Journal of Systemics, Cybernetics and Informatics (2024) 22(2), 37-47
https://doi.org/10.54808/JSCI.22.02.37

Cyber Risks: Systematic Literature Analysis

Alona BAHMANOVA
Faculty of Engineering Economics and Management, Riga Technical University
Riga, LV-1048, Latvia

Natalja LACE
Faculty of Engineering Economics and Management, Riga Technical University
Riga, LV-1048, Latvia

ABSTRACT

This systematic literature review focuses on the digitalization theme and its associated risks, particularly cyber risks. Conducted through a comprehensive exploration of the Scopus database over two decades, employing keywords such as "digitalization," "digitization," and "digital risks," this research aimed to understand the evolution of terminology and scholarly discourse in this domain. The investigation initially targeted "digital risks" but shifted towards keywords like "cyber risks," "cybersecurity," and "cyber resilience" to reflect the changing landscape. The review traces the origins of the often-employed keyword "industry 4.0" and its impact on research interests, prompting a focus on more recent publications due to the rapid pace of development in the field. The study follows a structured process for systematic literature review, providing insights into researchers' perceptions, challenges, and approaches in addressing cyber risks and related concepts. Each section of the study offers a concise overview based on the findings in published articles, contributing to a deeper understanding of cyber risks across interdisciplinary perspectives.

Keywords: Cyber Risks, Cyber Threats, Cyber Security, Cyber Resilience, Industry 4.0, Digitalization, Literature Review

1. INTRODUCTION

The study is centered around the theme of digitalization and its associated risks, particularly focusing on cyber risks. The previous literature review was conducted within the Scopus database spanning two decades, employing keywords such as "digitalization," "digitization," and "digital risks." The Umbrella method was utilized to facilitate a broader comprehension of existing research while highlighting areas yet to be explored within the scope of the research topic. Specific criteria guided the search for publications in Scopus to ensure relevance and comprehensiveness. Despite retrieving 176 sources across various scientific domains, only systematic literature reviews were considered, revealing a notable scarcity of information regarding the keyword "digital risks" and a lack of publications establishing a nexus between "cybersecurity" and either "digitalization" or "digitization". This conclusion is used for further research.

Furthermore, the review delineated the evolutionary trajectory of terminology surrounding digitization and digital risks. The initial focus on "digitalization" shifted towards terms like "digital transformation" and "digital maturity," often incorporating the concept "industry 4.0." This prompted a revised inquiry towards keywords such as "cyber risks," "cyber security," and "cyber resilience," suggesting a metamorphosis in terminology.

While initially intending to survey literature spanning from 2004 to 2024, the study's scope was narrowed following an exploration of the origins of the term "industry 4.0" Recognizing its continued interest among researchers, attention was directed towards recent publications, influenced by the rapid pace of development within the research areas. This decision was further motivated by insights from publications like Klaus Schwab's books "The Fourth Industrial Revolution"[1] and "Shaping the Future of the Fourth Industrial Revolution" [2], alongside the impact of the COVID-19 pandemic on social processes and technology described by Klaus Schwab et al. in the book "COVID-19: The Great Reset" [3].

To ensure a comprehensive overview, articles spanning 20 years were initially considered for bibliometric review, followed by a selection process focusing on articles published within the past four years. This methodological approach was motivated by contemporary interest in the subject matter and the swift evolution of research topics, necessitating a focus on recent literature.

Research Questions (RQs)
RQ1: How do researchers across different scientific areas perceive cyber risks, considering the multifaceted nature of the term "risks" and its contextual variations?

RQ2: What are the primary challenges researchers encounter when addressing cyber risks in various fields of science?
RQ3: What strategies and approaches do researchers propose for mitigating cyber risks based on their respective disciplinary perspectives?
This study's primary objective is to explore researchers' perspectives across various scientific areas on cyber risks and related concepts, elucidating the principal challenges they encounter and identifying potential mitigation strategies.
The aim of the research is to establish precise terminology and conduct a comprehensive literature review.

Research tasks

- Conduct a literature review utilizing the Scopus database and "grey literature" sources,
- Narrow the focus to recent literature to glean contemporary insights,
- Elucidate the distinctions between cyber risks, cyber threats, cybersecurity, and cyber resilience, and explore the perceptions of researchers across different scientific areas regarding these concepts.

The research employs a structured methodology for the literature review, utilizing the Scopus database and "grey literature" sources. It also involves analyzing perceptions of researchers across different scientific areas regarding cyber risks and cyber threats.

2. METHODOLOGY

The primary data source in this study was the Scopus database, recognized as the most extensive abstract and citation repository for peer-reviewed literature. Additionally, supplementary sources such as select books categorized as "gray literature" were consulted to augment the breadth of information examined. The initial period chosen was 20 years to provide a more complete picture of research in the field (from 2004 to 2024).
The search methodology comprised several sequential steps.
1. Initially, keywords were employed to filter the database:
1.1. "cyber risk*", "cyberrisk*", "cyber-risk*" (cyber AND risk* OR cyberrisk* OR cyber-risk*).
The result was: 13,805 publications.
1.2. "cyber security", "cybersecurity", "cyber-security" (cyber AND risk* OR cyberrisk* OR cyber-risk*) resulted in 10,377 publications.
1.3. "cyber resilience", "cyberresilience", "cyber-resilience" (cyber AND resilience OR cyberresilience OR cyber-resilience) resulted 690 matches.
2. Subsequently, the selection process focused on articles published within specific subject areas:

- Computer Science: 402 articles
- Social Sciences: 133 articles
- Decision Sciences: 93 articles
- Business, Management, and Accounting: 65 articles
- Economics, Econometrics, and Finance: 34 articles

