ADBA Computer Science
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8544
RESEARCH ARTICLE
Vol.2 / No.1 / 2025 / pp.19-29
https://doi.org/10.69882/adba.cs.2025014

Bibliometric Analysis of Studies on Cyber Crimes Between 2000-2023

Murat Erdoğan *,1 **and Ömer Faruk Akmeşe** β,2
*Hitit University, Department of Forensic Sciences, 19030, Corum, Turkiye, βHitit University, Faculty of Engineering, Department of Computer Engineering, 19030, Corum, Turkiye.

ABSTRACT The increasing use of internet-based technologies and computer networks, which grow and develop daily, has brought problems. A new type of crime called cybercrime has emerged and is committed through computers. There are various research and studies on cyber crimes. This study presents a bibliometric analysis of studies on the keywords "Cyber Crimes", "Internet Crimes" and "Computer Crimes" indexed in Web of Science between 2000 and 2023. This study aims to reveal the scientific map of research and studies on cybercrimes, make sense of the data, understand the current situation, trends, and relationships in this field, and create a resource for future cybercrime studies. Bibliometric analyzes were performed using Bibliometrix and Microsoft Excel programs. A total of 2566 studies by 5590 different authors were determined to be used in the research. Jaishankar, K. was the most prolific writer with 21 articles. University College Dublin was the university with the most publications, with 56 articles. IEEE Access became the most-published journal with 151 articles. The most cited work is Stuxnet and the Future of Cyber Wars by Farwell, JP, and Rohozinski, R. Bibliometric analysis results such as most used keywords, including the most influential and productive countries, authors, universities and journals in the field of cybercrime are included. In studies on cybercrime, the relationships and collaborations between countries and authors are presented with visuals.

KEYWORDS
Cyber
Cyber crimes
Bibliometric analysis
Citation analysis
Internet crimes

INTRODUCTION

Before explaining the concept of cybercrime, which has been defined in many different ways, the word cyber must be understood. The word cyber was first used in 1958 by Louis Couffignal, who studied the communication between living things and machines. Cyber is used to make sense of and explain concepts related to complex areas such as computers and computer networks. Cyberspace is the abstract and concrete space where people communicate and interact through interconnected hardware and software systems (Klimburg 2018).

The rapid entry of e-commerce into the Internet environment as a business model and people communicating with each other through social media platforms have increased the use of the Internet and computers. The increase in the use of the Internet and computers, which provide the easiest and fastest access to information, has caused crime to shift to the virtual environment. As the Internet has become the target of malicious users, illegal and criminal activities have also increased (Phillips *et al.* 2022).

Many terms are used to describe crimes committed via the Internet and computers. Terms such as cyber crimes, computer crimes, internet crimes, information technology crimes, and high technology crimes have been used (Goodman and Brenner 2002). Although the terms "cyber crime", "computer crimes", "information crimes" and "virtual crimes" are preferred in general use, these expressions may vary depending on the computer, internet network, and technological devices used in the commission of the crime. "Computer crimes" was a concept used in the periods before the invention of the Internet. Today's accepted and widely used term is "cybercrime" (Moitra 2005).

Although there is no entirely accepted definition of cybercrime, different definitions have been made. Crimes committed against computers, depending on the orientation of a group, are considered cybercrime (Marsh and Melville 2009). According to another group, any crime committed via the Internet or computer-related is called cybercrime (Wall 2024). Cybercrime is a crime that targets the user and data security of another information system by using the information system (R. Ch and Al-Ahmari 2020). Cybercrime is crimes such as illegally entering information systems without permission, seizing data, deleting, changing, and blocking access to the system (IBM 2024). Cybercrime is any criminal activity that targets or uses computers, computer networks, or network-connected devices. Hackers who want to damage computer systems usually commit cybercrimes to gain profit or make money (W. A. Al-Khater and Khan 2020). In the most general sense, entering computer networks and all devices connected to these networks without permission and acting in a way that causes material and moral damage to individuals or institutions is a cybercrime (Wall 2024).

Manuscript received: 11 January 2025,
Revised: 24 January 2025,
Accepted: 24 January 2025.

[1]muraterdogan41@gmail.com (**Corresponding author**).
[2]ofarukakmese@hitit.edu.tr

For a cybercrime to occur, a crime triangle consisting of a victim, reason, and opportunity must be present (Lallie *et al.* 2021). The victim is the person attacked; the reason is the factor that pushes the criminal to commit the attack, and the chance to commit the crime is the opportunity. Cyber crimes committed today have become more complex. Sometimes, attacks are made against specific targets for reasons such as revenge, money, or espionage, while sometimes, attacks can be carried out with unclear motivations, which are opportunistic and aimless. The method of committing cyber crimes is changing day by day. For this reason, it is becoming increasingly difficult to intervene in cyber attacks and take security measures (K. Shaukat and Xu 2020).

With the increase in internet usage worldwide, the rate of cyber crimes has also increased (C. Lu and Chang 2007). Cyber crimes have caused significant financial losses to individuals, institutions, and countries. According to a report by the FBI in the USA, cyber crimes caused financial losses of 4.2 billion dollars worldwide in 2020, estimated to reach 6.9 billion dollars in 2021 (Cldy 2023). These results show us that more studies need to be done on cybercrime.

With the acceleration of scientific studies, large volumes of data have emerged. Making sense of these data and producing meaningful outputs for future research and studies is necessary. Bibliometric methods help researchers to examine previous studies in the literature before starting to examine a field of science and to discover the most influential studies in that field (Zupic and Čater 2015). Bibliometrics performs numerical analysis using different methods and techniques, such as data from various databases. The most influential authors, institutions, countries, keywords, and most cited sources, journals, and authors on a subject are found with bibliometric analysis. With bibliometric analysis, research and studies in the field of science are evaluated, the current situation is determined, and predictions for the future are made with these data (Şakar and Cerit 2013). Bibliometrics is used to measure the current status of institutions, journals, and authors and identify the most current topics, the most influential authors and documents, and collaborations in the field (Wang *et al.* 2018).

In their article titled "Trends in computer crime and cybercrime research during the period 1974-2006: A bibliometric approach", C. Lu and Chang (2007) conducted a bibliometric analysis of 292 publications related to cybercrime from 1974 to 2006. The study includes the review of publications in the form of articles, editorial materials, reviews, and meeting abstracts without any language or document type limitation. The study also states that computer crimes increased with the increase in internet users and internet applications from 1991 to 2000, after the development of web browsers. It was also announced that research on cybercrime is needed to reduce and prevent cybercrime activities.

Ho and Luong (2022) made a bibliometric analysis of the victimizations encountered after cybercrimes in their article titled " Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis". The research analyzed 387 articles bibliometrically from the Web of Science database on cyber crime victimization between 2010 and 2020. Keywords related to cybercrime victimization: "cyber bullying" (174 times), "cyber victimization" (90 times), "adolescent" (79 times), "bullying" (66 times), "victimization" (56 times), ' It was determined that 'cyber crime' (40 times) and 'cyber aggression' (37 times) were mentioned. The study aimed to identify global collaborations, research gaps, and existing gaps in cybercrime victimization research.

