

CYBER RISKS AND CYBER INSURANCE: A TAXONOMICAL STUDY USING BIBLIOMETRIC VISUALIZATION

Valentina Ninova¹
Nikolay Ninov

Received 06.10.2025.

Revised 20.11.2025.

Accepted 03.01.2026.

Keywords:

Cyber insurance, Cyber risks, Digitalization, Insurance Industry, Vosviewer, Scopus.



ABSTRACT

The Primary objective of this bibliometric analysis is to study the topic of „Cyber risks and cyber insurance,” which involves an examination of publications listed in the Scopus bibliographic database. According to predefined criteria, using the software tool VOSviewer, the current trends within 566 documents were surveyed and outlined. As a result of the study, the following research objectives were met: (i) scientific publications by year were surveyed and an upward trend in publication activity was identified; (ii) based on an analysis of co-authorship and most active authors, the leading researchers on the topic were highlighted; (iii) as a result of an analysis of the co-occurrence of keywords and the ten most frequent among them, specific terms were identified; (iv) using the analysis of documents on the topic, the most cited were specified; and (v) analyzing the number of publications by country, the most active representatives were highlighted.

© 2026 Global Economic Horizons

1. INTRODUCTION

The global development of information technology in every aspect of human cognition and practices has resulted in the generation and subsequent expansion of new risks and vulnerabilities, including the intensification of cyber incidents observed in recent decades. The axiomatic assertion that risks underpin insurance activity (Ninova & Ninov, 2023), largely explains the need to study cyber insurance, unconditionally accepted as an innovative activity offering insurance products, in the form of an insurance service, in response to emerging cyber risks. The negative trend identified about the diversity of constantly emerging and dynamically transforming cyber risks, viewed through the prism of insurance activity, has resulted in the emergence of a new paradigm, at the centre of which a special place is given to cyber insurance as a tool to reduce and/or neutralise the negative consequences of the manifestation of the said risks. The observed dynamics of emerging risks logically and

invariably follow the trend of development of the modern world in relation to the massive use of digital technologies in combination with artificial intelligence (Kumar et al., 2019). This is why the emerging threats to business and society, which are proven to be cyber in origin, require an adequate response, including from the insurance business. Cyber insurance can help cover the costs and liabilities associated with potential losses and provide insurance consumers with reimbursement for losses and damages incurred (Eling & Zhu, 2018). Cyber incidents include, e.g., cyber crime, IT network and service disruptions, malware/ransomware, data breaches, fines, and penalties are in the first position in the ranking „The most important business risks in 2025: global“ (Allianz 2025, 2025). The presented ranking of business risks is the result of voting by 3778 risk management experts from 106 countries and territories (Allianz 2025, 2025), concerning the ranking of corporate risks. The results of this ranking are eloquent – the first position, the experts give to cyber incidents (38% of the answers, with a record 7% lead over other risks).

¹ Corresponding author: Valentina Ninova
Email: v.ninova@uni-svishtov.bg

Attention should also be paid to the fact that in the same ranking, the risk impact of new technologies and developments in the field of artificial intelligence (AI) is a new entrant in the top 10 global risks in 10th place (Ninova, 2024a; Allianz 2025, 2025). Defining and evaluating cyber incidents as leading risks reflects the importance of today's digital economy, where IT disruptions, the evolving threat of ransomware, data breaches, and extortion, as well as geopolitical rivalries and conflicts, are considered valid reasons for the paradigm shift mentioned in the text above. As a result of this new reading, insurance protection is no longer perceived solely as a solid cost for individual entities, but is attributed the importance of an investment, and one with extremely high returns. Moreover, in purely economic terms, cyber insurance can also be seen as an instrument that guarantees both the prevention and repression of cyber risks. In addition to the thesis put forward, we would point out that it is precisely cyber incidents that result in significant safety damage and negatively impact the economy (Rizov, 2024; Eling & Schnell, 2016).

Placing the focus of research on cyber incidents automatically highlights the scale and number of areas that appear to be related to them. Addressing emerging and modified cyber risks, about digitalization in insurance, in the face of InsurTech (Ninova & Ninov, 2024b), outlines interconnections with SupTech and Cyber Underwriting and Resilience (European Insurance and Occupational Pensions Authority, 2025; Berman et al., 2021; InsurTech World, 2022; FinTech Global, 2023; Grand View Research, 2021; Chang, 2023; Insurance Information Institute, Inc., 2020; Business Wire, 2020; TIBCO, 2025). By their nature, cyber-related risks are a kind of "combination of the likelihood of cyber incidents and their impact", according to the Financial Stability Board's (FSB) Cyber Lexicon (Financial Stability Board, 2023). Cyber risks are a global problem, affecting not only the insurance industry but the economy as a whole. Cybercrime is projected to cost humanity \$10.5 Trillion Annually By 2025 (Cybersecurity Ventures, 2020), and cyber risks are emerging as a constant threat to humanity (Perforce, 2025). In 2025, Veeam® Software is releasing a Europe-focused Ransomware Trends Report for 2024, which is based on lessons learned from 350 victims (Veeam® Software, 2024). Everstream analytics announces the "2025 Supply Chain Annual Risk Report" highlighting the top five most likely supply chain events that could potentially impact businesses and supply chains in 2025 (Everstream analytics, 2025).

The high (recorded and expected) frequency of cyber risks, inevitably accompanied by negative consequences for society and business, directly affects the insurance business. In the context of the approbation of cyber insurance, the place and importance of insurance as an important economic activity that can help neutralise and/or minimise the consequences of the manifestation of risks, including those with a cyber genesis, are reaffirmed. The latter, in turn, appears to be a kind of motive of the author's team to carry out a taxonomical

study by applying bibliometric visualization based on data extracted from Scopus. With the help of the software tool for construction and visualization of bibliometric networks – VOSviewer, data were processed, and the obtained results were analysed, and on this basis, the conclusions were generalised.

The main research objective that the authors set for this taxonomical study is to present and analyse information extracted from the Scopus indexing database on the topic of "Cyber risks and cyber insurance" using bibliometric visualization. In this way, the main trends in the world literature on the topic under consideration will be outlined, with a focus on analyzing: i) scientific publications, according to the criterion of years; ii) co-authorship and highlighting the most active authors, according to the criterion of number of documents; iii) co-occurrence of keywords and the most frequent of them; iv) documents on the topic and which of them are most frequently cited; and v) countries and the most active representatives among them, according to the number of published documents.

To achieve the main research objective, the following research questions are posed in the framework of this research study, which will be sought to be answered:

RQ 1: What is the trend in terms of the number of scientific publications in the Scopus database, analysed by the criterion "Year"?

RQ 2: Which are the authors whose scientific works on the topic "Cyber risks and cyber insurance" are included in the Scopus database, and which are the most active among them?

RQ 3: Which are the keywords in the publications on the topic "Cyber risks and cyber insurance" and which of them are the most frequent?

RQ 4: Which papers on the topic "Cyber risks and cyber insurance" form part of the Scopus database, and which of them are the most cited?

RQ 5: Which countries generate research papers on the topic "Cyber risks and cyber insurance" and which stand out among them with the highest number of papers? The answers to the research questions are presented in the Results and Discussion section.

The present research is concerned on the one hand with the economic view of the problem arising from the scale of cyber incidents, a direct result of the manifestation of cyber risks, and on the other hand, the impact of these risks on insurance activity (Jooycar, 2023; R&I Editorial Team, 2024; MarketsandMarkets Research Private Ltd., 2023; Ayaz et al., 2023; Carfora et al., 2019; Ninov & Ninova, 2018) and in particular on the development of cyber insurance as a specialised type of insurance.

In essence, the dynamics in the development of cyber insurance and its symbiosis with the evolution of services resulting from cyber threats find their application in responding to the demand for cyber security (Schatz et al., 2017; Geer et al., 2020; Levite et al., 2018; Zureich & Graebe, 2015) for both individuals and legal entities. This only further highlights the sense and importance of society to demand and subsequently offer this specific type of insurance protection. From a scientific

perspective, an opportunity is created for a peculiar increase in the thematic range of research questions - the subject of potential future developments on the topic of „Cyber risks and cyber insurance“.

In this line of thought, this research is directed at all experts – both theoreticians and practitioners – who have scientific interests related to the knowledge of the established directions, development, and trends in specialised scientific publications dedicated to cyber risks and cyber insurance. The results of the present study can serve as a kind of “guide” – a landmark in the impressive variety and quantity of scientific publications devoted to the topic.

The presented document is structured in five sections. The first part of the paper (Introduction) is devoted to the clarification of the necessity of conducting research in the field of cyber risks and cyber insurance, while justifying the relevance of the topic. The second part is a brief overview of the publications on the topic under consideration, grouping them into different sub-topics in the context of the diversity of publications/ papers. In the third part, the research algorithm and methodology are described in detail, and the method for extracting the data necessary for the research is presented. The fourth part presents and discusses the results obtained as a consequence of the analyses carried out in terms of: i) scientific publications by year; ii) co-authorship and most active authors; iii) results of co-occurrence of keywords and the ten most frequent keywords; iv) documents and specifically the ten most cited documents; and v) publication activity by country and the most active countries according to the number of documents published. The last part (Conclusion) generalises and discloses the results and, on this basis, draws the relevant logical conclusions as a result of the research carried out.

2. LITERATURE REVIEW

Scientific inquiries, or research, into cyber risks, seen as the result of technological advances in every aspect of human life, have logically evolved and increased over time, from their emergence to today. With the unabashed adoption of digital technologies, the number of cybersecurity threats has also increased tremendously, while at the same time, to date, the degree of their sophistication has also been reported to have increased compared to when they first emerged. It is because of these two parallel processes that the importance and relevance of countermeasure tools have increased, ensuring the desired “cyber hygiene” and providing a reliable and sustainable cyber framework (CISA (Cybersecurity and Infrastructure Security Agency), 2025). It is an undeniable fact that both individuals and organisations of various sizes are constantly falling victim to cyber crimes (for example: cyber attack, data breach, etc.), to cover the financial losses of which, cyber insurance comes to the rescue. Based on our analytical review, we have invariably concluded that the topic of cyber risks and cyber insurance, in a purely etymological

aspect, is a derivative of two completely independent, extremely well-analysed and scientifically exploited topics. Within the framework of the present study, the literature review on the topic under study covers, as a matter of priority, publications in the following three main areas: 1) Cyber risks, 2) Cyber insurance and 3) Cyber risks and cyber insurance, and in this regard only those sub-areas on these sub-areas will be highlighted where a critically high mass of publications has been reported. Covering all perspectives (sub-areas within the three main areas) is an extremely difficult task given the multifaceted nature of the subject matter and the continuously emerging new fields of research – a direct consequence of the dynamically evolving subject matter, the transformations that have occurred, and the evolution of theory and practice in the field of cyber risks and cyber insurance.