Following this, 514 articles remained under consideration.
3. Further refinement of the selection was carried out through additional criteria:
3.1. Limited to articles only: 189 articles resulted,
3.2. Limited to open access publications: 103 articles resulted,
3.3. Limited publications were in English: 102 articles resulted.
4. The dataset comprising the resulting 102 articles was imported into VOS Viewer, a specialized software tool utilized for constructing and visualizing bibliometric networks. An analysis employing co-occurrence was chosen, with all keywords serving as units for analysis. The list of recurring or misspelled keywords underwent refinement using Microsoft Excel. Consequently, from the initial 1025 keywords, the list was streamlined to 991 keywords. Employing a default repetition threshold of "5," only 7 keywords met the specified criterion. Subsequently, to glean further insights into bibliometric networks and the relationships among clusters of keywords, the default repetition threshold was adjusted to "3," resulting in the identification of 44 keywords and their interconnections in the visualization.
The dataset of 102 articles was also uploaded to the Bibliometrix online tool utilized for bibliometric analysis to get additional information.

3. RESULTS

Resulted publication count for reviewing: 102 articles in four research areas. The timespan of reviewed articles is limited to 4 recent years (from 2020 through 2024).
The following data are generated using the Bibliometrix online tool:
Number of Documents / Articles - 102
Annual Growth Rate % - 25.89
Document Average Age - 2.31
The following enumeration presents the top five most frequently cited articles within each of the designated subject areas:

Computer Sciences (60 articles)
1. Fake News, Disinformation, and Deep fakes: Leveraging Distributed Ledger Technologies and Block-chain to Combat Digital Deception and Counterfeit Reality [4] - 44 citations;
2. Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem [5] - 33 citations;
3. Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem [5] - 33 citations;

4. A framework for effective corporate communication after cyber security incidents [7] - 28 citations;
5. Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the digital transformation era [8] - 19 citations.

Social Science (30 selected articles)
1. A framework for effective corporate communication after cyber security incidents [7] - 28 citations;
2. Resilience assessment of water quality sensor designs under cyber-physical attacks [9] - 16 citations;
3. An operational approach to maritime cyber resilience [10] - 11 citations;
4. A system to calculate cyber-value-at-risk [11] - 8 citations;
5. The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath [12] - 6 citations.

Business, Management, Accounting Science (13 selected articles)
1. Who cares? Supply chain managers’ perceptions regarding cyber supply chain risk management in the digital transformation era [8] - 19 citations;
2. Insurance and enterprise: cyber insurance for ransomware [13] - 5 citations;
3. Challenges and threats of the digital economy to the Sustainability of the National Banking System [14] - 4 citations;
4. Dimensions of cybersecurity performance and crisis response in critical infrastructure organizations: an intellectual capital perspective [15] - 4 citations;
5. The Risky-Opportunity Analysis Method (ROAM) to Support Risk-Based Decisions in a Case-Study of Critical Infrastructure Digitization [16] - 3 citations.

Economics, Econometrics, Finance Science (8 selected articles)
1. Insurance and enterprise: cyber insurance for ransomware [13] - 5 citations;
2. Challenges and threats of the digital economy to the Sustainability of the National Banking System [14] - 4 citations;
3. The Risky-Opportunity Analysis Method (ROAM) to Support Risk-Based Decisions in a Case-Study of Critical Infrastructure Digitization [16] - 3 citations;
4. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools [17] - 2 citations;
5. Managing cyber risk, a science in the making [18] - 2 citations.

Annual Scientific Production by number of articles
From 2004 to 2017 it was just 1 article published per year,
in 2018 – 4 articles,
in 2019 – 7 articles,
in 2020 – 6 articles,
in 2021 – 11 articles,
in 2022 – 24 articles,
in 2023 – 35 articles,
in 2024 – 11 articles;
The following journals published articles on the topic of interest: IEEE Access, Computers and Security, Electronics (Switzerland), Sustainability (Switzerland), and Applied Sciences (Switzerland).

Geographical distribution by authors
The list of top-10 countries are listed below:
USA - 40 articles,
United Kingdom – 32 articles,
Italy – 12 articles,
Netherlands – 10 articles,
Germany – 9 articles,
Greece – 7 articles,
China – 6 articles,
Norway – 6 articles,
South Korea – 6 articles,
Canada – 5 articles;

Keyword Mapping in VOS Viewer
VOS Viewer application was used to categorize keywords. 991 keywords were categorized into 7 clusters as follows:
1. attack graph, Bayesian network, decision support system, denial-of-service attack, electric power system control, risk assessment, smart grid, smart power grids;
2. 5g mobile communication systems, anomaly detection, artificial intelligence, block-chain, machine learning, organizational, security and privacy;
3. cyberattacks, cyber physical system, cyber-physical attacks, decision theory, optimization, power, power system, sociotechnical systems;
4. critical infrastructure, cyber-physical security, risk, safety, supervisory control and data acquisition;
5. computer crime, covid-19, governance, ransomware, security of data;
6. cyber resilience, cyber risk, cyber security, internet;
7.threats analysis;
Method applied in the network mapping visualization: association strength.

4. FINDINGS

Cyber Risks
The concept of risk has evolved over centuries, initially rooted in gambling mathematics in the seventeenth century, representing the blend of probability and potential gains and losses. Still, by the nineteenth century, it acquired a predominantly negative connotation in economics, engineering, and science, associated with hazards from modern technological advancements, though fundamentally it remains a combination of the probability or frequency of occurrence of a defined hazard and the magnitude of the consequences of the occurrence. All risks can be calculated as [19]:

$$\textit{Risk} = \textit{Likelihood} \times \textit{Consequences}$$

A typical classification of risks is based on the level of knowledge about a risk event's occurrence and may lead to four possibilities:

- Known–knowns (knowledge),
- Unknown–knowns (impact is unknown, but existence is known, i.e., untapped knowledge),
- Known–unknowns (risks), and
- Unknown–unknowns (unfathomable uncertainty) [21].

