IJCCS (Indonesian Journal of Computing and Cybernetics Systems)
Vol.18, No.1, January 2024, pp. 107~118
ISSN (print): 1978-1520, ISSN (online): 2460-7258
DOI: https://doi.org/10.22146/ijccs.92636

Developments and Trends in Cybersecurity Against Human Factors and Time Pressure Using Bibliometric Analysis

Aprilia Mayang Saputri*[1], Syaifullah[2], Muhammad Lutfi Hamzah[3], Tengku Khairil Asyar[4], Eki Saputra[5],
[1,2,3,4,5] Program Study Information Systems, Faculty of Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru-Riau, Indonesia.
e-mail: ***[1]12050320351@students.uin-suska.ac.id**, [2]syaifullah@uin-suska.ac.id, [3]muhammad.luthfi@uin-suska.c.id, [4]tengkukhairil@uin-suska.ac.id, [5]eki.saputra@uin-suska.ac.id

Abstrak

Memahami keamanan siber sangat penting di era digital saat ini, Faktor manusia berperan penting dalam keamanan siber, dengan lebih dari 95% serangan yang berhasil dilakukan. Selain faktor manusia tekanan waktu juga tidak boleh diabaikan. Penelitian terkait cybersecurity terhadap human factor dan time pressure masih terdapat kekurangan literature. Oleh karena itu Penelitian ini bertujuan untuk menganalisis perkembangan dan tren Keamanan Siber mengenai faktor manusia dan tekanan waktu dari tahun 2014 hingga 2023 menggunakan Analisis Bibliometrik dari perangkat lunak R studio. Data yang didapatkan dalam penelitian ini sebanyak 110. Metodologi penelitian meliputi perencanaan, identifikasi kata kunci, pencarian data Scopus, bibliometric dan biblioshiny, tren terkait cybersecurity, human factor dan time pressure dan terakhir peta tematik. Hasil dari penelitian ini memberikan gambar terkait perkembangan jumlah publikasi yang terus meningkat pada tahun 2023 dengan sebanyak 30 artikel, Computer and security dan Journal of cognitive engineering and decision making merupakan jurnal yang paling relevan, Adam Mtp dan Chowdhury Nh menjadi penulis yang teratas. Selain itu juga memberikan gambaran terkait tren cybersecurity, human factor dan time pressure melalui peta tematik dengan Information security, cybersecurity awarenness, cybersecurity, phising, human factor dan security menjadi tren topik untuk penelitian selanjutnya.

Kata kunci*— Cybersecurity, Human Factor, Time Pressure, Analisis Bibliometric*

Abstract

Understanding cyber security is very important in today's digital era. Human factors play an important role in cyber security, with more than 95% of successful attacks being carried out. Apart from the human factor, time pressure should not be ignored. Research related to cybersecurity on human factors and time pressure still lacks literature. Therefore, this research aims to analyze Cyber Security developments and trends regarding human factors and time pressure from 2014 to 2023 using Bibliometric Analysis from R studio software. The data obtained in this research was 110. The research methodology included planning, keyword identification, Scopus data search, bibliometrics and biblioshiny, trends related to cybersecurity, human factors and time pressure and finally a thematic map. The results of this research provide a picture regarding the development of the number of publications which will continue to increase in 2023 with as many as 30 articles, Computer and security and Journal of cognitive engineering and decision making are the most relevant journals, Adam Mtp and Chowdhury Nh are the top authors. Apart from that, it also provides an overview of cybersecurity trends, human factors and

Received December 30th,2023; Revised January 23th, 2024; Accepted January 25th, 2025

time pressure through a thematic map with information security, cybersecurity awareness, cybersecurity, phishing, human factors and security being trending topics for further research.

Keywords— *Cybersecurity, Human Factor, Time Pressure, Bibliometric Analysis*

1. INTRODUCTION

The presence of increasingly sophisticated technology has created various security challenges including cyber attacks that can threaten critical information and infrastructure [1]. Having a good understanding of Cybersecurity is very important in today's digital era. A large amount of research has been conducted to understand the factors that influence the success or failure of Cybersecurity [2]. Failure in Cybersecurity is not just about designing and providing sophisticated information technology (IT) artifacts, but human factors as well [3].

Experts have long recognized that human factors play an important role in Cybersecurity [3]. In 2017, more than 200,000 computers in 150 countries were affected by the largest ransomware attack due to negligence in updating Windows patches and opening suspicious emails [4] and it is estimated that more than 95% of successful attacks were caused by human error [5]. Apart from human factors, time pressure is also a factor that should not be ignored. Organizations often face high time pressure in a competitive and dynamic business environment, which can influence decisions related to Cybersecurity [6].

According to [7] research entitled Towards an Improved Understanding of Human Factors in Cybersecurity discusses human factors and cyber security. The results of this research show that human factors in cyber security are still the main concern rather than technology. According to [6] research A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers which discusses a team's understanding of human factors in cyber security. The results of this research are the need to consider human factors and the need for good teamwork in improving cyber security. [8] through an article entitled The Impact of Time Pressure on Cybersecurity Behavior: a systematic literature review. This research discusses the impact of time pressure on cybersecurity behavior. The results of this research show that human firewalls under time pressure in cyber security often experience threats that have the potential to cause disaster for users.

