REVISTA CIENTÍFICA

Vol. 21, No.3 (2025) septiembre-diciembre, ISSN electrónico: 1683-8947

bibliotecas anales de investigación

BIBLIOTECA NACIONAL DE CUBA JOSÉ MARTÍ

FROM FOUNDATIONS TO FRONTIERS: A BIBLIOMETRIC EXAMINATION OF CYBER THREAT INTELLIGENCE STUDIES

DESDE LOS FUNDAMENTOS A LAS FRONTERAS: UN EXAMEN BIBLIOMÉTRICO DE ESTUDIOS DE INTELIGENCIA SOBRE CIBERAMENAZAS

Jeena Joseph
Marian College Kuttikkanam Autonomous, Kerala, India
jeenajoseph005@gmail.com
https://orcid.org/0000-0003-4070-5868

Binu Thomas
Marian College Kuttikkanam Autonomous, Kerala, India
binu.thomas@mariancollege.org
https://orcid.org/0000-0003-1594-2159

Jobin Jose
Marian College Kuttikkanam Autonomous, Kerala, India
jobin.jose@mariancollege.org
https://orcid.org/0000-0003-1596-733X

Received: 3 de febrero 2025
Revised: 14 mayo de 2025
Approved: 27 de agosto de 2025

How to cite: Joseph J; Thomas, B. & Jobin J. (2025). From foundations to frontiers: a bibliometric examination of cyber threat intelligence studies. *Bibliotecas. Anales de Investigacion;21*(3), 1-19

ABSTRACT

Objective. Cyber threat intelligence (CTI), which focuses on gathering, analyzing, and sharing data on new threats and adversaries, has become a crucial area of cybersecurity. Understanding the academic and practical environment of CTI is essential given the growing relevance of proactive defense measures and the developing cyber threats. A thorough bibliometric examination of the CTI literature from its inception, encompassing articles from 2012 through 2023, is presented in this paper. **Design/Methodology/Approach**. Using a collection of over 611 scholarly publications from the Scopus database, we aim to monitor this developing subject's growth, trends, and research tendencies. Authors, groups, and countries are identified as significant contributors to CTI research in our analysis, along with recurring themes and topics that have influenced the discourse over time. **Results/Discusion**. Key findings indicate a significant rise in CTI publications following 2012, with a clear shift from theoretical discussions to practical applications and real-world case studies. Collaboration networks among researchers and institutions highlight the interdisciplinary nature of CTI, drawing expertise from fields such as computer science, information security, and international relations. The study also identifies emerging areas of interest, including the integration of artificial intelligence in CTI and the challenges of threat intelligence sharing in a globalized digital landscape.

Conclusions. In conclusion, the bibliometric study underscores the dynamic and evolving nature of cyber threat intelligence, highlighting its growing significance in the fight against cyber threats. Continuous research, interdisciplinary collaboration, and innovation are vital for staying ahead of these threats and safeguarding digital assets in an increasingly interconnected world. **Originality/Value**. By providing a holistic overview of the CTI research landscape, this bibliometric analysis offers valuable insights for scholars, practitioners, and policymakers engaged in ongoing efforts to enhance cyber resilience and security.
KEYWORDS: Cyber threat intelligence (CTI); bibliometric analysis; cybersecurity

RESUMEN

Objetivo. La inteligencia de ciberamenazas (CTI), que se centra en la recopilación, el análisis y el intercambio de datos sobre nuevas amenazas y adversarios, se ha convertido en un área crucial de la ciberseguridad. Comprender el entorno académico y práctico de la CTI es esencial dada la creciente relevancia de las medidas de defensa proactiva y el desarrollo de las ciberamenazas. En este artículo se presenta un análisis bibliométrico exhaustivo de la literatura sobre CTI desde su inicio, que abarca artículos de 2012 a 2023. **Diseño/Metodología/Enfoque**. Utilizando una colección de más de 611 publicaciones académicas de la base de datos Scopus, nuestro objetivo es monitorear el crecimiento, las tendencias y las tendencias de investigación de este tema en desarrollo. En nuestro análisis, se identifican autores, grupos y países como contribuyentes significativos a la investigación sobre CTI, junto con temas recurrentes que han influido en el discurso a lo largo del tiempo. **Resultados/Discusión.** Los hallazgos clave indican un aumento significativo en las publicaciones sobre CTI desde 2012, con una clara transición de las discusiones teóricas a las aplicaciones prácticas y los estudios de casos reales. Las redes de colaboración entre investigadores e instituciones resaltan la naturaleza interdisciplinaria de la CTI, aprovechando la experiencia de campos como la informática, la seguridad de la información y las relaciones internacionales. El estudio también identifica áreas emergentes de interés, incluyendo la integración de la inteligencia artificial en la CTI y los desafíos del intercambio de inteligencia sobre amenazas en un panorama digital globalizado. **Conclusiones.** En conclusión, el estudio bibliométrico subraya la naturaleza dinámica y evolutiva de la inteligencia sobre ciberamenazas, destacando su creciente importancia en la lucha contra las ciberamenazas. La investigación continua, la colaboración interdisciplinaria y la innovación son vitales para anticiparse a estas amenazas y proteger los activos digitales en un mundo cada vez más interconectado. **Originalidad/Valor.** Al proporcionar una visión general del panorama de la investigación sobre CTI, este análisis bibliométrico ofrece información valiosa para académicos, profesionales y legisladores que participan en esfuerzos continuos para mejorar la ciberresiliencia y la seguridad.
PALABRAS CLAVE: Inteligencia sobre ciberamenazas (CTI); análisis bibliométrico; Ciberseguridad

INTRODUCTION

The widespread use of the internet has revolutionized how we communicate, do business, and even wage war in the contemporary digital age, when information technology is deeply woven into society (Conti *et al.*, 2018). Cyberspace has become a crucial area for both opportunity and danger as our globe gets more interconnected (Sufi, 2023). The internet has brought us previously unheard-of conveniences and efficiency. However, it has also given rise to a new frontier of risks that cut beyond national boundaries and threaten the fundamental underpinnings of our digital existence (Wagner *et al.*, 2019). The term "Cyber Threat Intelligence" (CTI) is prominent in this setting.

Cyber threat intelligence is crucial in the continuous struggle to protect our digital ecosystem (Lee, 2023). This study goes into the complex world of CTI, examining its underlying ideas, practices, and unquestionable importance in the current cybersecurity environment. The need for a proactive, educated, and intelligence-driven approach to cybersecurity has never been more pressing in a time of unrelenting assaults, data breaches, and an intensifying arms race between attackers and defenders (Dennehy *et al.*, 2022).

CTI provides security professionals and decision-makers with actionable insights that help companies stay one step ahead of cyber threats by leveraging the power of information, data analysis, and cutting-edge technologies (Schlette *et al.*, 2021). In order to give direction to researchers in this area, this article aims to

clarify the nuances of cyber threat intelligence, focusing on the growth of scientific production, combinations of different keywords in CTI, article citations, etc.

Bibliometric analysis refers to the quantitative assessment of scientific literature, aiming to evaluate the impact, structure, and trends in research publications (Bales *et al.*, 2020; Chen *et al.*, 2014; Dibbern *et al.*, 2023; Fauzi, 2023; Mukherjee, 2020; Singh *et al.*, 2022; Tomaszewski, 2023). Bibliometric analysis provides insights into the prominence and influence of specific articles, journals, researchers, or institutions within a particular field or discipline by analyzing metrics such as citation counts, publication frequencies, and authorship patterns. This method is commonly used to gauge the evolution of research topics over time, identify core researchers and institutions, and inform research policy and funding decisions (Al Mamun *et al.*, 2022; Donthu *et al.*, 2021; Godin, 2006; Pinto *et al.*, 2019; Rojas-Sánchez *et al.*, 2023; Sharma *et al.*, 2023).

The Bibliometrix R-package's GUI, Biblioshiny, is a graphical user interface (GUI). A thorough bibliometric study of scientific literature is possible using the bibliometrix program (Racine, 2012; Salim *et al.*, 2019; Souza de Cursi, 2023). While Bibliometrix offers a comprehensive range of tools for those acquainted with R programming, biblioshiny makes these tools available to people who may not be comfortable with coding by delivering a more user-friendly, web-based interface (Agbo *et al.*, 2021; Aria and Cuccurullo, 2017; Shekhar and Shah, 2023).