Risk is a necessary part of doing business, and in a world where enormous amounts of data are being processed at increasingly rapid rates, identifying and mitigating risks is a challenge for any company [20].

ISO Guide 73:2009 defines risk as the effect of uncertainty on objectives, encompassing both positive and negative deviations from the expected outcomes. This definition acknowledges that objectives can vary in nature and scope, spanning financial, health and safety, and environmental aspects at different levels such as strategic, organizational, project, product, and process levels. Risk is often described in terms of potential events and their consequences, or a combination thereof, expressed through the likelihood of occurrence alongside the associated outcomes. Uncertainty, as highlighted in the definition, refers to any deficiency in information or understanding regarding an event, its consequences, or the likelihood of its occurrence. The term includes responsibility for decisions made.

The essence of risk remains elusive due to its subjective nature, intertwined with individuals' decision-making and probability assessment, spanning various societal domains, with a particular focus on emerging cyber risks amid advancements in technology such as computers, the Internet, and artificial intelligence. The term "cyber-" originates from cybernetics, introduced by Norbert Wiener in 1948 to describe self-regulating control systems in biological organisms and mechanical networks, later popularized in the 1970s by the Control Data Corporation (CDC) for their supercomputers, thereby becoming synonymous with computing

The ongoing transition to cyberspace, driven by technological advancements and human activities, underscores the need to comprehend cyber risks stemming from both intentional and accidental threats within this socio-technical system, emphasizing the importance of cybersecurity in safeguarding societal interests and values [22], [10]. Technically, a 'cyber' or information security risk entails the possibility of threats exploiting vulnerabilities in information assets, potentially causing harm to organizations or other entities, based on the adverse impacts and likelihood of occurrence as outlined in ISO/IEC 27005 (2011). It is a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence [23].

Cyber risk can be defined as a function of:

$$R = \{ s_i, p_i, x_i\},\ i= 1,2,\ \dots,\ N$$

where R is the risks; s - is the description of an undesirable scenario; p - is the probability of this scenario; x - is the measure of consequences or damages caused by an occurred scenario; and N -is the number of possible scenarios that may cause damage to a system. [19] Cyber risk management, extending beyond IT, requires comprehensive enterprise-wide oversight and integration into overarching risk management frameworks, emphasizing the urgency of defining strategies and metrics for prompt presentation to the board. Businesses relying on Internet technologies face multifaceted cyber risks, including those related to availability, security, performance, compliance, and culture, which, if not managed effectively, can undermine various aspects of business operations and value [20;24].

The following risks to economic security are most likely to require thorough assessment: risks to the resilience of supply chains, including energy security; risks to the physical and digital security of critical infrastructure; risks that are related to the security of technology and technology leakage; risks of weaponing economic dependencies and economic coercion [25].

Another author defines the following risks for small and medium entrepreneurs (SMEs): Businesses (and Staff) under Stress, Becoming a (New) Target, Supply Chain, and Customer Privacy. Small enterprises face significant cyber threats such as malware, ransomware, social engineering, and data breaches, highlighting the importance of proactive cybersecurity management despite time constraints, particularly as ransomware emerges as a prominent menace. Additionally, online entrepreneurs often exhibit insufficient self-protective behaviors, influenced by perceived vulnerability, severity, efficacy, threat awareness, affective response, and subjective norms [12;26].

Industry 4.0 brings significant advancements through the convergence of information technology and operational technologies, leading to transformative improvements in production processes and service delivery across industries [27]. As cyber risk emerges as a primary concern, organizations must conduct comprehensive assessments encompassing personnel, procedures, and technological infrastructure, prompting the development of enhanced cybersecurity strategies integrated with cyber resilience measures to effectively manage evolving threats and regulatory mandates [20;24]. Cyber risk management involves strategies such as threat and vulnerability modeling, maturity frameworks, cyber insurance, regulatory compliance, and adherence to standards like ISO/IEC 27000 series to mitigate threats and enhance organizational cybersecurity [19]. However, defining specific terms for digital risk remains challenging, with each organization urged to choose clear definitions tailored to their context for consistent usage [21].

The article selection process delineated four distinct subject areas' perspectives on cyber risk: computer science focusing on technical aspects; social sciences on societal vulnerabilities; business and management on operational disruptions and financial implications; and economics and finance on systemic risks and regulatory responses. Despite these diverse perspectives, cyber risk universally entails threats and disruptions to digital systems, individuals, organizations, societies, business operations, and economic activities, urging organizations to continually evolve their cyber risk management strategies to address escalating and evolving cyber threats [24]. The groundbreaking advancements substantially alter and transition the risks associated with adopting contemporary technologies and Industry 4.0 principles. The extensive interconnectivity and data aggregation provide opportunities for malicious cyberattacks, with mounting pressure observed in domains like the Internet of Services (IoS), the Internet of Things (IoT), and others [27].

In contrast to cyber risks, where involved actors bear some accountability for the outcomes, cyber threats frequently compel their targets into circumstances where minimal control is absent, leaving them to confront imminent peril with restricted choices. In the upcoming section, we will delve into the characteristics of cyber threats, which are encountered more frequently in recent articles.

