Business Continuity Management of Critical Infrastructures from the Cybersecurity Perspective

Timo Savolainen[1] *Nora McCarthy* [2], Karen Neville [3], and Harri Ruoslahti[4]

[1] University of Applied Sciences, 02650 Espoo, Finland
[2] University College Cork, Cork T12 K8AF, Ireland
[3] University College Cork, Cork T12 AK54, Ireland
[4] University of Applied Sciences, 01300 Vantaa, Finland

Abstract. In today's society, nearly all processes are connected to IT systems, which means that there is a universal need to investigate how organizations in the CI network can improve their resilience from a cybersecurity perspective. This study, done as an overview type of literature review looks at different approaches to business continuity management (BCM), and addresses challenges to the resilience of critical infrastructures by looking at business continuity management, concentrating on cybersecurity and artificial intelligence (AI) from a human factor perspective. BCM systems can be very complex and time-consuming and approaches to BCM differ. These BCM systems have in common that they all try to identify threats and, based on these, offer solutions that ensure the continued operation of critical processes of the organization in terms of maintaining business continuity and resilience. While artificial intelligence (AI) can be used to make the process more efficient, the importance of addressing human factors is critical to BCM. Through the addition of a 'learn and adapt' phase in the proposed BCM framework, the importance of training and education in human factors as part of BCM in cybersecurity is acknowledged. This paper proposes a new practical BCM resilience framework that adds in a core phase of 'learn and adapt', currently lacking from existing models, thus recognizing the importance of training and education in human factors.

Keywords: AI, Cyber security, BCM, Risk Management, Human Factors.

1 Introduction

Societies depend on a network of physical and cyber assets called "critical infrastructures" (CI). These include financial services, energy, transportation, transit services, information and communication, water supply, military, police, health and medical services, public administration, and government. (Giacomello & Pescaroli, 2019). Because nearly all processes in today's society are connected to IT systems, there is a universal need to investigate how organizations in the CI network can improve their resilience from a cybersecurity perspective. Cybersecurity education can draw from the principles of business continuity management (BCM) to build methods and capabilities that promote situational awareness and critical risk assessment.

Business continuity management (BCM) is a complex multidisciplinary topic, which involves different perspectives, such as business, risk management, security, technology, and psychology. More holistic approaches are needed to successfully combine BCM and cybersecurity management, with an imperative in this to address the impact of human factors. Human factors are considered the weakest link in mitigating relevant cybersecurity risks (Reason, 1990; Chapanis, 1965; Aaltola, Ruoslahti & Heinonen, 2022; Ruoslahti, & Tikanmäki, 2022; Nifakos et al.,2021; Vieane et al., 2016). People are responsible for using and maintaining machines and computer programs, and people are integral to making designs and developing them. In other words, human factors play a crucial role in BCM. This study, through a qualitative rapid review and synthesis, proposes a new practical framework for BCM that integrates human factors into BCM. Cybersecurity is the example through which BCM and human factors are explored. This approach can improve cybersecurity education of BCM-based methods that can help build capabilities to promote situational awareness and critical risk assessment.

Following this introduction, the paper describes its literature review process. It then explores the role of human factors in cybersecurity, together with a discussion on the opportunities and challenges that artificial intelligence (AI) in cybersecurity has created. This is followed by a discussion on BCM, with various examples highlighted. The discussion then introduces a new BCM framework, which aims to facilitate critical information infrastructure protection (CIIP) networks while managing human-related cybersecurity risks.

2 Methods

The execution of this study's literature review can be described as a non-systematic overview. According to Grant and Booth (2009), the aim of a non-systematic overview is to describe the characteristics of the phenomenon that is investigated. Researchers followed Snyder's (2019) literature review phases as follows: 1) making the design, 2) conducting the search, 3) analyzing the documents, and 4) structuring and writing the review. More precisely researchers first identified keywords, searched material from digital databases, chose the documents, made draft summaries, and wrote a literature review to organize important concepts.

In other words, after choosing the non-systematic overview approach researchers started searching literature by using databases such as Google Scholar, and EBSCO by employing search words: AI, Cybersecurity, BCM, and Risk Management. The most suitable sources included articles, conference papers, standards, books, and doctoral dissertations. These were first investigated by reading their titles and abstracts. Based on this initial screening, a subsequent exploration of those articles deemed suited to describing the topic and for future development of the new BCM framework occurred. Finally, the researchers wrote draft summaries, organized the important concepts, and developed a new BCM framework based on the summarized concepts of Human Factors, BCM, Risk Management, AI and Cybersecurity.