Bibliometric networks may be visualized and examined using the software program VOSviewer (Barrot, 2023; Dao *et al.*, 2023; van Eck and Waltman, 2014; Sawangwong and Chaopaisarn, 2023; Waltman *et al.*, 2010). Data on publications, authors, journals, and phrases taken from publication titles and abstracts are just a few examples of the data that may be used to build these networks. Due to its capacity to manage big datasets and provide understandable visualizations, VOSviewer is particularly well-liked by academics and industry experts in bibliometrics and scientometrics (Abbas *et al.*, 2021; Guleria and Kaur, 2021; Husaeni and Nandiyanto, 2022; Nandiyanto *et al.*, 2021; Thomson *et al.*, 2023).

The research objectives for the bibliometric analysis of cyber threat intelligence are:

- Historical Overview: To trace the chronological development and growth of research on cyber threat intelligence, identifying critical periods of increased activity or shifts in focus.
- Key Publications and Journals: To determine the most influential journals, conferences, and publications that have significantly contributed to the field of cyber threat intelligence.
- Collaboration Analysis: To identify and visualize collaboration networks, understanding which institutions, countries, or authors frequently collaborate on cyber threat intelligence research.
- Keyword and Topic Analysis: To extract and analyze the most frequently used keywords and topics, providing insights into the main themes, methodologies, tools, and techniques associated with cyber threat intelligence.
- Citation Analysis: To identify the most cited papers, authors, and journals in the field, indicating the foundational and impactful research on cyber threat intelligence.
- Geographical Distribution: To map the global distribution of cyber threat intelligence research, highlighting regions or countries leading or emerging in this domain.
- Research Gaps and Opportunities: To pinpoint areas within cyber threat intelligence that are under-researched, suggesting potential avenues for future studies and innovations.
- Interdisciplinary Connections: To explore how cyber threat intelligence research intersects with other disciplines, such as cybersecurity, information technology, criminology, and geopolitics.

Review of literature

Abu, et al. (2018), recognized threat intelligence products and services like threat intelligence data feeds, standards, and CTI tools. They have discovered that specific sectors attempt to provide only pertinent threat intelligence data streams, including the Financial Services Information on the major significant dangers the international financial services industry faces. They define four research problems in cyber threat intelligence and examine recent work done in each area after reviewing the CTI definition, standards, and technologies (Abu *et al.*, 2018).

Sean Barnum unveiled the Structured Threat Information eXpression (STIXTM) endeavor to define and establish a language to describe structured threat information as collaborative, rapidly changing, and community-driven. The STIX language aims to be expressive, adaptable, extensible, automatable, and human-readable to represent the whole range of cyber threat information. Despite being relatively recent and expanding as a part of an open, collaborative community, it is diligently explored for acceptance by a broad spectrum of cyber threat-related organizations and groups globally (Barnum, 2012).

Mavroeidis, V., and Bromander, S. advocate using ontologies, sharing standards, and taxonomies in their research study. They presented the Cyber Threat Intelligence (CTI) paradigm, which allows cyber defenders to examine their threat intelligence capabilities and comprehend their position about the constantly shifting cyber threat landscape. Ontologies, sharing standards, and other current taxonomies pertinent to cyber threat intelligence may be analyzed and evaluated using the model. They stress the importance of creating a multi-layered cyber threat intelligence ontology based on the CTI model as the basis for future studies (V. Mavroeidis and S. Bromander, 2017).

In their research article Schlette, D et al. suggested standardization of the security incident response perspective. They introduced 18 core concepts to establish and assess current standardization approaches in CTI. They also provided a detailed analysis of 6 incident response formats in the areas of cyber threat. They also demonstrated how core concepts can determine a suitable format for a given use case by synthesizing structural elements and identifying the format deficiencies. The findings consistently focus on incident response actions within all formats, while organizations can leverage and combine multiple formats (D. Schlette *et al.*, 2021).

The commercial organizations adopting the best cyber security standards cannot withstand sophisticated cyber-attacks. Kotsias, J et al. developed procedures and guidelines for directing a sizeable multinational finance corporation to adopt and integrate CTI into their operations. This will transform cybersecurity-related practices and behavior in the organization to mitigate modern security threats. This research contributed practical know-how on the organizational adoption and integration of CTI. A transformation of cybersecurity practice and enterprise-wide implementation of a novel solution to package CTI for commercial contexts was suggested. The study focuses on commercial organizations' inputs, processes, and outputs during online transactions (Kotsias *et al.*, 2023).

This study by Kayode-Ajala explores how Cyber Threat Intelligence (CTI) might strengthen the security framework of financial firms and highlights significant obstacles that might prevent its successful deployment. CTI offers the financial sector several benefits, including real-time threat information that actively empowers institutions to defend against cyberattacks. Offering information about attacks in their context dramatically boosts the effectiveness of incident response teams. Furthermore, CTI helps organizations comply with legislative frameworks by offering insights into potential hazards. Other applications include improving fraud detection capabilities through data correlation, evaluating and managing vendor risks, and allocating resources to address the most urgent cyber threats (Kayode-Ajala, 2023).

Application and corresponding metadata are analyzed for potential risks as part of cyber threat intelligence. Static malware can be located in Windows executable files by analyzing Portable Executable (PE) program file headers. A new dataset referred to as SOMLAP (Swarm Optimization and Machine Learning Applied to PE Malware Detection) was produced using a critical analysis as a valuable supplement to the benchmark dataset in the work by Santosh Jhansi Kattamuri et al. (Kattamuri *et al.*, 2023). The SOMLAP data comprises 51,409 samples of pure PE file header characteristics, encompassing benign and malicious files, with 108 pure PE file header attributes. Additionally, they improved the Malware Detection System's (MDS) speed by minimizing features using swarm optimization methods, including Ant Colony Optimization (ACO) and Cuckoo Search Optimization (CSO).

METHODOLOGY

We chose the Scopus database for our study due to its comprehensive coverage of scientific literature across various disciplines. A systematic search was conducted using the keyword "cyber threat intelligence." This search encompassed all languages and was narrowed to journal articles and conference papers. All relevant metadata, including titles, authors, affiliations, keywords, abstracts, and citations, were extracted from the Scopus database. Duplicate entries were identified and removed. Inconsistencies in author names and affiliations were rectified. Altogether, we amassed 611 articles from 299 distinct sources, spanning 2012 to 2023. The findings were recorded in a 'CSV' file, and we conducted a bibliometric analysis of the gathered data utilizing VOSviewer version 1.6.19 and Biblioshiny software. Figure 1 illustrates our methodology visually, while Table 1 furnishes comprehensive information concerning our investigation's crucial elements and facets.

Figure 1. *The methodology phases*

Table 1. *Essential aspects of the investigation*

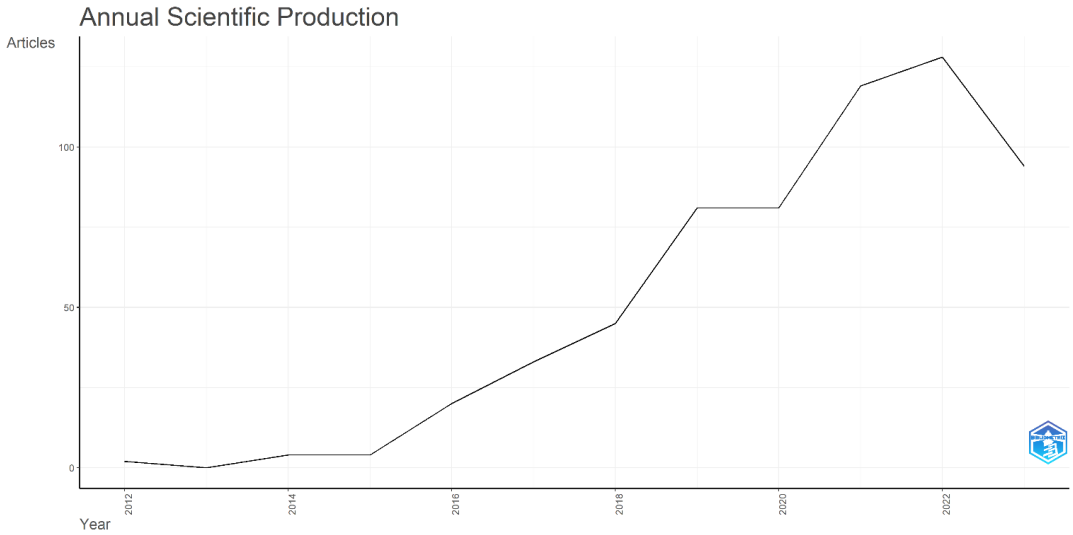
Description	**Results**
Search Query	TITLE-ABS-KEY ("cyber threat intelligence") AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar"))
Main Information about Data	
Timespan	2012:2023
Sources (Journals, Books, etc)	299
Documents	611
Annual Growth Rate %	41.91
Document Average Age	2.6
Average citations per doc	8.62
References	16966
Document Contents	
Keywords Plus (ID)	2875
Author's Keywords (DE)	1361
Authors	
Authors	1659
Authors of single-authored docs	25
Authors Collaboration	
Single-authored docs	27
Co-Authors per Doc	3.94
International co-authorships %	22.91
Document Types	
Article	222
conference paper	389

RESULTS

Annual Scientific Production

Figure 2 depicts the yearly tally of scientific articles from 2012 to 2023, as Biblioshiny shows. There was a significant increase in articles from 2012 to 2022. The peak was reached in 2022 with 128 articles, followed by 119 in 2021 and 94 in 2023. The graph highlights the growing importance of cyber threat intelligence in the recent era. Over the past decade, there has been a steady rise in research output. The annual growth rate averages 41.91%, which could be attributed to better research methods, increased funding, or a growing body of researchers. Consistent publication growth over the years highlights the escalating significance of cyber threat intelligence. This could reflect the increasing cyber threats globally, necessitating more research and understanding.