Although several previous reports have been conducted to demonstrate an understanding of the Cybersecurity and human factors categories, there is still a lack of literature regarding the development and trends of time pressure [8]. From this context, knowledge about thematic development and expansion patterns of Cybersecurity trends, human factors, and time pressure is still lacking [9]. Therefore, this research aims to analyze Cybersecurity developments and trends regarding human factors and time pressure from 2014 to 2023 using Bibliometric Analysis from the R Package in RStudio. including biblioshiny which is a shiny application that provides a web interface for bibliometrics. From this context, the application of bibliometric analysis methods can summarize data, namely in the form of publication units [10]. Bibliometric analysis is also used to determine global research developments, analyze distribution maps, and interpret cybersecurity regarding human factors and time pressure. This research describes questions related:

RQ1: How will cybersecurity develop regarding human factors and time pressure from 2014-2023?

RQ2: What are cyber security trends regarding human factors and time pressure in the future?

2. METHODS

2.1 Planning

The planning stage begins with determining a theme, where the theme in this research is related to cybersecurity. This research uses data from 2014-2023. This data was obtained from the SCOPUS database which contains various quotes regarding keyword searches used for bibliometric analysis. This database is often used to retrieve data in systematic reviews [11] and bibliometric analysis [12] because it contains the highest quality scientific publications. In this case, the procedure produced a data document containing 110 articles. The metadata is then extracted in bib style format.

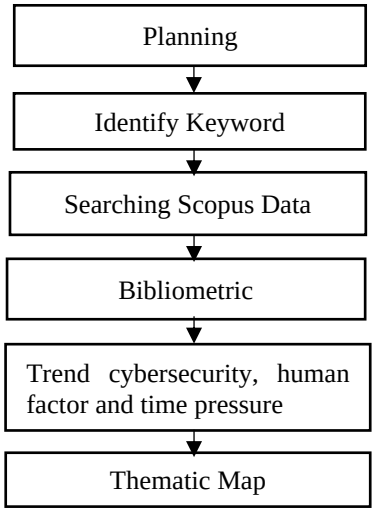

Figure 1 Methodology

2.1. *2.2 Identify Keyword*

Keyword identification is a step taken by researchers to find the keywords to be used. Keyword identification was carried out by collecting various articles and journals related to Cybersecurity, human factors, and time pressure [13]. In bibliometric analysis, the use of keywords allows researchers to better measure the trends, quantity, and impact of research related to a particular topic. Apart from that, keywords are also used to facilitate searching and understanding relevant scientific literature in a knowledge domain. Researchers use Boolean logic operators such as AND/OR in determining keywords [14].

This research uses the search keywords " Cybersecurity", "Human Factor", "Time Pressure" with the search syntax: ALL (Cybersecurity OR "Cyber Security" OR "Information security" AND "human factor" AND "time pressure" OR "time limit" OR “time stress” OR “time constraint”) AND (LIMIT-TO (DOCTYPE, “ar”)) AND (LIMIT-TO (PUBSTAGE, “final”)) AND (LIMIT-TO (SRCTYP, “j”)) AND (LIMIT-TO (LANGUAGE, “English”)). This keyword will be used by researchers in searching for data in the Scopus database regarding this topic. Searching for keywords in the Scopus database can be seen in Figure 2.

Figure 2 Keyword search in the Scopus database

2. 3 Searching Scopus Data

Research on Cybersecurity can be found in various scientific publication media, whether journals, conference proceedings, or books. These media have different qualities. One thing that determines quality is the peer review process [15]. Therefore, this research chose Scopus and Web of Science as data sources because scientific articles indexed by Scopus go through a peer review process. Scopus is a citation and abstract database supervised by experts in the field [16]. Based on information from the Scopus website (http://www.scopus.com) which was accessed on 07 November 2023, data was generated for 226 articles that were in accordance with the research theme. Scopus is the world's largest data center covering millions of scientific literature published decades ago by Elsevier. Scopus helps researchers to search, analyze and visualize research effectively [17]. A total of 226 articles were filtered to prevent duplicate keywords and filters, such as (1) search in "all fields" (2) Selected Criteria 10 Years (2014-2023), (3) Filter based on Document Type, (4) Publication Stage, (5) Source Type, and (6) Language. In this case, the procedure produced a data document containing 110 articles whose metadata was then extracted in bib-style format. This results in the retrieval of a variety of information, including citations, bibliograpic, abstract & keywords. This can be seen in the figure 2.

2. 4 Bibliometrics

Professor Massimo Aria launched Bibliometrics in 2017. Bibliometrics is a package used in R software. In R, there is also biblioshiny which is an application that provides a web interface for bibliometrics[18]. To use bibliometric and biblioshiny techniques, you can install R from Rstudio. After installing, run the command “install.packages (“bibliometrix”), this is used to install the bibliometrix package. When finished, then "library(bibliometrix) where this command is to load the bibliometrix package. The final step is to enter the command “biblioshiny()”, this command opens the interface. The metadata is extracted in the form of bibs, the data will be imported and converted to data frame collection. The biblioshiny interface will display analysis and plot results for four different level metrics including: source, author, document, and Clustering by Coupling. Followed by an analysis of three knowledge structures (K-structures) such as: conceptual structure, intellectual structure and social structure. Of the 7 analysis menu, each contains a submenu where this supports scholars in using bibliometrix's main features easily. The biblioshiny interface can be seen in the figure 3.

