


# A Bibliometric Analysis on Cybersecurity Using VOSviewer: An Evaluation for Public Security

Vedat Yilmaz

**Abstract—** This bibliometric study conducts a comprehensive analysis of the field of cybersecurity, particularly in the context of law enforcement and security strategies, to examine key trends, author influence, and interdisciplinary connections within the literature. In the WoS database, 6606 articles were reached by using the search expression in the title, abstract and keywords fields ("Cyber security" or "cyber-attacks" or "cyber protection" or "spam cyber security" or "data security" or "network security" or "anomaly detection" or "cyber countermeasures") and restricting the year of publication to after 2000. The analysis includes metrics such as keyword co-occurrence frequency, author citation impact, co-authorship networks, bibliographic coupling of documents, co-citation analysis of authors, and institutional bibliographic connections. This study highlights the relationship between cybersecurity, law enforcement, and public safety, assessing the role of methodologies and technologies in mitigating security threats and reducing their impacts. When the keywords in the articles obtained as a result of the keyword analysis were examined, it was seen that the words "anomaly detection", "cybersecurity", and "deep learning" were the most frequently used keywords. It is noteworthy that the word "deep learning" was not included in the words generated when determining the articles, but it was used as a keyword in the articles obtained as a result of the determined keywords. Author citation analysis revealed influential contributors such as Quin Du, Wei Li, and Liangpei Zhang. Country-level analysis shows that China and the United States are leading in the field of research output, and institutional analysis highlights the prominent role of the Chinese Academy of Sciences. In conclusion, this research provides valuable insights into how law enforcement and security strategies intersect with academic studies in cybersecurity, offering a roadmap for future research.

**Index Terms—** Cyber Security, Anomaly Detection, Cyber Attacks, Security Technologies, Law Enforcement

Vedat YILMAZ, is with Department of Institute of Forensic Sciences, Gendarmerie and Coast Guard Academy, Ankara, Türkiye, (e-mail: [vedat.yilmaz@jsga.edu.tr](mailto:vedat.yilmaz@jsga.edu.tr)).

 <https://orcid.org/0000-0002-3112-9371>

Manuscript received Dec 27, 2024; accepted Feb 07, 2025.

DOI: [10.17694/bajece.1608364](https://doi.org/10.17694/bajece.1608364)

## I. INTRODUCTION

CYBERSECURITY HAS become increasingly important in the technology-driven world that permeates every aspect of our lives. In this context, security policies and various technical and strategic approaches have been developed based on the three pillars of cybersecurity: confidentiality, integrity, and availability. Cybersecurity, especially in areas such as anomaly detection, network security, and system monitoring, plays a critical and vital role in the early detection of potential threats and the prevention of cyber-attacks. However, the rapidly developing and expanding literature in this field reveals that new cyber-attack methods should be evaluated as hostile actions that include national security as well as individual security, in parallel with technological developments. For this reason, the concept of Cybersecurity is widely researched in interdisciplinary areas, and its importance against new threats that we can describe as hostile actions is increasing day by day. These challenges include tracking and understanding developments, staying informed about current cybersecurity trends, and monitoring necessary precautions. In addressing these challenges, bibliometric analyses provide an effective solution by systematically examining key concepts in the literature, especially the commonalities among authors and scientific research trends [1, 2]. Visualization tools such as VOSviewer enhance the accessibility of these analyses, enabling a comprehensive examination of scientific productivity and interactions in the fields of cybersecurity and anomaly detection. VOSviewer is a data analysis software that makes it possible to provide bibliometric analysis, visualization, and scientific maps used by researchers to analyze and determine the content of Academic citations [3-5]. In the 21st century, characterized by the accelerated pace of digital transformation, the daily activities of both individuals and institutions are increasingly becoming digitized. By 2030, numerous technologies, such as 6G, the decentralized Internet, and the Internet of Senses, are expected to become integral to our lives [6, 7]. Digital systems are employed in nearly every domain, from law enforcement and national security to financial transactions and authentication processes, from digital identities and healthcare services to e-government systems and personal communication tools. While the use of these systems offers significant advantages for both individuals and organizations, it has also highlighted the critical importance of data security, particularly for data stored and transferred in digital environments. Consequently, these developments have

prompted individuals and government institutions to take substantial precautions against potential threats to these systems.