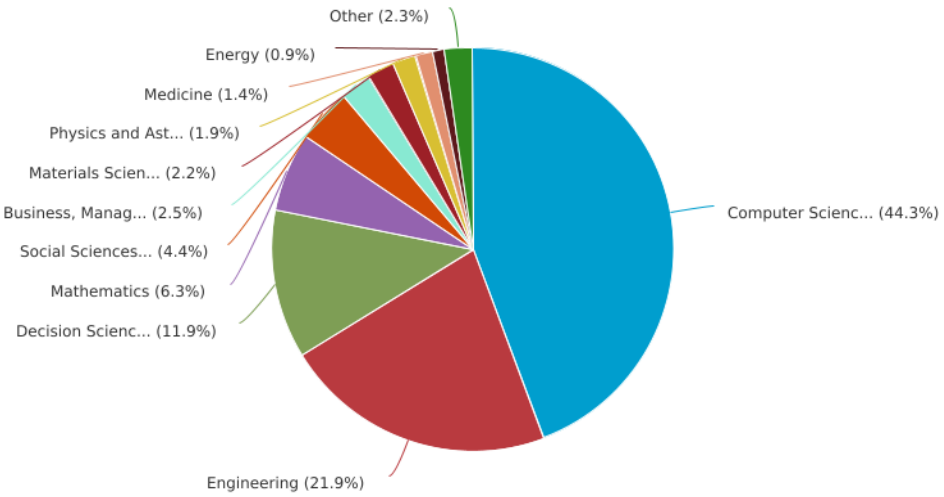
Figure 2. *Yearly scientific output from 2012 to 2023 illustrated using Biblioshiny*



Subject Area Analysis

Figure 3 displays a pie chart depicting the distribution of subject areas in cyber threat intelligence. The field of Computer Science leads with 574 papers, making up 44.3% of the total. Following in second is Engineering, with 284 papers, representing 21.9%. Other significant domains where cyber threat intelligence is utilized include Decision Sciences with 154 papers, Mathematics with 82, Social Sciences with 57, Business, Management and Accounting with 32, Materials Science with 29, Physics and Astronomy with 24, Medicine with 18, Energy with 12, Chemical Engineering with 7, Arts and Humanities with 4, Chemistry with 4, Economics, Econometrics and Finance with 4, Biochemistry, Genetics and Molecular Biology with 3, Environmental Science with 3, Psychology with 2, Health Professions with 1, Multidisciplinary with 1, and Neuroscience with 1.

Figure 3. *Documents by subject area*



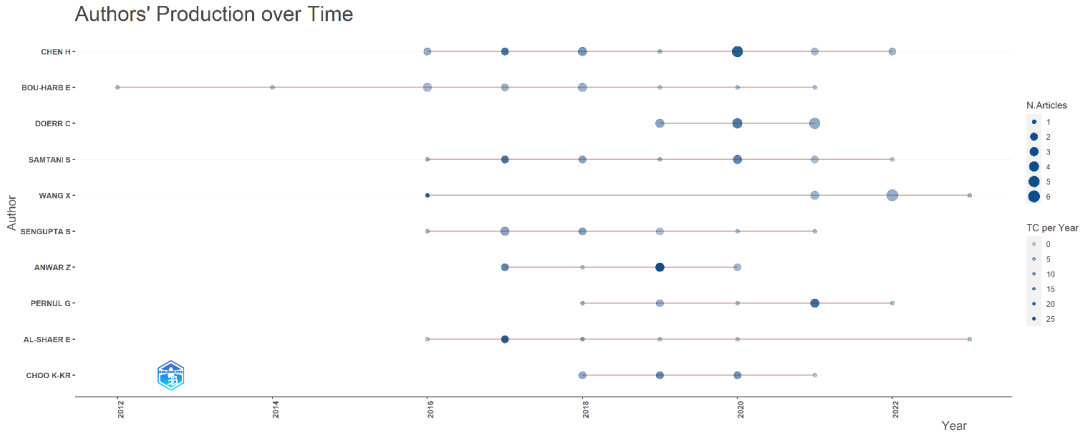
Most Significant Authors

A total of 1,659 authors contributed to the study of cyber threat intelligence. The number of their publications indicates their significance in the field. Chen H was the top author with 17 papers, followed by Bou-Harb E with 13. Doerr C. and Samtani S. both contributed 12 papers. Table 2 provides an overview of the top authors' publication counts. Their expertise and depth of knowledge have established them as leading experts in the area, amplifying their impact. Figure 4 displays the publication trends of these authors, emphasizing their yearly article contributions.

Table 2. *The top authors*

Authors	**Articles**
Chen H	17
Bou-Harb E	13
Doerr C	12
Samtani S	12
Wang X	11
Sengupta S	10
Anwar Z	8
Pernul G	8
Al-Shaer E	7
Choo K-Kr	7
Debbabi M	7
Liu J	7
Wang J	7
Wang S	7

Figure 4. *Authors' Production over Time*



Most relevant sources and affiliations

We examined 299 journal references and gathered 611 papers. The ACM International Conference Proceeding Series was the most significant contributor, offering 38 papers. Following that, the Lecture Notes in Computer Science (which includes subseries like Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) provided 26 papers. The top 10 journals with the highest number of research articles on Cyber Threat Intelligence are showcased in Figure 5.

