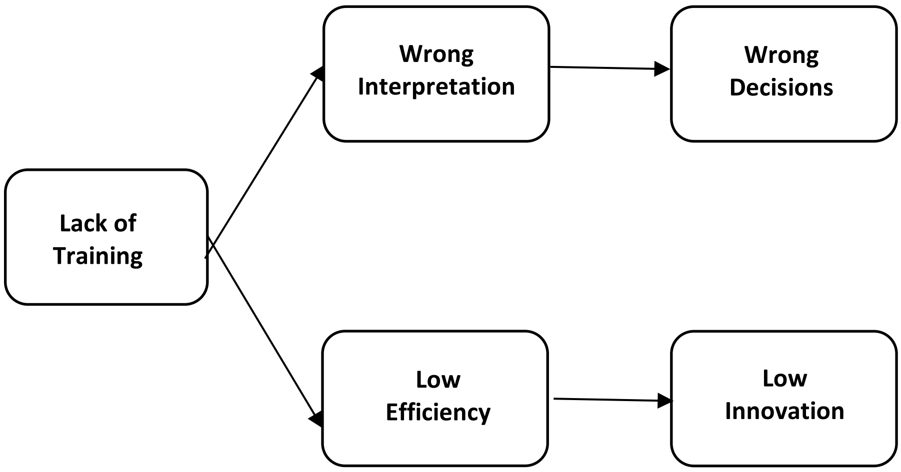
(Source: Author's research)

Figure 5: The chain of knowledge loss risk

The most important knowledge risk discussed in the literature is knowledge loss (DeLong, 2004; Durst & Zieba, 2020). We can identify two major knowledge vulnerabilities that generate knowledge loss risk: a high percentage of ageing employees and a high level of turnover as a result of toxic management that drives experts to leave for other companies. Knowledge loss will happen when a significant percentage of employees retire almost at the same time, taking with them a huge amount of knowledge (both explicit and tacit knowledge), and when there is a toxic management that ignores the real value of people and rewards incompetence. That creates frustrations among creative people and makes them leave for other companies. Here, the rational, emotional, and spiritual knowledge contribute together in generating the motivation to leave the company. As major consequences of such a knowledge loss, we may anticipate low levels of innovation, low levels of knowledge entropy, and low levels of competitive advantage. All of them contribute to the decrease in the company's performance.

The emergence of artificial knowledge transformed human knowledge management systems into hybrid knowledge management systems that integrate human and artificial knowledge. Hybrid knowledge management systems are more complex than human knowledge management systems, and they imply more knowledge vulnerabilities and knowledge risks. One of the major knowledge vulnerabilities in this case is a lack of training in using GenAI applications correctly and efficiently. Not understanding that artificial knowledge is different than human knowledge and that computers do not think can lead to misinterpreting the outputs of ChatGPT or similar applications and making wrong decisions. Also, a lack of adequate training leads to inefficient interactions between humans and machines, and that will not contribute to enhancing innovation. Figure 6 illustrates these issues. Lack of adequate training in using artificial knowledge may lead to difficulties in identifying ChatGPT hallucinations and misjudgment of possible solutions for solving a given problem. This is just an example. Managers may consider all kinds of knowledge vulnerabilities generated by GenAI applications (Alavi, Leidner & Mousavi, 2024).

Integrating human and artificial knowledge in solving different types of problems (i.e., in health systems, in educational systems, in managerial systems, etc.) requires a solid and coherent system of ethical values. If users do not have such a system and they are interested in creating shortcuts by using GenAI applications, then the final solutions may lead to harming people or damaging the environment. Hybrid knowledge management systems are much more complex than human knowledge management systems, and therefore, it is necessary to identify the knowledge vulnerabilities caused by the artificial knowledge and use tree diagrams to see the causality chains with knowledge risks and their probable negative consequences.