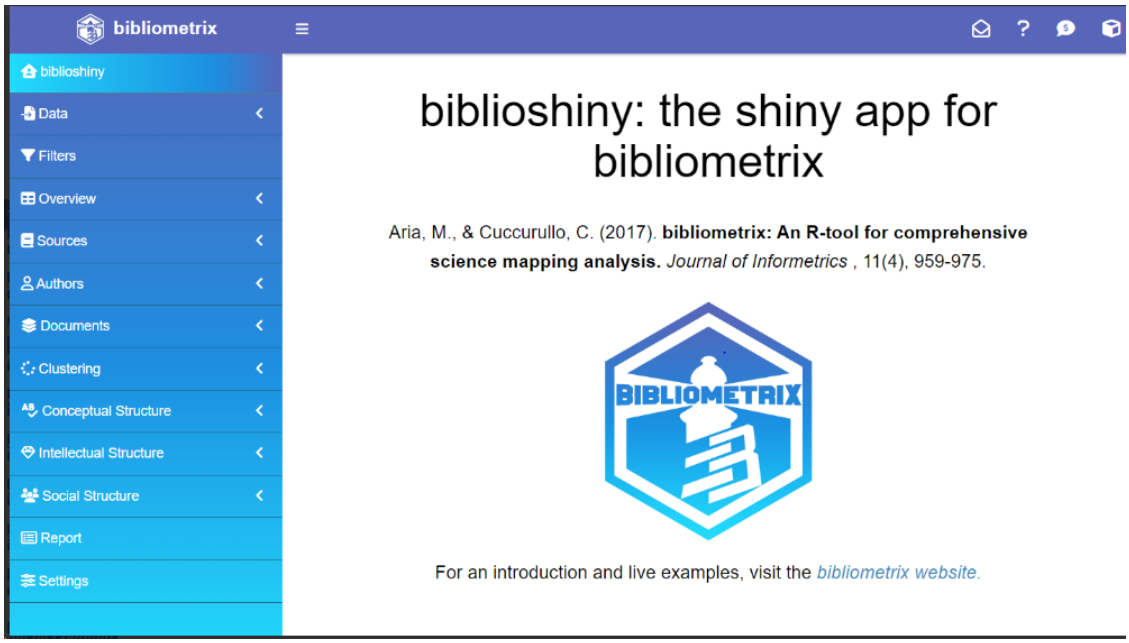

Figure 3 biblioshiny interface

2. 5 Trends Cybersecurity, Human Factors, and Time Pressure

Along with technological advances and increasingly complex cyber threats, Cybersecurity trends, human factors, and time pressure continue to experience major developments. Trend analysis can be performed after importing Scopus data in bibliometrics [19]. Bibliometric Cybersecurity trends, human factors, and time pressure can be seen on the thematic map which is clustered into several clusters. This thematic map will later become a reference for future researchers to research the themes of Cybersecurity, human factors, and time pressure [20].

2. 5.1 Thematic Map

Thematic map analysis of Cybersecurity, human factors and time pressure is linked to two dimensions, namely density and centrality. Furthermore, the themes on the thematic map are grouped based on 4 different categories, namely, motorbike themes, niche themes, emerging of declining themes, and basic themes [21]. Motor Themes is located in the first quadrant, top right with a cluster network that has high centrality and density, indicating that the themes have been well developed and are important for structuring research subjects [22]. Niche Themes or special themes are located in the second quadrant, top left with high density themes and low centrality which indicates that its relevance is limited [23]. Emerging of declining themes is located in the third quadrant, bottom left with low centrality and low density themes and indicates that they are both minimally advanced and margin [24]. Lastly, Basic Themes which are located in the fourth quadrant, bottom right with high centrality and low density, these themes are very important for transdisciplinary research issues [25]. In a visual representation, identifying a trajectory is shown by dividing time into segments in other words a movement towards the top right over time indicates an increasing trend while a path towards the bottom left indicates a decreasing trend.

3. RESULTS AND DISCUSSION

3.1 Cybersecurity Development Against Human Factors and Time Pressure

The data used in this research amounted to 110 articles originating from the Scopus database taken from 2014-2023 which were identified based on document type, journal source type, year of research, search within "all fields" and research trends. Next, the data was processed using a bibliometric approach with R Studio software based on 110 existing article data. The processed data results display graphs of statistical data based on the data in the article.

3.1.1 Cybersecurity research on human factors and time pressure based on publications and average annual citations

Based on the available publication results, it describes the total number of publications and article citations so that the volume of article publications can be measured. Figure 4 and Figure 5 show the development of Cybersecurity regarding human factors and time pressure from 2007 to 2023.