Figure 5. *The ten leading sources based on the number of publications*

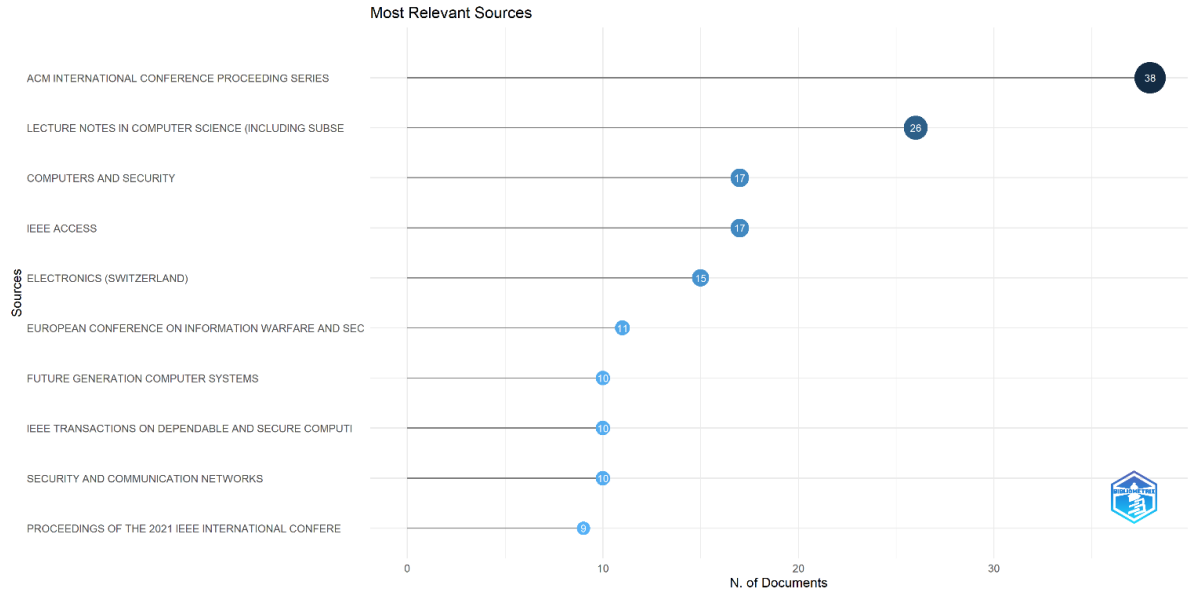
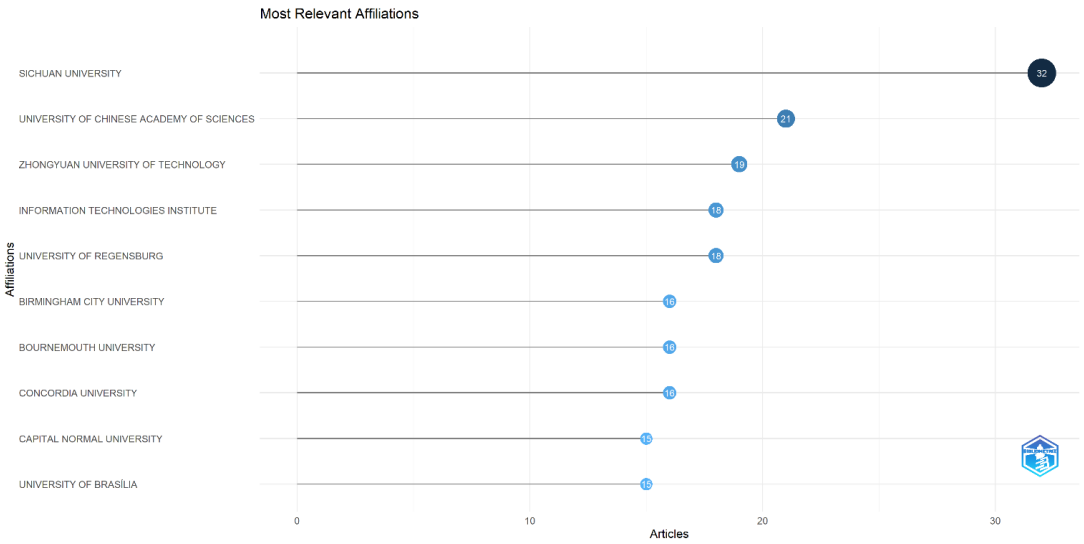


Figure 6 highlights the foremost institutions in Cyber Threat Intelligence. Sichuan University leads with 32 publications, while the University of Chinese Academy of Sciences follows with 21. Other notable institutions in this domain include Zhongyuan University of Technology with 19 papers, Information Technologies Institute and University of Regensburg both with 18, Birmingham City University, Bournemouth University, and Concordia University each with 16, and both Capital Normal University and University of Brasília with 15 papers each.

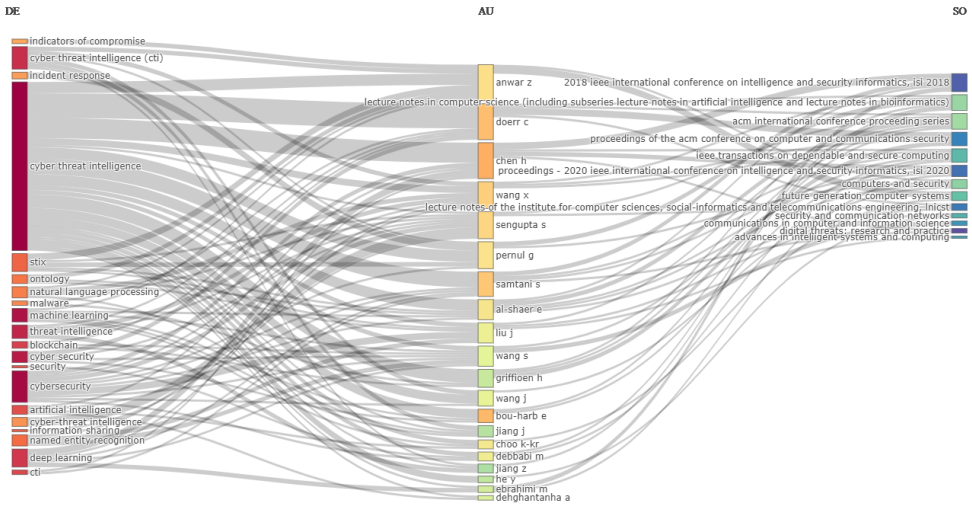
Figure 6. *Most significant affiliations based on the number of publications*



Three Field Plot of keyword, author and source

Figure 7 presents a diagram exploring the connections between keywords (on the left), authors (in the middle), and publications (on the right) in the Cyber Threat Intelligence field. The research aimed to identify terms frequently used by authors in their articles. An analysis of the main keywords, authors, and journals revealed phrases like "cyber threat intelligence," "cyber threat intelligence (cti)," “cyber security,” “machine learning,” and "deep learning." Notably, authors such as Anwar Z, Doerr C, Chen H, Wang X and more often incorporated these terms in their work, which appeared in publications like Lecture Notes in Computer Science (including its subseries on Artificial Intelligence and Bioinformatics), ACM International Conference, 2018 IEEE international conference on intelligence and security informatics, among others.

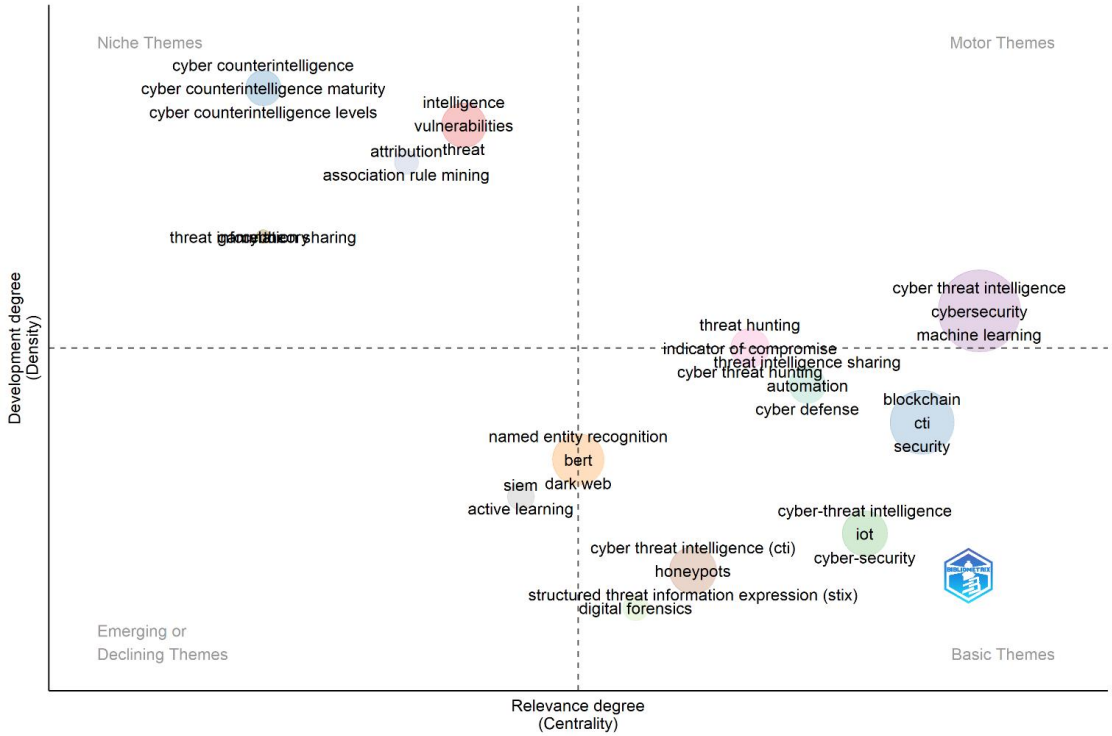
Figure 7. *Three Field Plot with the keyword on the left, the author in the middle, and the source on the right using Biblioshiny.*



Thematic Map

The illustration in Figure 8 showcases multiple bubbles, each representing a distinct topic. The size of each bubble indicates the volume of related publications, while their proximity to one another reflects the similarity between topics. This thematic chart is set against two main axes: density (y-axis) and centrality (x-axis). Centrality evaluates the importance of a topic, whereas density assesses its developmental stage. The chart is divided into four quadrants. The lower-left quadrant features topics that are either emerging or declining, such as "siem" and "active learning." Their future relevance in research might increase or decrease. The lower-right quadrant contains foundational topics that remain central to the field despite being extensively researched (low density). The upper-left quadrant includes well-developed (high-density) topics but has fewer connections to other research areas due to their reduced centrality. The upper-right quadrant houses "motor themes," which are both well-researched and central. In this analysis, key motor themes are "machine learning," "cyber security," "threat hunting," and "cyber threat intelligence."