From an exploration of literature from diverse perspectives, the formulation of “cyber risk” is as follows:

Risk is a complex phenomenon shaped by centuries of evolution, encapsulating the likelihood of adverse events and their ramifications, influenced by uncertainties and organizational goals. In cyberspace, cyber risk arises from cyber threats, whether intentional or unintentional, presenting formidable obstacles for individuals, institutions, and communities. Its scope transcends mere technical weaknesses, encompassing broader societal, economic, and psychological dimensions, demanding holistic risk management approaches focused on identifying, addressing, and fortifying against threats.

Cyber Threats

Cyber risk has long been present since the advent of the digital era. Still, the escalation of cyber threats targeting organizations is now occurring at an unprecedented pace, driven by advancements in technology, criminal and state-level motivations, and evolving work practices like big data, remote access, cloud computing, social media, and mobile technology.

The media and insurance industry's increased attention to severe security breaches underscores the risks of financial, physical, and reputational harm to critical organizational and state infrastructures [24]. With the surge in cybercrime incidents since February 2020, organizations face significant disruptions to operations and business continuity due to their heavy reliance on technology, including artificial intelligence [28;29]. The convergence of human beings, the Internet, and computers in cyberspace presents threats ranging from inadvertent errors to malicious attacks, necessitating robust information security measures to mitigate risks from human errors to cyberterrorism [20;30] .

Gombar et al. [27] categorized the cyber threats into five sections, which the author calls pillars as follows:

- Cyber spying
- Disrupting or reducing IT infrastructure resilience
- Enemy campaigns
- Disrupting or reducing e-Government security
- Cyberterrorism

Perozzo et al. [31] list the most relevant potential sources of threats deriving from digitization: Web portals, websites, and social media platforms.

Understanding emerging technologies like IoT and process mining involves utilizing diverse data from business functions and customer interactions. Effective cybersecurity strategies must consider the perception of cyber threats, as individuals' attitudes and behaviors in cyberspace are shaped by their awareness and understanding of these risks, influenced by cognitive and psychological factors [27].

Cyber threats, evolving into acts of terrorism, aim to sow fear and erode trust in government agencies [30]. However, operationalizing cyber resilience faces challenges due to a predominantly technical outlook, often overlooking social dynamics, which are crucial for effective coping strategies [22]. Navigating uncertainties in cyber threat evaluation necessitates organizations to balance risk thresholds with rapid response tactics to maintain stakeholder trust amidst unforeseen consequences [23].

Cyber threat intelligence (CTI) enhances cybersecurity preparedness by providing detailed insights into threats, enabling organizations to proactively defend against potential cyberattacks, especially as risk-based approaches replace prescriptive methods, emphasizing the integration of CTI into enterprise frameworks to bolster defenses against increasingly sophisticated threat actors [32].

From an exploration of literature from diverse perspectives, the formulation of “cyber threat” is as follows:

Cyber threats are the evolving dangers posed by malicious cyberspace activities targeting individuals and organizations across various sectors. These threats encompass various challenges, including cybercrime, cyberterrorism, and espionage, driven by advancing technologies and criminal tactics. Unlike cyber risk, which encompasses the probability and potential consequences of undesirable events influenced by uncertainty and organizational objectives, cyber threats focus on malicious activities and the potential harm they can cause to digital assets and infrastructure.

In summary, we will examine the following terms, frequently used interchangeably, elucidating their commonalities and distinctions:

Table 1. Cyber risks vs. threats: similarities and differences

	Similarities	Differences
Cyber Risk	- Integral to understanding and managing risks in the cyberspace, - Both concepts concern malicious activities targeting digital systems, networks, or data.	Cyber risks focus on the potential for harm or loss resulting from vulnerabilities, irrespective of malicious intent.
Cyber Threat		Cyber threats refer to malicious activities or actors seeking to exploit vulnerabilities for harmful purposes.

Cyber Security

Cybersecurity's pervasive uncertainty stems from epistemic uncertainty, relating to incomplete or contradictory knowledge, and ontologically inherent uncertainty, tied to human behaviors shaping cybersecurity discourse [22]. Additionally, the lack of uniform definitions for terms like "cyber security" and "cyber defense" across national policies contributes to ambiguity, hindering analysis and exacerbating the challenge of establishing standardized terminology [21]. Researchers have outlined four primary paradigms in cyber security [33]:

- fixing and breaking technical objects;
- erroneous use of computers;
- malicious political actions using digital tools;
- social construction of expertise around what is deemed worth protecting;

Sustaining effective cybersecurity measures and ensuring long-term cyber resilience relies on technological advancements and the intricate nature of risk perception, particularly concerning human factors. [27]

When confidence in our cybersecurity risk measurements exists, it is possible to respond to events and make decisions quickly, e.g.: [21]

- Be able to identify and prioritize risks that we aren't prepared to for the control improvements necessary to reduce these risks to an acceptable level;
- To have a better understanding of the implications of threat intelligence and data analytics, allowing faster, better-targeted responses;
- To develop risk-based justifications for investment in cyber security solutions and services.

However, it is not possible to identify all risks in advance, in part for the following reasons [21]:

- Some risks are inherently unknowable.
- Some risks are time-dependent.
- Some risks are progress-dependent.
- Some risks are response-dependent.