In their article titled "Research trends in cybercrime and cybersecurity: A review based on Web of Science core collection database", L. Wu and Lembke (2023) conducted a bibliometric review of research trends in cybercrime and cybersecurity between 1995 and 2021. The research examined 3635 publications containing the keywords "cyber crime" and/or "cyber security" using the bibliometric method. The study aims to comprehensively reveal the scientific landscape of the field by examining publications on cybercrime and cyber security and presenting multiple perspectives. The research shows that studies in Cyber Crime and Cyber Security have increased rapidly in recent years and that this field is a developing field of research.

In their article titled "The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index", Subektiningsih and Hariyadi (2022) conducted a bibliometric analysis of research on the field of Cyber Crime and/or Computer Forensics in Indonesia between 2010 and 2021. In the research, 281 articles were accessed from the Scopus database with the keywords "Cyber Crime" or "forensic investigation" or "digital forensics" or "computer crimes" and "Indonesia". 281 articles related to this field in Indonesia were analyzed with bibliometric analysis tools. The study identified universities and academicians working in cybercrime and digital forensics in Indonesia. The research is thought to positively impact law enforcement agencies solving cybercrime investigations by making scientific publications of computer forensic experts. In their article titled "Cybersecurity Trend Analysis Using Web of Science: A Bibliometric Analysis", Shukla and Gochhait (2020) analyzed cybersecurity-related articles between 1998 and 2020 using bibliometric methods. For the research, more than 2000 thousand studies were analyzed bibliometrically with VOSviewer and Excel programs using the keywords "Cyber Security" or "cyber security" from the Web Of Science database. The literature of every study published in cybersecurity was analyzed.

In their article titled "Cyberbullying research — Alignment to sustainable development and impact of COVID-19", K. Achuthan and Raman (2023) aimed to provide a bibliometric perspective on cyberbullying research between 2010 and 2021, including post-COVID-19. The research analyzed 7045 publications written about Cyberbullying between 2010 and 2021 using bibliometric methods. In the research, it was determined which countries contributed to publications on Cyberbullying and how much. The study sought answers to questions such as whether COVID-19 impacts Cyberbullying and whether Cyberbullying research is compatible with sustainable development goals. The research includes examining where we come from and where we will go in the future regarding Cyberbullying through bibliometric analysis.

M. M. Alashqar and Aziz (2021), in their article "Examining the trend of research on chemometric analysis: a bibliometric review", conducted a bibliometric analysis to evaluate cyber crime research. The study analyzed 377 publications from the Spocus database with bibliometric methods in searches related to "cyber crime" from 1998 to 2022. The study found that the most effective countries in cybercrime are the USA, Australia, and the UK. It was observed that the English language was used in 98% of 377 publications. It has been emphasized that the increase in the addiction level of internet use of businesses, communities, and individuals has led to an increase in cyber crimes. These studies are thought to contribute to academics, students, and experts' understanding of the development of cyber security as a research field.

This study presents the bibliometric analysis of 2566 studies indexed in the Web of Science database between 2000 and 2023. The spread of the internet and computer technologies worldwide since 2000 caused us to choose this year as the starting point. Our study

aims to reveal the scientific landscape of the cyber crime field. This study, which covers the best authors, countries, keyword features, collaborations, and the review of the most important articles, offers the opportunity to track the studies on cybercrime historically using appropriate bibliometric analysis techniques. This study aims to evaluate the published studies on cybercrime numerically, make sense of the data related to cybercrimes, reveal how the subject has developed over time, and create a scientific map of the field.

MATERIAL AND METHODS

Bibliometric analyses allow a numerical analysis of the effectiveness of publications in a certain field. Bibliometric techniques offer us an examination method with data sets to examine the relationship between scientific studies and evaluate research activities (Borgman and Furner 2001). WoS is both a research tool that supports comprehensive scientific examination of studies from various disciplines and the world's leading scientific citation search platform that allows working with large-scale data (K. Li and Yan 2018). WoS includes more than 21 thousand journals and over 200 thousand conference proceedings from more than 250 disciplines. For this reason, the WoS database was preferred to collect the data set. WoS is a website that regularly scans many journals, publications, and conferences worldwide. It also gives researchers access to numerous databases for more comprehensive bibliometric studies. Researchers dealing with bibliometric analysis use WoS as a data source in their research (Soydal and Al 2014).

All publications indexed in WoS regarding Cyber Crimes between 2000 and 2023 (accessed on 15.01.2024) were analyzed with bibliometric methods. The keywords "Cyber Crimes" or "Internet Crimes" or "Computer Crimes" were used for the search. Documents were searched by filtering by article title, abstract, and keywords. WoS codes used in our search: ("Cyber Crimes" or "Internet Crimes" or "Computer Crimes") and (EXCLUDING PUBYEAR,1980) and(EXCLUDING PUBYEAR,1999) and (EXCLUDING PUBYEAR,2024). Using this search method, all publications published in the WoS database between 2000 and 2023, containing "Cyber Crimes" or "Internet Crimes" or "Computer Crimes" in their title, abstract and keywords, were found. The bibliometric mapping and visualization processes used Microsoft Excel and Bibliometrix software.

BIBLIOMETRIC ANALYSIS OF PUBLICATIONS RELATED TO CYBER CRIMES

Literature Research Review

There are 2566 studies published in different genres from 2000 to 2023. Articles (1317, 52%), proceedings (925, 36%), book chapters (130, 5%), review articles (58, 2%), book reviews (28, 1%), and others (108, 4%) were found as. As shown in Figure 1, articles on Cyber Crime are in different disciplines; "Computer Science" (2123, 46%), "Engineering" (731, 16%), "Criminology" (462, 10%), "Telecommunications" (446, 10%), "Law" (178, 4%), "Multidisciplinary et al" (625, 14%). Since the studies can fall into more than one discipline category, the total number of studies is more than 2566.

Development of Publications

Figure 2 shows the total number of publications by year. Despite some fluctuations, there is a general increase in publications from 2000 to 2023. The fact that studies on cybercrime started to develop after 2000 and are still developing shows us that the field

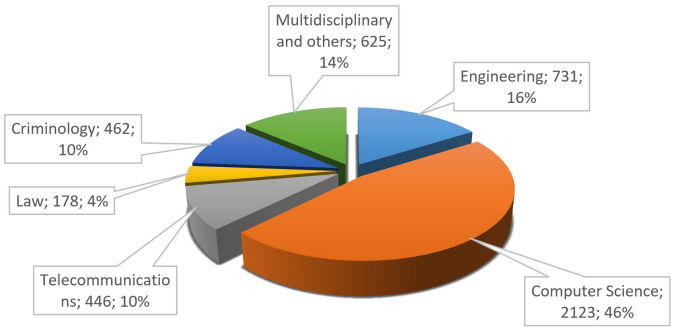

Figure 1 The Distribution of Subject Areas

is widespread. The fact that the number of studies has increased significantly between 2019 and 2023 reveals that studies on cyber crimes are very current. Although the number of publications has decreased in 2023, cyber crimes continue to affect our daily lives and all sectors.