Having made this important clarification, in the following lines of the exposition, we proceed to fulfil our intention, namely: to present a literature review on the stated three directions of the topic, focusing on publication activity, including their fundamentally significant sub-directions.

And since cyber risk is at the heart of everything, it will serve as our starting point. Cyber risk, in all its facets, has become a widely discussed topic and a dynamically developing field in science, the subject of analyses by several researchers who contribute to enriching its discourse and enhancing our understanding of it. It is quite logical that a part of the research in the thematic area of cyber risk is devoted to its definition and detailed characterisation of its “anatomy” (understood as specifics and features) (Strupczewski, 2021; Cains et al., 2022), (Curti et al., 2023; Jamilov et al., 2023; Oltramari & Kott, 2018; Cains et al., 2022). The existence of a wide variety of cyber risks, distinguished by their different origins, frequency, and severity, leads to the need to classify them and thus to systematise them into risk classes. Authors who have devoted their efforts to trying to build and introduce a classification of cyber risks (Böhme & Kataria, 2006; Sheehan et al., 2021; Muravskiy et al., 2021; Malavasi et al., 2024), address, in parallel with this issue, the cyber risk classification framework (Sheehan et al., 2019; Sheehan et al., 2021; Ye et al., 2006; Zadeh et al., 2023; Rabitti et al., 2024). The management of cyber risks has been the focus of several publications discussing the options and means to manage them (Ghadge et al., 2020; Evans, 2019; Rosado et al., 2022; Evans, 2019; Refsdal et al., 2015; Johnson, 2015; Eling et al., 2021; Gatzert & Schubert, 2022; Kosub, 2015) (Dacorogna & Kratz, 2023; Biener et al., 2015). Systematic cybersecurity risk assessment is the next highly researched topic (Kandasamy et al., 2020; Radanliev et al., 2018a; Akinrolabu et al., 2019; Radanliev et al., 2018a; Ahmed et al., 2022; Ralston et al., 2007; Bolbot et al., 2020; Tsiodra et al., 2023). A significant body of published research has focused on the impact of cyber risks on particular economic sectors, such as:

- financial (Bouveret, 2018; Pollmeier et al., 2023);

- energetic (Ige et al., 2024; Apostolou et al., 2018; Venkatachary et al., 2017);
- healthy (Sardi et al., 2020; Ksibi et al., 2023; Nifakos et al., 2021).

Significant scientific attention, given the causal relationship, is paid to the cyber risk-cyber security relationship (Cremer et al., 2022; Lee I., 2020; Leuprecht et al., 2016). Differentiated views of cyber risk (including computer science, network engineering, economics, and actuarial science) are the foundation for building a fundamental approach to cyber risk analysis (Bhme et al., 2019) and assessing the real cost of cyber risk events (Eling & Wirfs, What are the actual costs of cyber risk events?, 2019b).

As we have already repeatedly pointed out, the continuous increase in cyber incidents, which are a direct consequence of the manifestation of cyber risks, has resulted in a growing number of studies dedicated to the search for alternatives to minimise and compensate for the damage caused by their implementation. As an economic activity, cyber insurance is an alternative to minimise and/or neutralise cyber risks. Its essence as an economic activity, possessing its own organisational and managerial logic and philosophy (and fully in line with the evolving understanding of the nature and diversity of cyber hazards), finding expression in a final product – cyber insurance – has invariably emerged as a field for several scientific analyses and research. Several researchers have set the working framework with respect to cyber insurance, introducing basic definitions (Tsohou et al., 2023; Böhme & Kataria, 2006; Pal et al., 2014). Other authors have an even more ambitious task – they propose a comprehensive and conceptual formal framework that aims to capture all the key processes and stages of policy development in the context of cyber insurance (Matejka et al., 2021; Woods & Simpson, 2017; Panda et al., 2025). The focus in some of the published research papers is on cyber insurance coverage (Xie et al., 2020; Granato & Polacek, 2019) and on the design of cyber insurance policies (Khalili et al., 2018; Dou et al., 2020; Barreto et al., 2021; Pal R. G., 2011; Awiszus et al., 2023; Kurmaiev et al., 2020). Obviously, no less important for science and practice is the topic of the insurance premium. In this regard, it is noteworthy that the large number of publications related to issues concerning the premium pricing process for cyber insurance (Antonio et al., 2021b; Chiaradonna & Lanchier, 2022; Snavely, 2023; Yang et al., 2020; Skeoch & Pym, 2023), their adjustment and optimisation (Antonio, 2021a; Uuganbayar et al., 2021), and evaluation (Chen et al., 2023). A concentration of analyses and developments, respectively, is observed in the cyber insurance market, within which issues related to:

- specifics and trends in national cyber insurance markets (USA, Germany, Norway, Israel, Sweden, UK, India, Finland, etc.) (Xie et al., 2020; Cole & Fier, 2020; Cremer et al., 2024);

- current and future legal regulations and legislative framework (Herr, 2021; Lemnitzer, 2021; Eling & Schnell, 2019a);
- cyber insurance contract, in the context of its parameters, attributes, and features – (Dou et al., 2020; Aziz, 2020), including in the context of blockchain technologies (Farao et al., 2024);
- the diversity and specificities of cyber insurance products (McGregor et al., 2023);
- the cost and management of IoT-related cyber risk (Leong & Chen, 2020).

Of course, this is the place to remind that the sub-topics of cyber insurance mentioned above in the text do not exhaust all existing sub-topics, but mainly those with a high concentration of publicity activity on them.

3. METHODOLOGY

3.1 Bibliometric visualization

One of the traditional approaches, e.g., systematic literature reviews, offers in-depth insights into a limited number of papers and yet may miss significant papers related to the field being studied (Jesson et al., 2011; Öztürk et al., 2024). When conducting scientific research, different software and tools can be used individually or complexly (within one study) to carry out bibliometric analysis (Long Island University, 2024): i) BibExcel (designed to assist in the analysis of bibliographic data); ii) CiteSpace (e Java application for visualizing and analyzing trends and patterns in scientific literature); iii) PoP (Publish or Perish is used to calculate citation metrics from Google Scholar data); iv) RStudio (open source software for data science, research and technical communication is an integrated development environment (IDE) for R); v) SITKIS (is a bibliometric tool); vi) VOSviewer (a software tool for constructing and visualizing bibliometric networks such as journals, researchers or individual publications and these can be constructed based on citation, bibliographic linkage, co-citation or co-authorship) (Long Island University, 2024). In addition to the above tools and software that can be used for bibliometric analysis, Bibliometrix (An open-source R-tool that is used to complete complex scientific bibliometric analysis. It uses data from Scopus, Web of Science, Dimensions, PubMed, and Cochrane. A version called biblioshiny has been released for use in R for non-coders (University of Illinois, 2023).

Bibliometric visualization analysis is a reliable and specific method for conducting scientific research and analysis when working with large volumes of scientific data, enabling the discovery of evolutionary nuances within a specific scientific field (Donthu et al., 2021). Bibliometric methods or “analysis” have become integral to research evaluation methodology, primarily in the scientific and applied fields (Ellegaard & Wallin, 2015). The application of bibliometric analysis is aimed at revealing emerging trends in the presentation of articles and journals, fixing patterns of collaboration and research components, as well as exploring the intellectual

structure of a specific field in the existing literature (Vermaa & Gustafsson, 2020; Redzwan & Ramli, 2022; Donthu et al., 2021). Back in 2015, Ole Ellegaard and Johan A. Wallin defined a normalised impact norm I_n , norm for a corpus of articles published over years to a year n (Ellegaard & Wallin, 2015). Naveen Donthu, Satish Kumar, Debmalya Mukherjee, Nitesh Pandey, and Weng Marc Lim, in 2024, in How to conduct a bibliometric analysis: an overview and guidelines, highlight the popularity and rigour of bibliometric analysis as a method for examining and analysing large volumes of scientific data (Donthu et al., 2021). In the research paper “How to design bibliometric research: an overview and a framework proposal” by Oğuzhan Öztürk, Rıdvan Kocaman & Dominik K. Kanbach from 2024, the authors present four “Stages and steps of bibliometric research” (Öztürk et al., 2024). In his scientific publication “Bibliometric Analysis: The Main Steps” from 2024, Ioannis Passas presents the 7 basic steps for bibliometric analysis, the possibility of using relevant tools/software, and the expected results (Passas, 2024). The bibliometric visualization approach enables the analysis of many literature sources and better explains complex research topics (Rodrigues et al., 2014). Within the present study, this was achieved by applying a specialised software tool to create maps based on network data and to visualise and explore these maps – VOSviewer (Nees Jan van Eck and Ludo Waltman; Version 1.6.20) (Jan van Eck & Waltman, 2023), which tool was used to identify and analyse use (Ellili et al., 2024) the co-occurrence of authors, co-occurrence of keywords, citation of documents, and bibliographic coupling by countries. When creating a grid visualization, items are represented by their label and by default also by a circle, with the label's size and the item's circle determined by the item's weight (Jan van Eck & Waltman, 2023). The software generates a map by identifying clusters, and the clusters are further analysed using systematic analysis (Ellili et al., 2024; Long Island University, 2024). To visualise the relevant maps and to perform the corresponding analyses (in terms of co-occurrence of authors, co-occurrence of keywords, citation of documents, and bibliographic coupling by countries), documents were extracted from the Scopus database.

