



How Should I Start Research in Cyber Security? Suggestions for Researchers According to Bibliometric Analysis Data

Aslıhan İSTANBULLU^a

^a:  0000-0002-1778-859X

 Amasya University, Türkiye

 aslihan.babur@amasya.edu.tr

Abstract

The aim of this study is to discover the research trends in the field of cyber security with performance analysis and to reveal the intellectual structure of the field of cyber security with scientific mapping. For this purpose, articles published in the field of cyber security between 1998-2021 in the WoS database were examined. The research was carried out in accordance with the bibliometric analysis guide. In the data collection phase, 1,631 articles were included in the study by taking into account the criteria determined among 15,781 studies using the PRISMA procedure. R program was used in bibliometric analysis. According to the findings of the study, there has been a significant increase in article productivity in the field of cyber security after 2020. Although IEEE Access is the journal with the highest number of publications in the field, IEEE Transactions on Smart Grid ranks first according to h-index and g-index values. Considering the topics studied according to the years, it is seen that in the first years, issues related to the law such as cybercrime and cyber terrorism were examined, and recently, in addition to these, current technological issues have been included. It is observed that the most effective publication is 'The Internet of Things for Health Care: a Comprehensive Survey' by Islam et al. which examines the security of the Internet of Things in health care, which is also a current issue.

Keywords

Cyber security, bibliometric analysis, current research trends, performance analysis.

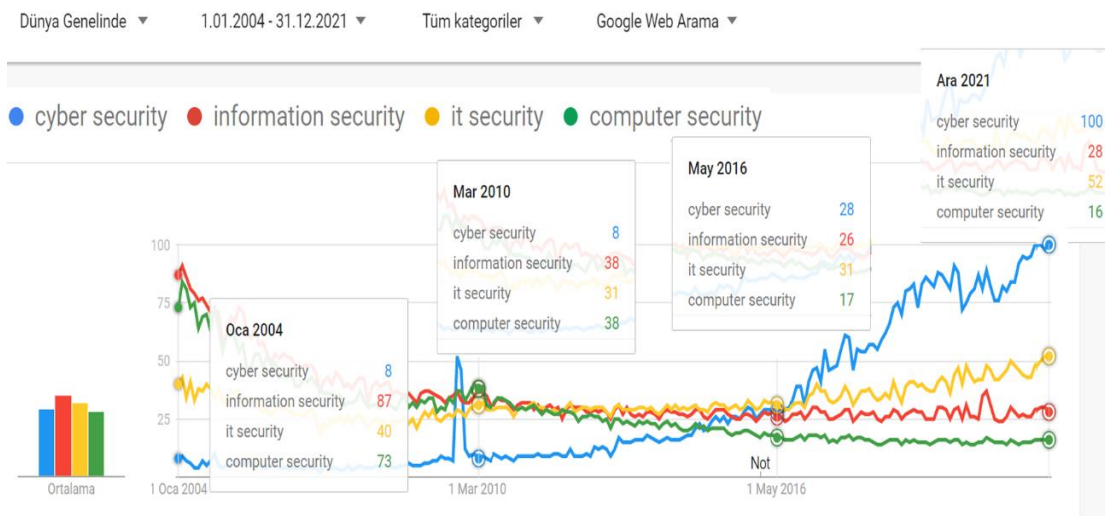
Suggested Citation: İstanbullu, A. (2023). How Should I Start Research in Cyber Security? Suggestions for Researchers According to Bibliometric Analysis Data. *Sakarya University Journal of Education*, 13(1), 119-139. doi: <https://doi.org/10.19126/suje.1219710>

INTRODUCTION

There has been a significant surge in internet usage due to technological developments and the impacts of the Covid-19 epidemic. While the percentage of households accessing the Internet was 82.5% (TUIK, 2018) according to the results of the Household Information Technologies Usage Survey conducted by the Turkish Statistical Institute (TURKSTAT) in 2018, the results of the 2021 survey indicated that this proportion increased to 92% (TUIK, 2022). The number of people exposed to cyber security threats increases with rising internet usage. All users, regardless of age, are exposed to various cyber security threats while spending significant time on the Internet. Multiple terms are used to describe such threats that Internet users are exposed to in their daily lives. Terms such as cyber security, information security, online security, online protection, and internet security are used interchangeably in the literature (Schatz et al., 2017; Quayyum et al., 2022). The analysis conducted via Google's search trends (Google Trends) revealed the changing trends in search of these terms in the web environment (Fig. 1).

Figure 1

Google search trends from 2004-2021 (Source: <https://trends.google.com/trends/explore?date=2004-01-01%202021-12-31&q=cyber%20security,information%20security,it%20security,computer%20security>)



Search trends is a free service provided by Google, and it reveals how frequently search terms are used. It provides data on which periods have the most searches for the chosen keyword(s) within a specific date range. Although these trends are indicative only, search engine-based data is considered beneficial and valuable for identifying trends (Schatz et al., 2017) as indicated in previous studies (Choi & Varian, 2012). The trendlines in Figure 1 were created by comparing the terms "cyber security," "information security," "it security," and "computer security" between 01/01/2004 and 12/31/2021 in all categories worldwide. Since Google started the trends year range from 2004, the start date was set to 2004. The search result can be accessed at the URL found in the reference section of Figure 1. Figure 1 demonstrates that the terms "information security" and "computer security" were the most used terms of 2004 and 2010. In 2016, while the use of "cyber security" increased, the use of "information

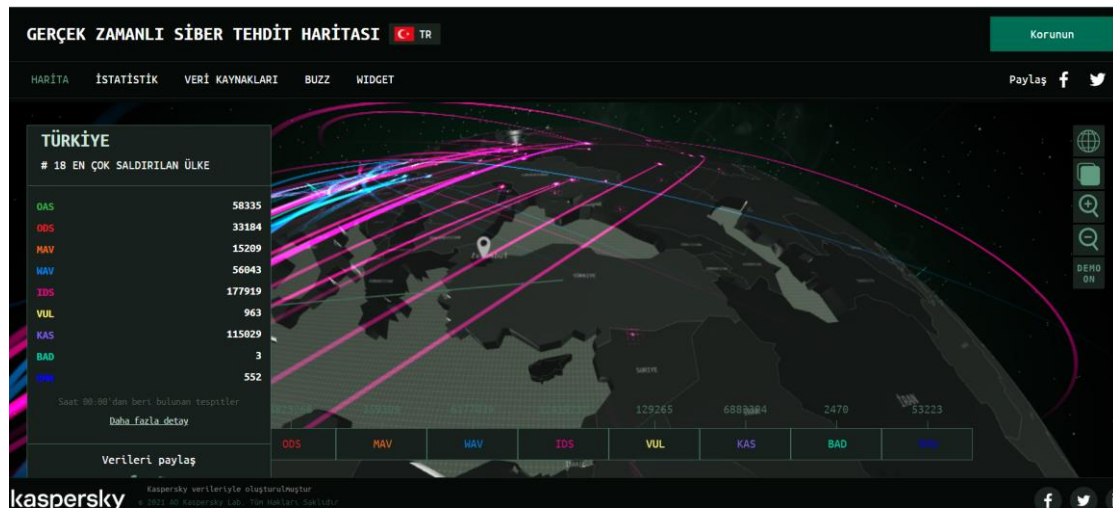
security" showed a decline, yet they were the most frequently used terms. At the end of 2021, however, there was a significant rise in the use of "cyber security," which became the most used query. Therefore, the term cyber security was preferred in this study.