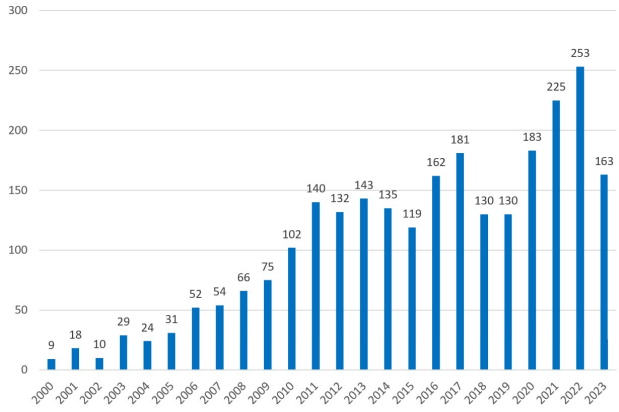

Figure 2 Annual Number of Publications by Year

Active Authors

5559 authors made a total of 2556 publications. Of these, 2829 authors' articles and 2032 authors' conference papers were published. Table 1 shows the 25 most influential authors with the highest h index on the topics "Cyber Crimes", "Computer Crimes" and "Internet Crimes". The top five authors with the highest h-index in the fields of "Cyber Crimes", "Computer Crimes" and "Internet Crimes" are Higgins G., Holt T., Liu Z., Choo K., L. J. There are indicators such as the number of publications, citations, h-Index, G-Index, and M-Index that measure the individual performance of authors. Having a large number of publications by an author is an important criterion that shows the performance of that researcher. However, the number of publications alone does not indicate the author's effectiveness. The number of citations received by authors in their studies is another performance indicator that shows the effectiveness of researchers. However, just because a study receives many citations does not indicate that it is important and effective. Moreover, just because a study has never been cited does not mean it is unimportant and inefficient (Kaleci 2023). H-index is an index used to measure the productivity and performance of researchers (S. Firat and Kurutkan 2023). In calculating the H-index, the number of citations and publications received by the author in other publications are used.

Table 1 The top 25 most influential authors

No	Author	h-index	g-index	m-index	TC	NP	PY_Start
1	HIGGINS GE	9	15	0.429	454	15	2004
2	HOLT TJ	8	12	0.500	728	12	2009
3	LIU Z	7	10	0.500	110	14	2011
4	CHOO KKR	6	12	0.429	515	12	2011
5	LI J	6	10	0.750	104	11	2017
6	LI Y	6	13	0.353	214	13	2008
7	MARCUM CD	6	10	0.429	189	10	2011
8	ROGERS MK	6	10	0.286	240	10	2004
9	WANG J	6	11	0.429	138	12	2011
10	WU J	6	9	1.200	95	9	2020
11	BOURKE ML	5	5	0.313	231	5	2009
12	BREITINGER F	5	8	0.417	105	8	2013
13	CHEN Y	5	9	0.357	126	9	2011
14	JAISHANKAR K	5	10	0.278	119	21	2007
15	LI Z	5	9	0.278	91	10	2007
16	SEIGFRIED-SPELLAR KC	5	10	0.357	103	10	2011
17	WANG L	5	7	1.000	62	7	2020
18	ZHANG H	5	9	0.556	99	9	2016
19	ALAZAB M	4	4	0.364	159	4	2014
20	ASRARI A	4	5	1.000	28	5	2021
21	BAGGILI I	4	12	0.250	161	12	2009
22	BOSSLER AM	4	5	0.250	576	5	2009
23	CARTHY J	4	4	0.308	127	4	2012
24	CASEY E	4	6	0.267	71	6	2010
25	CRAUN SW	4	4	0.364	90	4	2014

TC: Total Citation, NP: Number of Publications, PY_Start: Publication Year Start

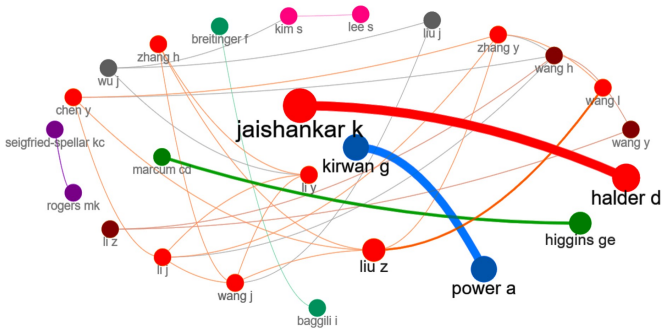

Figure 3 Authors Collaboration Network

Figure 3 shows the collaboration network among authors in publications related to cybercrime. The larger the circle, the greater the collaboration. Clusters are separated by colors. The power of collaboration between authors is expressed in the thickness of the lines.

Active Institutions

Figure 4 shows the graph of universities' publication production on cybercrime between 2000 and 2023. Figure 5 shows the co-operation network map of universities in the field. The greater the cooperation between universities, the greater the number and thickness of the lines. The more work there is, the larger the flat size.

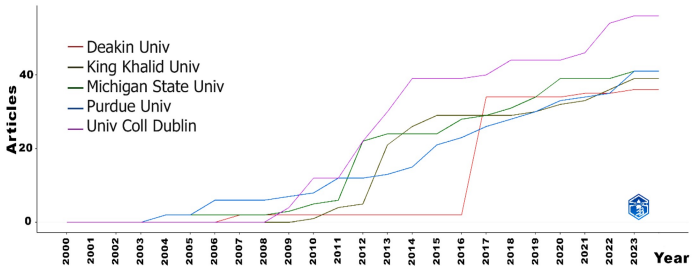

Figure 4 Number of Publications by Institutions in the Period 2000-2023

Table 2 shows the top 25 universities across countries that publish the most on "Cyber Crimes", "Computer Crimes" and "Internet Crimes". The universities with the most publications on cybercrime were College Dublin University, with 56 publications; Michigan State University, with 41 publications; Purdue University, with 41 publications; King Khalid University, with 36 publications; and Deakin University, with 31 publications.

Table 2 Top 25 Universities by Total Publications

No	University Name	Total Publications
1	UNIV COLL DUBLIN	56
2	MICHIGAN STATE UNIV	41
3	PURDUE UNIV	41
4	KING KHALID UNIV	36
5	DEAKIN UNIV	31
6	KOREA UNIV	31
7	DUN LAOGHAIRE INST ART DESIGN AND TECHNOL	28
8	KING SAUD UNIV	28
9	UNIV ALABAMA	28
10	UNIV LOUISVILLE	28
11	UNIV PRETORIA	27
12	KING ABDULAZIZ UNIV	26
13	TSINGHUA UNIV	25
14	UNIV WISCONSIN	25
15	CENT POLICE UNIV	24
16	MANONMANIAM SUNDARANAR UNIV	24
17	UNIV NEW HAMPSHIRE	24
18	UNIV S FLORIDA	24
19	UNIV TEXAS SAN ANTONIO	24
20	CTR CYBER VICTIM COUNSELLING	23
21	UNIV NEW HAVEN	23
22	A (CORRESPONDING AUTHOR)	22
23	DEPT COMP SCI	22
24	UNIV NEW SOUTH WALES	22
25	NATL INST TECHNOL	21

Figure 5 shows the collaboration network of the top 25 institutions. The larger the circle, the greater the collaboration. Clusters are separated by colors. The power of interinstitutional collaboration is expressed in the thickness of the lines.