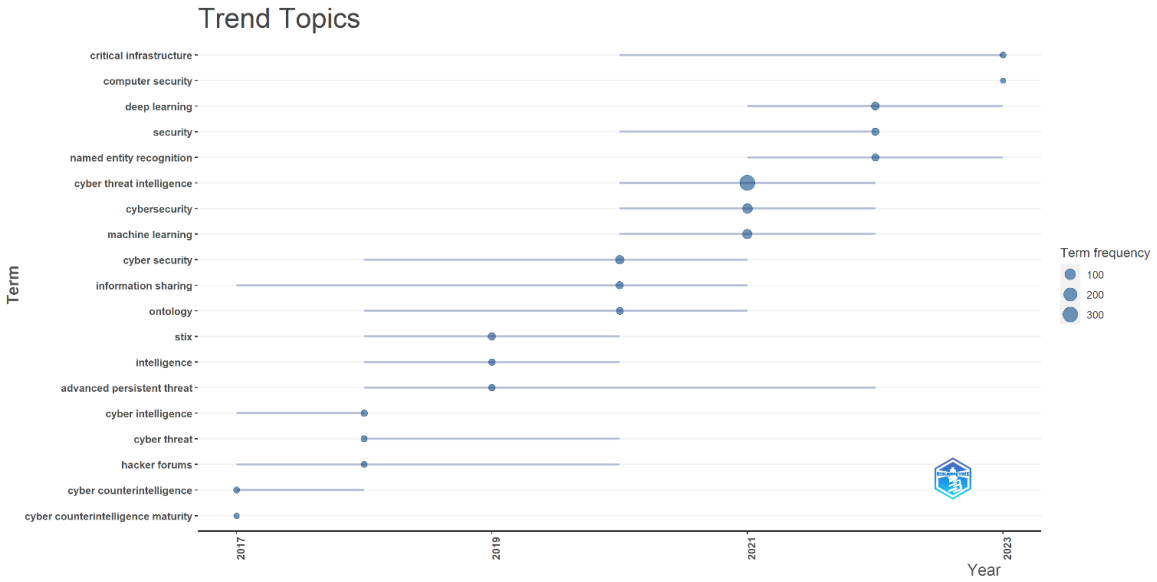
Figure 8. *Thematic Map using Biblioshiny*



Trend Topics

The research explored trend topics by examining the keywords authors chose from the provided data. The criteria for this examination were specific: it spanned from 2017 to 2023, keywords needed to appear at least five times, three keywords were selected for each year, and a word label size of five was utilized. Typically, the keywords selected by authors indicate the central theme of their writings, offering insights into the primary topics in the domain. This examination highlights the prevailing topics in the literature on cyber threat intelligence over the years. Figure 9 visually represents the arrangement of these keywords, emphasizing annual discussions on various facets of cyber threat intelligence by scholars. These topics are related to cyber threat intelligence. For instance, "cyber security" was the foremost subject in 2020, with 44 references; "cyber threat intelligence" was predominant in 2021, with 314 references; and in 2022, "deep learning" was mentioned 24 times.

Figure 9. *Trend topics identified using Biblioshiny from 2017 to 2023*



Top Ten Most Cited Papers

Table 3 highlights the ten leading articles most frequently cited in Cyber Threat Intelligence. These articles have earned significant acclaim within the academic community. Among them, the paper titled "Cybersecurity data science: An overview from machine learning perspective," authored by Sarker I.H. and his team in 2020, stands out, having been cited 195 times. Another influential piece is "Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence," penned by Liao X. and colleagues in 2016, which boasts 176 citations.

Table 3. *The ten top-cited papers*

Authors	Title	Year	Cited by
Sarker I.H.; Kayes A.S.M.; Badsha S.; Alqahtani H.; Watters P.; Ng A.	Cybersecurity data science: an overview from machine learning perspective	2020	195
Liao X.; Yuan K.; Wang X.; Li Z.; Xing L.; Beyah R.	Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence	2016	176
Mavroeidis V.; Bromander S.	Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence	2017	147

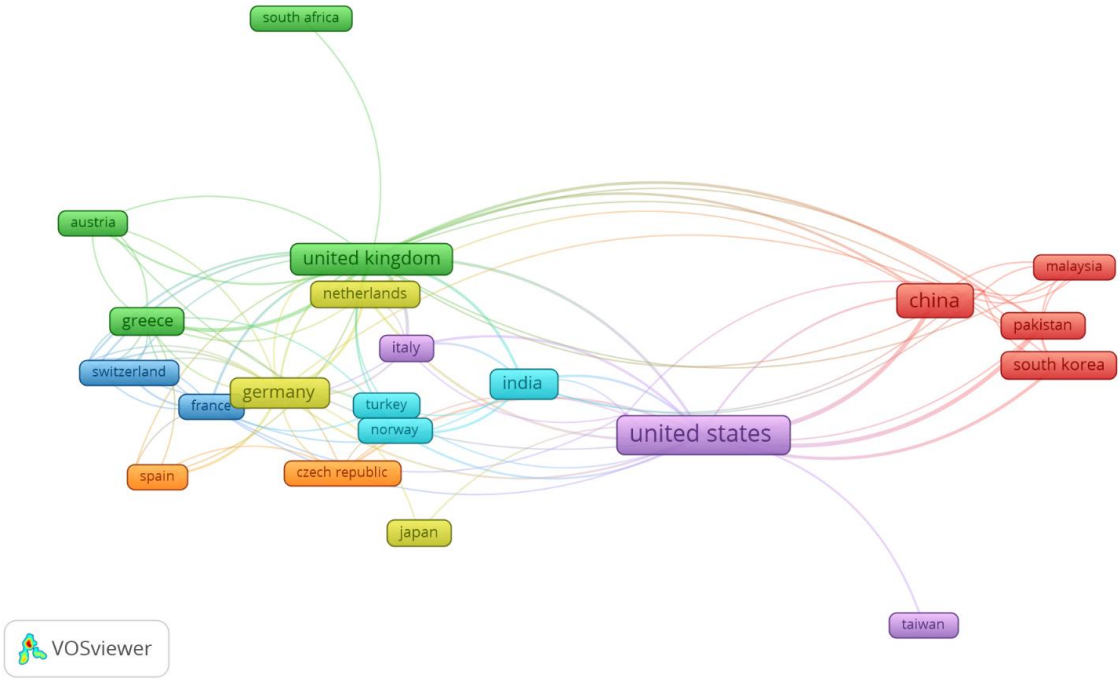
Sarker I.H.; Abushark Y.B.; Alsolami F.; Khan A.I.	IntruDTree: A machine learning based cyber security intrusion detection model	2020	128
Nunes E.; Diab A.; Gunn A.; Marin E.; Mishra V.; Paliath V.; Robertson J.; Shakarian J.; Thart A.; Shakarian P.	Darknet and Deepnet mining for proactive cybersecurity threat intelligence	2016	128
Wagner T.D.; Mahbub K.; Palomar E.; Abdallah A.E.	Cyber threat intelligence sharing: Survey and research directions	2019	100
Burger E.W.; Goodman M.D.; Kampanakis P.; Zhu K.A.	Taxonomy model for cyber threat intelligence information exchange technologies	2014	92
Samtani S.; Chinn R.; Chen H.; Nunamaker J.F., Jr.	Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence	2017	88
Qamar S.; Anwar Z.; Rahman M.A.; Al-Shaer E.; Chu B.-T.	Data-driven analytics for cyber-threat intelligence and information sharing	2017	83
Husari G.; Al-Shaer E.; Ahmed M.; Chu B.; Niu X.	TTPDrill: Automatic and accurate extraction of threat actions from unstructured text of CTI Sources	2017	78

Country Co-Authorship Analysis

Within the realm of Cyber Threat Intelligence research, a country co-authorship analysis offers a visual representation of the collaboration and influence of various nations. As depicted in Figure 10, the interconnected nodes and links provide insights into the depth and breadth of international collaborations. Each node's size signifies a country's influence, while the links represent collaborations between institutions across borders. The intensity and proximity of these links underscore the strength of their collaborative efforts. The map's diverse color palette represents the spectrum of research areas. Leading the pack in publication counts is the United States, with 152 publications, followed by China (79), the United Kingdom (60), and India (40). Regarding citations, the United States stands out with 2410, trailed by Australia (599) and the United Kingdom (537), highlighting their profound impact in the domain. Furthermore, the United States, the

United Kingdom, and Germany dominate in total link strength, underscoring their pivotal roles in this global co-authorship network.