Cyber security protects information, information processing, or storage systems by providing hardware and software solutions (Tam et al., 2021). Although there is no standard definition of cyber security, the International Telecommunication Union (ITU) defines it as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. (ITU, 2022). It involves institution, organization, and user's assets, connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. In short, the term cyber security can be defined as protecting the Internet of things (IoT), networks, and programs against internal or external threats.

Cyber security is a significant issue for institutions and organizations' infrastructure. It is also vital for individuals who want to keep their information, data, and devices secure. In today's world, a large amount of data is stored on IoT devices, and countries are becoming more dependent on technology. As a result, countries become vulnerable to cyber-attacks. According to The Cyber security and Infrastructure Security Agency (CISA, 2022), attacks that occurred every 39 seconds in 2019 increased dramatically to every 11 seconds in 2021. In addition, according to Cyberthreat Real-Time Map by Kaspersky, our country, which ranked 19th among the most attacked countries in 2021, ranked 18th on February 23th, 2022, as demonstrated in Fig. 2.

Figure 1

Kaspersky real-time Turkey cyber threat map (Source: <https://cybermap.kaspersky.com/tr>)



Understanding cyber security begins with the basic assumption that anyone can be a target for attacks by cybercriminals in cyberspace (Sule et al., 2021). While there are also targeted attacks, most attacks are un-targeted. Individuals, institutions, or countries may cause severe problems by gaining access to data or organizing assaults through cyberattacks. It is possible to share sensitive information, change

data, and even attack countries' energy or natural gas lines. There have been severe cyberattacks on governments throughout history. In this regard, cyber security threats jeopardize a country's security, economy, and health, causing monetary and moral costs. At this point, education is a savior. Offering cybersecurity training to end users is one way to reduce losses. It's an unfortunate fact that, while cybersecurity in Education is necessary to protect against financial loss and prevent disruption, it's also crucial to protect students from harm.

Besides the importance of education, governments bear significant responsibility for reducing the risk of cyberattacks. Countries all around the globe develop cyber security plans both at a national and international level and implement cyber security policies. Similarly, in our country, the Ministry of Transport, Maritime Affairs, and Communications issued the National Cyber security Strategy and Action Plan for 2020-2023 in 2020. The action plan includes the cyber security objectives that our country has determined within its vision 2023. However, although cyber security is one of the most critical challenges countries face today, studies on cyber security are limited. It is vital to emphasize cyber security studies and assure their continuity to comprehend the significance of cyber security, anticipate potential problems, discover solutions as quickly as possible, and ensure security. Also, those wishing to pursue a cyber security-related research career should be aware of the scope of cyber security research areas to design studies so that they make fundamental contributions to the discipline (Suryotrisongko & Musashi, 2019). Therefore, the current study examines the trends in cyber security studies on a large scale through bibliometric analysis, referring to the significance of cyber security.

There are very few bibliometric analyses on cyber security studies published internationally (Cojocarú & Cojocarú, 2019). Some of these analyses have focused on applying cyber security in specific research areas such as healthcare (Bradea et al., 2015; Jalali et al., 2019). Others focus on the bibliometric analysis of various aspects and components of cyber security such as big data, malware (Razak et al., 2016), mobile forensics (Gill et al., 2018), cybercrime victimization (Ho & Luong, 2022), cyber behavior (Serafin-Plasencia et al., 2019), cyber security, cyber parental control (Altarturi et al., 2020). Ho and Luong (2022) examined the bibliometric analysis of 387 Social Science Citation Index (SSCI) articles on cybercrime victimization on the Web of Science database during 2010-2020 (Ho & Luong, 2022). Their study identified research trends and distribution of publications by five main areas, including time, prolific authors, leading sources, active institutions, and leading countries/regions. Altarturi et al. (2020) examined a bibliometric analysis of publications on cyber parental control on Scopus and WoS between 2000 and 2019 (Altarturi et al., 2020). They determined the trends of articles, books, book chapters, and conference proceedings in terms of author, country, and collaborative network. Serafin-Plasencia et al. (2019) examined the bibliometric analysis of cyber behavior articles published in four journals on the Scopus database between 2000 and 2018 (Serafin-Plasencia et al., 2019). Their study identified trends of the most productive country, scientific collaboration, most prolific authors, and the most frequently used words. Moreover, Cojocarú and Cojocarú (2019) also explored the total number and geographical distribution of publications on cyber security in Eastern Europe, the cyber security document types of the authors in the Republic of Moldova, the languages used, the institutions of the authors, and publication sources using the database of the Republic of Moldova and Scopus Elsevier and WoS (Cojocarú & Cojocarú, 2019). When the studies are examined, although there are several bibliometric analysis studies published on cyber security and its sub-themes, it seems that there is a need for further studies that reveal the status of cyber security at the international level.

Reviewing a vast volume of literature aids in identifying research themes and gaps in the literature, which is helpful for prospective future studies (Tranfield et al., 2003). Given the importance of cyber

security for countries, this study attempts to fill a gap in the field by examining existing publications and disclosing the current state of cyber security research trends. In this regard, the present research focuses on cyber security studies published between 1998 and 2021 and indexed in the Web of Science (WoS) database. The dates were chosen based on the established criteria, including the date of the first cyber security research in WoS. Furthermore, the current study is crucial in terms of detecting the gaps and significant aspects in the discipline, as it indicates the present condition, academic performance, and intellectual framework of cyber security research. This study also reveals the most influential constituents of the field, including the productivity of cyber security studies, the most cited journals, publications, and explored themes. The study's findings may inspire further research in the field. This study also provides practical information for researchers who wish to study cyber security to understand the basis of the concept better and discover new trends in cyber security. Seeing publication trends in the field of cyber security can also contribute to increasing cyber security measures and awareness. Determining scientific fields' intellectual structure and status is essential for research, policymaking, and implementation (Aria & Cuccurullo, 2017).