Cybersecurity policies predominantly focus on protecting civilian infrastructures like banking systems, while cyber defense, linked to classified government operations, receives less public attention [21]. The Swiss cybersecurity strategy outlines ten key areas: competence development, threat analysis, resilience reinforcement, standards adoption, incident management, cybercrime prosecution, defense enhancement, international policy engagement, and public awareness campaigns [34]. Furthermore, the materiality of entities in cybersecurity plays a crucial role in understanding their transformation into agents of social change, highlighting the interconnectedness of discourse and materiality. Lastly, risk management in cybersecurity involves qualitative and quantitative dimensions, with challenges in assessing security risks due to scientific constraints, necessitating a holistic approach that considers asset criticality, attacker motivations, budget constraints, and broader societal implications [33]. National cybersecurity and cyber defense policies vary significantly, reflecting diverse priorities and approaches. Cyber defense, focusing on thwarting, identifying, and responding to cyber threats, is crucial for safeguarding sensitive data and assets. Intravenous initiatives like Active Cyber Defense (ACD) are implemented by entities like the United States Department of Defense to enhance real-time threat detection and mitigation. Within organizations, effective cybersecurity implementation requires board members to integrate cyber risks into enterprise risk management, ensuring access to cybersecurity expertise, setting clear expectations for management, and fostering dialogues on risk identification and management strategies, including avoidance, acceptance, mitigation, or transfer through insurance. Additionally, maintaining cybersecurity visibility is vital for proactive risk management, involving risk assessment, tolerance setting, mitigation strategy development, and assigning responsibilities based on comprehensive evaluations to enable informed decision-making and validation of security investments [21;24].

Maintaining cybersecurity visibility involves evaluating current risk levels, setting thresholds, prioritizing mitigation strategies, and assigning responsibilities to manage risks and prevent breaches [28] proactively.

Enhanced cybersecurity awareness influences vulnerability identification, while trust in cybersecurity capabilities affects perceptions of effectiveness, highlighting the need to acknowledge uncertainty as a constant in cyber systems and inform strategies for enhancing cyber resilience amid evolving threats [22;30].

From an exploration of literature from diverse perspectives, the formulation of "cyber security" is as follows:

Cybersecurity encompasses the measures and strategies implemented to safeguard digital assets and infrastructure from various threats, including cybercrime, cyberterrorism, and espionage. It involves technical and non-technical aspects, addressing challenges arising from *evolving technologies, human actions, and societal factors. Despite varying national perspectives and priorities shaping the conceptualization of cybersecurity, its core objective remains consistent: to prevent, detect, and respond to cyber threats effectively, ensuring the resilience and security of digital ecosystems.*

Cyber resilience

Resilience, explored across various fields, involves effectively navigating challenges by adjusting and reacting constructively to adversity, emphasizing adaptability and strength in the face of stress [35; 36].

In cybersecurity, distinguishing between engineering and ecological resilience frameworks is crucial, with cyber resilience focusing on safeguarding data, ensuring prompt restoration of business operations post-attack, and encompassing preparatory measures, absorption of disruptions, restoration, and adaptation phases in event management to sustain service accessibility and operational availability [37;38;39].

Cyber resilience goes beyond traditional approaches by emphasizing organizations' ability to absorb and adapt to cyber incidents, yet public awareness and emphasis on promoting cyber resilience remain limited [35], [42].

Cybersecurity readiness intertwines technical and social dimensions within organizations, necessitating recognition of their interconnectedness for effective strategies [31], [22]. Understanding the socio-technical landscape of cyberspace is crucial for prioritizing resilience over mere technological fixes, requiring adaptive coping strategies and consideration of societal dynamics [36], [40]. Additionally, active participation and education are essential for bolstering overall resilience against cyber threats, as reflected in cyber culture and the maturity of cybersecurity risk management [41].

Cyber resilience, an essential modern concept, complements cybersecurity efforts by enabling organizations to withstand cyber threats through proactive measures and adaptive capacities, encompassing foresight, reinforcement, recuperation, and adjustment within a dynamic environment [37].

While cybersecurity primarily focuses on safeguarding systems and data, cyber resilience ensures efficient rebounding from cyber risks, emphasizing the integration of technological principles with interdisciplinary research, public dialogues, and political discussions to safeguard critical systems and infrastructures in the complex socio-technical landscape of cyberspace [22].

From an exploration of literature from diverse perspectives, the formulation of "cyber resilience" is as follows:

Cyber resilience denotes a capacity to endure and recover from cyber threats by integrating anticipation, support, recovery, and adaptation measures within a dynamic cyberspace. While cyber security primarily concentrates on defending systems and minimizing data risks, cyber resilience complements these efforts by preparing organizations and individuals to effectively rebound from cyber hazards and ensure system performance despite adversities. This comprehensive approach includes proactive threat response measures before, during, and after incidents, aligning with planning, absorption, recovery, and adaptation stages. Cyber resilience encompasses technological aspects, interdisciplinary research, public debates, and political discourse, thereby safeguarding critical systems and infrastructures from risks inherent in complex socio-technical environments.

In summary, we will compare the definitions of "cyber security" and "cyber resilience":

Table 2. Cyber security vs. resilience: similarities and differences

	Similarities	Differences
Cyber security	- Both aim to safeguard digital assets and ensure information confidentiality, integrity, and availability. - Both emphasize the need for proactive measures to mitigate risks and strategies for response and recovery.	Cyber security encompasses broader measures beyond addressing threats, including prevention, detection, and response.
Cyber resilience		Cyber resilience emphasizes the ability to adapt and recover from cyber threats, going beyond mere protection to ensure continuity of operations.

5. DISCUSSION

Articles from four distinct scientific disciplines were gathered to shed light on the concept of cyber risk and its related concepts. Each field offers a nuanced perspective. Below a summary of the selected articles is provided.