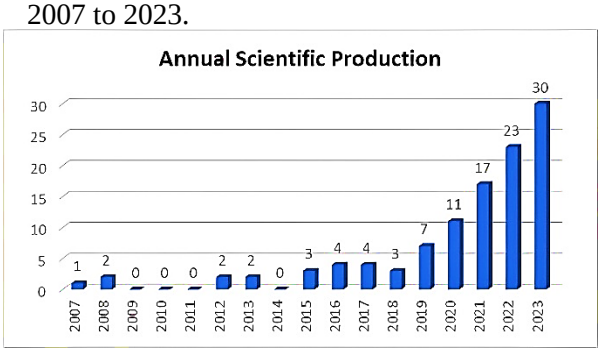

Figure 4 Research developments based on publications

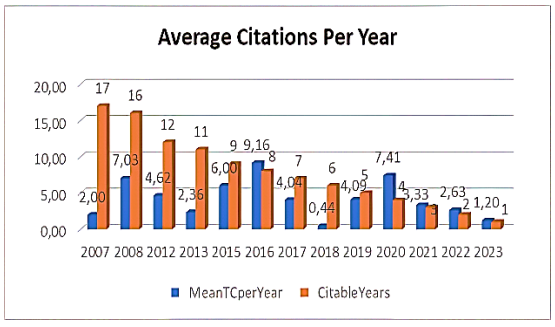

Figure 5 Research development based on average annual citations

Figure 4 presents the evolution of Cybersecurity publications on human factors and time pressure based on the number of publications from 2007 to 2023. During this period, the 110 most relevant scientific publications were presented. In 2007, 2008, 2012, 2013, 2015, until 2018 the development of publications was at a medium level with the number of articles being 1, 2, 2, 2, 3, 4, 4, and 3 articles. However, in 2009, 2010, 2011, and 2014 there was no increase in the number of article publications. The number of article publications began to increase in 2019 with a total of 7 articles. The number of publications continues to increase in the following years until 2023 with an increase in the number of publications by 30 articles.

Based on Figure 5, the average number of article citations per year is depicted. Since the emergence of research on Cybersecurity on human factors and time pressure in 2007, the average number of annual citations has gone through several different phases. In the first phase, the average value increased progressively from 2007 to 2008, reaching 7.03 in 2008, before decreasing to 4.62 and 2.36 respectively in 2012 and 2013. For the second phase, Cybersecurity on human factors and time pressure increased and peaked in 2016 with an average of 9.16 citations. This was accompanied by a third phase where the average value decreased to 4.04 and 0.44 in 2017 and 2018. In 2019 the average citation increased by 4.09 and continued to increase significantly in 2020 with an average citation of 7.41. Average citations peaked in 2016 and 2020 with average citations of 9.16 and 7.41 from early 2007 to the present. This shows that the period starting in 2021 and ending in 2023 continues to experience a decline in the average number of citations with the lowest value of 1.20 occurring in 2023.

3.1.2 Cybersecurity research on human factors and time pressure based on the most relevant journals

Table 1 Research developments based on the most relevant journals

Sources	Articles
Computers and Security	6
Behavior and Information Technology	5
Information and Computer Security	4
International Journal of Human-Computer Studies	4
Journal Of the Association for Information Systems	3
Sensors	3
Acm Transactions on Privacy and Security	2
Applied Ergonomics	2
Computers In Human Behavior	2
Journal Of Cognitive Engineering and Decision-Making	2

Based on Table 1, there are the top 10 published journals with the highest number of publications. Computer and Security and Behavior and Information Technology journals were ranked first and second with 6 and 5 articles respectively. Information and Computer Security and the International Journal of Human-Computer Studies were ranked third with 4 articles each. The Journal of the Association for Information Systems and Sensors was ranked fourth with a total of 3 articles. Further publications such as Acm Transactions on Privacy and Security, Applied Ergonomics, Computers in Human Behavior, and Journal of Cognitive Engineering and Decision Making were ranked last with a total of 2 articles.

3.1.4 Cybersecurity research on human factors and time pressure based on the most relevant keywords

Word co-occurrence networks are used to map and combine terms taken from keywords, titles, or abstracts in a bibliography to analyze words and determine the conceptual structure of a framework. Describe terms from textual fields such as abstract, title, keywords, and author as well as remove words and apply a stemming algorithm porter. Stemming is the reduction of changed

(or sometimes derived) words to their basic form in a written format that emphasizes the words that appear most frequently in a text or reader's collection.

Cybersecurity analysis of human factors and time pressure, and identification of the most important topics, concepts, and themes are also facilitated by analyzing the most frequently used words. The frequency of the author's keywords in Cybersecurity publications regarding human factors and time pressure can be seen in Figure 6. Cybersecurity is ranked first out of 978 keywords that frequently appear with 15 occurrences, phishing, time pressure, decision making, cyber security, technostress, and human-computer. interaction, human factors, information security, and literature review with 10, 8, 5, 4, 4, 3, 3, 3, and 3 word occurrences respectively.