Therefore, the aim of this study is to discover research trends in the field of cyber security with performance analysis and to reveal the intellectual structure of the field of cyber security with scientific mapping, especially for researchers who want to work in the field of cyber security. While performance analysis explains the contributions of research components to the field, scientific mapping focuses on the relationships between research components (Baker et al., 2021; Donthu et al., 2021;). In this regard, the current study was designed by considering the following two research questions:

1. What is the performance analysis of the papers published in cyber security?
 - 1.1. What is the productivity trend of the papers in the field of cyber security by years?
 - 1.2. What is the performance status of journals that publish cyber security studies in the field?
2. What is the intellectual state of the cyber security field?
 - 2.1. What is the relationship between themes in the field of cyber security?

What are the most influential publications in the field of cyber security?

METHOD

In this section, the information about the research method, the universe-sample-study group and the data collection tool are presented respectively.

Research design

A systematic literature review and bibliometric analysis were conducted as part of the study's scope. Bibliometric analysis is a type of statistical analysis that employs data from a database to provide in-depth information on the development of a specific field (Leung et al., 2017). Based on the social, intellectual, and conceptual frameworks of the disciplines, it is an acceptable approach to examine the evolution of scientific disciplines, including themes and authors. (Donthu et al., 2021). The bibliometric analysis allows for the tracking of studies, authors, institutions, and scientific flow concerning a certain scientific topic (Martí-Parreño et al., 2016). Bibliometric studies enable measuring the basic features of scientific publications in certain criteria such as citation, author, co-author, cited bibliography. They also help detect patterns in the study discipline revealing the overall structure of the field through the

interpretation of the findings. (Kasemodel et al., 2016). The research was carried out taking into account the (Donthu et al., 2021) bibliometric analysis guidelines included in the study. Table 1 demonstrates the four stages of the guideline.

Table 1

Bibliometric Analysis Guide (Adapted from Donthu et al., 2021)

Stage 1: Defining purpose and scope	Define the aims and scope of the bibliometric study
Stage 2: Selection of techniques for bibliometric analysis to be used	Select appropriate bibliometric analysis techniques according to the aims of the study
Stage 3: Data collection for bibliometric analysis	Design the search query based on the scope defined in step 1 Select the database according to the adequacy of the scope Collect bibliometric data according to bibliometric analysis technique Clear data.
Stage 4: Report bibliometric analysis findings	Performance Analysis (Summarize performance of productive research components using publication, citation, and publication-citation criteria) Scientific Mapping (Summarize bibliometric structure and intellectual structure using scientific mapping techniques and bibliometric analysis development techniques) Create a bibliometric summary and write a discussion of the findings along with the results

Table 1 presents the first step of the study, in which the aim and scope of the study were determined. This study aims to discover the research trends in cyber security through performance analysis and to reveal the intellectual structure of the cyber security field through scientific mapping. Performance analysis examines the contributions of research constituents to a particular field (Cobo et al., 2011; Ramos-Rodríguez & Ruíz-Navarro, 2004). Countless measures for performance analysis exist. The most prominent measures are the number of publications and citations per year or research constituent; wherein publication is a proxy for productivity, whereas citation is a measure of impact and influence. Other measures, such as citations per publication and the h-index, combine both citations and publications to measure the performance of research constituents (Donthu et al., 2021). To determine the intellectual structure of the cyber security field, the relations between the themes were examined through the author keywords. Author keywords are a clear, representative, and concise description of the research content. Therefore, it makes sense to identify emerging trends of research themes and themes by co-word analysis (Zheng et al., 2016). In addition, the most cited publications were examined using co-citation analysis, and the intellectual structure of the field was attempted to be ascertained. Co-citation analysis is a fundamental technique for scientific mapping that is based on the assumption that citations represent the intellectual connections generated when one publication cites another (Appio et al., 2014). It also defines the intellectual structure of a field of knowledge by determining the quantity and authority of the literature cited. In this analysis, a publication's influence is determined by the number of citations it receives. Research questions and sub-research questions

were developed for this aim. In the second stage, techniques for bibliometric analysis were chosen to meet the aims and scope of the study. Performance analysis was conducted in order to determine the number of publications on cyber security per year (number of publications per year) and in which journal the most publications were made. To determine the intellectual structure of the cyber security field, the most cited publications, the relationship between the themes, and the interaction between the authors were examined. The third stage is the collection of necessary data for the bibliometric analysis techniques chosen in the second stage. At this stage, the database is selected, the basic dataset is filtered and the data is exported from the selected database. This stage involves the construction of the study's database (Waltman, 2016). In the third and fourth stages of the study, the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) procedure, demonstrated in Table 2, was conducted to collect data, create the dataset and report the data (Moher et al., 2009).

Table 2

PRISMA procedure showing the procedure followed in the research [adapted from Moher et al., (2009)]

identification	Records identified by database search (n=15.781) AB=((Cyber security) or (Cyber security) or (Cyber-security))		
Screening	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top;"> Included records (n=15.781) </td> <td style="width: 50%; vertical-align: top;"> Excluded records (9.150) Publications Years: 2022 (132) Document Types: Proceedings Papers (8.311), Review Articles (469), Book Chapters (263), Others (124) Language: Russian (65), Spanish (54), Turkish (18), German (15), Others (69) </td> </tr> </table>	Included records (n=15.781)	Excluded records (9.150) Publications Years: 2022 (132) Document Types: Proceedings Papers (8.311), Review Articles (469), Book Chapters (263), Others (124) Language: Russian (65), Spanish (54), Turkish (18), German (15), Others (69)
Included records (n=15.781)	Excluded records (9.150) Publications Years: 2022 (132) Document Types: Proceedings Papers (8.311), Review Articles (469), Book Chapters (263), Others (124) Language: Russian (65), Spanish (54), Turkish (18), German (15), Others (69)		
Eligibility	Records that meet the criteria (n=6.631)		
Included	Records included in the analysis (n=6.631)		

Studies included in the identification phase of the PRISMA in Table 2 were determined by the search conducted on the WoS database. WoS, Scopus, and Google Scholar are databases that provide bibliometric data for literature search (Abrizah et al., 2013; Mingers & Leydesdorff, 2015). WoS is the first database since the 1900s to include the literature and facilitate bibliometric analysis (Mingers & Leydesdorff, 2015). An important feature of the WoS database is that it includes all article types and indexes authors and bibliographic references for each article (Mongeon & Paul-Hus, 2016). When compared to Scopus or Google Scholar, WoS is said to have the most comprehensive and greatest amount of highly cited articles. (Mingers & Leydesdorff, 2015). For this reason, the WoS database was preferred to search for keywords in this study. Using the advanced search section in the Web of Science (WoS) database, a search was conducted within all fields through the following code line typed in the query preview section: AB=((Cyber security) or (Cyber security) or (Cyber-security)). The goal of creating this code is to search for terms relevant to cyber security in the abstract section. In the literature, cyber

security is also referred to as Cyber security or Cyber-security. At the identification stage, a total of 15.781 articles were retrieved. During the screening stage, these articles were filtered down according to the excluded criteria (Table 1), and 6.631 entries were obtained during the eligibility stage. Following a review of the study abstracts in the included stage, 6.631 were included in the analysis. The inclusion and exclusion criteria are presented in Table 3.