3 Business Continuity Management

According to Herbane (2010), "Business continuity management (BCM) has evolved since the 1970s in response to the technical and operational risks that threaten an organization's recovery from hazards and interruptions. However, as already mentioned, BCM is a complex multidisciplinary topic, which involves different perspectives, such as business, risk management, security, technology, and psychology. According to ISO (22301:2019), business continuity means the *"capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption*." The key here is that what is acceptable for one organization might be different for others, depending on the risk appetite of the management. Every scholar (e.g., Lindstedt, 2017; Graham & Kaye, 2015; Linkov et al., 2014) usually has a slightly different approach to BCM. Some pay more attention to risk management and risk assessment whereas others pay more attention to Business Impact Analysis (BIA). The common factor of all BCM approaches is the goal of improving organizational resilience. The traditional approach to BCM has six phases: 1) Produce a business impact analysis (BIA), 2) Set Recovery time targets, 3) Conduct a risk assessment (RA), 4) Obtain explicit executive support, 5) Test the process, 6) Deliver training and awareness. with the importance of human factors, while being implicit in the phases, not being explicitly highlighted as an integral feature. The alternative approach called the Adaptive Business Continuity approach is based on a rapid and continuous improvement of recovery capabilities that provide value to the organization. The approach is non-linear and perceives BIA as complicated and time-consuming (Lindsted, 2017).

BIA is a *"process of analysing the impact over time of a disruption on the organization "*(ISO 22301:2019). Setting recovery time targets includes e.g., maximum tolerable downtimes (MTD), Recovery point objectives (RPO), Recovery time capabilities (RTC), and other time-centric considerations for critical processes (Lindsted, 2017). RA is an essential part of the Risk Management (RM) process. In the RM process, the organization first chooses the scope (e.g., cybersecurity) and then starts to assess risks. According to ISO (31000:2018), the first step of RA is risk identification. The second is risk analysis where the organization estimates the likelihood of unwanted events. The third step of RA is risk evaluation. In that phase, the organization evaluates the consequences of identified risks. The final phase in the RM process is risk treatment. In the risk treatment phase, organizations can remove the risk, change the likelihood (such as training personnel to avoid human errors using IT systems), and/or change the consequences by sharing the risk e.g., through cooperation with partners or retaining and mitigating the risk through an informed decision-making process. (ISO 31000:2018.)

Several organizations, such as ISO (International Organization for Standardization), BCI (Business Continuity Institute), DRII (Disaster Recovery Institute International), and FFIEC (Federal Financial Institutions Examination Council) have also published different guidelines for BCM (Herbane 2010). ISO's standards relating to BCM include e.g., ISO 22301 "Societal security - Business continuity management systems - Requirements", ISO 22313 "Societal security - Business continuity management systems - Guidance", and ISO 27031:2011 "Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity". ISO 22313:2020 and Linkov et al.'s (2014) models toward BCM were chosen for closer investigation due to their holistic and systematical approach towards BCM. It can be argued that if one does not have a clear target e.g., MTD, it is hard to see what the resilience of critical function is. The essence of these two approaches will be described in the following two subsections.

3.1 ISO 22323:2020 Security and Resilience. Business continuity management systems. Guidance on the use of ISO 22301

ISO 22313 (2020) follows Edwards Deming's (2018) commonly known Quality Management Plan-Do-Check-Act cycle. It is used for planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and continually improving the effectiveness of an organization's BCM approach (See: Figure 1) (ISO 22313:2020).

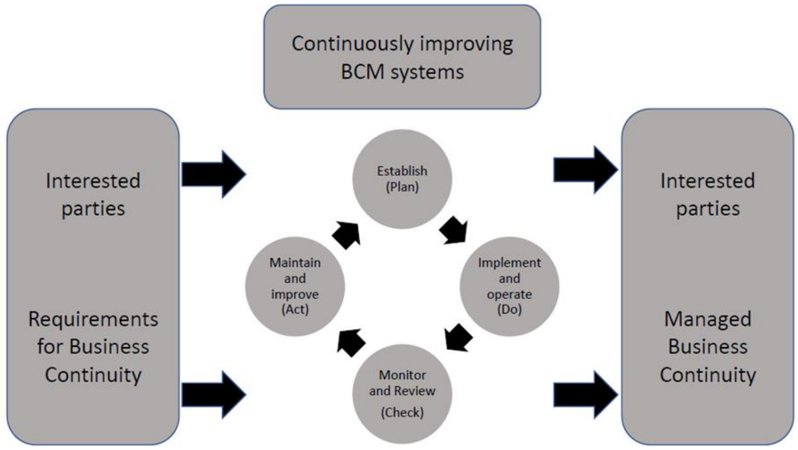

Fig. 1. Modified PDCA cycle in BCM processes Source: (ISO 22313:2020)