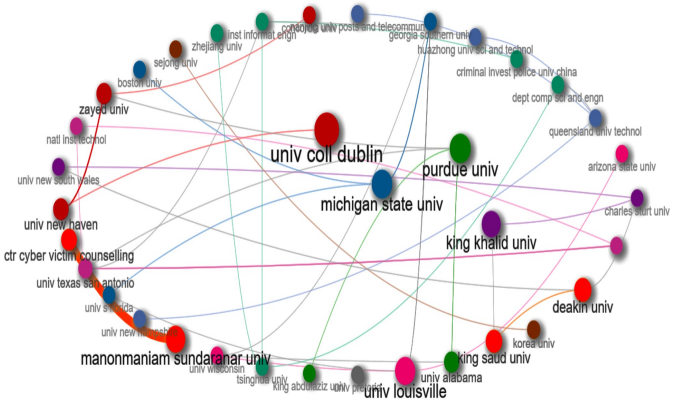

Figure 5 Inter-institutional Collaboration Network

Active Journals

In total, 1510 articles were published in 1243 journals. Table 3 shows the top 25 most influential journals with the highest *h_index* value on the subjects of "Cyber Crimes", "Computer Crimes", and "Internet Crimes." According to the table, *IEEE Access*, *International Journal of Cyber Criminology*, *Digital Investigation*, *Computers & Security*, and *IEEE Internet of Things Journal* are the most productive journals, respectively. Approximately 21% of the 1510 articles were published in these 25 journals.

The first five most influential journals are journals that support open access. Open communication journals are journals where scientific content can be accessed freely over the Internet. These journals aim to provide open and free access to scientific knowledge, often by eliminating financial barriers such as subscription, licensing fees, or pay-per-view. Enabling researchers to access scientific information more easily has made journals such as *IEEE Access*, *International Journal of Cyber Criminology*, *Digital Investigation*, *Computers & Security*, and *IEEE Internet of Things Journal* the most effective journals and resources.

Figure 6 shows data on the co-citation network among the 25 most influential journals. The size of the circle shows us that there are many of citations from that circle. Clusters are separated by colors. The greater the cooperation between journals, the greater the line thickness. Figure 7 shows the article production amounts of the six journals with the most articles by year. The remarkable result here is the IEEE Access journal started publishing in this field in 2016 and was a journal that published a small number of publications before 2018. However, IEEE Access magazine has rapidly increased its publications on cybercrime since 2018. The International Journal of Cyber Criminologists started publishing on cyber crimes in 2007, and the journal steadily increased its publication production until 2023.

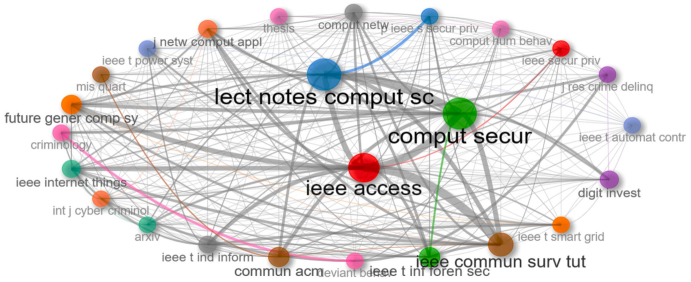

Figure 6 Sources Co-Citation Network

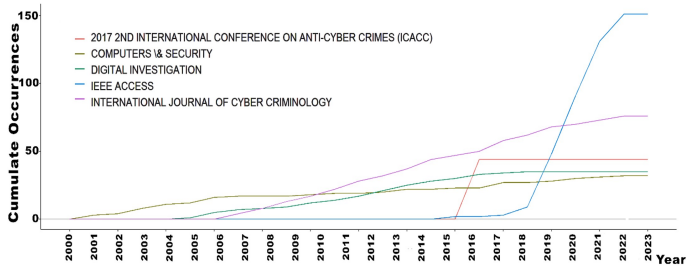

Figure 7 Top 6 Journals with the Most Articles

Distribution by Countries

Figure 8 shows the cooperation map between countries in articles on "Cyber Crimes", "Computer Crimes" and "Internet Crimes". The greater the cooperation between countries, the greater the number and thickness of the lines. Countries such as the USA (USA), China, India, and the UK (United Kingdom) are the most cooperative and leading countries in Cyber Crimes. Figure 9 shows the annual production amounts of publications on cybercrime by

Table 3 Top 25 Journals with h-index in Cybercrime Research

No	Journals	h-index	g-index	m-index	TC	NP	PY_Start
1	IEEE ACCESS	24	36	2.667	1920	151	2016
2	INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY	21	34	1.167	1293	76	2007
3	DIGITAL INVESTIGATION	17	23	0.85	602	35	2005
4	COMPUTERS & SECURITY	15	32	0.625	1330	32	2001
5	IEEE INTERNET OF THINGS JOURNAL	10	18	2	337	23	2020
6	IEEE SYSTEMS JOURNAL	10	16	2	268	21	2020
7	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	10	14	0.667	234	14	2010
8	IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT	10	19	1.667	378	20	2019
9	IEEE TRANSACTIONS ON SMART GRID	9	12	1.8	187	19	2020
10	2017 2ND INTERNATIONAL CONFERENCE ON ANTI-CYBER CRIMES	8	12	1	223	44	2017
11	CRIME LAW AND SOCIAL CHANGE	8	8	0.4	185	8	2005
12	IEEE TRANSACTIONS ON CYBERNETICS	8	10	1.6	285	10	2020
13	IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	8	17	0.727	314	24	2014
14	IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS	8	17	1.6	306	17	2020
15	IEEE COMMUNICATIONS SURVEYS AND TUTORIALS	7	8	0.7	409	8	2015
16	IEEE SECURITY & PRIVACY	7	11	0.467	198	11	2010
17	IEEE NETWORK	6	8	0.429	181	8	2011
18	IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT	6	14	0.286	214	15	2004
19	IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS	6	6	2	200	6	2022
20	POLICING-AN INTERNATIONAL JOURNAL OF POLICE STRATEGIES	6	7	0.286	193	7	2004
21	VICTIMS & OFFENDERS	6	6	0.375	105	6	2009
22	COMPUTER STANDARDS & INTERFACES	5	7	0.278	63	7	2007
23	CYBER CRIMINOLOGY: EXPLORING INTERNET CRIMES	5	9	0.357	101	25	2011
24	DIGITAL FORENSICS AND CYBER CRIME	5	9	0.333	89	16	2010
25	DIGITAL FORENSICS AND CYBER CRIME, ICDF2C 2012	5	9	0.417	98	20	2013

TC: Total Citation, NP: Number of Publications, PY_Start: Publication Year Start

country. Figure 10 shows the top 25 countries that publish the most on cybercrime. The USA, China, India, England, and Australia are the five countries with the most broadcasts. Figure 11 shows the cooperation network between countries in studies on cyber. The greater the cooperation, the greater the line thickness between countries. The more work there is, the larger the flat size. Table 4 shows the total number of citations received by countries. The USA, the UK, China, Australia, and India are the countries most cited in studies on cybercrime.