Table 3

Inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Database	WoS	Elsevier's Scopus, Google Scholar, IEEE Explore, ScienceDirect, Association for Computing Machinery (ACM), Springer
Time range	1998-2021	2022
Language	English	Russian, Spanish, German and other languages
Document type	Article	Paper, book chapter and others

The fourth and final stage is to perform the bibliometric analysis and report the findings. At this stage, one or more bibliometric or statistical software tools are used for data analysis. The most used visualization tools are BibExcel, Gephi, Pajek, VOSviewer, Excel, HistCite, SciMat, and the R bibliometrics library. R is a free and open-source tool and offers several packages for effective bibliometric analysis (Aria & Cuccurullo, 2017; Donthu et al., 2021; Firdaus et al., 2019). In this study, R was preferred because it is a well-known software for statistical computing, is free, and allows the integration of various statistical and visualization packages.

FINDINGS

Research findings should be included in this section. APA6 version should be followed for table, shape, graphic, picture, diagram etc. and their impressions. For this, the author guidelines section should be read. Findings can be prepared in sub-headings.

In this section, the findings corresponding to the two research questions determined at the beginning of the study are presented respectively.

Performance Analysis Of The Papers Published On Cyber Security

The performance analysis of the papers published cyber security field was examined according to their productivity trends and the performance status of the journals, and the findings were presented.

Productivity Trend of The Cyber Security Papers Per Year

The study investigated the productivity trend of the cyber security papers per year, and the findings are presented in Figure 3.

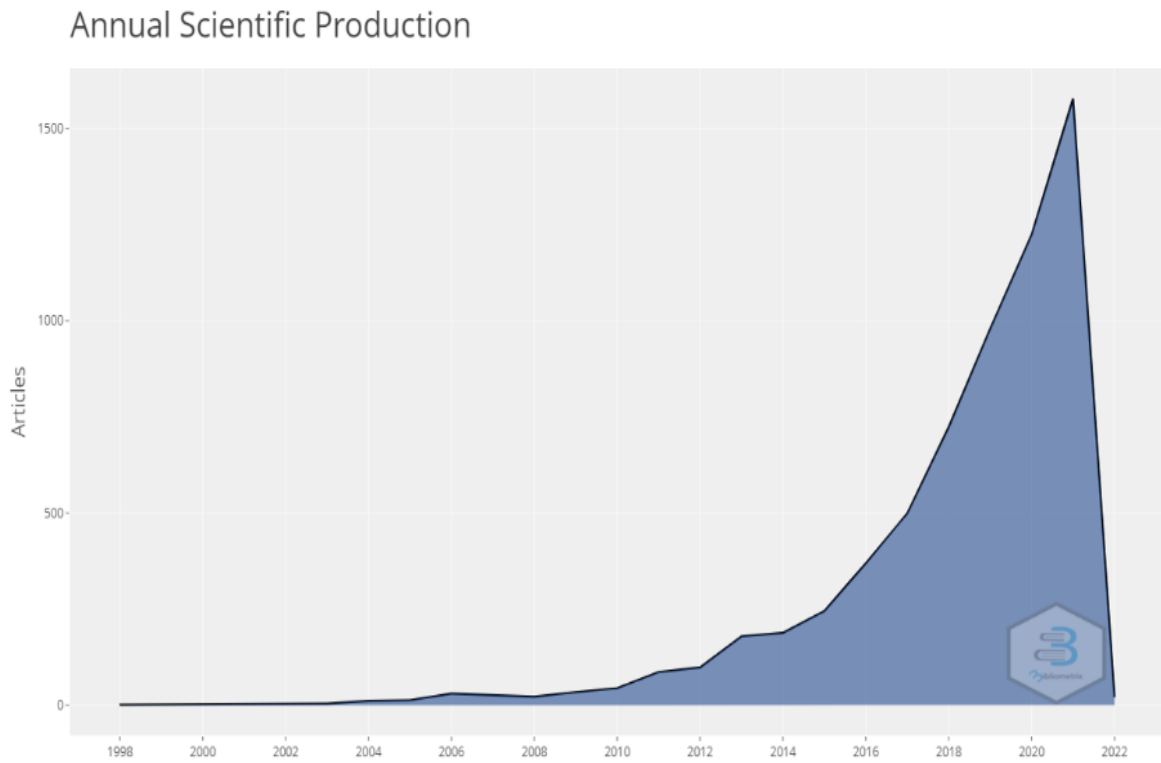
Figure 3*Cyber security annual scientific production (1998–2021)*

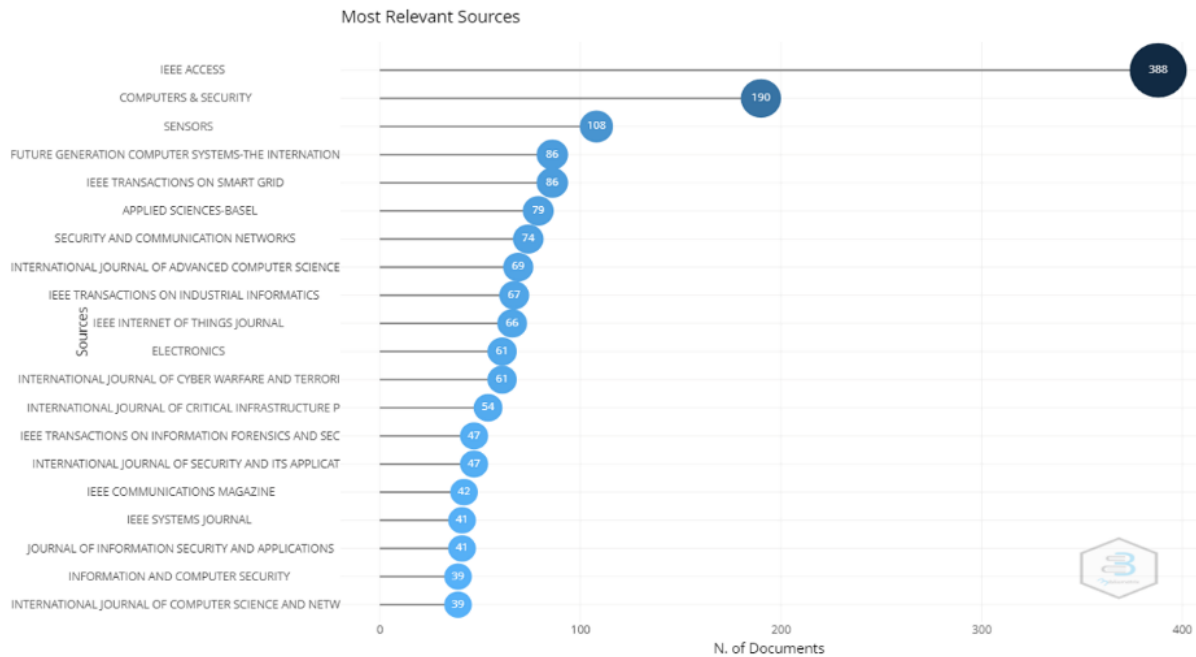
Fig. 3 shows an increasing trend from 1998 to 2021 in cyber security papers found in the WoS database. Although there were minor fluctuations in the number of articles published each year until 2019, there was a significant increase in the number of publications published after 2019. The total number of papers published during this period is 6631, which may be divided into two sub-periods as 1998–2018 and 2019–2021. Although the first period covers twenty years, the number of papers published (2572) is smaller than the number of articles published (4059) in the second era, including the last three years. Cyber security research showed a remarkable development with 1023 articles in 2019 and reached its peak with 1736 articles published in 2021.