3.2 Data Collection

The data collection method followed an algorithm containing four main steps applied to the Scopus database to identify only publications on „cyber risks and cyber insurance“. A string of keywords is the result of a search in the specified database, where search within is carried out as follows: (TITLE-ABS-KEY (cyber AND risks) AND TITLE-ABS-KEY (cyber AND insurance)). As of January 3, 2025, the search results yielded 577 documents that met the set criteria.

An additional limitation was imposed on the next phase of data collection for conducting the study (TITLE-ABS-KEY (cyber AND risks) AND TITLE-ABS-KEY (cyber AND insurance)) AND (LIMIT-TO (

LANGUAGE , “English”)). As a result, 566 documents were selected, but excluded were Italian, Chinese, Ukrainian, German, Polish, and French. It is important to note that no additional restrictions regarding document type were applied during the data collection process (see Table 1).

Table 1. Number of document types

No.	Document type	Number
1	Article	264
2	Conference paper	203
3	Book chapter	46
4	Review	16
5	Book	16
6	Conference review	12
7	Editorial	3
8	Short survey	2
9	Note	2

Source: (Elsevier, 2025 a)

Notably, the predominant number of documents in the Scopus bibliographic database are of the article type, followed by the conference paper type, and with a significantly smaller number of book chapters. Another equally essential „technical detail,, of the analysis is that the task is to analyse the documents indexed in Scopus for the period 2001-2025.



Figure 1. Search Criteria for Scientific Publications
 Source: Author’s data (Chandrarathne et al., 2023)

Ultimately, the bibliometric analysis was officially performed on 566 documents after the selected search criteria for scientific publications were applied in Scopus. The search criteria for scientific documents and their sequence of application are presented in Figure 1.

4. DISCUSSION AND ANALYSIS

4.1 Documents by year

Figure 2 presents the relevant documents selected according to the criterion – year of publication. The results obtained for the selected period 2001-2025 are characterised by noticeable dynamics. After 2012, there is a clear trend towards an increase in the number of documents indexed in Scopus on the topic of “Cyber risks and cyber insurance”. A peak of sorts in the number of published documents on the topic is observed in 2023,

during which 77 documents were indexed. The causal link can be sought in the fact of increasing incidents resulting from the implementation of cyber risks and the search for alternatives to overcome them, including cyber insurance.

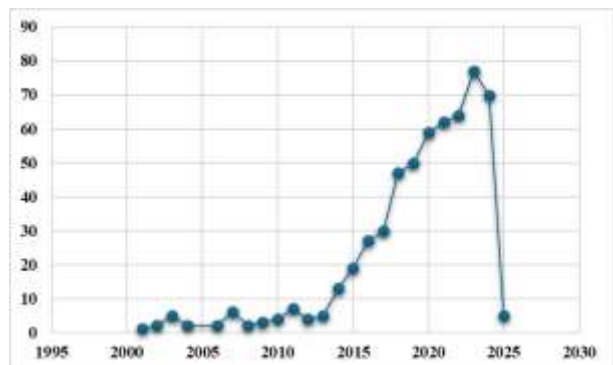


Figure 2. Documents Trends By Year
Source: (Elsevier, 2025 a)

Table 2 presents the five years in which the most articles on the topic were published, and the period they cover is from 2020 to 2024. Of the 566 publications identified, 332 are papers published in the 5 years mentioned, or approximately 58.66% of the total number of all publications that are part of this study and specifically retrieved from the Scopus database.

Table 2. Top Five Years With The Most Documents

No.	Year	Number of documents
1	2023	77
2	2024	70
3	2022	64
4	2021	62
5	2020	59

Source: Authors based on (Elsevier, 2025 a)

The results obtained so far from this part of the research, including the analysis of the documents per year on the topic of “Cyber risks and cyber insurance”, as well as the identification of the top 5 years with the highest number of scientific publications on the topic, accumulated in the Scopus database, provide an answer to the first of the research questions mentioned in the Introduction.

4.2 Co-authorship Analysis and the Most Active Authors

Co-authorship mapping is performed using VOSviewer, with authors represented by labels and circles. The label's size and the item's circle are determined by the weight relative to the encounters (Jan van Eck & Waltman, 2023). The criteria for the minimum number of documents per author are 2. Thus, out of 1230 authors, 226 meet the requirements. Figure 3 visualises the information representing the largest set of 19 items, separated into 5 clusters with 45 links (weights – document).

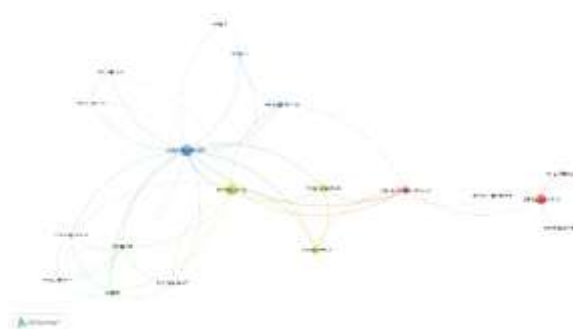


Figure 3. Co-Authorship Network Visualization:
Author: Largest Set

The largest set consists of 5 clusters. Cluster 1 (red, $n = 5$) and includes the authors Martin Eling (13 documents, 4 links, and 6 TLS), Lawrence A. Gordon (2 documents, 2 links, and 2 TLS), Kwangmin Jung (3 documents, 1 link, and 2 TLS), Werner Schnell (2 documents, 1 link, and 2 TLS), Shaun Shuxun Wang (6 documents, 7 links, and 21 TLS). The following authors fall within Cluster 2 (green, $n = 5$) Hai Jiang (3 documents, 6 links, and 12 TLS), Xiao Lu (3 documents, 6 links, and 12 TLS), H. Vincent Poor (2 documents, 4 links, and 4 TLS), Nicolas Privault (2 documents, 5 links, and 8 TLS), Shaun S. Wang (2 documents, 4 links, and 4 TLS). Cluster 3 (blue, $n = 4$) consists of Zhu Han (2 documents, 4 links, and 5 TLS), Dinh Thai Hoang (4 documents, 4 links, and 10 TLS), Dusit Niyato (17 documents, 14 links, and 54 TLS), and Li Wang (2 documents, 2 links, and 2 TLS). Cluster 4 (yellow, $n = 3$) consists of Shaohan Feng (7 documents, 4 links, and 25 TLS), Ping Wang (14 documents, 12 links, and 46 TLS), and Zehui Xiong (7 documents, 4 links, and 25 TLS). The following authors fall within Cluster 5 (purple, $n = 2$): Sivadon Chaisiri (2 documents, 3 links, and 5 TLS), Ryan K. I. Ko (2 documents, 3 links, and 5 TLS).

Table 3 shows the top ten authors with at least 2 papers on „cyber risks and cyber insurance“. The ranking criterion is the number of indexed documents. Each author's TLS (Total Link Strength) is also presented in the table.

Table 3. The Top Ten Most Active Authors

No.	Author	Documents	TLS
1	Dusit Niyato	17	54
2	Ranjan Pal	15	48
3	Ping Wang	14	46
4	Martin Eling	13	6
5	Arunabha Mukhopadhyay	11	17
6	Minguan Lin	10	33
7	Artsiom Yautsiukhin	9	26
8	Fabio Martinelli	8	21
9	Jens Grossklags	8	13
10	Ulrik Franke	8	2

* TLS (Total link strength)

*The results obtained and presented were extracted after using the software tool VOSviewer.

The results obtained from the presented analysis provide an answer to the second research question posed on the topic.

4.3 Co-occurrence Analysis of Keywords and Top Ten Most Frequent Keywords

Figure 4 maps the network of all keywords. A constraint is set on the minimum number of occurrences of a keyword, namely 2 occurrences. This requirement is tailored to the version of the software application and to the specifics of – by default, a maximum of 1000 rows representing the 1000 strongest links between elements are displayed. In the network visualization, keywords are defined by their label and by default, as well as by a circle (Jan van Eck & Waltman, 2023). The weight of the matches determines the label's size and the keywords' circle; in general, the more similar the two keywords are, the stronger their connectivity (Jan van Eck & Waltman, 2023).

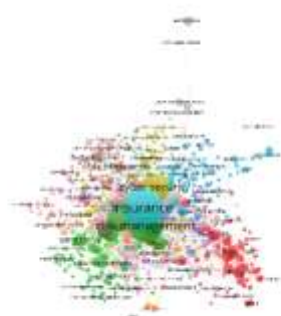


Figure 4. Co-Occurrences of Keywords Network Visualization

Table 4. The Top Ten Most Frequent Keywords in Cyber Risks and Cyber Insurance, and Occurrences in Scopus

No.	Keyword	Occurrences	TLS	Cluster
1	Insurance	230	2440	6
2	Risk management	164	1883	2
3	Cyber insurance	136	1039	15
4	Risk assessment	126	1517	3
5	Cyber security	122	1355	4
6	Cybersecurity	121	1334	7
7	Network security	95	1209	2
8	Cyber risk	81	474	15
9	Security of data	59	655	18
10	investments	43	564	2

* TLS (Total link strength)

*The results obtained and presented were extracted after using the software tool VOSviewer.

In this study, 3240 keywords were identified, and after introducing a minimum threshold of two occurrences, the number was reduced to 784, classified into 19 clusters. 16,250 links and 26,713 TLS were identified.

Table 4 presents the top ten most frequent keywords from the information extracted from the Scopus database on the topic “Cyber risks and cyber insurance”. These are presented by indicating the occurrences of the keywords, the overall strength of the relationship, and the cluster to which each of them belongs.

The data from the obtained results highlight “Insurance” as a kind of leader, for which 230 matches were found, TLS was 2440, and the cluster was 6th. This is not a coincidence, as cyber insurance is a peculiar part of insurance activity, i.e., from “Insurance”. On the other hand, significant items when considering the mentioned topic are namely “Risk management” (164 matches TLS is 1883, the cluster is 2nd); “Cyber insurance” (136 matches TLS is 1039, the cluster is 15th); “Risk assessment” (126 matches TLS is 1517, the cluster is 3rd) and “Cyber security”(122 matches TLS is 1355, the cluster is 4th).