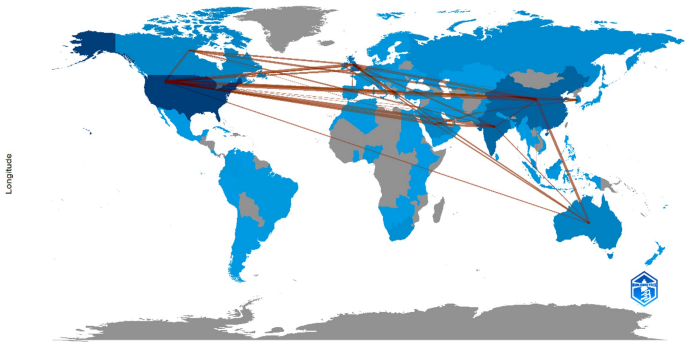

Figure 8 Countries Cooperation Map

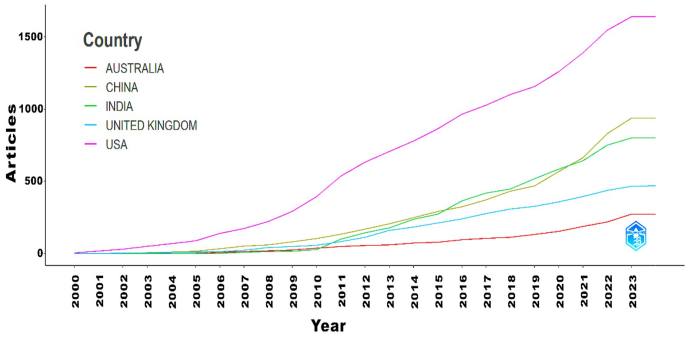

Figure 9 Production of Countries Over Time

Information About The Most Cited Journals, Publications, and Authors

Within the scope of the research on cyber crimes, the most cited journals, publications, and authors among 2566 studies were examined. Table 5 shows the first 25 publications according to the number of citations. The Stuxnet and the Future of Cyber War study is the most cited publication. The top 25 most cited journals are given in Table 6. The most cited journal is IEEE Access. The top 25 most cited authors are given in Table 7. The most cited author

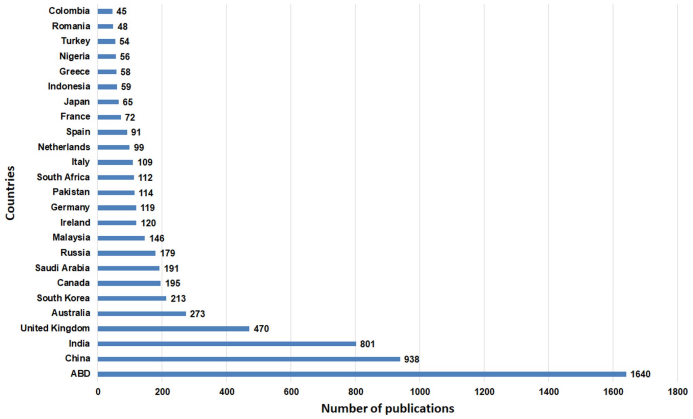

Figure 10 Bar Chart Showing the World's 25 Most Productive Countries

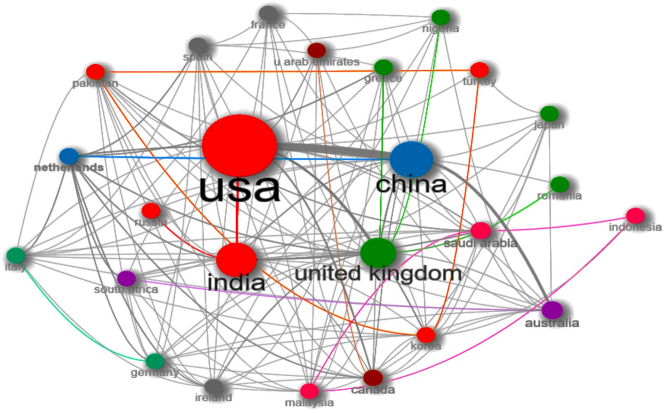

Figure 11 International Cooperation Network Map of Countries on Cybercrime

Table 4 Top 10 Countries by Total Citations in Cybercrime Research

No	Countries	Total Citation	Average Article Quotes
1	USA	8378	15.70
2	UNITED KINGDOM	2267	13.70
3	CHINA	2206	7.80
4	AUSTRALIA	1513	18.70
5	INDIA	1145	4.10
6	CANADA	718	11.60
7	SAUDI ARABIA	430	7.50
8	MALAYSIA	399	8.00
9	NETHERLANDS	384	12.00
10	SPAIN	373	10.70

is Higginsge, with a total of 93 citations. Writer Willison R follows Higgins Ge with 31 citations and writer Holt Tj with 30 citations.

Keyword Analysis

The change in keywords over time is an important indicator for understanding and monitoring developments in a research field. These changes may reflect changes in a topic's popularity, importance, and focus. It is also important to keep abreast of new terms and concepts that arise due to technological advances, societal changes, or other factors. In addition, keywords reflect the authors' work in the best way. These keywords are important elements that summarize the field and highlight research trends. Figure 12 shows the network visualization map analysis of the 25 most frequently used keywords across studies. The size of the circles increases depending on the frequency of use of keywords. The line thickness between keywords increases as the words are used together frequently, which shows the strength of the relationship between them. Clusters are separated by different colors. Computer crime, cybercrime, security, Internet, digital forensics, and machine learning were publications' most frequently used keywords. Table 8 shows the top 25 keywords most used in cybercrime-related publications. In the studies, the word computer was used 601 times, the word cybercrime 410 times, the word security 253 times, the word Internet 128 times, and the word digital forensics 127 times. Figure 12 shows the top 25 most used word clouds. Font sizes are large compared to the word repetition used.