The performance status of journals publishing cyber security studies in the field

The leading journals in terms of the number of publications linked to cyber security are investigated in Fig. 4 to establish the performance status of the journals that publish cyber security studies. With 388 articles, IEEE Access takes the first position, followed by Computers & Security with 190 articles, and Sensors in third place with 108 articles.

Figure 2

The relevant sources in terms of the number of publications



The number of papers published is an essential measure for determining the journal's productivity. However, it is not a sufficient criterion on its own since it does not give information regarding the journal's importance or its impact (Akgün, 2017). As a result, the impact of the top ten journals according to the number of publications is investigated in Table 4 below using the h-index, g-index, total number of citations, and publication year. Evaluating the h-index alone would be an inaccurate measure of research evaluation, especially for highly cited journals. A combination of h-index and g-index gives a better measure of global citation performance and individual research impact (Ali, 2021). In his work (Egghe, 2006), Egghe (2006) suggests combining the g-index with the h-index. As a result, the h and g index values were analyzed together in the study.

Table 4

Impact of the journals

Journals	NP	h_ndeks	g_indeks	TC	PY_Start
IEEE Transactions on Smart Grid	86	33	62	3896	2010
IEEE Access	388	29	60	5014	2014
IEEE Internet of Things Journal	66	25	55	3066	2014
Computers & Security	190	32	54	3670	1999
Future Generation Computer Systems-The International Journal of Escience	86	25	46	2336	2012
IEEE Transactions on Industrial Informatics	67	22	39	1644	2013
Applied Sciences-Basel	79	9	16	352	2017
Security and Communication Networks	74	9	15	352	2011

International Journal of Advanced Computer Science and Applications	69	5	7	87	2013
Sensors	108	5	6	48	2018

NP: Number of publication, TC: Total citations, PY_start: Publication year start

Although IEEE Access has the most citations and articles, IEEE Transactions on Smart Grid is the most influential journal in terms of h-index and g-index values. IEEE Access is ranked second, and IEEE Internet of Things Journal is ranked third. Journals (according to 2021) have a minimum of three and a maximum of twenty-two years of history. It is noteworthy that the Computers & Security journal, which ranks fourth in Table 4 and has been published since the notion of cyber security first evolved, has 190 articles on the topic. In contrast, IEEE Access journal, which has been publishing for seven years, has 388 publications. Furthermore, when the IEEE Access journal's g-index and h-index values are considered, it is more influential than the Computers & Security journal.

The intellectual state of the cyber security field

The relationship between themes in the field of cyber security

A co-word analysis was performed to uncover the existing relationships between the themes in cyber security and to detect thematic trends. The results are presented in Fig. 5.

Figure 5

Use of words by years

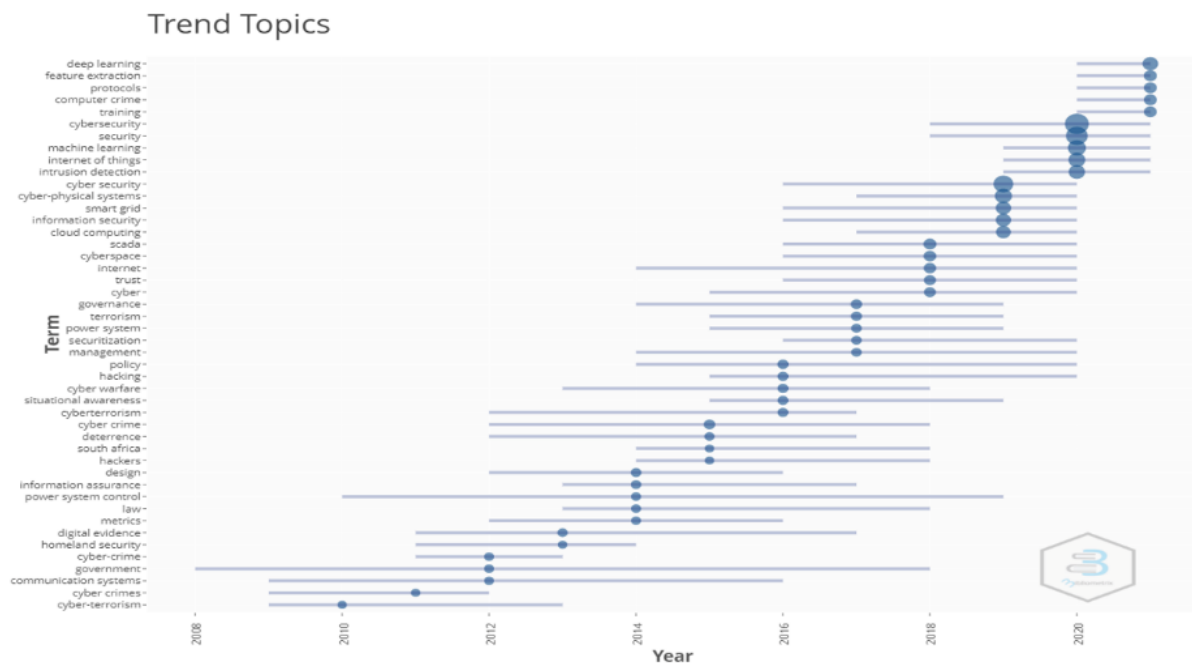


Fig. 5 illustrates the years in which the words were used and which words were used frequently per year. The following terms were used between 2008 and 2021: government, cyber-terrorism, cyber crimes, communication systems, power system control, digital evidence, homeland security, design, metrics, determination, cyberterrorism, information assurance, law, cyber warfare, hackers, south

Africa, policy, governance, management, internet, hacking, situational awareness, terrorism, power system, cyber, securitization, cyberspace, trust, cyber security, smart grid, information security, cyber-physical systems, cloud computing, security, machine learning, internet of things, intrusion detection, deep learning, feature extraction, protocols, computer crime, and training. Furthermore, the word government has been examined in cyber security for a decade. Also, cyber crime (cybercrime, cyber crimes) has been addressed between 2008 and 2018 and has recently obtained its position in the literature as computer crime. The most frequently used words per year are presented in Table 5.