Computer Sciences

Scholarly articles extensively examine cyber risks, threats [43], security [44], and resilience, particularly focusing on issues like geopolitical manipulation of internet infrastructure [45], [46], [47], [48], [49] and supply chain vulnerabilities [50], [51]. They highlight the need for improved risk management tools like Cyber-Value-at-Risk (CVaR) [11] and comprehensive threat analysis for sectors such as automotive safety amidst the proliferation of connected smart cars [52], [53]. Additionally, challenges arising from AI adoption [28], [54] and cyber resilience across sectors like healthcare [54], [55] maritime [56] , [10], [57] power systems [58], agriculture [59] and urban transit [60] are thoroughly discussed, underscoring the complexities within the subject area of computer science. Post-incident communication challenges within organizations (Knight & Nurse, 2020) , insurance against ransomware [61], [26] and tensions in cyber-resilience implementations [36] are explored.

Social Sciences

The articles offer a thorough analysis of cyber risks, threats [43], security, and resilience, shedding light on vulnerabilities within critical infrastructures [45], [33] and the socio-economic implications of cybersecurity investments [25]. They emphasize the importance of delving into motivational factors influencing protective measures against ransomware, highlighting the crucial role of cyber resilience [36] in organizational survival [7] and reputation management [42]. These insights underscore the intersection between cybersecurity [36], [22] and social science [57], emphasizing the need for interdisciplinary approaches to address contemporary challenges effectively.

Business, Management and Accounting

The articles explore various aspects of cyber resilience within business, management, and accounting areas, highlighting the vulnerability of SMEs [31] and banking system [14] to cyber threats and the importance of cyber culture [8], [22], [41] in organizational security [37]. They emphasize the challenge of balancing insurance-based governance [13], [35] with cyber resilience amidst evolving threats [22] and the development of situational awareness models [62] for effective cybersecurity risk assessment [17], [16]. Additionally, the correlation between organizational cyber risk climate, cybersecurity performance, and investments is explored, while a gap in open Cyber Threat Intelligence (CTI) [32] sharing underscores the need for further research in this area to establish industry standards.

Economics, Econometrics and Finance

Articles in economics, econometrics, and finance explore various facets of cyber resilience, including the role of cyber insurance [13], [35] on incentive risk management, and the preparedness of regulatory frameworks to address cyber risks in the financial sector [14], [63]. They emphasize the development of situational awareness models [17] for assessing cybersecurity risks [18] and highlight the need for interdisciplinary approaches and advanced econometric modeling techniques to develop comprehensive risk management strategies [16]. Furthermore, empirical studies analyzing regulatory interventions' impact on economic and financial system resilience to cyber threats could offer insights into effective governance mechanisms for mitigating risks and ensuring financial stability.

Challenges

The perception of risk as a multifaceted concept influenced by societal norms poses a significant challenge, leading to varied interpretations across diverse domains such as business, social, economic, safety, investment, military, and political spheres. This complexity blurs the boundaries between natural and social sciences, resulting in diverse literature on risk. In modern business environments, integrating cyber risk into enterprise risk management frameworks presents obstacles for many boards, including insufficient commitment to IT security, failure to align cybersecurity evaluations with organizational goals, omission of cybersecurity from strategic plans, overemphasis on internal controls, and inadequate awareness of residual risk [19], [24].

As outlined in the literature, the primary hurdles to crafting models for estimating cyber risk revolve around the difficulties associated with pinpointing risk factors in cybersecurity. Unlike the finance domain, where abundant data on risk factors is available, the realm of cybersecurity often lacks such data or is still in its nascent stages of development [11].

Investigating technological proficiency entails exploring situated routines, the tools used in daily tasks, and discussions regarding advancements in technology and science [33].

Internet users' attitudes towards governments and major corporations are shaped by their individual cognition and perception of cyber threats. There is a psychological disparity between how users perceive the potential cyber threats and organizations' efforts to safeguard against cybersecurity risks. Despite the increasing significance of cybersecurity concerns, limited research has been conducted on individual perceptions of cyber threats and readiness for cybersecurity, nor has attention been given to the gap between these perceptions. Given the paucity of relevant research, it is valuable to examine cyber threats and organizational preparedness from citizens' viewpoint [30].

Cyber Threat Intelligence (CTI) is recognized as essential for bolstering cybersecurity resilience, yet its complete utility is impeded by silos and exclusivity, primarily benefiting larger organizations. Despite the significance of open CTI for its rapid and efficient enhancement of preparedness against cyber threats, obstacles such as concerns over confidentiality and market dynamics inhibit its widespread adoption. This underscores the necessity for collective efforts to surmount these challenges [32]. Cybersecurity issues are globally pervasive, demanding multifaceted strategies owing to the extensive influence of digital technology and interconnections across various sectors. Despite international endeavors such as the Budapest Convention and events like the World Summits on the Information Society fostering cooperation, some countries continue to face cybersecurity challenges despite regional initiatives spearheaded by organizations [64] .

6. CONCLUSION

This study examined cyber risks, cybersecurity, and related topics such as cyber threats and resilience. The literature review identified various challenges in cyber risk management and resilience. These challenges encompass difficulties pinpointing risk factors due to the scarcity of pertinent data in cybersecurity, obstacles to effective board-level management such as a lack of senior management ownership and alignment with organizational goals, and disparities between perceived cyber threats and actual organizational preparedness. The gaps identified in this study will serve as focal points for future research endeavors. Despite the challenges posed by the evolving IT landscape, pursuing solutions for modeling cyber risk is imperative. Like the pursuit of constants in nature, scientists must strive to develop models capable of accurately predicting the risk associated with cyber-attacks.

7. REFERENCES

[1] K. Schwab, **The Fourth Industrial Revolution.** Currency; Illustrated edition, 2017.

[2] K. Schwab and N. Davis, **Shaping the Fourth Industrial Revolution,** World Economic Forum, 2018.

[3] Schwab K. and Malleret T., **COVID-19: The Great Reset,** World Economic Forum, 2020.

[4] P. Fraga-Lamas and T. M. Fernandez-Carames, **Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality,** IT Prof, vol. 22, no. 2, pp. 53–59, 2020.