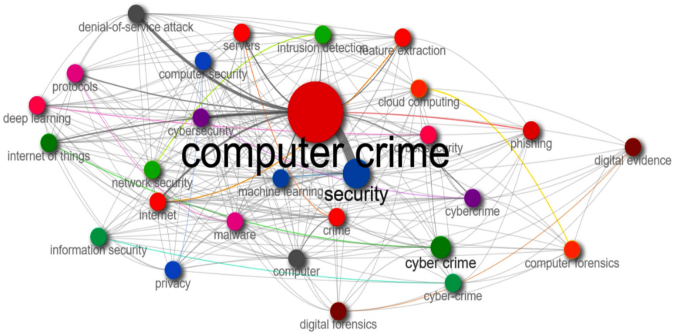

Figure 12 Keyword Analysis

Figure 13 Top 25 Most Used Word Clouds

Thematic Evolution

Keywords are the words that authors think best reflect their work. Therefore, it is very important to see which terms have been used in studies conducted on cybercrime to date to understand the current literature and future trends. This helps you evaluate the popularity and importance of certain terms. For this reason, keywords in the literature were determined, and the frequency of use and change of these words over time were analyzed. Figure 14 shows the analysis of the change and transformation of the most frequently used keywords in studies over the years. In this analysis, 2010 was chosen as the cutting year. Examining Figure 14 reveals that between 2000 and 2010, many terms, such as hacker, security, privacy, computer crime, internet crime, technology, etc., have evolved into cybercrime and computer crime in subsequent years.

Table 5 Top 25 Papers in Cybercrime Research by Total Citation

No	Paper	Total Citation	Annual Citation	Normalized Citation
1	Stuxnet and the Future of Cyber War	460	32.86	43.45
2	Beyond Deterrence: An Expanded View Of Employee Computer Abuse	294	24.50	27.25
3	Password Cracking Using Probabilistic Context-Free Grammars	253	15.81	10.41
4	Examining The Applicability Of Lifestyle-Routine Activities Theory For Cybercrime Victimization	235	14.69	9.67
5	The Cyber Threat Landscape: Challenges And Future Research Directions	231	16.50	21.82
6	Botnet Detection Based On Traffic Behavior Analysis And Flow İntervals	185	15.42	17.15
7	On-Line Activities, Guardianship, And Malware Infection: An Examination Of Routine Activities Theory	169	10.56	6.96
8	Cyber Security İn The Age Of Covid-19: A Timeline And Analysis Of Cyber-Crime And Cyber-Attacks During The Pandemic	161	40.25	16.61
9	A Survey On Technical Threat İntelligence İn The Age Of Sophisticated Cyber Attacks	161	23.00	23.00
10	Secure Cooperative Event-Triggered Control Of Linear Multiagent Systems Under Dos Attacks	160	32.00	11.34
11	A Survey Of Botnet And Botnet Detection	159	9.94	6.55
12	Low Self-Control, Deviant Peer Associations, And Juvenile Cyberdeviance	144	11.08	15.15
13	The 'Butner Study' Redux: A Report Of The Incidence Of Hands-On Child Victimization By Child Pornography Offenders	141	8.81	5.80
14	Insiders' Protection Of Organizational Information Assets: Development Of A Systematics-Based Taxonomy And Theory Of Diversity For Protection-Motivated Behaviors	140	11.67	12.97
15	Hidden Wholesale: The Drug Diffusing Capacity Of Online Drug Cryptomarkets	135	15.00	14.63
16	Botnet In Ddos Attacks: Trends And Challenges	133	13.30	13.76
17	Can Low Self-Control Help With The Understanding Of The Software Piracy Problem?	130	6.50	9.10
18	The Law Of Cyber-Attack	125	9.62	13.15
19	Exploring The Attack Surface Of Blockchain: A Comprehensive Survey	120	24.00	8.51
20	Choice And Chance: A Conceptual Model Of Paths To Information Security Compromise	118	7.38	4.86
21	A Survey On Machine Learning Techniques For Cyber Security In The Last Decade	117	23.40	8.29
22	Predicting Online Harassment Victimization Among A Juvenile Population	117	9.00	12.31
23	Sexual Violence In The Digital Age: The Scope And Limits Of Criminal Law	114	12.67	12.35
24	Lucid: A Practical, Lightweight Deep Learning Solution For Ddos Attack Detection	114	22.80	8.08
25	Estimating The Contextual Risk Of Data Breach: An Empirical Approach	113	11.30	11.69

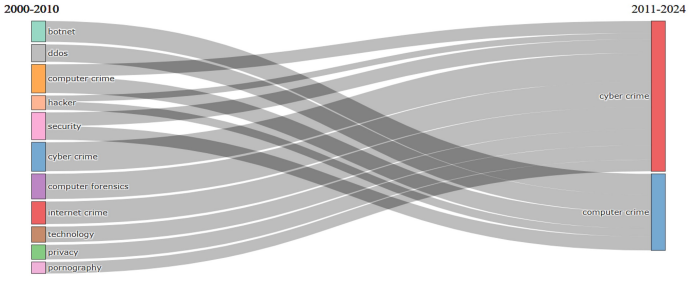

Figure 14 Thematic Development According to Author's Keywords

Trending topics

Based on the analysis of keywords, it was found which topics were more popular and which areas were researched between 2011 and 2023. Figure 15 shows which words and topics were used in publications related to cybercrime during specific years. It is possible to see that these topics evolved according to developments in the literature and new trends in the field of cybercrime. When we examine Figure 14, we see that in 2019, the most frequently used words were cybercrime, crime, and computer. In 2020, security, malware, and botnet were most commonly used. In 2021, the words computer crime, cybersecurity, and machine learning were prominent. In 2022, deep learning, Internet of Things (IoT), and denial-of-service attacks were the most frequently used words. The size of the circles increases with the frequency of word usage. The lines indicate the years during which the words were used. Based on this information, the most current and popular subtopics in cybercrime are deep learning, the Internet of Things, denial-of-service attacks, machine learning, and security. Therefore, researchers in the field of cybercrime should also pay attention to these topics.