Table 5

Most frequently used words by year

Year	Words
2010	Cyber-terrorism
2011	Cyber-crimes
2012	Cyber crimes, communication systems, government
2013	Digital evidence, homeland security
2014	Design, metrics, law, power system control, information assurance
2015	Cyber crimes, deterrence, hackers, south africa
2016	Cyberterrorism, cyber warfare, policy, hacking, situational awareness
2017	Management, securitization, governance, terrorism, power system
2018	Cyber, trust, internet, cyberspace, scada
2019	Cyber security, cyber-physical systems, smart grid, information security
2020	Cyber security, security, machine learning, internet of things, intrusion detection
2021	Deep learning, feature extraction, protocols, computer crime, training

A co-occurrence analysis demonstrated the relationship between the keywords in Table 5. Fig. 7 shows the findings of the investigation, which highlight some of the main themes in the field of cyber security and their interrelationships. The size of the circles represents the impact of the word clusters and the frequency with which the authors use them in the field. A line connects words to the cluster based on the strength of their association with it. The thickness of the line indicates the intensity of the word's association with the cluster in which it is located. The most commonly used terms were grouped in three clusters, as seen in Fig. 7. Cyber security, security, and machine learning have the largest and most effective word clusters.

The most influential publications in the field of cyber security

The most influential publications in the field were investigated with co-citation analysis to reveal the cyber security field's intellectual status, and the five most-read papers ranked according to citation are given in Table 7.

Table 7

Top five most read papers ranked according to citation

Article Title	Authors	Year	DOI	TC
The internet of things for health care: a comprehensive survey	Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S.	2015	10.1109/ACCESS.2015.2437951	1037
A survey on internet of things: architecture, enabling technologies, security and privacy, and applications.	Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W.	2017	10.1109/JIOT.2017.2683200	970
A survey of data mining and machine learning methods for cyber security intrusion detection	Buczak, A. L., & Guven, E.	2015	10.1109/COMST.2015.2494502	824
Cyber–physical security of a smart grid infrastructure	Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B.	2011	10.1109/JPROC.2011.2161428	615
Cyber–physical system security for the electric power grid.	Sridhar, S., Hahn, A., & Govindarasu, M.	2011	10.1109/JPROC.2011.2165269	577

With 1037 citations, the paper published by Islam et al. in 2015 is the most read according to Table 7. Also, Lin et al. published an article in 2017 with 970 citations. Buczak and Guven's work from 2015 ranks third with 824 citations. The paper by Mo et al., published in 2011, is in fourth place with 615 citations, while the article by Sridhar et al., published in 2012, is in fifth place with 577 citations. In general, current themes in cyber security have been examined, such as the internet of things, machine learning, and big data.

RESULTS, DISCUSSION AND CONCLUSION

This study aimed to discover the research trends in cyber security through performance analysis and reveal the field's intellectual structure via scientific mapping. The contributions of research constituents to the field were analyzed using performance analysis, and the intellectual structure was

examined using scientific mapping, and the findings were presented. The findings were discussed in this perspective considering the research questions.

To establish the performance of articles published in cyber security, the article productivity trend per year and the performances of the journals in which the articles were published the most were investigated. When the article productivity per year in cyber security was evaluated, a fluctuating trend was identified between 1998 and 2021. The number of articles surged dramatically in 2020, after a slow increase until 2018. It is believed that the steady growth till 2018 is due to countries having technology, using technology, and having access to the internet. Given that the internet connects us to the cyber world, a lack of access to technology and internet connection will minimize our vulnerability to cyberattacks. Studies show that the increased usage of information technology and other communication devices has a favorable impact on the expanding trend in cyberspace research (Altarturi et al., 2020; Leung et al., 2017; Serafin-Plasencia et al., 2019;). Given the significant increase in 2020, it's reasonable to assume that the reason is a global pandemic and a better understanding of the necessity of cyber security for both individuals and countries. Cyber-attackers always wait for the best time to strike. Natural disasters, continuing crises, and major public events are all instances of such circumstances. (Tysiac, 2022). As a result of the pandemic, there has been a significant increase in internet usage, and individuals of all ages have been forced to transition to the online environment in many areas, including education, health, trade, banking, lifestyle, and business life. Therefore, the frequency of cyberattacks in the cyber environment has grown, as has the likelihood of successful cyberattacks. (Lallie et al., 2021; Williams et al., 2020). This increase is thought to encourage researchers to conduct cyber security research, thus affecting the number of publications published after 2020.

The leading journals in terms of the number of publications dedicated to cyber security were reviewed in order to establish the performance status of the journals that publish cyber security articles. Accordingly, IEEE Access is ranked top, Computers & Security is second, and Sensors is third. When the influence of the journals is examined, however, this ranking appears to have shifted. IEEE Transactions on Smart Grid ranked first, IEEE Access second, and IEEE Internet of Things Journal third. The disparity in the number of articles is assumed to be related to the publication policies, despite the fact that these journals are the three most influential journals according to the h index and g index values. Generally, the Institute of Electrical and Electronics Engineers (IEEE) publishes these journals (IEEE). IEEE is a non-profit technical organization committed to the development of engineering theory and practice in electrical, electronics, computer, automation, telecommunications, and a variety of other fields. Journals are also included in the Engineering & Computer Science category on Google Scholar. It is possible to state that research on cyber security is mostly conducted in the field of engineering. Also, researchers who wish to publish in cyber security should prefer these journals according to the scope and publication policies of the journals.