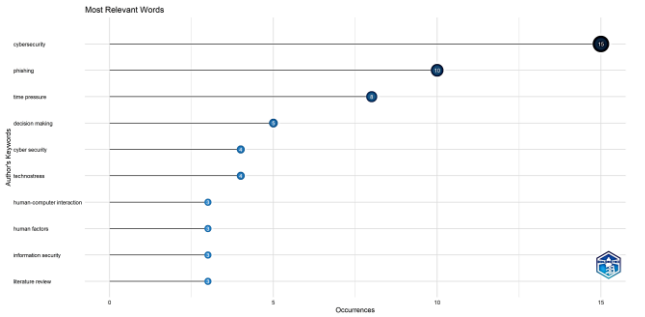

Figure 6 Research developments based on the most relevant keywords

Figure 7 WorldCloud

WorldCloud can be seen in Figure 7, where WorldCloud describes the author's keywords with the font size of a term indicating its frequency level. Even though Figure 6 and Figure 7 have different shapes, the content remains the same with a different presentation concept.

3.1.7 Cybersecurity research on human factors and time pressure based on Collaboration Country

International cooperation between countries can be seen in Figure 8 with the red line showing connections when cooperation is found between two countries or regions. Circles are used to indicate the frequency with which a particular topic trend appears with horizontal lines indicating the range between quartiles, indicating the period in which a topic trend reaches its popularity. In this case, the line width is proportional to the degree of collaboration. Australia, Austria, Canada, and China are also centers of publication with many red lines visible between these countries and others. Australia has specifically established 6 cooperative relationships with other countries regarding the publication of 2, 1, 3, and 1 articles with Germany, Lithuania, Malaysia, and the United Kingdom. Austria currently has partnerships with the countries of Canada and Germany which have resulted in the publication of 1 and 1 articles. Canada also established partnerships and published 1 and 1 articles with New Zealand and Serbia. Lastly, China collaborated with Australia and produced 2 articles. China and the United Kingdom also collaborated and produced 1 article.

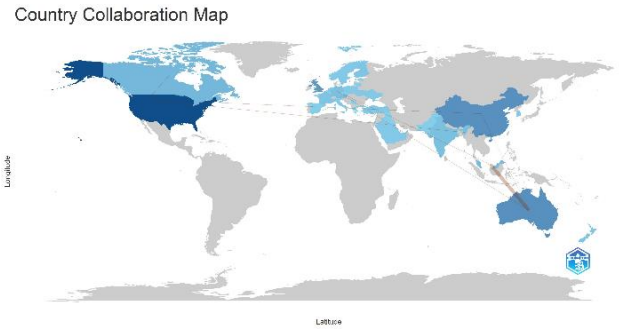

Figure 8 Research developments based on country collaboration

3.1.8 Cybersecurity research on human factors and time pressure based on trends topic

The circles that can be seen in Figure 9 show the frequency of occurrence of certain keywords, with the horizontal line showing the range between the first quartile and the third quartile. Where the circle shows the period and extent to which the keyword achieved popularity. Based on an analysis of 978 occurrences of words in Cybersecurity regarding human factors and time pressure, network security, there are 10 trending topics from 2017 to 2023. In 2019 computer security became a trending topic until 2023. Not only that, female, male, and adult, are trending topics or research that are often discussed in 2020 until 2023. in 2022. Human research and articles are trending discussion topics in 2021. Not only that, Cyber security, phishing, and computer crime, are discussions that are often discussed by research until now in 2023. However, it can be seen in Figure 13 of the thematic map, Information security, cybersecurity awareness, cybersecurity, phishing, human factors, and security are trending topics for further research.

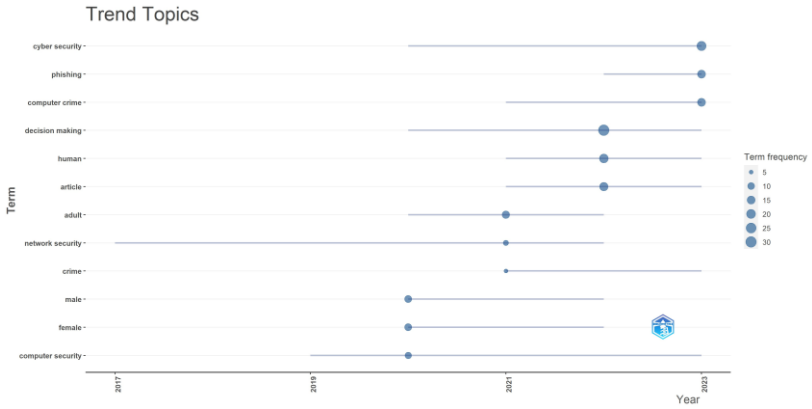

Figure 9 Research developments based on trends topic

3.1.9 Cybersecurity research on human factors and time pressure based on the Co-occurrence Network

Based on Figure 10, it can be observed that 5 clusters are grouped and interconnected, with each group represented by the most dominant element. These results, decision making, cyber security, behavioral research, computer crime, phishing, cyber security, electronic mail, and time pressure are the first clusters marked with red nodes and represent the other clusters. The second cluster is shown with blue nodes. Meanwhile, the third cluster is marked with green nodes. Human, human experiment, adult, female, and male is the fourth cluster marked in purple. Finally, cluster 5 is shown with an orange node. According to the keyword cumulative degree plot in mobile exploration, cyber security is a keyword with a plot degree of 0.867. Human is the most central keyword with a level of 1.00. This is accompanied by decision-making, computer crime, electronic mail, adult, phishing, female, male, behavioral research, Cybersecurity, computing security, and time pressure with degrees 0.926, 0.691, 0.628, 0.59, 0.569, 0.569, 0.569, 0.537, 0.521, 0.511, and 0.484.