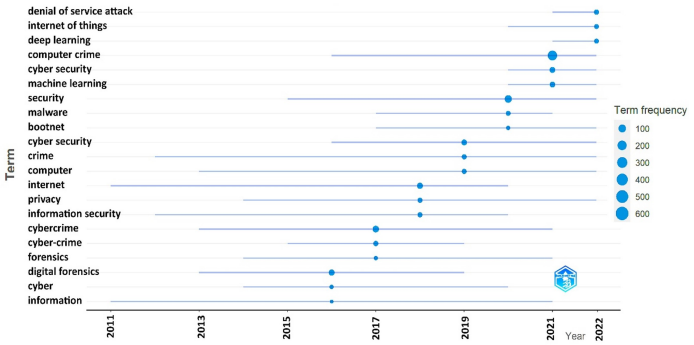

Figure 15 Popular topics used in cybercrime studies over time

Table 6 Top 25 Journals by Total Citations in Cybercrime Research

No	Journals	Total Citation
1	IEEE ACCESS	1920
2	COMPUTERS & SECURITY	1330
3	INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY	1293
4	DIGITAL INVESTIGATION	602
5	IEEE INTERNET OF THINGS JOURNAL	337
6	IEEE SYSTEMS JOURNAL	268
7	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	234
8	IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT	378
9	IEEE TRANSACTIONS ON SMART GRID	187
10	2017 2ND INTERNATIONAL CONFERENCE ON ANTI-CYBER CRIMES (ICACC)	223
11	CRIME LAW AND SOCIAL CHANGE	185
12	IEEE TRANSACTIONS ON CYBERNETICS	285
13	IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	314
14	IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS	306
15	IEEE COMMUNICATIONS SURVEYS AND TUTORIALS	409
16	IEEE SECURITY & PRIVACY	198
17	IEEE NETWORK	181
18	IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT	214
19	IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS	200
20	POLICING-AN INTERNATIONAL JOURNAL OF POLICE STRATEGIES	193
21	VICTIMS & OFFENDERS	105
22	COMPUTER STANDARDS & INTERFACES	63
23	CYBER CRIMINOLOGY: EXPLORING INTERNET CRIMES AND CRIMINAL BEHAVIOR	101
24	DIGITAL FORENSICS AND CYBER CRIME	89
25	DIGITAL FORENSICS AND CYBER CRIME, ICDF2C 2012	98

Table 7 Top 25 Authors by Total Citations in Cybercrime Research

No	Authors	Total Citation
1	HIGGINS GE	93
2	WILLISON R	31
3	HOLT TJ	30
4	MARCUM CD	28
5	MAKIN DA	23
6	BOSSLER AM	20
7	CHOO KKR	19
8	JAISHANKAR K	18
9	BACKHOUSE J	16
10	GRABOSKY P	15
11	ROGERS MK	15
12	SIPONEN M	15
13	ALAZAB M	14
14	BROADHURST R	14
15	CHON S	14
16	DONNER CM	14
17	HEARTFIELD R	14
18	JENNINGS WG	14
19	LOUKAS G	14
20	EPIPHANIOU G	13
21	EROLA A	13
22	LALLIE HS	13
23	MAPLE X	13
24	NURSE JRC	13
25	SHEPHERD LA	13

Table 8 Top Keywords in Cybercrime Research by Frequency of Use

No	Keyword	Number of Uses
1	Computer Crime	601
2	Cyber crime	410
3	Security	253
4	Internet	128
5	Digital Forensics	127
6	Cyber security	121
7	Machine Learning	108
8	Cyber security	105
9	Denial of Service Attack	79
10	Cyber crime	77
11	Crime	71
12	Computer	70
13	Privacy	68
14	Information security	67
15	Malware	64
16	Deep Learning	62
17	Internet of Things	62
18	Computer Security	61
19	Intrusion Detection	58
20	Servers	56
21	Cloud computing	55
22	Digital Evidence	54
23	Computer Forensics	51
24	Feature Extraction	51
25	Phishing	49

DISCUSSION

The dependence of societies and individuals on computers and the Internet is increasing daily. With the widespread use of the Internet and computers in business, entertainment, and government, crimes have moved to the virtual environment, and cybercrime has become increasingly important. Today, the majority of businesses and individuals are exposed to cybercrime. This situation has caused academics to search for solutions and research how to deal with cybercrime. For this reason, it has been observed that the interest in the field of research on cybercrime has increased significantly in recent years, and the demand for scientific research on this subject has increased. Due to the lack of knowledge and increasing dangers in the field of cybercrime, the importance of research in this field is increasing. The rapid and consistent growth of publications on cybercrime over time shows that the subject is a growing and developing field of research.

Cyber crimes, which cause material and moral losses to individuals, institutions, and countries, are committed in multiple ways and for different reasons. Privacy is violated due to phishing, theft, and breach of personal data through phishing. Personal information is used to obtain material and moral benefits. Cybercrime, which is the deletion, corruption, and modification of data belonging to individuals and institutions, is committed by seizing information systems and computer networks. Again, bank and credit card information is obtained through phishing and spam e-mail methods, and this information is misused. With romantic fraud, financial benefits are obtained by exploiting people's well-intentioned feelings and thoughts. By infecting the system with malware and viruses, both information is seized, and a type of

cyber extortion is carried out by demanding ransom.

In our research, despite the fluctuations in the distribution of the number of publications related to cybercrime over the years 2000 to 2023, it is seen that the number of publications has generally increased. It was observed that the number of publications increased rapidly from 2019 to 2022, and the number of publications decreased slightly from 2013 to 2015 and from 2017 to 2018. It was observed that the number of publications remained the same from 2018 to 2019. When the production amounts of publications are examined by years, approximately 85% of the 2566 studies were published after 2010. It was observed that most publications in the field of cybercrime were published in 2022 (253 studies). It was found that the most common type of publication in the field was articles with 1317 studies. This was observed, followed by papers with 925 studies, book chapters with 130 studies, and review articles with 58 studies. When the WoS science network categories for studies on cybercrime were examined, it was found that most studies were in the computer science category, with 2123 studies. The computer science category was followed by engineering with 731 studies, criminology with 462 studies, and telecommunications with 446 studies.

Authors with the highest h_index on the subject: Higgins Ge, Holt Tj, Choo Kkr, Marcum Cd. Wang J. The journals with the highest h_index on the subject are *IEEE Access*, *International Journal of Cyber Criminologists*, *Digital Investigation*, *Computers & Security*, and *IEEE Internet of Things Journal*. The institutions with the highest h-index in this subject area are University College Dublin, Michigan State University, Purdue University, King Khalid University, and Deakin University. It is thought that the geographical locations of countries impact international cooperation. When the number of publications by country is evaluated, it is seen that the countries with high populations or great economic power, such as the USA, China, India, the United Kingdom, and Australia, publish the most studies on cybercrime.

The most cited article was published in *Survival* magazine, "Stuxnet and the Future of Cyber War," by authors Farwell and Rohozinski (2011). The study became the most cited article, with 460 citations. The next most cited article was published in *MIS Quarterly* magazine by authors Willison and Warkentin (2013), titled "Beyond Deterrence: An Expanded View Of Employee Computer Abuse". The article ranked second with a total of 294 citations. The next most cited article was published in the *IEEE Xplore* journal by authors M. Weir and Glodek (2009), titled "Password Cracking Using Probabilistic Context-Free Grammars". This study ranks third with a total of 253 citations.

When the words used in the articles are evaluated, computer crime, cybercrime, security, Internet, digital forensics, cyber security, and machine learning are the most frequently used keywords. The word *computer* was used 601 times, the word *cybercrime* 410 times, the word *security* 253 times, the word *Internet* 128 times, and the word *digital forensics* 127 times. One of the limitations of the current study is that it does not include data from bibliometric databases other than the WoS database. Again, the study is limited since the research and publications in the WoS database will be used from 2000 to 2023.