Co-word analysis was used to examine the relations between the themes in order to determine the intellectual status of the cyber security field. Considering the terms studies focused per year, the studies initially focused on a certain theme such as cyberterrorism, cybercrime, government. However, the focus then evolved into the following themes: information security, computer security, computer crime, deep learning, machine learning, cloud computing, etc. The reason for this is believed to be that as computers and the internet become more prevalent in our lives, governments become more vulnerable to computer-based attacks. Society has witnessed a rapid and frightening expansion in both information and communication systems, as well as information violations, as a result of the advent of

the internet and social media. Cybercrime progresses along a path that includes advancements in information and communication technology, computer generations, network expansion, and the emergence of anti-security methods (Li, 2017). As a result, it is reasonable to conclude that researchers focus primarily on criminal aspects of cyber security. Today, however, researchers' focus is on current issues related to cyber security such as deep learning, internet of things, machine learning, etc.

To identify the most influential publications in the field of cyber security and to understand the intellectual dynamics of the field, co-citation analysis was carried out. Co-citation analysis was used to determine the most influential publications on cyber security, and the most cited paper was 'The Internet of Things for Health Care: a Comprehensive Survey' by Islam et al. (Islam et al., 2015). The paper was published in the journal *IEEE Access* in 2015. From a healthcare perspective, the study examines many security and privacy issues of the IoT, including security requirements, threat models, and classification of the attacks. Although the Internet of Things (IoT) is widely referred to in healthcare (Samhale, 2022) it has yet to be thoroughly studied theoretically and empirically in the context of security. Security is critical for IoT applications, according to Al-Fuqaha et al. (Al-Fuqaha et al., 2015). Calvillo-Arbizu et al. (2021) noted in their study that IoT in healthcare services has significant potential, although it lags behind other fields. IoT is one of the most popular technological developments in healthcare, according to Ansari et al. (Ansari et al., 2020), although its implementation seldom matches sectoral standards. As a result, the article's influence may be due to the fact that it filled a gap in the literature regarding the security aspect of the internet of things, which is a critical issue in the field of health. The most cited articles were all published between 2011 and 2017, and they addressed current themes including the internet of things, security, data mining, and machine learning. This finding confirms the previous research finding. Considering the study's time frame as a limitation, it is important to remember that the number of citations will alter as well.

Within the constraints of some limitations, the research reveals the present state of the cyber security field and research trends. In this regard, the study is limited to the publications cyber security published between 1998 and 2021 and found in the WoS database and whose abstracts include the terms cyber security, cyber-security, or cyber security. Therefore, it is recommended that the database and document type in future research be expanded. Although WoS is considered the most effective tool for bibliometric analysis (Alnajem, 2021), working with a single database may have missed some important research on cyber security. In order to better understand the studies carried out, other types of documents can be included in the research and a systematic literature review can be conducted to strengthen and improve the findings of this research. The study is limited to co-citation analysis and co-word analysis in terms of bibliometric analysis. Therefore, it will be beneficial for the field to examine and support the studies conducted in the field of cyber security qualitatively.

Due to the increasing attacks and threats in cyberspace, the security of not only institutions but also personal data has gained extra importance. Although there is increasing interest in the field of cyber security, there is still a need to address relevant research gaps. Although most current research deals with the different sub-dimensions of cybersecurity, the overall state of the cybersecurity field remains completely unexplored. Therefore, there is a work gap in this area. In this study, first of all, the performance status and intellectual status of the cyber security field have been revealed in order to help researchers who want to do research in the field of cyber security. So this study is designed to be implemented in the first phase of the development of a new study. According to the results of the study, researchers can investigate the reasons for this situation (not mentioned in the article) by examining how many articles were produced in which years. In addition, by taking into account the

performance status of the journals, they can examine the journal that has the most publications on cyber security. They can even review these journals first to submit their publications. In our study, the most frequently used words by the authors and the relationship of these words with each other were revealed, and the trends of the field were revealed. By taking these words into account, researchers can choose research topics that dominate the field and determine which subtopics they can work with. Considering the result of the study, the issue of how security is ensured, especially in the Internet of Things, can be examined. The result of this study may enable the relevant references of the literature to be taken into account for the construction of new studies. Researchers can access the most cited articles and start the literature search from these articles. In the study, author collaboration, which is one of the factors that will reveal the intellectual state, was not mentioned. Researchers can reflect social ties by revealing the relationship and social networks between authors with co-author analysis. The enhanced understanding of science through bibliometric analysis can facilitate knowledge creation.

REFERENCES

- Abrizah, A., Zainab, A. N., Kiran, K., & Raj, R. G. (2013). LIS journals scientific impact and subject categorization: A comparison between Web of Science and Scopus. *Scientometrics*, *94*(2), 721–740. <https://doi.org/10.1007/s11192-012-0813-7>
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. <https://doi.org/10.1109/COMST.2015.2444095>
- Ali, M. J. (2021). Understanding the ‘g-index’ and the ‘e-index.’ *Seminars in Ophthalmology*, *36*(4), 139–139. <https://doi.org/10.1080/08820538.2021.1922975>
- Alnajem, M., Mostafa, M. M., & ElMelegy, A. R. (2021). Mapping the first decade of circular economy research: A bibliometric network analysis. *Journal of Industrial and Production Engineering*, *38*(1), 29–50. <https://doi.org/10.1080/21681015.2020.1838632>
- Altarturi, H. H. M., Saadoon, M., & Anuar, N. B. (2020). Cyber parental control: A bibliometric study. *Children and Youth Services Review*, *116*, 105134. <https://doi.org/10.1016/j.childyouth.2020.105134>
- Ansari, S., Aslam, T., Poncela, J., Otero, P., & Ansari, A. (2020). Internet of Things-Based Healthcare Applications [Chapter]. *IoT Architectures, Models, and Platforms for Smart City Applications*; IGI Global. <https://doi.org/10.4018/978-1-7998-1253-1.ch001>
- Appio, F. P., Cesaroni, F., & Di Minin, A. (2014). Visualizing the structure and bridges of the intellectual property management and strategy literature: A document co-citation analysis. *Scientometrics*, *101*(1), 623–661. <https://doi.org/10.1007/s11192-014-1329-0>
- Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959–975. <https://doi.org/10.1016/j.joi.2017.08.007>
- Baker, H. K., Kumar, S., & Pandey, N. (2021). Forty years of the Journal of Futures Markets: A bibliometric overview. *Journal of Futures Markets*, *41*(7), 1027–1054. <https://doi.org/10.1002/fut.22211>