[5] N. U. I. Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton, **Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: A system of systems problem,** J Comput Des Eng, vol. 7, no. 3, pp. 352–366, 2020.

[6] Z. Liu and L. Wang, **Leveraging Network Topology Optimization to Strengthen Power Grid Resilience against Cyber-Physical Attacks,** IEEE Trans Smart Grid, vol. 12, no. 2, pp. 1552–1564, 2021.

[7] R. Knight and J. R. C. Nurse, **A framework for effective corporate communication after cyber security incidents,** Comput Secur, vol. 99, 2020.

[8] A. Creazza, C. Colicchia, S. Spiezia, and F. Dallari, **Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era,** Supply Chain Management, vol. 27, no. 1, pp. 30–53, 2022.

[9] D. Nikolopoulos, A. Ostfeld, E. Salomons, and C. Makropoulos, **Resilience assessment of water quality sensor designs under cyber-physical attacks,** Water (Switzerland), vol. 13, no. 5, 2021.

[10] E. Erstad, R. Ostnes, and M. S. Lund, **An operational approach to maritime cyber resilience,** TransNav, vol. 15, no. 1, pp. 27–34, 2021.

[11] A. Erola, I. Agrafiotis, J. R. C. Nurse, L. Axon, M. Goldsmith, and S. Creese, **A system to calculate cyber-value-at-risk,** Comput Secur, vol. 113, 2022.

[12] T. Tam, A. Rao, and J. Hall, **The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath,** Digital Government: Research and Practice, vol. 2, no. 2, 2021.

[13] T. Baker and A. Shortland, **Insurance and enterprise: cyber insurance for ransomware,** Geneva Papers on Risk and Insurance: Issues and Practice, vol. 48, no. 2, pp. 275–299, 2023.

[14] M. N. Dudin and S. V. Shkodinsky, **Challenges and threats of the digital economy to the Sustainability of the National Banking System,** Finance: Theory and Practice, vol. 26, no. 6, pp. 52–71, 2022.

[15] A. Garcia-Perez, M. P. Sallos, and P. Tiwasing, **Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective,** Journal of Intellectual Capital, vol. 24, no. 2, pp. 465–486, 2023.

[16] A. A. Ardebili, E. Padoano, A. Longo, and A. Ficarella, **The Risky-Opportunity Analysis Method (ROAM) to Support Risk-Based Decisions in a Case-Study of Critical Infrastructure Digitization,** Risks, vol. 10, no. 3, 2022.

[17] N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, **Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools,** Risks, vol. 10, no. 8, 2022.

[18] M. Dacorogna and M. Kratz, **Managing cyber risk, a science in the making,** Scand Actuar J, vol. 2023, no. 10, pp. 1000–1021, 2023.

[19] R. Keyun, **Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics,** Academic Press, 2019.

[20] S. Moyo, **Executive's Guide to Cyber Risk: Securing the Future Today**. Wiley, 2022.

[21] D. Galinec and L. Luić, **Design of conceptual model for raising awareness of digital threats,** WSEAS Transactions on Environment and Development, vol. 16, pp. 493–504, 2020.

[22] M. Dunn Cavelty, C. Eriksen, and B. Scharte, **Making cyber security more resilient: adding social considerations to technological fixes,** J Risk Res, vol. 26, no. 7, pp. 801–814, 2023.

[23] I. Skierka, **When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis,** Gov Inf Q, vol. 40, no. 1, 2023.

[24] D. Antonucci, **The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities,** 1st edition. Wiley, 2017.

[25] W. Scherpenisse, E. Stamhuis, and A. Quintavalla, **Investment Screening Against Strategic Cyber Risks,** Erasmus Law Review, vol. 2022, no. 4, pp. 290–298, 2022.

[26] B. Luuk, V. H.-D. G. (Maria) Susanne, M.-T. H. Ellen, V. H. Ynze, S. Remco, and L. Eric Rutger, **Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model,** Comput Secur, vol. 127, 2023.

[27] M. Gombár, A. Vagaská, A. Korauš, and P. Račková,

Application of Structural Equation Modelling to Cybersecurity Risk Analysis in the Era of Industry 4.0, Mathematics, vol. 12, no. 2, 2024.

[28] I. Jada and T. O. Mayayise, **The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review,** Data Inf Manag, 2024.

[29] M. Ulsch, **Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks**, 1st edition. Wiley, 2014.

[30] T. Nam, **Understanding the gap between perceived threats to and preparedness for cybersecurity,** Technol Soc, vol. 58, 2019.

[31] H. Perozzo, F. Zaghloul, and A. Ravarini, **CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective,** Complex Systems Informatics and Modeling Quarterly, vol. 2022.

[32] V. Jesus, B. Bains, and V. Chang, **Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence,** IEEE Trans Eng Manag, 2023.

[33] O. Michalec, S. Milyaeva, and A. Rashid, **When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?,** Big Data Soc, vol. 9, no. 1, 2022.

[34] M. Baezner, **Cybersecurity in Switzerland: Challenges and the way forward for the Swiss armed forces,** Connections, vol. 19, no. 1, pp. 63–72, 2020.

[35] G. Mott, J. R. C. Nurse, and C. Baker-Beall, **Preparing for future cyber crises: lessons from governance of the coronavirus pandemic,** Policy Design and Practice, vol. 6, no. 2, pp. 160–181, 2023.

[36] T. Toma, D. Décary-Hétu, and B. Dupont, **The benefits of a cyber-resilience posture on negative public reaction following data theft,** Journal of Criminology, vol. 56, no. 4, pp. 470–493, 2023.