According to Deming's terms the first Plan- phase includes establishing a business continuity policy, objectives, controls, processes, and procedures that are relevant to improving business continuity. The aim of the first phase is to ensure that all activities are aligned with the organization's overall policies and objectives. The second Do-phase contains the implementation of the business continuity policy, controls, processes, and procedures. The third Check- phase includes monitoring and reviewing that the performance is in-line with business continuity policy and objectives. In this phase, reporting of results to management for review purposes is made. In addition, during this phase management determines and authorizes actions for possible improvements. The final Act-phase includes maintaining and improving the BCM by taking corrective actions, based on the results of the management review and possible changes in the scope of the BCMS and business continuity policy and objectives. (ISO 22313:2020.)

3.2 Linkov's approach to BCM

According to Linkov et al. (2014), BCM is based on resilience, risk, and quality management principles. The idea is to identify, assess and treat risks that can have a major impact on business continuity. Usually, in the risk assessment phase, quantitative methods are used to calculate predictable situations. However, these RM-based resilient business continuity solutions may be unrealistic because of the multifactorial dimensions of social, technological, and economic connections, and many times the approach is reactive (Linkov et al., 2014.) Figure 2 shows Linkov et al. (2014) approach, the goal of which is to enhance the resilience of organizations

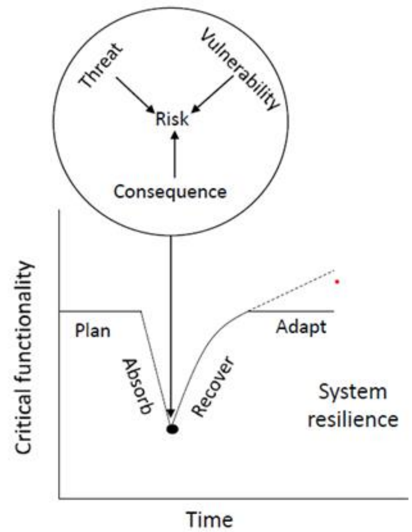

Fig. 2. A resilience management framework. Source: (Linkov et al. 2014)

The y-axis on Linkov et al.'s (2014) resilience management framework, presented in Figure 2, describes the critical functionality of the organization from a BCM perspective. These functions can vary depending on the organization. However, cybersecurity is becoming more important, especially for critical infrastructures, because they are the backbone of a safe society. For example, if the energy field is compromised because of cyber threats, it can cause a negative domino effect on the whole of society. The x-axis presents a time where initially everything goes as planned (risks are managed) and then something happens, and the risk actualizes (e.g., a cyber-attack that cuts down the communication systems). In addition, the x-axis shows what kind of phases there are for organizations to "bounce" back to normal. (Linkov et al. 2014.) Linkov et al (2014) model does not take into account learning from mistakes and the important role that training and education in human factors can play.

Linkov et al.'s (2014) resilience management framework mirrors the well-recognized emergency or disaster management cycle (ref FEMA n.d.). The emergency management cycle aims to reduce vulnerabilities and facilitate a planned approach to disaster risk management in terms of the pre-, during, and after stages of an emergency event. It provides a holistic approach to disaster management (GSScore, n.d.) and has various phases. Mitigation, preparedness, response, and recovery are common to many disaster or emergency management cycles, with the prevention or hazard analysis being another stand-alone recognized stage in some emergency management cycles (MajoremMgt n.d.).