The results obtained in this part of the study, related to the co-occurrence of the keywords highlighting the ten most frequent among them, serve to achieve the main objective of the present study, namely answering the above research questions, and, more specifically, the research question posed under number 3 is answered here.

4.4 Document Analysis

Next, an analysis of the most cited documents on the topic is presented. In the Scopus bibliographic database, 566 documents were identified (with the specified limitations) at the time of the study. In the network visualization, the documents are represented by their label using a circle (Jan van Eck & Waltman, 2023), and the weight of the citations determines the size of the label and the range of documents. Thus, the more similar two documents are, the stronger their connectivity (Jan van Eck & Waltman, 2023). A minimum requirement of at least 2 citations per document was pre-set, resulting in 338 out of 566 documents being detected by the control. The following figure presents the largest item set, consisting of 202 documents, separated into 25 clusters.

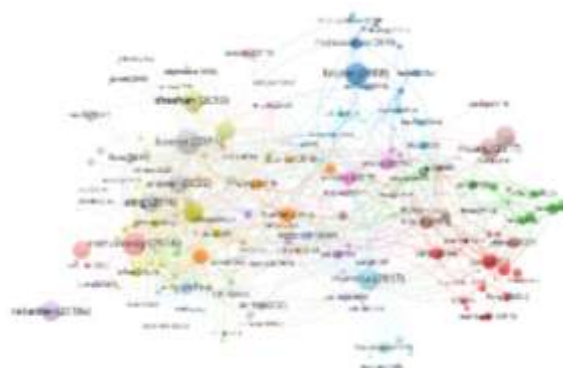


Figure 5. Network Visualization of Citation Analysis of Documents

In terms of subject area, the largest share of papers is in Computer Science, followed by Engineering, Mathematics, Business, Management and Accounting, Economics, Econometrics and Finance, Social Sciences, etc. According to the document type criterion, the leading position is occupied by Article, followed by Conference paper. The next positions are allocated to Conference paper, Book chapter, Book, Review, etc., respectively. The ten most cited documents are listed in the following table by the number of citations.

Table 5. The Ten Most Cited Documents by Number of Citations from Scopus

No.	Author(s)	Citations	Part of the largest set
1	(Rajapathirana & Hui, 2018)	596	-
2	(Sabottke et al., 2015)	252	-
	(Biener et al., 2015)	202	
3	Insurability of Cyber Risk: An Empirical Analysis, 2015)		+
4	(Romanosky, 2016)	173	+
5	(Gordon et al., 2003)	165	-
6	(Bojanc & Jerman-Blažič, 2008)	158	+
7	(Marotta et al., 2017)	147	+
8	(Sheehan et al., 2019)	147	+
9	(Hoang et al., 2017)	136	+
10	(Radanliev et al., 2018a)	122	+

Source: (Rajapathirana & Hui, 2018) (Sabottke et al., 2015) (Biener et al., 2015) (Romanosky, 2016) (Gordon et al., 2003) (Bojanc & Jerman-Blažič, 2008) (Marotta et al., 2017) (Sheehan et al., 2019) (Hoang et al., 2017) (Radanliev et al., 2018a)

**The results obtained and presented were extracted after using the software tool VOSviewer.*

Although the research paper by R.P. Jayani Rajapathirana and Yan Hui (Relationship between innovation capability, innovation type, and firm performance) from 2018 is the most cited document from the Scopus database, with its 596 citations, it is not in the largest set and is not part of the “Network Visualization Of Citation Analysis Of Documents” (Rajapathirana & Hui, 2018). This study aims to effectively manage innovation capacity, helping to achieve more effective innovation outcomes to generate better performance (Rajapathirana & Hui, 2018). The peculiar leader in prefacing this analysis was followed by the 2015 scholarly work on “Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits” by the author team of Carl Sabottke, Octavian Suci, and Tudor Dumitras (representing the University of Maryland), which accumulated 252

citations (Sabottke et al., 2015), development which also focuses on detection techniques that have applications in risk modelling for cyber insurance and these highlight the value of information provided by victims of attacks (Sabottke et al., 2015). Another among the most cited papers is “Insurability of Cyber Risk: An Empirical Analysis” from 2015, by researchers Christian Biener, Martin Eling & Jan Hendrik Wirfs, with 202 citations generated from the Scopus database (Biener et al., 2015). This is an article that discusses the adequacy of cyber risk management insurance by extracting 994 cyber loss events (Biener et al., 2015).

The results obtained, after the research carried out by mapping and analysing the documents from the Scopus database, as well as highlighting the top ten of them, have the “consequence”, in a way, of obtaining an answer to RQ4.

4.4 Analysis by Countries

In the present study, space was allocated, and an analysis of the bibliographic linkage of countries was carried out based on information extracted from the Scopus database. After determining the minimum requirements in terms of i) the maximum number of countries per document – 25; and ii) the minimum number of documents per country – 2. After the constraints were introduced, they found that of the 81 countries, 52 met the thresholds. The visualization of the obtained final result is presented in the following figure. We focus on the fact that within the network visualization: i) countries are represented by their label using a circle (Jan van Eck & Waltman, 2023); and ii) the weight of the document determines the size of the label and the range of countries (Jan van Eck & Waltman, 2023), calculating for each of the 52 countries the total strength of bibliographic links with other countries.

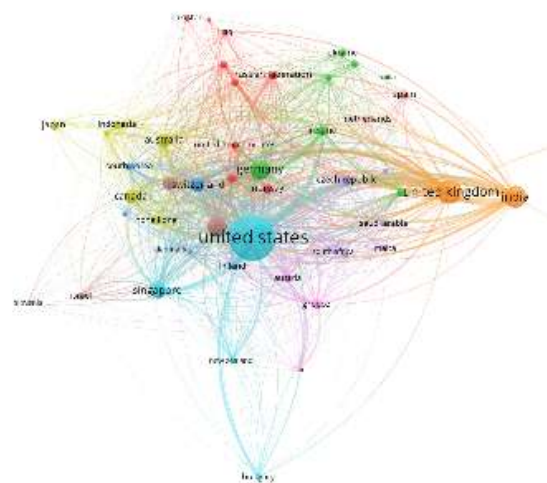


Figure 6. Network Visualization of Bibliographic Coupling of Countries

The United States had the highest number of documents ($n = 210$), the citations ($n = 3383$), and the highest

total link strength (17009). The United Kingdom had the number of documents ($n = 58$), the citations ($n = 491$), and the total link strength (8097). India had the number of documents ($n = 48$), the citations ($n = 335$), and the total link strength (4630).

Table 6 ranks the ten countries with the most scientific publications. It indicates each country's total number of citations and the overall strength of the relationship.

Table 6. The top ten countries by the number of documents

No.	Country	Documents	Citations	TLS
1	United States	210	3383	17009
2	United Kingdom	58	491	8097
3	India	48	335	4630
4	Germany	39	495	7469
5	Italy	39	506	5735
6	Singapore	26	418	3023
7	China	26	757	2947
8	Switzerland	20	722	4886
9	Australia	19	58	3154
10	Canada	19	250	2583

* *TLS (Total link strength)*

**The results obtained and presented were extracted after using the software tool VOSviewer.*

Based on the information extracted in Table 6, we will briefly present one part of the documents for each country. In this line of thought, we will first focus on the leader that is brought out in this ranking based on the number of documents from the Scopus database, namely the United States:

i. (Brho et al., 2025) – a publication in which the author's team found that, contrary to a significant increase in the number of publications on cybersecurity investments, there are significant gaps, and they also found that there is still no distinction between cybersecurity spending and investment.

ii. (Xiang et al., 2024) – The authors acknowledge that the cyber risk insurance market is in its infancy and further develop a “Bonus-Malus” model for cyber risk insurance (Xiang et al., 2024).

iii. (Arce et al., 2024) – The researchers presenting this research paper note that cyber insurance is a popular tool used to manage cyber risk (Arce et al., 2024).

iv. (Lee T. , 2024) – The author focuses on the problem of software monoculture and adopts the idea that there is a common, popular software that is used by all firms, and is thus a source of correlated risk (Lee T. , 2024).

v. (Jung et al., 2024) – the research team explores the opportunity related to how enterprise risk management can be used to address a firm's vulnerability to cyber risk (Jung et al., 2024).

The second position is occupied by the United Kingdom. Here we present key points from the following scientific publications:

i. (Baker & Shortland, 2023) – This document is the result of collaborative research between representatives of the United Kingdom and the United States. It highlights consequential loss minimisation as a form of insurance-based management and is based on interviews with industry people.

ii. (Pal R. et al., 2020) – After conducting an empirical study, the researchers found that third-party commercial cyber risk management (CRM) markets, including cyber insurance, are steadily, albeit slowly, gaining in popularity. Thus, providing a kind of conduit for transferring so-called residual cyber risk to ecosystem managers after attack events (Pal R. et al., 2020).

iii. (Pal R. et al., 2021) – and in this publication, the author's team focuses on the growing popularity of cyber insurance, but in parallel finds that there is a certain probability that the nature of a successful attack is of such a magnitude that the insurer will find itself unable to cover the multiple aggregate losses suffered by its customers and their successors in the supply chain. This is, in fact, a prerequisite for the need for reinsurance through other cyber insurance companies (Pal R. et al., 2021).

iv. (Woods et al., 2021) – In the referenced research paper, the researchers present information extracted from the regulatory filings of 26 insurers about cyber insurance pricing. In addition, empirical observations are provided within the paper regarding the variation of premiums according to the type of coverage, the amount and type of insurer, and over time (Woods et al., 2021).

v. (Laszka et al., October, 2018) – already in 2018, during a scientific conference, a solution was presented by modelling the interaction between a potential client and an insurer as a game of signals with two players, to a problem arising from the so-called information asymmetry. In this regard, insurers often require potential customers to self-report their risks, and thus, adverse selection arises, resulting in unfair premiums and reduced acceptance of cyberinsurance (Laszka et al., October, 2018).