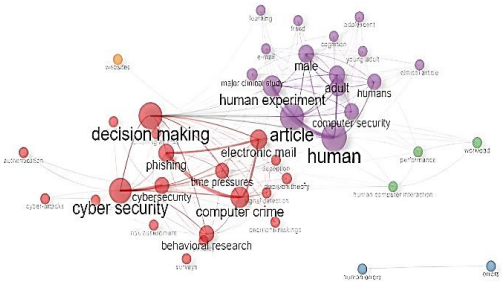

Figure 10 Research developments based on co-occurrence networks

3.2 Trends Cybersecurity to Human Factors and Time Pressure

The analysis method is responsible for the visualization of data through maps such as social networks and two-dimensional maps. Network Analysis also allows statistical analysis of the resulting map to show differences in the relationships of the various detected clusters. Visualization describes the results of analysis contained in scientific maps such as thematic maps, where thematic maps depict a network that shows the proximity between objects that have similarities [26]. However, the purpose of the analysis is to determine the conceptual, intellectual, or social evolution of a field of analysis by identifying patterns, trends, seasonality, and outliers. The aim of this analysis is to identify features with high intensity in a limited time. In this context, a series of clusters and thematic areas are used to describe evolution over several periods [27].

3.2.1 Thematic Map

Thematic map analysis of Cybersecurity, human factors, and time pressure is associated with two dimensions, namely density and centrality. Furthermore, the themes on the thematic map are grouped based on 4 different categories, namely, motorbike themes, niche themes, emerging or declining themes, and basic themes.

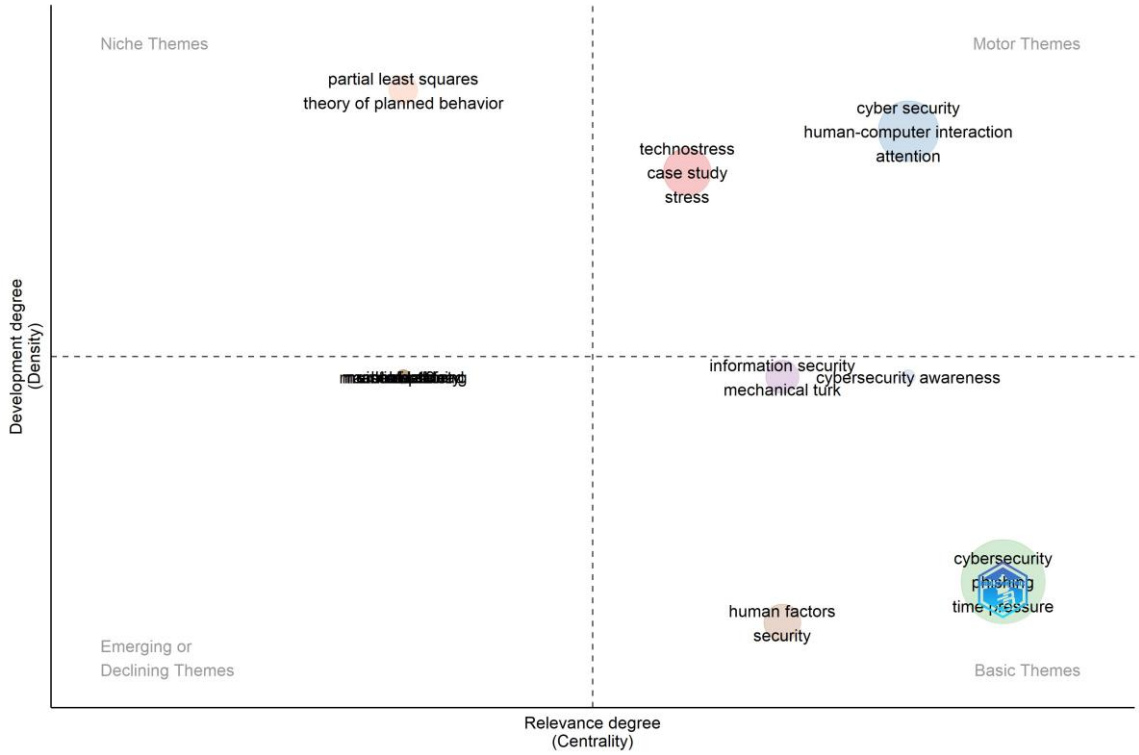

Figure 3 Thematic Map

Based on Figure 11 Cyber security, human-computer interaction, attention, technostress, case study, and stress are part of the motor themes. Partial least squares and the theory of planned behavior are part of the niche themes in the upper left quadrant. Automation is in the Emerging of declining Themes section which is located in the third quadrant, bottom left. Information security, cybersecurity awareness, mechanical, cyber security, phishing, time pressure, human factors, and security are part of the Basic Themes. On basic themes Information security, cybersecurity awareness, mechanical, cyber security, phishing, time pressure, human factors, and security are important topics that are not developed optimally. However, among several topics in the basic theme quadrant cybersecurity, human factors, information security, and cybersecurity awareness have a high centrality rank and a low-density rank which can be seen in Table 3.