[37] S. Bagheri, G. Ridley, and B. Williams, **Organisational Cyber Resilience: Management Perspectives,** Australasian Journal of Information Systems, vol. 27, 2023.

[38] D. R. Vuță et al., **Extending the Frontiers of Electronic Commerce Knowledge through Cybersecurity,** Electronics (Switzerland), vol. 11, no. 14, 2022.

[39] E. Bellini, S. Marrone, and F. Marulli, **Cyber resilience meta-modelling: The railway communication case study,** Electronics (Switzerland), vol. 10, no. 5, pp. 1–26, 2021.

[40] S. A.-L. Akacha and A. I. Awad, **Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders,** Sustainability (Switzerland), vol. 15, no. 19, 2023.

[41] D. J. Borkovich, R. J. Skovira, and F. Kohun, **Foundation of cybersecurity infoscapes: it's all about the culture,** Issues in Information Systems, vol. 24, no. 3, pp. 1–14, 2023.

[42] S. Durst, C. Hinteregger, and M. Zieba, **The effect of environmental turbulence on cyber security risk management and organizational resilience,** Comput Secur, vol. 137, 2024.

[43] M. F. Safitra, M. Lubis, and H. Fakhrurroja, **Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity,** Sustainability (Switzerland), vol. 15, no. 18, 2023.

[44] K. Renaud and L. Coles-Kemp, **Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge,** SN Comput Sci, vol. 3, no. 5, 2022.

[45] D. Broeders and A. Sukumar, **Core concerns: The need for a governance framework to protect global Internet infrastructure,** Policy Internet, 2024.

[46] R. Sahay, D. A. S. Estay, W. Meng, C. D. Jensen, and M. B. Barfod, **A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS,** Comput Secur, vol. 128, 2023.

[47] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, and K. Salonitis, **Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations,** Sensors, vol. 23, no. 9, 2023.

[48] A. Alqudhaibi, A. Krishna, S. Jagtap, N. Williams, M. Afy-Shararah, and K. Salonitis, **Cybersecurity 4.0: safeguarding trust and production in the digital food industry era,** Discover Food, vol. 4, no. 1, 2024.

[49] D. K. Decker and K. Rauhut, **Incentivizing Good Governance Beyond Regulatory Minimums: The Civil Nuclear Sector,** Journal of Critical Infrastructure Policy, vol. 2, no. 2, pp. 19–43, 2021.

[50] P. Kyranoudi and N. Polemi, **Securing small and medium ports and their supply chain services,** Front Comput Sci, vol. 5, 2023.

[51] G. Moraitis et al., **Exploring the Cyber-Physical Threat Landscape of Water Systems: A Socio-Technical Modelling Approach,** Water (Switzerland), vol. 15, no. 9, 2023.

[52] D. Zelle, C. Plappert, R. Rieke, D. Scheuermann, and C. Krauß, **ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering,** Microprocess Microsyst, vol. 90, 2022.

[53] D. Said, M. Elloumi, and L. Khoukhi, **Cyber-Attack on P2P Energy Transaction between Connected Electric Vehicles: A False Data Injection Detection Based Machine Learning Model,** IEEE Access, vol. 10, pp. 63640–63647, 2022.

[54] M. Dart and M. Ahmed, **CYBER-AIDD: A novel approach to implementing improved cyber security resilience for large Australian healthcare providers using a Unified Modelling Language ontology,** Digit Health, vol. 9, 2023.

[55] J. Zhang and Y. Tai, **Secure medical digital twin via human-centric interaction and cyber vulnerability resilience,** Conn Sci, vol. 34, no. 1, pp. 895–910, 2022.

Todorov, **Maritime Cyber(in)security: A Growing Threat Imperils EU Countries,** Connections, vol. 20, no. 3–4, pp. 73–93, 2021.

[57] E. Erstad, R. Hopcraft, A. Vineetha Harish, and K. Tam, **A human-centred design approach for the development and conducting of maritime cyber resilience training,** WMU Journal of Maritime Affairs, vol. 22, no. 2, pp. 241–266, 2023.

[58] A. Umunnakwe, A. Sahu, M. R. Narimani, K. Davis, and S. Zonouz, **Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality,** IET Cyber-Physical Systems: Theory and Applications, vol. 6, no. 3, pp. 139–150, 2021.

[59] K. Taji, B. Elkhalyly, Y. Taleb Ahmad, I. Ghanimi, and F. Ghanimi, **Securing Smart Agriculture: Proposed Hybrid Meta-Model and Certificate-based Cyber Security Approaches | Protección de la agricultura inteligente: Propuesta de metamodelo híbrido y enfoques de ciberseguridad basados en certificados,** Data and Metadata, vol. 2, 2023.

[60] R. Lu, H. Dong, H. Wang, D. Cui, L. Zhu, and X. Wang, **A Resilience-Based Security Assessment Approach for CBTC Systems,** Complexity, vol. 2021, 2021.

[61] A. Mukhopadhyay and S. Jain, **A framework for cyber-risk insurance against ransomware: A mixed-method approach,** Int J Inf Manage, vol. 74, 2024.

[62] K. Awiszus, Y. Bell, J. Lüttringhaus, G. Svindland, A. Voß, and S. Weber, **Building resilience in cybersecurity: An artificial lab approach,** Journal of Risk and Insurance, 2023.

[63] M. Demertzis and G. Wolff, **Hybrid and cyber security threats and the EU's financial system,** Journal of Financial Regulation, vol. 6, no. 2, pp. 306–316, 2020.

[64] M. Ramírez, L. R. Ariza, M. E. G. Miranda, and Vartika, **The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index,** Sustainability (Switzerland), vol. 14, no. 3, 2022.