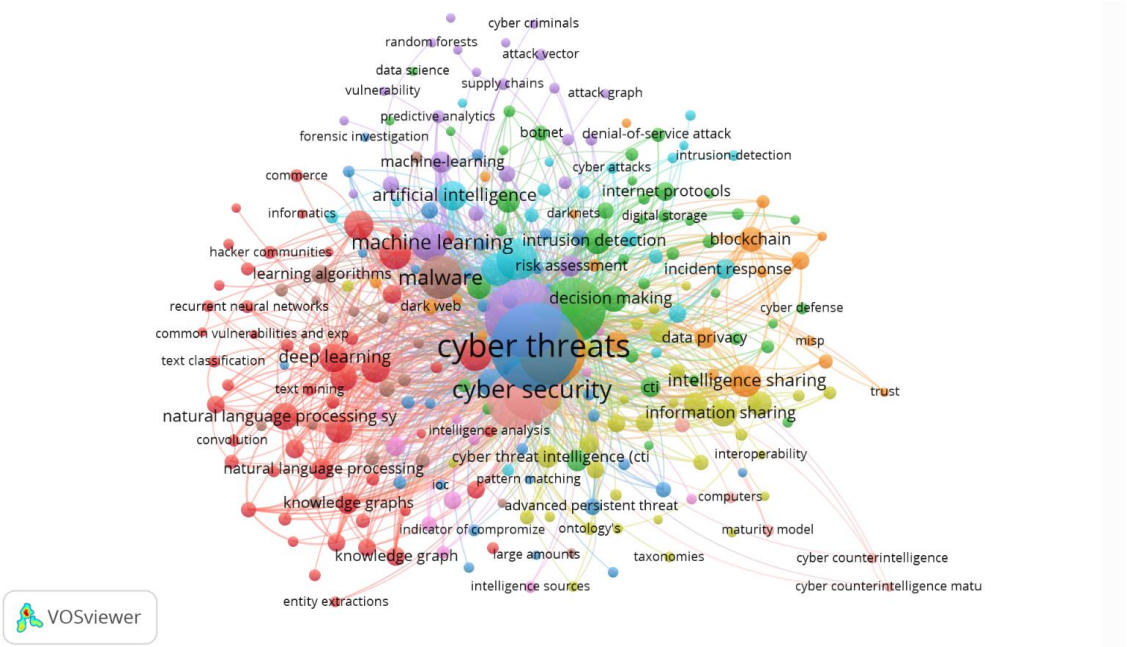
Figure 10. *The network visualization of country co-authorship analysis through the use of VOSviewer*



Co-occurrence of Keywords

The VOSviewer software was employed to visually represent clusters of frequently used keywords associated with Cyber Threat Intelligence. Out of 3574 keywords, 271 were selected for analysis based on their appearance at least five times. The visualization in Figure 11 illustrates the findings. Here, the magnitude and typography of each circle correlate with the keyword's frequency. Larger circles and fonts signify more prevalent keywords. Connections between circles depict keyword relationships, with the line's thickness indicating the strength of their connection. Thicker lines suggest that the keywords are frequently paired. The analysis discerned ten distinct clusters, with varying numbers of keywords in each. Notably, "cyber threats" was a dominant keyword, appearing 392 times, followed by “cyber threat intelligence” at 312 times and “cyber security” at 232 times.

Figure 11. *The network visualization of keyword co-occurrence using VOSviewer*



DISCUSION

The study's methodological rigor, coupled with the comprehensive nature of the Scopus database and the analytical power of the employed software tools, yielded a rich, multidimensional understanding of the cyber threat intelligence landscape. Therefore, this study contributes a significant scholarly resource for further investigations in this critical cybersecurity domain.

The data over the past ten years reveals a consistent and robust upward trajectory in research contributions, with an impressive average annual growth rate of 41.91%. Several factors might be driving this surge, including the advent of advanced research methodologies, an influx of financial research support, or perhaps an expanding community of researchers focusing on this domain. The increased number of publications annually accentuates the growing prominence of cyber threat intelligence in the academic and professional spheres. This trend mirrors the global rise in cyber threats, emphasizing an urgent need for more profound research and a comprehensive understanding of the subject.

The analysis provides a comprehensive overview of the interdisciplinary nature of cyber threat intelligence, showcasing a predominant inclination towards Computer Science and Engineering domains, which collectively encompass 66.2% of the total scholarly output with 574 and 284 papers, respectively. This dominance underscores the critical role of technical and engineering expertise in advancing the field of cyber threat intelligence. Following these, Decision Sciences, Mathematics, and Social Sciences emerge as notable contributors, reflecting the growing recognition of cyber threat intelligence and its applicability in diverse analytical and societal contexts. A wide array of other disciplines, albeit with lesser representation, further accentuates the multidisciplinary character of cyber threat intelligence. The engagement of fields like Medicine, Arts and Humanities, and Environmental Science, albeit minimal, hints at the expansive potential of cyber threat intelligence in addressing a broad spectrum of contemporary challenges. The minimal representation of certain domains could also point towards untapped avenues for integrating cyber threat intelligence with disciplines like Psychology, Neuroscience, and Health Professions, thereby fostering a more holistic, cross-disciplinary approach to tackling cyber threats. The analysis accentuates the existing interdisciplinary engagements and the potential for further explorations and collaborations across a broader spectrum of academic and practical realms, enriching the cyber threat intelligence landscape.

Cyber threat intelligence has witnessed significant contributions from many authors, with a staggering 1,659 individuals dedicating their expertise to this domain. Their publications' sheer volume underscores their

pivotal role in advancing the field. Among these luminaries, Chen H has emerged as the most prolific, boasting 17 papers. Not far behind, Bou-Harb E has made his mark with 13 publications. Doerr C. and Samtani S. have enriched the field equally with their 12 papers. Their profound expertise and unwavering commitment have rightfully earned them the reputation of being the torchbearers in cyber threat intelligence.

In our comprehensive examination of 299 journal references, we amassed 611 papers, underscoring the vast body of research dedicated to Cyber Threat Intelligence. Notably, the ACM International Conference Proceeding Series emerged as a pivotal contributor, accounting for 38 papers. This was closely followed by the Lecture Notes in Computer Science, which, when considering its subseries such as Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, contributed 26 papers. Such findings highlight the significant role of these platforms in advancing research in Cyber Threat Intelligence. Furthermore, for a more granular understanding of the distribution of research articles, this study provides a snapshot of the current landscape of Cyber Threat Intelligence research. It underscores the pivotal role of specific journals and conferences in propelling the field forward.

The study underscores the pivotal role certain institutions play in the realm of Cyber Threat Intelligence (CTI). Sichuan University emerges as a vanguard in this field with a commendable tally of 32 publications, reflecting a robust scholarly engagement with CTI. Trailing behind, yet with a significant contribution, is the University of Chinese Academy of Sciences with 21 publications. The competitive scholarly landscape is further enriched by the active involvement of other institutions such as Zhongyuan University of Technology, Information Technologies Institute, and the University of Regensburg, each marking their presence with around 18 to 19 publications. The close competition extends to Birmingham City University, Bournemouth University, and Concordia University, each boasting 16 publications, demonstrating a concerted effort towards advancing CTI. Lastly, with a respectable count of 15 publications each, Capital Normal University and the University of Brasília further augment the collective endeavor in pushing the frontiers of CTI. This distribution of contributions reflects global interest in CTI and hints at potential collaborative opportunities that could further catalyze advancements in this critical domain. Through a collaborative lens, these institutions could potentially harness their strengths, fostering a conducive environment for groundbreaking discoveries and innovations in Cyber Threat Intelligence.

This research was driven by discerning the most recurrent terms authors employ in their scholarly articles. The findings underscore the prominence of terms such as "cyber threat intelligence," its abbreviation "cyber threat intelligence (cti)," as well as related concepts like “cyber security,” “machine learning,” and "deep learning." These keywords reflect the field's evolving nature and highlight the integration of advanced technologies like machine learning in addressing cyber threats. The involvement of authors like Anwar Z, Doerr C, Chen H, and Wang X, among others, in frequently using these terms indicates their significant contributions and possibly areas of expertise in the domain. The analysis underscores the pivotal role of specific keywords in shaping the discourse in the Cyber Threat Intelligence field. The consistent appearance of these terms across various publications suggests a concentrated focus on leveraging advanced technologies to enhance cyber threat intelligence capabilities. The association of these terms with renowned authors and top-tier publications further validates their importance. It also offers a roadmap for researchers and practitioners, directing them toward the field's most influential works and authors. The prominence of publications like Lecture Notes in Computer Science and its subseries and conferences like the ACM International Conference and the 2018 IEEE International Conference on Intelligence and Security Informatics indicates their standing as leading platforms for disseminating cutting-edge research in Cyber Threat Intelligence.