4 Human Factors and Artificial Intelligence in Cybersecurity

Żebrowski, Couce-Vieira, and Mancuso (2022) say that "*Critical infrastructures are increasingly reliant on information and communications technology (ICT) for more efficient operations, which, at the same time, exposes them to cyber threats*". However, it is good to notice that human factors play a critical role in the cybersecurity field. It can be argued that behind every error there can be found various causal factors, with humans, in many times, being the root cause (Reason, 1990). Human factors refer to environmental, organizational, and job factors, as human and individual characteristics, which influence behavior at work in a way, which can affect health and safety (Health and Safety Executive 2023). One of the most recognized researchers and experts on human factors, Alphonse Chapanis, studied how people interact with machines and different systems and argued that the human factor in engineering is often entirely neglected (Chapanis, 1965). Today, there are many studies (e.g., Aaltola, Ruoslahti & Heinonen, 2022; Ruoslahti, & Tikanmäki, 2022; Nifakos et al.,2021; Vieane et al., 2016) that investigate what kind of cybers skill and human factors play a role in protecting against cyber threats and making the organization resilient. Most of them still argue that human factors are frequently excluded from cybersecurity protocols.

According to Aaltola, Ruoslahti, and Heinonen (2022), the key cybersecurity skills for employees are related to 1) Situational awareness, 2) Communication, 3) Leadership, 4) Writing, 5) Understanding the IT domain, 6) Programming, 7) Cloud security, 8) Analytic mindset, 9) Hacker mindset, 10) Architecture, 11) Databases. Ruoslahti & Tikanmäki (2022) argues, "*that changes in the words used in man-machine systems may produce greater improvements in performance than human engineering changes in the machine itself*". Healthcare organizations' cyber threats can be classified into three main categories as follows: 1) attacks that exploit IT infrastructure vulnerabilities resulting from misconfigurations of network components, 2) ransomware attacks being launched against healthcare organizations, with the intention of causing service disruption and holding the healthcare organization data hostage for economic gains, 3) the emerging threat of exploiting a human vulnerability in gaining access to healthcare infrastructure (Nifakos et al., 2021). Awareness, behavior, trust, motivation, and company culture seem to be major factors in cybersecurity (Gcaza, & Von Solms, 2017; Bada, Sasse, & Nurse, 2019).

In recent times Artificial intelligence (AI) in cyber security has created advantages and opportunities as well as challenges. According to Zhang et al. (2022), "AI *plays an important role in the prevention and detection of high-risk network behaviors, but there are some bad factors that will interfere with its correct judgment."* In other words, AI can help organizations with cybersecurity issues by improving threat detection and response times because it is better at identifying patterns and anomalies from raw data compared to traditional approaches. However, it lacks transparency in decision-making and can be used in adversarial attacks. This means that AI assists security specialists, but it does not replace them. (Zhang et al., 2022.) Despite the opportunities and advantages offered by AI, training, and education around human factors seem to be major determinants in enhancing cybersecurity awareness (e.g., Aaltola, Ruoslahti & Heinonen, 2022), with this training and education often lacking. For example, employees may not have enough cybersecurity training, or they use weak passwords. (Gcaza, & Von Solms, 2017; Bada, Sasse, & Nurse, 2019).

This all means that human factors are important to recognize in the implementation of policies and training programs because they raise awareness of cybersecurity risks and best practices. In other words, it can be argued that when cyber threat response plans are made, it is critical to address the human element to mitigate risks. It is also important to remember that AI, while helping to minimize human errors, also creates a threat to BCM from a cybersecurity perspective.

5 Discussions

This paper proposes a modification of Linkov et al.'s (2014) model according to ISO's BCM and disaster management principles and develops a more streamlined resilience cycle approach, with the addition of a 'learn and adapt' phase into the proposed resilience cycle addressing the importance of human factors (see Figure 3).