Table 2 Visual interpretation based on thematic map clusters

Clusters	RankCentrality	RankDensity
Technostress	9	12
Cyber Security	12.5	13
Cybersecurity	14	2
Information Security	10.5	7
Machine Learning	4.5	7
Human Factors	10.5	1
Mental Workload	4.5	7
Visualization	4.5	7
Ahp	4.5	7
Partial Least Squares	4.5	14
Cybersecurity Awareness	12.5	7
Covid-19	4.5	7
Maritime Safety	4.5	7
Automation	4.5	7

4. CONCLUSIONS

RQ1: How will cybersecurity develop regarding human factors and time pressure from 2014-2023? The development of cybersecurity regarding human factors and time pressure based on article publications from 2009 to 2014 did not find any development in the number of publications. The number of article publications began to increase in 2019 with a total of 7 articles and continues to increase with a total of 30 articles in 2023. The average citation reached its peak in 2016 and 2020 with an average citation of 9.16 and 7.41. Computer and security ranked first with the highest number of publications with 6 articles. The Journal of Cognitive Engineering and Decision Making was ranked last with the number of published articles of 2. Adam Mtp and Chowdhury Nh were ranked first and second with the number of articles of 4. Based on an analysis of 978 occurrences of words in cybersecurity regarding human factors and time pressure cyber security, phishing, and computer crime are trending discussions until now in 2023. Information security, cybersecurity awareness, cybersecurity, phishing, human factors, and security are trending topics for further research.

RQ2: What are cyber security trends regarding human factors and time pressure in the future? Cybersecurity trends regarding human factors and time pressure can be seen with a thematic map. There are 4 different categories in the thematic map, including motor themes, niche themes, emerging of declining themes, and basic themes. Research trends can be seen in basic themes where cybersecurity, human factors, information security, and cybersecurity awareness have a high centrality rank and a low-density rank. Cybersecurity has a RankCentrality of 9 and a RankDensity of 12, Human factor has a Rank Centrality of 10.5 and a Rank density of 1, information security has a Rank centrality of 10.5 and a Rank density of 7, and finally cybersecurity awareness has a Rank centrality of 12.5 and a rank density of 7.

REFERENCES

[1] G. D. Moody, M. Siponen, and S. Pahnila, “TOWARD A UNIFIED MODEL OF INFORMATION SECURITY POLICY COMPLIANCE Appendix B Validation and Analysis Details for Analysis of Eleven Theories Used in Previous IS Behavioral Security

Research: Appendix," *MIS Q.*, vol. 42, no. 1—Appendices, 2018, [Online]. Available: https://misq.org/skin/frontend/default/misq/pdf/appendices/2018/V42I1Appendices/14_13853_RA_MoodyAppendices.pdf

[2] H. Young, T. van Vliet, J. van de Ven, S. Jol, and C. Broekman, "Understanding human factors in cyber security as a dynamic system," *Adv. Intell. Syst. Comput.*, vol. 593, no. March 2022, pp. 244–254, 2018, doi: 10.1007/978-3-319-60585-2_23.

[3] M. S. Jalali, M. Siegel, and S. Madnick, "Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment," *J. Strateg. Inf. Syst.*, vol. 28, no. 1, pp. 66–82, 2019, doi: 10.1016/j.jsis.2018.09.003.

[4] Washington, "More than 150 countries affected by massive cyberattack, Europol says." Accessed: Oct. 05, 2023. [Online]. Available: http://wapo.st/2pKyXum

[5] IBM, "Analysis of cyber attack and incident data from IBM's worldwide security operations," *IBM Secur. Manag. Secur. Serv.*, p. 11, 2014, [Online]. Available: http://public.dhe.ibm.com/common/ssi/ecm/en/sew03031usen/SEW03031USEN.PDF

[6] B. P. Hámornik and C. Krasznay, "A team-level perspective of human factors in cyber security: Security operations centers," *Adv. Intell. Syst. Comput.*, vol. 593, pp. 224–236, 2018, doi: 10.1007/978-3-319-60585-2_21.

[7] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, "Towards an improved understanding of human factors in cybersecurity," *Proc. - 2019 IEEE 5th Int. Conf. Collab. Internet Comput. CIC 2019*, no. Cic, pp. 338–345, 2019, doi: 10.1109/CIC48465.2019.00047.

[8] M. T. P. A. & G. S. Noman H. Chowdhury, "Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures," *Comput. Secur.*, vol. 97, p. 101963, 2020, doi: 10.1016/j.cose.2020.101963.