(Source: Author's research)

Figure 6: A tree illustration for using GenAI applications

5. Conclusions and Limitations

Researchers in knowledge management have focused their efforts so far on knowledge risks, especially on their ontologies. However, the roots of knowledge risks are knowledge vulnerabilities, which represent the weak elements of knowledge management systems. Any system optimization aiming at reducing knowledge risks should start with the identification of knowledge vulnerabilities. By reducing knowledge vulnerabilities, managers can reduce knowledge risks and their negative consequences. Reducing knowledge vulnerabilities leads to a decrease in the probability of producing knowledge risks. However, there are no clear methods for such an activity. It is more of an expert's investigation than a managerial procedure.

Tree diagrams used in risk management and nuclear reactor safety analysis can be used with good results in knowledge management systems. The present paper shows how to construct such tree diagrams for connecting knowledge vulnerabilities with knowledge risks and their negative consequences. Also, we present some examples for the case of human knowledge and that of artificial knowledge. These diagrams are not universal. They are specific for each organization, but their structure and many elements can be transferred from one company to another. Implementing tree diagrams in the design of hybrid knowledge management systems can lead to a significant reduction of the knowledge risks and their negative consequences. They integrate both human knowledge and artificial knowledge, vulnerabilities, and risks.

Although it is a new perspective on researching knowledge management systems, the present research has some limitations. The most important one is that it is a qualitative approach. However, researchers can go deeper and find out some quantitative correlations between the main constructs. That would help in designing the knowledge strategies of the company. Another limitation is that the paper presents only a few examples of how to construct tree diagrams and does not develop the analysis to show how to reduce in practice knowledge vulnerabilities, as well as knowledge risks. These stages could be future directions of research.

Ethics Declaration: Ethical clearance was not required for the present research.

AI Declaration: The authors have not used any of the AI tools for creating and writing this paper.

References

Alavi, M., & Leidner, D.E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, Vol. 25, Issue 1, pp. 107-136.

Alavi, M., Leidner, D., & Mousavi, R. (2024). A knowledge management perspective of Generative Artificial Intelligence (GenAI). *Journal of the Association for Information Systems*, Vol. 25, Issue 1, pp. 1-12. https://doi.org/10.17705/1jais.00859.

Baker, P. (2023). *ChatGPT for dummies*. John Wiley & Sons, Hoboken.

Baker, P. (2025). *Generative AI for dummies*. John Wiley & Sons.

Baron, J. (2000). *Thinking and judgment*. 3rd Edition. Cambridge University Press, Cambridge.

Blake, C. (2008). *The art of decisions: How to manage an uncertain world*. Prentice Hall, London.

Bratianu, C. (2018). A holistic approach to knowledge risk. *Management Dynamics in the Knowledge Economy*, 6(4), 593-607. https://doi.org/10.25019/MDKE/6.4.06.

Bratianu, C. (2025). Artificial knowledge and its challenges for the knowledge management systems. *Business Excellence and Management*, Vol. 15, Special Issue 5, 257-268. https://doi.org/10.24818/beman/2025.S.I.5-20.

Bratianu, C., Agapie, A., Orzea, I., & Agoston, S. (2010). Intergenerational learning dynamics in universities. *Proceedings of the 11th European Conference on Knowledge Management*, 146-155.

Bratianu, C., & Anagnoste, S. (2011). The role of transformational leadership in emergent economies. *Management & Marketing. Challenges for the Knowledge Society*, 6(2), 319-326.

Bratianu, C., & Bejinaru, R. (2019). The theory of knowledge fields: A thermodynamic approaches. Systems, 7(2), 1-12. https://doi.org/10.3390/systems7020020.

Bratianu, C., & Bejinaru, R. (2020). Knowledge dynamics: A thermodynamics approach. Kybernetes, 49(1), 6-21. https://doi.org/10.1108/K-02-2019-0122.

Bratianu, C., & Bejinaru, R. (2023). From knowledge to wisdom: Looking beyond the knowledge hierarchy. *Knowledge*, Vol. 3, pp. 196-214. https://doi.org/10.3390/knowledge3020014.

Bratianu, C., Bejinaru, R., & Ursache, V. (2024). The impact of knowledge vulnerabilities on knowledge risks. *Review of International Comparative Management*, 25(1), 70-79. https://doi.org/10.24818/RMCI.2024.1.70.