Next, some of India's leading learned publications will be presented, which for the period under review number 48:

i. (Sood et al., 2023) – In the book *The impact of climate change and sustainability standards on the insurance market*, from 2023, the authors discuss issues related to data science use cases for claims processing. In addition, space is given to fraud detection and prevention, policy administration, pricing and underwriting, and last but not least, issues relating to cybersecurity, data protection, and big data regulatory reforms (Sood et al., 2023).

ii. (Biswas et al., 2024) – In the scientific paper “A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks”, a hybrid framework based on explainable AI techniques is proposed for assessing cyber-risks posed by correlated phishing attacks. The

proposal is built upon and goes through five phases in which the probability of expert phishers is calculated, the probability of phishing attacks against a firm is calculated, phishing and genuine URLs are categorized, followed by estimating the joint distribution of phishing attacks, and concluding with recommendations to firms based on calculating optimal cyber insurance investments relative to IT security (Biswas et al., 2024).

iii. (Bhamidipati et al., 2021) – In the framework of the scientific conference “2021 IEEE International Conference on Blockchain (Blockchain)”, a scientific paper was presented, in which a proposal for a new “ClaimChain” consortium blockchain platform was made. It is a platform that uniquely transforms the state-of-the-art approach of the NICB/ISO database architecture. This is done through increased shared intelligence, and at the same time, there is participation from insurance companies (Bhamidipati et al., 2021).

iv. (Mukhopadhyay et al., 2019a) – To mitigate cyber risks, the researchers who authored the aforementioned research paper present a Cyber Risk Assessment and Mitigation (CRAM) framework. Generalised linear models were used in the preparation of the study (GLM) (Mukhopadhyay et al., 2019a).

v. (Mukhopadhyay et al., 2013) – This paper addresses the issue of how to minimise the impact of financial losses caused by security breaches. The author's team focuses on the use of cyber insurance products by proposing models to help firms decide on the usefulness of cyber insurance products and the extent to which they can use them (Mukhopadhyay et al., 2013).

The presented detailed analysis of the bibliographic linking of countries, based on information extracted from the Scopus database on the topic of “Cyber risks and cyber insurance”, by its very nature and significance, answers the research question posed under number 5 in the “Introduction” section, which the author's team set out to achieve the main research objective.

5. MAJOR FINDINGS AND OUTCOMES

Following the above algorithm and adhering to the adopted methodology, it can be concluded that the result of this study is the fulfilment of the main author's stated goal, namely, using bibliometric visualization to present and analyse information extracted from the Scopus indexing database, on the topic of „Cyber risks and cyber insurance“. This is a fact in the context of the following generalised scientific conclusions:

i. The growing number of scientific publications is proof of the unconditional and categorical evolution on issues of „Cyber risks and cyber insurance“, emerging as a centre of attraction for researchers, making it key in the field of insurance.

ii. The period 2020-2024 illustrates the highest share of papers in the Scopus database on the topic, making it the most intensive and “fruitful” period for authors of publications.

iii. From the analysis of the most active authors, it was found that the leading author according to the criterion of the number of published papers in the Scopus database is Dusit Niyato with 17 scientific papers on the topic of „Cyber risks and cyber insurance“.

iv. The leader in terms of most frequent keywords is unquestionably the term “Insurance” (230 occurrences), followed by terms representing a combination of keywords such as “Risk management” (164 occurrences), “Cyber insurance” (136 occurrences), “Risk assessment” (126 occurrences), and “Cyber security” (122 occurrences).

v. A place is also given to the analysis of the documents, after a preliminary limitation on the number of citations per document, namely a minimum of 2 citations, has been introduced, and a map of the highlighted documents has been visualised and generated. The presented ranking of the most cited documents in Scopus highlights (Rajapathirana & Hui, 2018), with 596 citations, although it does not fall into the largest set of documents.

vi. In the course of the research, the leading countries that generated the largest number of documents on the topic of „Cyber risks and cyber insurance“ were identified. The United States is the leader with 210 documents and 3,383 citations (the country also ranks first in the number of citations reported in the Scopus database), followed by the United Kingdom with 58 documents and India with 48 documents.

Findings based on a taxonomical study using bibliometric visualization on the topic of “Cyber risks and cyber insurance” result in new semantic information needed to optimise and streamline insurance business and science. By conducting this research, definitive answers are provided to the five key research questions posed in the Introduction section, aimed at uncovering 1) relevant trends in the scientific literature on the topic of “Cyber risks and cyber insurance”; 2) highlighting the leading authors on the topic at hand; 3) as well as the most common keywords (after introducing certain criteria); 4) identifying the leading papers in the field of cyber risks and cyber insurance; and last but not least; 5) illustration of the leading countries in terms of the number of documents each of them generates.

6. CONCLUSION

Limitations

Only files from the Scopus bibliographic database were used for the network analysis. The choice of this database was dictated by the fact that Scopus has a rigorous selection process and is one of the largest citation databases (Baas et al., 2020). Outside the scope of the study remain documents from the following databases: Web of Science and Dimensions. Lens, PubMed, and reference manager files (i.e., RIS, EndNote, and RefWorks files) were also not included.

When collecting data from Scopus, no restrictions were placed on scientific publications in terms of document

type, source title, subject area, affiliation, funding sponsor, country/territory, and open access.

The taxonomical study presented here, using bibliometric visualization and analysis of the information extracted from the Scopus database, the author team does not define it as completely comprehensive and definitive. According to the research team, there are some limitations in the study conducted. The focus is mainly on emerging and escalating cyber risks and the importance of insurance activity in this regard, and more specifically in the face of cyberinsurance as an economic activity aimed at minimising and/or neutralising the consequences of these risks.

In terms of the practical orientation of this publication, it is necessary to note another limitation related to the non-exhaustive presentation of trends and forecasts related to cyber incidents resulting from the manifestation of cyber risks. Despite the presentation of more than one piece of research by insurance experts, the viewpoint of all insurance industry experts regarding the prospects for the development of cyber insurance as an economic activity significant for humanity to address the threats of cyber attacks is not fully presented. With this in mind, the Results and Discussion section of this publication is based on a limited number of academic research papers, and the research itself has the characteristics of a theoretical desk study based on skills associated with the use of a purpose-specific bibliometric visualization software tool.

Given the flexibility and adaptability of the insurance industry, in the face of cyber insurance and the increasing connection with the negative and turbulent development of cyber risks, the author's team does not aim to explore all aspects, both theoretically and empirically. There are several controversies in the scientific literature, in relation to and regarding the interdisciplinarity of part of the chosen topic, namely the subject matter related to cyber risks, the ethical issues that the development of the same raises, and others. In conclusion, it may be noted

that the present paper is constrained by a systematic framework that is partly a consequence of the existing controversies on the subject of „Cyber risks and cyber insurance“.

7. RECOMMENDATIONS FOR FUTURE WORKS

Future research, based on a bibliometric analysis, could, for example, focus on a deeper investigation of the relationship between cyber insurance and cybersecurity. Another avenue for potential future research relates to more in-depth and detailed studies of cyber insurance and outlining its interrelationships with cyber attacks and possibly subsequent cyber incidents.

Acknowledgment

Author contributions

Conceptualisation, Valentina Ninova and Nikolay Ninov; Writing – preparation of original draft, Valentina Ninova and Nikolay Ninov; Introduction – Valentina Ninova and Nikolay Ninov; Literature review – Valentina Ninova and Nikolay Ninov; Methodology – Valentina Ninova; Data collection – Valentina Ninova and Nikolay Ninov; Results and discussion – Valentina Ninova; Conclusion – Valentina Ninova and Nikolay Ninov; Software – Valentina Ninova. All authors have read and agreed with the published version of the manuscript.

Data Availability Statement

Upon request from the corresponding author.

Conflicts of Interest The author declares no conflict of interest.

References:

- Ahmed, M., Panda, S., Xenakis, C., & Panaousis, E. (2022). MITRE ATT&CK-driven cyber risk assessment. *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security*, (pp. 1-10). <https://doi.org/10.1145/3538969.3544420>
- Akinrolabu, O., Nurse, J. R., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security*, 87, 101600. <https://doi.org/10.1016/j.cose.2019.101600>
- Allianz 2025. (2025, January). *Allianz Risk Barometer: Identifying the major business risks for 2025*. Retrieved from Allianz 2025.: <https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>
- Antonio, Y. (2021a). Adjusting cyber insurance premiums based on frequency in a communication network. *International Journal of Advances in Intelligent Informatics*. <https://doi.org/10.26555/IJAIN.V7I3.698>
- Antonio, Y., Indratno, S. W., & Saputro, S. W. (2021b). Pricing of cyber insurance premiums using a Markov-based dynamic model with clustering structure. *PLoS One*, 16(10), e0258867. <https://doi.org/10.1371/journal.pone.0258867>
- Apostolou, B., Apostolou, N., & Schaupp, L. C. (2018). Assessing and responding to cyber risk: The energy industry as example. *Journal of Forensic & Investigative Accounting*, 10(1), 73-86. Retrieved from <http://web.nacva.com.s3.amazonaws.com/JFIA/Issues/JFIA-2018-No1-5.pdf>