[9] M. T. P. A. & G. S. Noman H. Chowdhury, "The impact of time pressure on cybersecurity behaviour: a systematic literature review," *Behav. Inf. Technol.*, vol. 38, no. 12, pp. 1290–1308, 2019, doi: 10.1080/0144929X.2019.1583769.

[10] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, no. April, pp. 285–296, 2021, doi: 10.1016/j.jbusres.2021.04.070.

[11] H. W. Awalurahman, I. H. Witsqa, I. K. Raharjana, and A. H. Basori, "Security Aspect in Software Testing Perspective: A Systematic Literature Review," *J. Inf. Syst. Eng. Bus. Intell.*, vol. 9, no. 1, pp. 95–107, 2023, doi: 10.20473/jisebi.9.1.95-107.

[12] O. Martorell Cunill, A. Socias Salvá, L. Otero Gonzalez, and C. Mulet-Forteza, "Thirty-fifth anniversary of the International Journal of Hospitality Management: A bibliometric overview," *Int. J. Hosp. Manag.*, vol. 78, no. September 2018, pp. 89–101, 2019, doi: 10.1016/j.ijhm.2018.10.013.

[13] X. Zhang, "A BIBLIOMETRIC ANALYSIS of SECOND LANGUAGE ACQUISITION between 1997 and 2018," *Stud. Second Lang. Acquis.*, vol. 42, no. 1, pp. 199–222, 2020, doi: 10.1017/S0272263119000573.

[14] A. Syahid and N. Mukminatien, "Thirty years of teflin journal: A bibliometric portrait through the lens of microsoft academic," *Teflin J.*, vol. 32, no. 1, pp. 134–166, 2021, doi: 10.15639/teflinjournal.v32i1/134-166.

[15] R. H. Raja Mohd Ali, A. Ahmi, and S. Sudin, "Examining the trend of the research on the internet of things (IoT): A bibliometric analysis of the journal articles as indexed in the Scopus database," *J. Phys. Conf. Ser.*, vol. 1529, no. 2, 2020, doi: 10.1088/1742-6596/1529/2/022075.

[16] A. Maalej and I. Kallel, "Does Keystroke Dynamics tell us about Emotions? A Systematic Literature Review and Dataset Construction," *Proc. 2020 16th Int. Conf. Intell. Environ. IE 2020*, no. August, pp. 60–67, 2020, doi: 10.1109/IE49459.2020.9155004.

[17] A. R. Saleh and E. Sumarni, "Studi Bibliometrik pada Jurnal Standardisasi Pasca Terakreditasi (2011 – 2015)," *Visi Pustaka*, vol. 18, no. Desember, pp. 231–240, 2016.

[18] M. Aria and C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *J. Informetr.*, vol. 11, no. 4, pp. 959–975, 2017, doi: 10.1016/j.joi.2017.08.007.

[19] H. C. Chang, "The synergy of scientometric analysis and knowledge mapping with topic models: Modelling the development trajectories of information security and cyber-security research," *J. Inf. Knowl. Manag.*, vol. 15, no. 4, pp. 4–6, 2016, doi: 10.1142/S0219649216500441.

[20] N. N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," *Scientometrics*, vol. 121, no. 2, pp. 1189–1211, 2019, doi: 10.1007/s11192-019-03222-9.

[21] M. J. Cobo, A. G. López-Herrera, E. Herrera-Viedma, and F. Herrera, "Science mapping software tools: Review, analysis, and cooperative study among tools," *J. Am. Soc. Inf. Sci. Technol.*, vol. 62, no. 7, pp. 1382–1402, 2011, doi: 10.1002/asi.21525.

[22] R. Alkhammash, "Bibliometric, network, and thematic mapping analyses of metaphor and discourse in COVID-19 publications from 2020 to 2022," *Front. Psychol.*, vol. 13, 2023, doi: 10.3389/fpsyg.2022.1062943.

[23] A. Parlina, K. Ramli, and H. Murfi, "Theme mapping and bibliometrics analysis of one decade of big data research in the scopus database," *Inf.*, vol. 11, no. 2, pp. 1–26, 2020, doi: 10.3390/info11020069.

[24] D. D. Mühl and L. de Oliveira, "A bibliometric and thematic approach to agriculture 4.0," *Heliyon*, vol. 8, no. 5, p. e09369, 2022, doi: 10.1016/j.heliyon.2022.e09369.

[25] A. Abdollahi, K. Rejeb, A. Rejeb, M. M. Mostafa, and S. Zailani, "Wireless sensor networks in agriculture: Insights from bibliometric analysis," *Sustain.*, vol. 13, no. 21, 2021, doi: 10.3390/su132112011.

[26] K. van Nunen, J. Li, G. Reniers, and K. Ponnet, "Bibliometric analysis of safety culture research," *Saf. Sci.*, vol. 108, no. November 2016, pp. 248–258, 2018, doi: 10.1016/j.ssci.2017.08.011.

[27] M. J. Cobo, A. G. López-Herrera, E. Herrera-Viedma, and F. Herrera, "An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field," *J. Informetr.*, vol. 5, no. 1, pp. 146–166, 2011, doi: 10.1016/j.joi.2010.10.002.