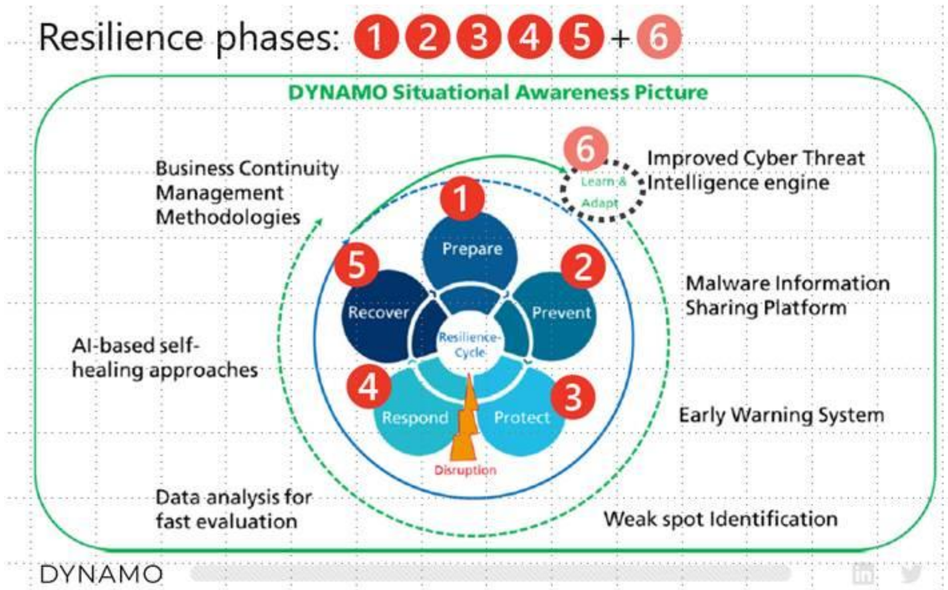

Fig. 3. Proposed Resilience Cycle

The proposed approach of Prepare, Prevent, Protect, Response, and Recovery mirrors the well-recognized concepts of the disaster management cycle while adding a core layer of 'learn and adapt' that is currently lacking from existing models. Prepare, Prevent, and Protect refer to activities that are performed before the attack shows itself to the organization. Prepare and Prevent are the actions undertaken before a cyber-attack occurs to reduce the cause, impact, and consequences of a cyber-attack and to prevent such an attack in the first place. These may include for example identifying key assets, having up-to-date policies, clearly defined roles and responsibilities, training and education, etc. Protect are actions undertaken before a cyber-attack occurs to protect from the impact, and consequences of a cyber-attack. This may include for example data encryption, security software, AI etc. Response takes place immediately before, during, and directly after a cyber-attack and includes activities such as implementing and testing response plans, personal safety, and well-being, addressing public perception, keeping essential business operations going, containing the attack, reporting and investigating the attack, etc. Recover takes place after a cyber-attack and may be immediate and more long-term. During the recovery period, restoration efforts occur concurrently with regular operations and activities. Activities here may include for example repairing and restoring equipment, keeping staff and customers informed, etc. Learn and Adapt involves learning from past mistakes as well as training and education in areas that play a critical role in the cybersecurity field, such as human factors.

6 Conclusions

There is a universal concern among BCM practitioners and scholars about the complexity and time-consuming nature of BCM approaches, which further creates a threat to business continuity. Addressing cybersecurity issues for critical infrastructures is imperative in this modern age, with the role of human factors being increasingly acknowledged. This paper suggests that by modifying Linkov et al.'s (2014) model according to ISO's BCM and RM principles, a more streamlined and efficient BCM resilience approach emerges that also emphasizes the importance of addressing human factors through a 'learn and adapt' phase. Cybersecurity is a useful example through which to explore the proposed approach because cyber-attacks can have a big impact on Critical infrastructure. BCM starts by preparing for cybersecurity threats. This can be done by comparing what has happened previously and/or by having brainstorming workshops where interdisciplinary experts come up with different kinds of risk scenarios, which can have a big impact on BC. In the second phase, the organization starts to develop prevention and protection procedures for identified and assessed risks. If risks after the second phase are actualised, the organization should start the response by applying risk mitigation procedures developed in the previous phase. Recovery can be enhanced by taking stakeholders and partners through the risk mitigation process. In the last phase, the organization learns from mistakes made in the response and recovery phases and adapts for similar future events by delivering awareness. AI can be used to enhance these phases. However, addressing human factors in each of the phases is the key, with the learn and adapt phase emphasizing the importance of learning from past experiences and mistakes.

This paper looked at BCM by following a non-systematic overview process. The general finding was that BCM systems can be very complex and time-consuming. Every approach to BCM is slightly different. However, they all try to identify threats and, based on that, create solutions to ensure the critical processes of an organization run appropriately, to make it more resilient. Based on the findings of the overview a new more streamlined BCM model for CIIPs can be developed, which can be used by other organizations to improve their BCM activities and to understand the roles and enhance cooperation between academia and industry in the development of cybersecurity workforce. While artificial intelligence can be used to speed up and enhance the BCM processes, the important role played by human factors, and the necessity of training and education in this area as part of a 'learn and adapt' phase, is highlighted.