- Arce, D., Woods, W., D., & Böhme, R. (2024). Economics of incident response panels in cyber insurance. *Computers & Security, 140*, 103742. <https://doi.org/10.1016/j.cose.2024.103742>
- Awiszus, K., Knispel, T., & Penner, I. e. (2023). Modeling and pricing cyber insurance. *Eur. Actuar. J., 13*, 1–53. <https://doi.org/10.1007/s13385-023-00341-9>
- Ayaz, M., Sharma, T., & Rao, S. H. (2023). Disruptive artificial intelligence (AI) use-cases in insurance. *AIP Conf. Proc.*, 2782(1). <https://doi.org/10.1063/5.0154760>
- Aziz, B. S. (2020). A systematic literature review of cyber insurance challenges,. *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, (pp. 357-363). Bandung, Indonesia. <https://doi.org/10.1109/ICITSI50517.2020.9264966>
- Baas, J., Schotten, M., Plume, A., Côté, G., & Karimi, R. (2020). Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies. *Quantitative Science Studies, 1*, 377–386. https://doi.org/10.1162/qss_a_00019
- Baker, T., & Shortland, A. (2023). Insurance and enterprise: cyber insurance for ransomware. *The Geneva Papers on Risk and Insurance-Issues and Practice, 48*(2), 275-299. <https://doi.org/10.1057/s41288-022-00281-7>
- Barreto, C., Schwartz, G., & Cardenas, A. (2021). Cyber-Insurance. In R. Ferrari, & A. Teixeira, *Safety, Security and Privacy for Cyber-Physical Systems. Lecture Notes in Control and Information Sciences* (Vol. 486). Springer, Cham. https://doi.org/10.1007/978-3-030-65048-3_15
- Berman, T., Schallmo, D., & Williams, C. A. (2021). Business model transformation through artificial intelligence in the Israeli InsurTech. In *ISPIM Conference Proceedings. The International Society for Professional Innovation Management (ISPIM)*, (pp. 1-42). Retrieved from https://www.researchgate.net/profile/Tal-Berman-3/publication/356695612_Business_Model_Transformation_through_Artificial_Intelligence_in_the_Israeli_InsurTech/links/61aa067129948f41dbbf615d/Business-Model-Transformation-through-Artificial-Intelligence-in-InsurTech/links/61aa067129948f41dbbf615d/Business-Model-Transformation-through-Artificial-Intelligence-in-InsurTech
- Bhamidipati, N. R., Vakkavanthula, V., Stafford, G., Dahir, M., Neupane, R., Bonnah, E., . . . l Calyam, P. (2021). ClaimChain: Secure Blockchain Platform for Handling Insurance Claims Processing. *2021 IEEE International Conference on Blockchain (Blockchain)* (pp. 55-64). Melbourne, Australia: IEEE. <https://doi.org/10.1109/Blockchain53845.2021.00019>
- Bhme, R., Laube, S., & Riek, M. (2019). A fundamental approach to cyber risk analysis. *Variance, 12*(2), 161-185. Retrieved from <https://variancejournal.org/article/120742-a-fundamental-approach-to-cyber-risk-analysis>
- Biener, C., Eling, M., & Wirfs, J. (2015). Insurability of Cyber Risk: An Empirical Analysis. *Geneva Papers on Risk and Insurance: Issues and Practice, 40*(1), 131–158. <https://doi.org/10.1057/gpp.2014.19>
- Biener, C., Eling, M., Matt, A., & Wirfs, J. H. (2015). *Cyber Risk: Risikomanagement und Versicherbarkeit*. St. Gallen: Institut für Versicherungswirtschaft der Universität St. Gallen. Retrieved from https://www.kessler.li/fileadmin/09_PDFs/Cyber_Risk_Risikomanagement_und_Versicherbarkeit_de.pdf
- Biswas, B., Mukhopadhyay, A., Kumar, A., & Delen, D. (2024). A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. *Decision Support Systems, 177*, 114102. <https://doi.org/10.1016/j.dss.2023.114102>
- Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. In *Weis, 2*(1), 3. Retrieved from <https://core.ac.uk/download/pdf/162458449.pdf>
- Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413-422. <https://doi.org/10.1016/j.ijinfomgt.2008.02.002>
- Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. *Safety science, 131*, 104908. <https://doi.org/10.1016/j.ssci.2020.104908>
- Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund. Retrieved from https://books.google.bg/books?hl=bg&lr=&id=n7QZEAAAQBAJ&oi=fnd&pg=PA3&dq=cyber+risk+definition&ots=48y4-Vzu__&sig=3jt_JF2NFVHnzkuV2ZMFHfIkvmE&redir_esc=y#v=onepage&q=cyber%20risk%20definition&f=false
- Brho, M., Jazairy, A., & Glassburner, A. V. (2025). The finance of cybersecurity: Quantitative modeling of investment decisions and net present value. *International Journal of Production Economics, 279*, 109448. <https://doi.org/10.1016/j.ijpe.2024.109448>
- Business Wire. (2020). *Global Insurtech Market (2020 to 2025) - Growth, Trends, and Forecast - ResearchAndMarkets.com*. (Business Wire) Retrieved 2024, from <https://www.businesswire.com/news/home/20200701005415/en/Global-Insurtech-Market-2020-to-2025---Growth-Trends-and-Forecast---ResearchAndMarkets.com>
- Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis, 42*(8), 1643-1669. <https://doi.org/10.1111/risa.13687>

- Carfora, M. F., Martinelli, F., Mercaldo, F., Nardone, V., Orlando, A., Santone, A., & Vaglini, G. (2019). A “pay-how-you-drive” car insurance approach through cluster analysis. *Soft Comput*, 23, 2863–2875. <https://doi.org/10.1007/s00500-018-3274-y>
- Chandrarathne, W., Gamage, S., & Perera, D. (2023). Research in Microinsurance: A Bibliometric Analysis and Review. *Journal of Management, Social Sciences and Humanities*, 4(2), 25 - 57. Retrieved from <https://fmsh.kdu.ac.lk/jmsh/assets/pdf/V4-2/MS2.pdf>
- Chang, V. Y. (2023). Do InsurTech startups disrupt the insurance industry? *Finance Research Letters*, 57, 104220. <https://doi.org/10.1016/j.frl.2023.104220>
- Chen, C. C., Chang, C. C., & Yu, M. T. (2023). Cyber Insurance Valuation with Endogenous Cyber Loss. SSRN 4793793. <https://doi.org/Chen, Chang-Chih and Chang, Chia-Chien and Yu, Min-Teh, Cyber Insurance Valuation with Endogenous Cyber Loss. Available at SSRN: https://ssrn.com/abstract=4793793 or http://dx.doi.org/10.2139/ssrn.4793793>
- Chiaradonna, S., & Lanchier, N. (2022). Exact insurance premiums for cyber risk of small and medium-sized enterprises. *Mathematical Modelling of Natural Phenomena*, 17(40). <https://doi.org/10.1051/mmnp/2022041>
- CISA (Cybersecurity and Infrastructure Security Agency). (2025). *Cybersecurity Best Practices*. Retrieved from CISA (Cybersecurity and Infrastructure Security Agency): <https://www.cisa.gov/topics/cybersecurity-best-practices>
- Cole, C. R., & Fier, S. G. (2020). An Empirical Analysis of Insurer Participation in the U.S. Cyber Insurance Market. *North American Actuarial Journal*, 25(2), 232–254. <https://doi.org/10.1080/10920277.2020.1733615>
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues Pract.*, 47(3), 698-736. <https://doi.org/10.1057/s41288-022-00266-6>
- Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B. J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. *Computers & Security*, 142, 103886. <https://doi.org/10.1016/j.cose.2024.103886>
- Curti, F., Gerlach, J., Kazinnik, S., Lee, M., & Mihov, A. (2023). Cyber risk definition and classification for financial risk management. *Journal of Operational Risk*, 18(2), 37-58. <https://doi.org/10.21314/JOP.2022.036>
- Cybersecurity Ventures. (2020, November 13). *Cybercrime To Cost The World \$10.5 Trillion Annually By 2025*. (S. Morgan, Editor) Retrieved from Cybercrime Magazine: <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal*, 10, 1000–1021. <https://doi.org/10.1080/03461238.2023.2191869>
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of business research*, 133, 285-296. <https://doi.org/10.1016/j.jbusres.2021.04.070>
- Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X., & Hu, C. (2020). An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences*, 527, 576-589. <https://doi.org/10.1016/j.ins.2018.12.051>
- Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5), 474-491. <https://doi.org/10.1108/JRF-09-2016-0122>
- Eling, M., & Schnell, W. (2019a). Capital Requirements for Cyber Risk and Cyber Risk Insurance: An Analysis of Solvency II, the U.S. Risk-Based Capital Standards, and the Swiss Solvency Test. *North American Actuarial Journal*, 24(3), 370–392. <https://doi.org/10.1080/10920277.2019.1641416>
- Eling, M., & Wirfs, J. (2019b). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109-1119. <https://doi.org/10.1016/j.ejor.2018.07.021>
- Eling, M., & Zhu, J. (2018). Which Insurers Write Cyber Insurance? Evidence from the U.S. Property and Casualty Insurance Industry. *Journal of Insurance Issues*, 41(1), 22–56. Retrieved from <http://www.jstor.org/stable/26441191>
- Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24(1), 93-125. <https://doi.org/10.1111/rmir.12169>
- Ellegaard, O., & Wallin, J. (2015). The bibliometric analysis of scholarly production: How great is the impact. *Scientometrics*, 105, 1809–1831. <https://doi.org/10.1007/s11192-015-1645-z>
- Ellili, N., Nobanee, H., Alodat, A., & al., e. (2024). Mapping marine insurance: a bibliometric review: a taxonomical study using bibliometric visualization and systematic analysis. *J Financ Serv Mark*, 29, 745–762. <https://doi.org/10.1057/s41264-023-00232-w>
- Elsevier. (2025 a, January 3). *Analyze search results*. Retrieved from Elsevier: <https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=7c5f7008aa426a54c920e5e423534d18&sot=a&sdt=a&cluster=scolang%2c%22English%22%2c t&sl=63&s=%28TITLE-ABS-KEY%28cyber+risks%29+AND+TITLE-ABS-KEY%28cyber+insurance%29%29&origin=resultslist&count=10&>