The thematic map comprehensively visualizes various research topics, with each bubble symbolizing a distinct subject. The chart is strategically divided into four sections. Topics in the lower-left quadrant, such as "siem" and "active learning," are either in their nascent stages or declining. Their trajectory in the academic world is unpredictable, and they may either gain prominence or fade away. Conversely, the lower-right quadrant is home to topics that have been extensively studied, yet they continue to hold a pivotal position in the research domain, indicating their foundational nature. The upper-left quadrant is populated by topics that have matured over time, as evidenced by their high density. However, their reduced centrality suggests they might not be as interconnected with other research areas. Lastly, the upper-right quadrant is the "motor themes" realm. These subjects have been thoroughly investigated and hold a central position in the research arena. Notably,

"machine learning," "cyber security," "threat hunting," and "cyber threat intelligence" emerge as the dominant motor themes in this study. Their presence in this quadrant underscores their pivotal role and enduring relevance in the field of research.

The research embarked on a journey to unearth the trending topics by meticulously analyzing the keywords the authors chose, derived from the given dataset. Conventionally, the choice of keywords by authors mirrors the essence of their discourse, thereby shedding light on the focal topics within a particular domain. This analysis accentuates the dominant themes pervading the literature on cyber threat intelligence throughout the stipulated timeframe. For instance, the year 2020 saw "cyber security" emerging as the paramount topic with 44 mentions, followed by "cyber threat intelligence" reigning supreme in 2021 with a whopping 314 mentions, and come 2022, "deep learning" made its mark with 24 mentions. The findings reflect the evolving focal points within the cyber threat intelligence sphere and potentially guide future scholarly endeavors aligning with the trending dialogues. The conclusions drawn herein are instrumental in understanding the trajectory of cyber threat intelligence discussions and could serve as a lighthouse for future research directions in this domain.

The frequency of citations serves as a testament to the impact and relevance of these articles within the academic and research community. Specific articles have set benchmarks in the domain, influencing subsequent research and shaping the discourse on Cyber Threat Intelligence. The prominence of the paper "Cybersecurity data science: an overview from machine learning perspective" by Sarker I.H. and his team, evidenced by its 195 citations, underscores its pivotal role in bridging cybersecurity and data science. Similarly, Liao X. and his team's work on "Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence," with 176 citations, highlights the evolving nature of threat intelligence and the importance of open-source intelligence in this realm. These articles reflect the dynamic landscape of Cyber Threat Intelligence and emphasize the continuous need for innovative research to address emerging challenges.

In delving into Cyber Threat Intelligence research, exploring country co-authorship analysis unveils a graphical elucidation of various nations' collaborative ventures and influence. The network of interconnected nodes and links sheds light on international collaborations' extensive and intensive nature. The United States emerged as a frontrunner in publication counts with 152 publications, followed by China (79), the United Kingdom (60), and India (40). Regarding citations, the United States is markedly ahead with 2410, followed by Australia (599) and the United Kingdom (537), underlining their significant imprint in this domain. Moreover, the United States, the United Kingdom, and Germany are predominant in total link strength, highlighting their crucial positions in this global co-authorship network. This analysis underscores the collaborative spirit pervading the Cyber Threat Intelligence research landscape and accentuates certain nations' influential roles in propelling the domain forward. Through this lens, the global co-authorship network reflects nations' collective endeavors and individual prowess in navigating the cyber threat landscape.

The findings from the VOSviewer analysis offer valuable insights into the core themes and topics that dominate the realm of Cyber Threat Intelligence. The emergence of ten distinct clusters suggests that while there are overarching themes, there are also specialized sub-domains within this field. The dominance of keywords such as "cyber threats," "cyber threat intelligence," and "cyber security" underscores their centrality in discussions and research related to Cyber Threat Intelligence. Their high frequency of appearance indicates that they are foundational to the domain and likely serve as primary focus areas for professionals and researchers alike. Through its visual representation, this study has effectively mapped out the keyword landscape of Cyber Threat Intelligence, providing a foundation for further research and exploration in the field.

CONCLUSION

In conclusion, the bibliometric study of cyber threat intelligence offers insightful knowledge about the dynamic environment of this vital area. It is clear from a review of scholarly articles that the importance and attention given to cyber threat intelligence have grown over time.

The amount of research produced in cyber threat intelligence has significantly increased, demonstrating its rising significance in tackling the cyber threat landscape's constant expansion. This expansion highlights the importance of solid defenses against online attacks. Information technology, data analysis, computer science, cybersecurity, and other fields are all incorporated into cyber threat intelligence. This interdisciplinary approach emphasizes the need to work together among specialists from various fields to address complicated problems successfully. The report highlights new trends in the industry, including the growing relevance of machine learning and artificial intelligence for threat detection, the value of sharing threat information among organizations, and the developing strategies of cyber adversaries. For practitioners and researchers, keeping up with these changes is essential. The data shows a global interest in tackling cyber dangers, which are not restricted to any geographic area. Collaboration across borders is essential for creating practical solutions and exchanging threat intelligence. The need for improved data-sharing channels, the ongoing development of threat actors, and the moral ramifications of intelligence collecting and distribution are just a few of the issues that still exist despite advances in cyber threat intelligence. Discussions on policy and research should keep these issues front and center. In conclusion, bibliometric examination of publications on cyber threat intelligence demonstrates a dynamic and developing sector essential to the security of digital systems and information. It emphasizes how crucial it is to do continual research, collaborate with others, and innovate to stay ahead of cyber dangers and safeguard crucial assets in a world that is becoming more linked. To successfully handle new issues and protect digital ecosystems as the sector advances, stakeholders must adapt and improve existing ways.

REFERENCES BIBLIOGRAFG

Abbas, A.F., Jusoh, A., Masod, A. and Ali, J. (2021), "A Bibliometric Analysis of Publications on Social Media Influencers Using Vosviewer", *Journal of Theoretical and Applied Information Technology*, Vol. 99 No. 23, pp. 5662–5676. https://www.jneonatalsurg.com/index.php/jns/article/view/2478

Abu, M.S., Selamat, S.R., Ariffin, A. and Yusof, R. (2018), "Cyber threat intelligence–issue and challenges", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 10 No. 1, pp. 371–379. https://ijeecs.iaescore.com/index.php/IJEECS/article/view/11065

Agbo, F.J., Oyelere, S.S., Suhonen, J. and Tukiainen, M. (2021), "Scientific production and thematic breakthroughs in smart learning environments: a bibliometric analysis", *Smart Learning Environments, 8*, (1), 1, https://orcid.org/10.1186/s40561-020-00145-4

Al Mamun, M.A., Azad, M.A.K., Al Mamun, M.A. and Boyle, M. (2022), Review of flipped learning in engineering education: Scientific mapping and research horizon, *Education and Information Technologies, 27* (1), 1261–1286, https://orcid.org/10.1007/s10639-021-10630-z

Aria, M. and Cuccurullo, C. (2017), "bibliometrix: An R-tool for comprehensive science mapping analysis", *Journal of Informetrics*, 11, (4), 959–975, https://orcid.org/10.1016/j.joi.2017.08.007

Bales, M.E., Wright, D.N., Oxley, P.R. and Wheeler, T.R. (2020), *Bibliometric visualization and analysis software: State of the art, workflows, and best practices*. https://ecommons.cornell.edu/items/e3561c0c-1651-4632-abbd-3a22c62a874f

Barnum, S. (2012), Standardizing cyber threat intelligence information with the structured threat information expression (stix), *Mitre Corporation, 11*, 1–22. https://www.mitre.org/sites/default/files/publications/stix.pdf

Barrot, J.S. (2023), *Trends in automated writing evaluation systems research for teaching, learning, and assessment: A bibliometric analysis*, Education and Information Technologies, https://orcid.org/10.1007/s10639-023-12083-y

Chen, C., Dubin, R. and Kim, M.C. (2014), Emerging trends and new developments in regenerative medicine: a scientometric update (2000 – 2014), *Expert Opinion on Biological Therapy, 14* (9), 1295–1317, https://orcid.org/10.1517/14712598.2014.920813