- Bradea, I., Delcea, C., & Paun, R. (2015). Healthcare Risk Management Analysis—A Bibliometric Approach. *Journal of Eastern Europe Research in Business & Economics*, 2015, 169472. <https://doi.org/10.5171/2015.169472>
- Calvillo-Arbizu, J., Román-Martínez, I., & Reina-Tosina, J. (2021). Internet of things in health: Requirements, issues, and gaps. *Computer Methods and Programs in Biomedicine*, 208, 106231. <https://doi.org/10.1016/j.cmpb.2021.106231>
- Choi, H., & Varian, H. (2012). Predicting the present with Google Trends. *Economic record*, 88, 2-9. <https://doi.org/10.1111/j.1475-4932.2012.00809.x>
- Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field. *Journal of Informetrics*, 5(1), 146–166. <https://doi.org/10.1016/j.joi.2010.10.002>
- 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>
- Egghe, L. (2006). Theory and practise of the g-index. *Scientometrics*, 69(1), 131–152. <https://doi.org/10.1007/s11192-006-0144-7>
- Firdaus, A., Razak, M. F. A., Feizollah, A., Hashem, I. A. T., Hazim, M., & Anuar, N. B. (2019). The rise of “blockchain”: Bibliometric analysis of blockchain study. *Scientometrics*, 120(3), 1289–1331. <https://doi.org/10.1007/s11192-019-03170-4>
- Gill, J., Okere, I., Haddadpajouh, H., & Dehghantanha, A. (2018). Mobile Forensics: A Bibliometric Analysis. In *Advances in Information Security* (pp. 297–310). https://doi.org/10.1007/978-3-319-73951-9_15
- Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: A bibliometric analysis. *SN Social Sciences*, 2(1), 4. <https://doi.org/10.1007/s43545-021-00305-4>
- CISA. (n.d.). Retrieved March 4, 2022, from <https://www.cisa.gov/> How cybercriminals prey on victims of natural disasters. (2018, September 14). *Journal of Accountancy*. <https://www.journalofaccountancy.com/news/2018/sep/cyber-criminals-prey-on-natural-disaster-victims-201819720.html>
- Islam, S. M. R., Kwak, D., Kabir, MD. H., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, 3, 678–708. <https://doi.org/10.1109/ACCESS.2015.2437951>
- Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health Care and Cybersecurity: Bibliometric Analysis of the Literature. *Journal of Medical Internet Research*, 21, e12644. <https://doi.org/10.2196/jmir.12644>
- Kasemodel, M.-G. C., Makishi, F., Souza, R. C., & Silva, V.-L. (2016). Following the trail of crumbs: A bibliometric study on consumer behavior in the Food Science and Technology field. *International Journal of Food Studies*, 5(1), Article 1. <https://doi.org/10.7455/ijfs/5.1.2016.a7>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks

- during the pandemic. *Computers & Security*, 105, 102248.
<https://doi.org/10.1016/j.cose.2021.102248>
- Leung, X. Y., Sun, J., & Bai, B. (2017). Bibliometrics of social media research: A co-citation and co-word analysis. *International Journal of Hospitality Management*, 66, 35–45.
<https://doi.org/10.1016/j.ijhm.2017.06.012>
- Li, J. X. (2017). Cyber Crime And Legal Countermeasures: A Historical Analysis.
<https://doi.org/10.5281/ZENODO.1034658>
- Martí-Parreño, J., Méndez-Ibáñez, E., & Alonso-Arroyo, A. (2016). The use of gamification in education: a bibliometric and text mining analysis. *Journal of computer assisted learning*, 32(6), 663-676. <https://doi.org/10.1111/jcal.12161>
- Mingers, J., & Leydesdorff, L. (2015). A review of theory and practice in scientometrics. *European Journal of Operational Research*, 246(1), 1–19. <https://doi.org/10.1016/j.ejor.2015.04.002>
- Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & and the PRISMA Group. (2009). Reprint— Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Physical Therapy*, 89(9), 873–880. <https://doi.org/10.1093/ptj/89.9.873>
- Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics*, 106(1), 213–228. <https://doi.org/10.1007/s11192-015-1765-5>
- Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343.
<https://doi.org/10.1016/j.ijcci.2021.100343>
- Ramos-Rodríguez, A.-R., & Ruíz-Navarro, J. (2004). Changes in the intellectual structure of strategic management research: A bibliometric study of the Strategic Management Journal, 1980–2000. *Strategic Management Journal*, 25(10), 981–1004. <https://doi.org/10.1002/smj.397>
- Razak, M. F. A., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of “malware”: Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, 75, 58–76.
<https://doi.org/10.1016/j.jnca.2016.08.022>
- Samhale, K. (2022). The impact of trust in the internet of things for health on user engagement. *Digital Business*, 2(1), 100021. <https://doi.org/10.1016/j.digbus.2022.100021>
- Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, 12, 53.
<https://doi.org/10.15394/jdfsl.2017.1476>
- Serafin Plasencia, M., Garcia-Vargas, G., García-Chitiva, M., Caicedo, M., & Correa, J. C. (2018). Cyberbehavior: A Bibliometric Analysis. <https://doi.org/10.31234/osf.io/prfcw>
- Siber güvenlik. (n.d.). ITU. Retrieved January 26, 2022, from <https://www.itu.int:443/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>
- Sule, M.-J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends. *Technology in Society*, 67, 101734.
<https://doi.org/10.1016/j.techsoc.2021.101734>

- Suryotrisongko, H., & Musashi, Y. (2019). Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective. 2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA), 162–167. <https://doi.org/10.1109/SOCA.2019.00031>
- Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cybersecurity implications for Australian small businesses. *Computers & Security*, 109, 102385. <https://doi.org/10.1016/j.cose.2021.102385>
- Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, 14(3), 207–222. <https://doi.org/10.1111/1467-8551.00375>
- TÜİK Kurumsal. (n.d.). Retrieved January 26, 2022, from [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanım-Arastirmasi-2018-27819](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanım-Arastirmasi-2018-27819)
- Waltman, L. (2016). A review of the literature on citation impact indicators. *Journal of Informetrics*, 10(2), 365–391. <https://doi.org/10.1016/j.joi.2016.02.007>
- Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research*, 22(9), e23692. <https://doi.org/10.2196/23692>
- Zheng, X., Le, Y., Chan, A. P. C., Hu, Y., & Li, Y. (2016). Review of the application of social network analysis (SNA) in construction project management research. *International Journal of Project Management*, 34(7), 1214–1225. <https://doi.org/10.1016/j.ijproman.2016.06.005>

Author Contributions

The article has a single author. The author has seen the final version of the article and approved its publication.

Conflict of Interest

No potential conflict of interest was declared by the author.

Supporting Individuals or Organizations

No grants were received from any public, private or non-profit organizations for this research.

Ethical Approval and Participant Consent

Ethical Approval and Participant Consent information is not needed for this article.

Copyright Statement

Authors own the copyright of their work published in the journal and their work is published under the CC BY-NC 4.0 license.

Plagiarism Statement

Similarity rates of this article was scanned by the iThenticate software. No plagiarism detected.

Availability of Data and Materials

Not applicable.

Acknowledgements

No acknowledgements.