In this study, we determined the most important and current topics in the field of cybercrime based on a map consisting of author keywords. We hope this type of analysis will help scholars understand the changing scientific landscape of cybercrime research. Generally speaking, deep learning, the Internet of Things, denial of service attacks, machine learning, and cyber security issues have been among the popular topics in cybercrime in recent years. This study emphasizes that the scientific literature on cybercrime is growing and important. The research aims to guide researchers who want to gain information about future studies and trends on these issues. This study guides academics in planning and conducting their research on cybercrime. Our study contributes to understanding the trends and developments of scientific research on cybercrime. Our research focuses on identifying trends in the field of cybercrime and addressing gaps in this field. In this context, it is important to focuscontext, it is important to focus more on policies and studies to combat cybercrime and protect societies, companies, and states is important in this context.

CONCLUSION

This study provides a complete review of studies and publications on cybercrime between 2000 and 2023. The research used bibliometric analysis to examine global trends in cybercrime investigations over the last 23 years. Web of Science (WoS) database was used for bibliometric analysis. A total of 2566 publications, countries, institutions, journals, authors, and subject categories were analyzed to evaluate the effectiveness of studies on cybercrime. Although there has been a decrease from time to time in the number of publications produced over the years, there is a general increase. The country that publishes the most on the subject and where the most effective studies are carried out is the USA. Jaishankar Karuppannan is the most published author. The author who wrote the most influential works and has the highest h_index is George E. Higgins. The journal with the highest h_index and the most publications is *IEEE Access*. Again, the institution with the most publications and the highest h_index is College Dublin University. The most frequently used keyword in research is the term *computer crimes*. The most cited article was published in *Survival* magazine titled *"Stuxnet and the Future of Cyber Warfare"*. The best countries in cybercrime investigations are economically developed and populous countries. This analysis determined which countries, institutions, journals, authors, and subject categories are more effective in this field or contribute more to scientific studies. Considering the number of publications on the subject, the rapid increase in studies in the last two to three years reveals the need for more research on cybercrime. Dealing with cybercrime poses a big problem as the way cybercrime is committed changes day by day. Therefore, more research is needed to prevent and reduce cybercrime activities.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

Borgman, A. and S. Furner, 2001 Scholarly communication and bibliometrics. Annual Review of Information Science and Technology **36**.

C. Lu, W. J. and W. Chang, 2007 Trends in computer crime and cybercrime research during the period 1974-2006: A bibliometric

approach. In *Intelligence and Security Informatics*, volume 4430 of *Lecture Notes in Computer Science*, pp. 244–250.
Cldy, 2023 Email spam statistics 2022 – find out more about spam emails. Accessed: Jan. 03, 2023.
Farwell, J. P. and R. Rohozinski, 2011 Stuxnet and the future of cyber war. Survival (London) **53**: 23–40.
Goodman, M. D. and S. W. Brenner, 2002 The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology **10**: 139–223.
Ho, H. T. N. and H. T. Luong, 2022 Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. Springer International Publishing **2**.
IBM, 2024 What is a cyberattack? | ibm. Accessed: Jan. 28, 2024.
K. Achuthan, R. K. S. R., V. K. Nair and R. Raman, 2023 Cyberbullying research — alignment to sustainable development and impact of covid-19: Bibliometrics and science mapping analysis. Computers in Human Behavior **140**: 107566.
K. Li, J. R. and E. Yan, 2018 Web of science use in published research and review papers 1997–2017: a selective, dynamic, cross-domain, content-based analysis. Scientometrics **115**: 1–20.
K. Shaukat, V. V. I. A. H., S. Luo and M. Xu, 2020 A survey on machine learning techniques for cyber security in the last decade. IEEE Access **8**: 222310–222354.
Kaleci, F., 2023 Ekonomi alanındaki İnovasyon konulu uluslararası bilimsel yayınların bibliyometrik analizi .
Klimburg, A., 2018 *National cyber security framework manual*. Accessed: Apr. 12, 2023.
L. Wu, Q. P. and M. Lembke, 2023 Research trends in cybercrime and cybersecurity: A review based on web of science core collection database. International Journal of Cybersecurity Intelligence and Cybercrime **6**: 5–28.
Lallie, H. S., L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, *et al.*, 2021 Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security .
M. M. Alashqar, A. B. A. R. and A. S. B. A. Aziz, 2021 Examining the trend of research on chemometric analysis: a bibliometric review. Accessed: Apr. 12, 2023.
M. Weir, B. D. M., S. Aggarwal and B. Glodek, 2009 Password cracking using probabilistic context-free grammars. In *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 391–405.
Marsh, I. and G. Melville, 2009 *Crime, Justice and the Media*. Routledge.
Moitra, S. D., 2005 Developing policies for cybercrime: Some empirical issues. European Journal of Crime, Criminal Law and Criminal Justice **13**: 435–464.
Phillips, K., J. C. Davidson, R. R. Farr, C. Burkhardt, S. Caneppele, *et al.*, 2022 Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic Science **2**: 379–398.
R. Ch, M. H. A., T. R. Gadekallu and A. Al-Ahmari, 2020 Computational system to classify cyber crime offenses using machine learning. Sustainability **12**: 4087.
S. Firat, G. G. Y. K., B. O. Alramazanoğlu and M. N. Kurutkan, 2023 H-İndeksi ve akademik başarıyı Ölçme sorunu: Eksiklikler ve sınırlılıkları aşma Çabası. Mehmet Akif Ersoy Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi pp. 1742–1777.
Shukla, G. and S. Gochhait, 2020 Cyber security trend analysis using web of science: A bibliometric analysis. European Journal of Molecular and Clinical Medicine **7**: 6.
Soydal, and U. Al, 2014 Akademinin atıf dizinleri ile savaşı. Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi **31**: 23–42, Accessed: Apr. 12, 2023.
Subektiningsih, S. and D. Hariyadi, 2022 The role of digital forensic experts in cybercrime investigations in indonesia based on the scopus research index **4**: 1665–1670.
W. A. Al-Khater, A. A. A. A. S. S., S. Al-Maadeed and M. K. Khan, 2020 Comprehensive review of cybercrime detection techniques. IEEE Access **8**: 137293–137311.
Wall, D. S., 2024 *Cybercrime: The Transformation of Crime in the Information Age*. Accessed: Mar. 28, 2024.
Wang, W., S. Laengle, J. M. Merigó, D. Yu, E. Herrera-Viedma, *et al.*, 2018 A bibliometric analysis of the first twenty-five years of the international journal of uncertainty, fuzziness and knowledge-based systems. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **26**: 169–193.
Willison, R. and M. Warkentin, 2013 Beyond deterrence: An expanded view of employee computer abuse-web of science core collection. Accessed: Apr. 12, 2023.
Zupic, I. and T. Čater, 2015 Bibliometric methods in management and organization. Organizational Research Methods **18**: 429–472.
Şakar, G. D. and A. G. Cerit, 2013 Uluslararası alan İndekslerinde türkiye pazarlama yazını: Bibliyometrik analizler ve nitel bir araştırma. Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi **27**: 274201337–274201362, Accessed: Apr. 04, 2023.

How to cite this article: Akmeşe, Ö. F., and Erdoğan, M. Bibliometric Analysis of Studies on Cyber Crimes Between 2000-2023. *ADBA Computer Science*, 2(1), 19-29, 2025.