Brusco Pletsch, A.L., Tonial, G., Matos, F., & Koch, L.L. (2026). Digital transformation: The role of generative AI in the evolution of knowledge management systems. *Journal of Knowledge Management*, Early Cite, pp. 1-27. https://doi.org/10.1108/JKM-09-2025-1398.

DeLong, D.W. (2004). *Lost knowledge: Confronting the threat of an ageing workforce*. Oxford University Press, Oxford.

Di Vaio, A., Latif, B., Gunarathne, N., Gupta, M., & D' Adamo, I. (2024). Digitalization and artificial knowledge for accountability in SCM: A systematic literature review. *Journal of Enterprise Information Management*, 37(2), 606-672. https://doi.org/10.1108/JEIM-08-2022-0275.

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. https://doi.org/10.1108/VJIKMS-10-2018-0087.

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

Durst, S., & Zieba, M. (2019). Mapping knowledge risks: Toward a better understanding of knowledge management. *Knowledge Management Research and Practice,* 17(1), 1-13. https://doi.org/ 14778238.2018.1538603.

Durst, S., & Zieba, M. (2020). Knowledge risks inherent in business sustainability. *Journal of Cleaner Production*. 251, Art. 119670, 1-10. https://doi.org/10.1016/j.jclepro.2019.119670.

Fuchs, S., Birkman, J., & Glade, T. (2012). Vulnerability assessment in natural hazards and risk analysis: Current approaches and future challenges. *Natural Hazards*, 64, 1969-1975. https://doi.org/10.1007/s11069-012-0352-9.

Harfouche, A., Quinto, B., Skandrani, S.R.., & Marciniak, R. (2017). A framework for artificial knowledge creation in organizations. *ICIS 2017*, Seoul, South Korea.

Joe, C., Yoong, P., & Petel, K. (2013). Knowledge loss when older experts leave knowledge-intensive organizations. *Journal of Knowledge Management*, 17(6), 913-927. https://doi.org/10.1108/JKM-04-2013-0137.

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux, New York.

Keeney, R.L. (1992). *Value-focused thinking: A path to creative decision making*. Cambridge University Press, Cambridge.

Krajewski, I.J., Ritzman, L.P., & Malhorta, M.K. (2007). *Operations management: Processes and value chains*. 8th Edition. Pearson, Upper Saddle River.

Kurzweil, R. (2024). *The singularity is near: When we merge with AI.* The Bodley Head, London.

Lindley, D.V. (2006). *Understanding uncertainty*. John Wiley & Sons, New York.

Massingham, P. (2020). *Knowledge management: Theory and practice*. SAGE, Los Angeles.

McCarthy, J.J., Cauziami, D.F., Leary, N.A., Dokken, D.J., & White, K.S. (Eds.). *Climate change 2001: Impacts, adaptation and vulnerability*. Cambridge University Press, Cambridge.

Mohamed, S., Mynors, D., Andrew, G., Chan, P., Coles, R., & Walsh, K. (2017). Unearthing key drivers of knowledge leakage. *International Journal of Knowledge Management Studies*, 1(3-4), 456-470.

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

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

Russell, S., & Norvig, P. (2023). *Artificial intelligence: A modern approach*. Fourth edition. Pearson, Upper Saddle River.

Simon, H. (1996). *The sciences of the artificial*. Third Edition. The MIT Press, Boston.

Spender, J.C. (2014). *Business strategy: Managing uncertainty, opportunity, and enterprises*. Oxford University Press, Oxford.

Sumbal, M.S., Amber, Q., Tariq, A., Raziq, M.M., & Tsui, E. (2024). Wind of change: How ChatGPT and big data can reshape the knowledge management paradigm? *Industrial Management & Data Systems*, Vol. 124, Issue 9, pp. 2736-2757. https://doi.org/10.1108/imds-06-2023-0360.

Taleb, N.N. (2007). *The black swan: The highly improbable*. Penguin Books, London.

Zieba, M., & Durst, S. (2018). Knowledge risks in the sharing economy. In Vatamanescu, E.M., & Pinzaru, F. (Eds.). *Knowledge management sharing in the sharing economy* (pp. 253-270). Springer International Publishing, Cham.