Conti, M., Dargahi, T. and Dehghantanha, A. (2018), *Cyber Threat Intelligence: Challenges and Opportunities", in Dehghantanha, A., Conti, M. and Dargahi, T*. (Eds.), Cyber Threat Intelligence, Springer International Publishing, Cham, 1–6, https://orcid.org/10.1007/978-3-319-73951-9_1

D. Schlette, M. Caselli, and G. Pernul. (2021), A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective, *IEEE Communications Surveys & Tutorials*, *23* (4), 2525–2556, https://orcid.org/10.1109/COMST.2021.3117338

Dao, L.T., Tran, T., Van Le, H., Nguyen, G.N. and Trinh, T.P.T. (2023), A bibliometric analysis of Research on Education 4.0 during the 2017–2021 period. *Education and Information Technologies*, *28* (3), 2437–2453, https://orcid.org/10.1007/s10639-022-11211-4

Dennehy, D., Griva, A., Pouloudi, N., Mäntymäki, M. and Pappas, I. (2022), Artificial intelligence for decision-making and the future of work, *International Journal of Information Management, Elsevier Ltd*, https://orcid.org/10.1016/j.ijinfomgt.2022.102574

Dibbern, T.A., Rampasso, I.S., Pavan Serafim, M., Bertazzoli, R., Leal Filho, W. and Anholon, R. (2023), Bibliometric study on SDG 6: analysing main content aspects by using Web of Science data from 2015 to 2021, *Kybernetes*, *52* No.(9) 3119–3135, https://orcid.org/10.1108/K-05-2021-0393

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N. and Lim, W.M. (2021), How to conduct a bibliometric analysis: An overview and guidelines, *Journal of Business Research*, *133*, 285–296, https://orcid.org/10.1016/j.jbusres.2021.04.070

van Eck, N.J. and Waltman, L. (2014), *Visualizing Bibliometric Networks, in Ding, Y., Rousseau, R. and Wolfram, D. (Eds.), Measuring Scholarly Impact: Methods and Practice*, Springer International Publishing, Cham, pp. 285–320, https://orcid.org/10.1007/978-3-319-10377-8_13

Fauzi, M.A. (2023), Cyberbullying in higher education: a review of the literature based on bibliometric analysis. Kybernetes, https://orcid.org/10.1108/K-12-2022-1667

Godin, B. (2006), On the origins of bibliometrics *Scientometrics*, *68* (1), 109–133, https://orcid.org/10.1007/s11192-006-0086-0

Guleria, D. and Kaur, G. (2021), Bibliometric analysis of ecopreneurship using VOSviewer and RStudio Bibliometrix, 1989–2019, *Library Hi Tech*, *Emerald Publishing Limited*, *39* (4), 1001–1024, https://orcid.org/10.1108/LHT-09-2020-0218

Husaeni, D.F.A. and Nandiyanto, A.B.D. (2022), Bibliometric computational mapping analysis of publications on mechanical engineering education using Vosviewer, 17. https://jestec.taylors.edu.my/Vol%2017%20Issue%202%20April%20%202022/17_2_23.pdf

Kattamuri, S.J., Penmatsa, R.K.V., Chakravarty, S. and Madabathula, V.S.P. (2023), Swarm Optimization and Machine Learning Applied to PE Malware Detection towards Cyber Threat Intelligence, *Electronics, MDPI*, 12, (2), 342. https://www.mdpi.com/2079-9292/12/2/342

Kayode-Ajala, O. (2023), Applications of Cyber Threat Intelligence (CTI) in Financial Institutions and Challenges in Its Adoption, *Applied Research in Artificial Intelligence and Cloud Computing*, *6*, (8), 1–21. https://core.ac.uk/download/pdf/588488097.pdf

Kotsias, J., Ahmad, A. and Scheepers, R. (2023), Adopting and integrating cyber-threat intelligence in a commercial organisation, *European Journal of Information Systems, Taylor & Francis*, 32 (1), 35–51, https://orcid.org/10.1080/0960085X.2022.2088414

Lee, M. (2023), Cyber Threat Intelligence, John Wiley & Sons. https://www.wiley.com/en-us/Cyber+Threat+Intelligence-p-00370670

Mukherjee, B. (2020), Analysis of Global Research Trends in Coronaviruses: A Bibliometric Investigation, *Journal of Scientometric Research*, *9* (2), 185–194, https://orcid.org/10.5530/jscires.9.2.22

Nandiyanto, A.B.D., Husaeni, D.N.A. and Husaeni, D.F.A. (2021), A bibliometric analysis of chemical engineering research using Vosviewer and its correlation with covid-19 pandemic condition, vol. 16. https://jestec.taylors.edu.my/Vol%2016%20Issue%206%20December%20%202021/16_6_4.pdf

Pinto, M., Fernández-Pascual, R., Caballero-Mariscal, D., Sales, D., Guerrero, D. and Uribe, A. (2019), Scientific production on mobile information literacy in higher education: a bibliometric analysis (2006–2017), *Scientometrics*, *120* (1), 57–85, https://orcid.org/10.1007/s11192-019-03115-x

Racine, J.S. (2012). "RStudio: a platform-independent IDE for R and Sweave", JSTOR.

Rojas-Sánchez, M.A., Palos-Sánchez, P.R. and Folgado-Fernández, J.A. (2023), "Systematic literature review and bibliometric analysis on virtual reality and education", *Education and Information Technologies*, *28* ,(1), 155–192, https://orcid.org/10.1007/s10639-022-11167-5

Salim, N., Gopal, K. and Ayub, A. (2019). Effects of using RStudio on statistics performance of Malaysian undergraduates" *Malaysian Journal of Mathematical Sciences*, 13 (3), 419–437. https://mjms.upm.edu.my/fullpaper/2019-September-13-3/Salim,%20N.%20R.-419-437.pdf

Sawangwong, A. and Chaopaisarn, P. (2023). The impact of applying knowledge in the technological pillars of Industry 4.0 on supply chain performance, *Kybernetes*, *52* (3), 1094–1126, https://orcid.org/10.1108/K-07-2021-0555

Schlette, D., Böhm, F., Caselli, M. and Pernul, G. (2021), Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, *20.* 1, 21–38, https://orcid.org/10.1007/s10207-020-00490-y

Scientific Mapping of Gravity Model of International Trade Literature: A Bibliometric Analysis. *Journal of Scientometric Research*, *11* (3), 447–457, https://orcid.org/110.5530/jscires.11.3.48

Shekhar, S.K. and Shah, M.A. (2023), Sports Marketing and Conceptual Evolution: A Bibliometric Analysis, SAGE Open, Vol. 13 No. 3, p. 21582440231192915, https://orcid.org/10.1177/21582440231192915

Singh, S., Solkhe, A. and Gautam, P. (2022). What do we know about Employee Productivity?: Insights from Bibliometric Analysis, *Journal of Scientometric Research*, 11 (2), 183–198, https://orcid.org/10.5530/jscires.11.2.20

Souza de Cursi, E. (2023), *Some Tips to Use R and RStudio*, *in Souza de Cursi, E.* (Ed.), Uncertainty Quantification Using R, Springer International Publishing, Cham, 1–108 https://orcid.org/10.1007/978-3-031-17785-9_1

Sufi, F. (2023), A New Social Media-Driven Cyber Threat Intelligence. *Electronics*, *2* (5), https://orcid.org/10.3390/electronics12051242

Thomson, R., Mosier, R. and Worosz, M. (2023), COVID research across the social sciences in 2020: a bibliometric approach. *Scientometrics 128* (6), 3377–3399, https://orcid.org/10.1007/s11192-023-04714-5

Tomaszewski, R. (2023), Visibility, impact, and applications of bibliometric software tools through citation analysis. *Scientometrics*, *128* (7), 4007–4028, https://orcid.org/10.1007/s11192-023-04725-2

V. Mavroeidis and S. Bromander. (2017), *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence*, *2017 European Intelligence and Security Informatics Conference (EISIC*), presented at the 2017 European Intelligence and Security Informatics Conference (EISIC), pp. 91–98, https://orcid.org/10.1109/EISIC.2017.20

Wagner, T.D., Mahbub, K., Palomar, E. and Abdallah, A.E. (2019), Cyber threat intelligence sharing: Survey and research directions, *Computers & Security*. *87*, 101589, https://orcid.org/10.1016/j.cose.2019.101589

Waltman, L., van Eck, N.J. and Noyons, E.C.M. (2010), A unified approach to mapping and clustering of bibliometric networks, *Journal of Informetrics*, *4* (4), 629–635, https://orcid.org/10.1016/j.joi.2010.07.002