- European Insurance and Occupational Pensions Authority. (2025). *Cyber insurance*. Retrieved from European Insurance and Occupational Pensions Authority: https://www.eiopa.europa.eu/browse/digitalisation-and-financial-innovation/cyber-insurance_en
- Evans, A. (2019). *Managing cyber risk*. <https://doi.org/10.4324/9780429057632>
- Everstream analytics. (2025). *2025 Supply Chain Annual Risk Report*. Retrieved from Everstream analytics: https://www.everstream.ai/special-reports/2025-supply-chain-annual-risk-report/?utm_medium=ppc&utm_source=google&utm_campaign=2025%20annual%20risk%20report&utm_content=special%20report&_bt=731993908990&_bk=risk%20analytics&_bm=b&_bn=g&_bg=174618016036&gad
- Farao, A., Papis, G., & Panda, S. e. (2024). INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. *Int. J. Inf. Secur.*, 23, 347–371. <https://doi.org/10.1007/s10207-023-00741-8>
- Financial Stability Board. (2023, April 13). *Cyber Lexicon: Updated in 2023*. Retrieved from Financial Stability Board: <https://www.fsb.org/2023/04/cyber-lexicon-updated-in-2023/>
- FinTech Global. (2023, October 22). *Global Insurtech investment falls short in H1 2023 whilst deal activity remains stable*. Retrieved 2024, from <https://fintech.global/2023/10/02/global-insurtech-investment-falls-short-in-h1-2023-whilst-deal-activity-remains-stable/>
- Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, 89(3), 725-763. <https://doi.org/10.1111/jori.12381>
- Geer, D., Jardine, E., & Leverett, E. (2020). On market concentration and cybersecurity risk. *Journal of Cyber Policy*, 9-29. <https://doi.org/10.1080/23738871.2020.1728355>
- Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal*, 25(2), 223-240. Retrieved from <https://www.emerald.com/insight/content/doi/10.1108/scm-10-2018-0357/full/html>
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3), 81–85. <https://doi.org/10.1145/636772.636774>
- Granato, A., & Polacek, A. (2019). The growth and challenges of cyber insurance. *Chicago Fed Letter*, 426, 1-6. <https://doi.org/https://www.chicagofed.org/publications/chicago-fed-letter/2019/426>
- Grand View Research. (2021). *Insurtech Market Size, Industry Report 2023-2030*. Retrieved from Grand View Research: <https://www.grandviewresearch.com/industry-analysis/insurtech-market>
- Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance*, 15(1), 98-114. <https://doi.org/10.1111/rego.12266>
- Hoang, D. T., Wang, P., Niyato, D., & Hossain, E. (2017). Charging and Discharging of Plug-In Electric Vehicles (PEVs) in Vehicle-to-Grid (V2G) Systems: A Cyber Insurance-Based Model. *IEEE Access*(5), 732-754. <https://doi.org/10.1109/ACCESS.2017.2649042>
- Ige, A. B., Kupa, E., & Ilori, O. (2024). Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources. *International Journal of Science and Research Archive*, 12(1), 2978-2995. <https://doi.org/10.30574/ijrsra.2024.12.1.1186>
- Insurance Information Institute, Inc. (2020, January 6). *Background on: Insurtech*. Retrieved 2024, from Insurance Information Institute, Inc.: <https://www.iii.org/article/background-on-insurtech>
- InsurTech World. (2022, february 11). <https://www.insurtechworld.org/post/102himc/bancassurance-neobanks-and-competing-with-insurers>. Retrieved from InsurTech World: <https://www.insurtechworld.org/post/102himc/bancassurance-neobanks-and-competing-with-insurers>
- Jamilov, R., Rey, H., & Tahoun, A. (2023). The Anatomy of Cyber Risk. *National Bureau of Economic Research*, 28906. <https://doi.org/10.3386/w28906>
- Jan van Eck, N., & Waltman, L. (2023, October 31). *documentation/Manual_VOSviewer_1.6.20*. Retrieved from VOSviewer: https://www.vosviewer.com/documentation/Manual_VOSviewer_1.6.20.pdf
- Jesson, J., Lacey, F. M., & Matheson, L. (2011). Doing your literature review: Traditional and systematic techniques. Retrieved from <https://www.torrossa.com/en/resources/an/4913523>
- Johnson, K. N. (2015). Managing cyber risks. In G. L. Rev. Retrieved from <https://heinonline.org/HOL/LandingPage?handle=hein.journals/geolr50&div=22&id=&page=>
- Jooycar. (2023, January 26). *How Usage-Based Insurance (UBI) is leveling the auto insurance industry*. Retrieved 2024, from Jooycar: <https://www.jooycar.com/2023/01/26/how-usage-based-insurance-ubi-is-leveling-the-auto-insurance-industry/>
- Jung, K., Kim, C., & Yun, J. (2024). The effect of corporate risk management on cyber risk mitigation: Evidence from the insurance industry. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 1-43. <https://doi.org/10.1057/s41288-024-00326-z>

- Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*(8), 1-18. <https://doi.org/10.1186/s13635-020-00111-0>
- Khalili, M. M., Naghizadeh, P., & Liu, M. (2018). Designing Cyber Insurance Policies: The Role of Pre-Screening and Security Interdependence. *IEEE Transactions on Information Forensics and Security*, 13(9), 2226-2239. <https://doi.org/10.1109/TIFS.2018.2812205>
- Kosub, T. (2015). Components and challenges of integrated cyber risk management. *ZVersWiss*, 104, 615–634. <https://doi.org/10.1007/s12297-015-0316-8>
- Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach. *Mobile Netw Appl*, 28, 107–127. <https://doi.org/10.1007/s11036-022-02042-1>
- Kumar, N., Srivastava, J. D., & Bisht, H. (2019). Artificial intelligence in insurance sector. *Journal of the Gujarat Research Society*, 21(7), 79-91.
- Kurmaiev, P., Seliverstova, L., Bondarenko, O., & Husarevych, N. (2020). Cyber insurance: the current situation and prospects of development. *Amazonia Investiga*, 9(28), 65–73. <https://doi.org/10.34069/AI/2020.28.04.8>
- Laszka, A., Panaousis, E., & Grossklags, J. (October, 2018). Cyber-insurance as a signaling game: Self-reporting and external security audits. In *Decision and Game Theory for Security: 9th International Conference, GameSec 2018*, 20, pp. 29–31. Seattle, WA, USA. https://doi.org/10.1007/978-3-030-01554-1_29
- Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, 12(9), 157. <https://doi.org/10.3390/fi12090157>
- Lee, T. (2024). Integrated cyber security risk management-insurance and investment cost analysis. *International Journal of Data Analysis Techniques and Strategies*, 16(3), 223-261. <https://doi.org/10.1504/IJDATS.2024.140651>
- Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, 6(2), 118–136. <https://doi.org/10.1080/23738871.2021.1880609>
- Leong, Y., & Chen, Y. (2020). Cyber risk cost and management in IoT devices-linked health insurance. *Geneva Pap Risk Insur Issues Pract*, 45, 737–759. <https://doi.org/10.1057/s41288-020-00169-4>
- Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, 33(2), 250-257. <https://doi.org/10.1016/j.giq.2016.01.012>
- Levite, A. E., Kannry, S., & Hoffman, W. (2018). *Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance*. Carnegie Endowment for International Peace.
- Long Island University. (2024, January 5). *Bibliometrics: Tools and Software*. Retrieved from LIU Post: <https://liu.cwp.libguides.com/c.php?g=225325&p=4966525>
- Malavasi, M., Peters, G. W., Treuck, S., Shevchenko, P. V., Jang, J., & Sofronov, G. (2024). Cyber Risk Taxonomies: Statistical Analysis of Cybersecurity Risk Classifications. <https://doi.org/10.48550/arXiv.2410.05297>
- MarketsandMarkets Research Private Ltd. (2023). *Usage based insurance market*. Retrieved from MarketsandMarkets Research Private: https://www.marketsandmarkets.com/Market-Reports/usage-based-insurance-market-154621760.html?gad_source=1&gclid=Cj0KCQiAwbitBhDIARIsABfFYIjPhrd_AyevPVo_SGP7zH98JCFZ8bZjlyxi-fOgxaom6H7mwUk3DcaAoHZEALw_wcB
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, 24, 35-61. <https://doi.org/10.1016/j.cosrev.2017.01.001>
- Matejka, V., Soto, J., & Franco, M. (2021). A framework for the definition and analysis of cyber insurance requirements. *Master Project*. Retrieved from <https://files.ifi.uzh.ch/CSG/staff/franco/extern/theses/MAP-VM-JAHS.pdf>
- McGregor, R., Reaiche, C., Boyle, S., & Corral de Zubielqui, G. (2023). Cyberspace and Personal Cyber Insurance: A Systematic Review. *Journal of Computer Information Systems*, 64(1), 157–171. <https://doi.org/10.1080/08874417.2023.2185551>
- Mukhopadhyay, A., Chatterjee, S., & Bagchi, K. e. (2019a). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, 21, 997–1018. <https://doi.org/10.1007/s10796-017-9808-5>
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, 56, 11-26. <https://doi.org/10.1016/j.dss.2013.04.004>
- Muravskiy, V., Pochynok, N., & Farion, V. (2021). Classification of cyber risks in accounting. Retrieved from <https://dspace.wunu.edu.ua/handle/316497/42587>
- 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>
- Ninov, N., & Ninova, V. (2018). The Need for Insurance during Maternity in Bulgaria. *International E-Journal of Advances in Social Sciences*, 392-405. <https://doi.org/10.18769/ijasos.455664>
- Ninova, V. (2024a). Artificial intelligence and insurance: A bibliometric analysis. In *Current Dynamics in Business and Economics: Theoretical Approaches and Empirical Discoveries* (pp. 115 - 141). Peter Lang AG. Retrieved from <https://www.scopus.com/record/display.uri?eid=2-s2.0-85214605042&origin=recordpage>