Limitations

Due to the nature of qualitative research and the study approach, the results have limited generalizability. However, it gives a good rapid overview of BCM approaches and cybersecurity as well as works as a good foundation for future testing and development in this field.

Acknowledgment

This research has received support from DYNAMO, which receives funding from the European Commission that aims to develop BCM approaches to mitigate cyber threats.

References

1. Aaltola, K., Ruoslahti, H., & Heinonen, J. (2022, June). Desired cybersecurity skills and skills acquisition methods in the organizations. In European Conference on Cyber Warfare and Security (Vol. 21, No. 1, pp. 1-9). Https://doi.org/10.34190/eccws.21.1.293
2. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? https://doi.org/10.48550/arXiv.1901.02672.
3. Chapanis, A. (1965). Words, words, words. Human factors, 7(1), 1-17. https://doi.org/10.1177/001872086500700101
4. Deming, W. E. (2018). Out of the Crisis, reissue. MIT press.
5. FEMA. (n.d.). Emergency Management in the United States. Retrieved from https://training.fema.gov/emiweb/downloads/is111_unit%204.pdf
6. Gcaza, N., & Von Solms, R. (2017). Cybersecurity culture: an ill-defined problem. In Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference, WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10 (pp. 98-109). Springer International Publishing. https://doi.org/10.1007/978-3-319-58553-6_9
7. Giacomello, G., & Pescaroli, G. (2019). Managing human factors. Cyber resilience of systems and networks, 247-263. https://doi.org/10.1007/978-3-319-77492-3_11
8. Graham, J., & Kaye, D. (2015). A risk management approach to business continuity: Aligning business continuity and corporate governance. Rothstein Publishing. https://doi.org/10.1007/978-3-319-77492-3_11
9. Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. Health information & libraries journal, 26(2), 91-108.

https://doi.org/10.1111/j.1471-1842.2009.00848.x
10. GSS. (n.d.). Disaster Management Cycle. Retrieved from https://ecajmer.ac.in/facultylogin/announcements/upload/DISASTER-MANAGEMENT-CYCLE%201.pdf. Last accessed 25 May 2017
11. Health and Safety Executive. (2023). Introduction to human factors. Retrieved from https://www.hse.gov.uk/humanfactors/introduction.htm. Last accessed 25 May 2023.
12. Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. Business history, 52(6), 978-1002. https://doi.org/10.1080/00076791.2010.511185
13. Ireland MajoremMgt.(n.d.). A Framework for Major Emergency Management. Retrieved from https://www.gov.ie/pdf/?file=https://assets.gov.ie/180183/5dca2e44-350b-492a-bdc3-e5b1135a918d.pdf#page=null. Last accessed 25 May 2023.
14. ISO 22301:2019. Societal security - Business continuity management systems - Requirements. Helsinki: Finnish Standards Association SFS.
15. ISO 22313:2020. Societal security - Business continuity management systems – Guidance. Helsinki: Finnish Standards Association SFS.
16. ISO 27031:2011. Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity.
17. ISO 31000:2018. Risk management. Principles and guidelines. Helsinki: Finnish Standards Association SFS.
18. Lindstedt, D. (2017). Adaptive business continuity: A new approach. Rothstein Publishing.
19. Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... & Thiel-Clemen, T. (2014). Changing the resilience paradigm. Nature Climate Change, 4(6), 407-409. https://doi.org/10.1038/nclimate2227
20. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119
21. Reason, J. (1990). Human error. Cambridge university press.
22. Ruoslahti, H., & Tikanmäki, I. (2022, October). E-Skills in Cybersecurity. In Multimedia Communications, Services and Security: 11th International Conference, MCSS 2022, Kraków, Poland, November 3–4, 2022, Proceedings (pp. 36-48). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-20215-5_4
23. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039
24. Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., & Wickens, C. (2016, September). Addressing human factors gaps in cyber defense. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 60, No. 1, pp. 770-773). Sage CA: Los Angeles, CA: SAGE Publications. https://doi.org/10.1177/1541931213601176
25. Żebrowski, P., Couce-Vieira, A., & Mancuso, A. (2022). A Bayesian framework for the analysis and optimal mitigation of cyber threats to cyber-physical systems. Risk Analysis, 42(10), 2275-2290. https://doi.org/10.1111/risa.13900
26. Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 1-25. https://doi.org/10.1007/s10462-021-09976-0