- Ninova, V., & Ninov, N. (2023). The Effect of the COVID-19 Pandemic on the Health Insurance Market in Bulgaria: Empirical Analysis of Market Concentration. *Optimizing Energy Efficiency During a Global Energy Crisis*, 165-177. <https://doi.org/10.4018/979-8-3693-0400-6.ch011>
- Ninova, V., & Ninov, N. (2024b). INSHURTECH: BIBLIOMETRIC ANALYSIS USING VOSVIEWER. *109th International Scientific Conference on Economic and Social Development - "Green Economy & Sustainable Development"* (pp. 125-134). Cakovec: Varazdin Development and Entrepreneurship Agency. Retrieved from https://www.researchgate.net/publication/379873296_INSHURTECH_BIBLIOMETRIC_ANALYSIS_USIN_G_VOSVIEWER
- Oltramari, A., & Kott, A. (2018). Towards a reconceptualisation of cyber risk: An empirical and ontological study. *Journal of Information Warfare*, 17(1), 49-73. Retrieved from <https://www.jstor.org/stable/26504129>
- Öztürk, O., Kocaman, R., & Kanbach, D. (2024). How to design bibliometric research: an overview and a framework proposal. *Rev Manag Sci*, 18, 3333–3361. <https://doi.org/10.1007/s11846-024-00738-0>
- Pal, R. G. (2011). Aegis A Novel Cyber-Insurance Mode. In J. Baras, J. Katz, & E. Altman (Ed.), *Decision and Game Theory for Security. GameSec 2011. Lecture Notes in Computer Science*. 7037. Heidelberg: Springer, Berlin. https://doi.org/10.1007/978-3-642-25280-8_12
- Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications* (pp. 235-243). IEEE.
- Pal, R., Huang, Z., L. S., Yin, X., Liu, M., Crowcroft, J., . . . Nag, B. (2021). Will Catastrophic Cyber-Risk Aggregation Thrive in the IoT Age? A Cautionary Economics Tale for (Re-)Insurers and Likes. *ACM Transactions on Management Information Systems*, 12(2), Article number 17. <https://doi.org/10.1145/3446635>
- Pal, R., Huang, Z., Yin, X., Lototsky, S., De, S., Tarkoma, S., . . . Sastry, N. (2020). Aggregate cyber-risk management in the IoT age: Cautionary statistics for (re) insurers and likes. *IEEE Internet of Things Journal*, 8(9), 7360-7371. <https://doi.org/10.1109/JIOT.2020.3039254>
- Panda, S., Farao, A., Panaousis, E., & Xenakis, C. (2025). Cyber-Insurance: Past, Present and Future. *Encyclopedia of Cryptography, Security and Privacy*. (S. Jajodia, P. Samarati, & M. Yung, Eds.) Springer, Cham. https://doi.org/10.1007/978-3-030-71522-9_1624
- Passas, I. (2024). Bibliometric Analysis: The Main Steps. *Encyclopedia*, 4(2), 1014-1025. <https://doi.org/10.3390/encyclopedia4020065>
- Perforce. (2025). *Protect Your Embedded Software From These Cybersecurity Vulnerabilities*. Retrieved from Perforce: https://www.perforce.com/p/kw/top-embedded-software-cybersecurity-vulnerabilities?utm_source=googleadwords&utm_medium=cpc&utm_campaign=KlocworkEMEA-Cybersecurity&utm_adgroup=Klocwork-EMEA-Cybersecurity-Search&utm_term=cyber%20security%20risks&gad_source=1
- Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science*, 159, 106022. <https://doi.org/10.1016/j.ssci.2022.106022>
- R&I Editorial Team. (2024, March 14). *Insurance Industry Increasingly Adopting AI Technologies, Study Shows*. Retrieved from Risk & Insurance: <https://riskandinsurance.com/insurance-industry-increasingly-adopting-ai-technologies-study-shows/>
- Rabitti, G., Khorrami Chokami, A., Coyle, P., & Cohen, R. D. (2024). A taxonomy of cyber risk taxonomies. *Risk Analysis*, 45(2), 376-386. <https://doi.org/10.1111/risa.16629>
- Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018a). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*(102), 14-22. <https://doi.org/10.1016/j.compind.2018.08.002>
- Rajapathirana, R. J., & Hui, Y. (2018). Relationship between innovation capability, innovation type, and firm performance. *Journal of Innovation & Knowledge*, 3(1), 44-55. <https://doi.org/10.1016/j.jik.2017.06.002>
- Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA transactions*. 46(4), 583-594. <https://doi.org/10.1016/j.isatra.2007.04.003>
- Redzwan, N., & Ramli, R. (2022). A Bibliometric Analysis of Research on Stochastic Mortality Modelling and Forecasting. *Risks*, 10(10), 191. <https://doi.org/10.3390/risks10100191>
- Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk Management. In *Cyber-Risk Management. SpringerBriefs in Computer Science* (pp. 33–47). Springer, Cham. https://doi.org/10.1007/978-3-319-23570-7_5
- Rizov, V. (2024). *SECURITY IN CYBERSPACE - COLLECTIVE RESPONSIBILITY*. Retrieved from https://www.dksi.bg/media/2583/rizov_doclad.pdf
- Rodrigues, S., van Eck, N., Waltman, L., & al, e. (2014). Mapping patient safety: a large-scale literature review using bibliometric visualisation techniques. *BMJ Open*, e004468. <https://doi.org/10.1136/bmjopen-2013-004468>
- Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135. <https://doi.org/10.1093/cybsec/tyw001>
- Rosado, D. G., Santos-Olmo, A., Sánchez, L. E., Serrano, M. A., Blanco, C., Mouratidis, H., & Fernández-Medina, E. (2022). Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Computers in Industry*, 142, 103715. <https://doi.org/10.1016/j.compind.2022.103715>

- Sabottke, C., Suciu, O., & Dumitraş, T. (2015). Vulnerability disclosure in the age of social media: Exploiting twitter for predicting {Real-World} exploits. In *24th USENIX Security Symposium (USENIX Security 15)* (pp. 1041-1056). USENIX Association. Retrieved from <https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/sabottke>
- Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*, 12(17), 7002. <https://doi.org/10.3390/su12177002>
- Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, 12(2), 8. Retrieved from <https://commons.erau.edu/jdfsl/vol12/iss2/8/>
- Sheehan, B., Murphy, F., Kia, A. N., & Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*, 24(12), 1619–1638. <https://doi.org/10.1080/13669877.2021.1900337>
- Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation research part A: policy and practice*, 124, 523-536. <https://doi.org/10.1016/j.tra.2018.06.033>
- Skeoch, H., & Pym, D. (2023). Pricing cyber-insurance for systems via maturity models. *arXiv preprint arXiv:2302.04734*. <https://doi.org/10.48550/arXiv.2302.04734>
- Snavelly, D. (2023). *Rapid Estimation for Cyber Insurance Premium Pricing for Company Decision-Makers*. The George Washington University. Retrieved from <https://www.proquest.com/openview/84def30630a9efe39dbed6a76d1321a7/1?cbl=18750&diss=y&pq-origsite=gscholar>
- Sood, K., Grima, S., Young, P. C., Ozen, E., & Balusamy, B. (2023). *The impact of climate change and sustainability standards on the insurance market*. John Wiley & Sons. <https://doi.org/10.1002/9781394167944>
- Strupczewski, G. (2021). Defining cyber risk. *Safety science*(135), 105143. <https://doi.org/10.1016/j.ssci.2020.105143>
- TIBCO. (2025). *What is Insurtech?* Retrieved from TIBCO: <https://www.tibco.com/reference-center/what-is-insurtech>
- Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber Risk Assessment and Optimization: A Small Business Case Study. *IEEE Access*, 11, 44467-44481. <https://doi.org/10.1109/ACCESS.2023.3272670>
- Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, 22(3), 737-748. <https://doi.org/10.1007/s10207-023-00660-8>
- University of Illinois. (2023). *Bibliometric Analysis and Visualization*. Retrieved from 2023 The Board of Trustees of the University of Illinois: <https://researchguides.uic.edu/c.php?g=1233392&p=9025976>
- Uuganbayar, G., Yautsiukhin, A., Martinelli, F., & Massacci, F. (2021). Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security*, 101, 102121. <https://doi.org/10.1016/j.cose.2020.102121>
- Veeam® Software. (2024). *2024 Ransomware Trends Report: EUROPE EXECUTIVE SUMMARY*. Retrieved from Veeam® Software: https://go.veeam.com/ransomware-trends-executive-summary-2024-emea?st=adwordspaidsearch&utm_source=google&utm_medium=cpc&utm_campaign=01P-PMIX_EMEA_EN_EAF_Paid-Search_WP_Ransomware-Trends-2024-NB_1AW&utm_content=cid|22093495882_ntw|g_adgr|172555495146_cre
- Venkatachary, S. K., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in energy sector: A review. *International Journal of Energy Economics and Policy*, 7(5), 250-262. Retrieved from <https://savearchive.zbw.eu/bitstream/11159/1315/1/1005320780.pdf>
- Vermaa, S., & Gustafsson, A. (2020). Investigating the emerging COVID-19 research trends in the field of business and management: A bibliometric analysis approach. *Journal of Business Research*, 118, 253-261. <https://doi.org/10.1016/j.jbusres.2020.06.057>
- Woods, D. W., Moore, T., & Simpson, A. C. (2021). The county fair cyber loss distribution: Drawing inferences from insurance prices. *Digital Threats: Research and Practice*, 2(2), 1-21. <https://doi.org/10.1145/3434403>
- Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*, 2(2), 209–226. <https://doi.org/10.1080/23738871.2017.1360927>
- Xiang, Q., Neufeld, A., Peters, G. W., Nevat, I., & Datta, A. (2024). A bonus-malus framework for cyber risk insurance and optimal cybersecurity provisioning. *European Actuarial Journal*, 14(2), 581-621. <https://doi.org/10.1007/s13385-023-00366-0>
- Xie, X., Lee, C., & Eling, M. (2020). Cyber insurance offering and performance: an analysis of the US cyber insurance market. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45, 690-736. <https://doi.org/10.1057/s41288-020-00176-5>
- Yang, Z., Liu, Y., Campbell, M., Ten, C. W., Rho, Y., Wang, L., & Wei, W. (2020). Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations. *IEEE Access*, 8, 78890-78900. <https://doi.org/10.1109/ACCESS.2020.2988548>
- Ye, N., Newman, C., & Farley, T. (2006). A System-Fault-Risk Framework for cyber attack classification. *Information Knowledge Systems Management*, 5(2), 135-151. <https://doi.org/10.3233/IKS-2006-00085>

- Zadeh, A., Lavine, B., Zolbanin, H., & Hopkins, D. (2023). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decision Analytics Journal*, 9, 100328. <https://doi.org/10.1016/j.dajour.2023.100328>
- Zureich, D., & Graebe, W. (2015). Cybersecurity: The continuing evolution of insurance and ethics. *Defense Counsel Journal*, 82(2), 192. Retrieved from <https://www.proquest.com/openview/7c6f05921f8bff2661a652fd12ad8113/1?pq-origsite=gscholar&cbl=545>

Valentina Ninova

Tsenov Academy of Economics,
Svishtov, Bulgaria,
v.ninova@uni-svishtov.bg
ORCID 0000-0002-6147-2293

Nikolay Ninov

Tsenov Academy of Economics,
Svishtov, Bulgaria,
n.ninova@uni-svishtov.bg
ORCID 0000-0003-1029-1318