Given these considerations, cybersecurity has not only become an essential element at both individual and institutional levels but has also emerged as a top priority for national security [8]. Cybersecurity, in its simplest terms, refers to the methods and technologies employed to ensure the confidentiality, integrity, and availability of data, often referred to as digital assets. However, today's rapid development of technology and the hostile actions that emerge in cyberspace in parallel with this development require constantly taking new measures for the fight to be carried out in cyberspace. New areas of work have emerged to protect the security of data stored on many different platforms for data and network security [8,9].

Recent developments have transformed the concept of cyber security from a purely defensive field to a multi-disciplinary structure that tries to understand the new methods used by attackers to enter systems [10,11]. This new structure has led to the development of new strategies and preventive measures [11].

Cyber threats are generally the compromise of the confidentiality, integrity, or availability of a person's or an organization's data, computer system, network, or device by attempting to gain unauthorized access or exploit any existing security vulnerabilities in the information sections. [12, 13].

Cyber threats: It covers all kinds of malicious activities targeting the digital assets of individuals, public institutions and organizations, and private sector companies. These malicious activities often include data theft, Distributed Denial of Service (DDoS) attacks aimed at partially or completely disrupting the operation of the system, or financial fraud exposure of individuals or institutions, which is considered cybercrime [14]. Today, not only has the number of these attacks increased, but their complexity has also escalated [15].

The increasing complexity of cyber-attacks means not only an increase in the number of attacks, but also the use of more sophisticated techniques, methods, and tools. This complexity can manifest itself in the following areas:

- Multi-Layered Attacks: A combination of multiple attack types (e.g., DDoS, phishing, and malware) rather than a single attack [16].
- Advanced Persistent Threats (APT): Infiltrating the target for extended periods, gathering information, discovering vulnerabilities, and using them to harm the target organization [17].
- Use of Machine Learning and AI: Attackers can use artificial intelligence and machine learning algorithms to analyze their targets more efficiently or bypass security systems [18].
- Knock-on Effects: Targeting a single vulnerability, such as supply chain attacks, causes a broader threat with knock-on effects [19].
- Encryption and Privacy: Malware, especially ransomware, is becoming harder to detect with stronger encryption techniques [20].
- Dynamic and Adaptive Attacks: Attacks change and adapt instantly according to the target's security measures [21].

The examples given can be increased. This complex situation forces cyber security experts to develop smarter and more effective security measures against constantly evolving threats. The evolution of cyberattacks into this more complex structure has popularized the use of anomaly detection systems, which have become a secure method for identifying deviations from the normal flow of network traffic or user behaviors, offering a solution for early prevention of potential attacks [22].

Another aspect of cyber threats is cybersecurity against spam. Spam content, sent via email and other communication tools, often intrigues users and is typically used for phishing attacks, the propagation of malicious software across networks, or the acquisition of financial information for fraudulent purposes. To effectively mitigate these spam threats, in addition to raising user awareness, technologies such as artificial intelligence are being utilized [23].

Critical communication systems and infrastructures, including GSM networks, electricity, water, natural gas, transportation systems, dams, e-commerce, banking systems, and digital government applications, have the potential to be partially or completely disabled, which could disrupt social order and jeopardize national security [24].

Therefore, public security, as part of national security, requires a more comprehensive approach supported by cybersecurity measures. Today, the necessary measures against cyber threats that emerge from the individual to the state should be taken, especially by institutions responsible for public security. In particular, public order and the security of citizens can be directly affected as a result of cyber-attacks that may target critical infrastructures [8]. In this context, the national cybersecurity policies put forward by the Digital Transformation Office in Turkey set forth the criteria that must be followed by all institutions [24]. Similarly, the United States National Cybersecurity Strategy document recommends the use of threat analysis tools for critical infrastructures [25]. Although state elements take the necessary measures, it should not be forgotten that the weakest link is individuals. For this reason, individual information at the national level is an important element for both national security and preventing individuals from being exposed to cybercrime. Awareness training should be provided for citizens, such as the cyber awareness campaign organized by the European Union [26].

While the Digital Transformation Office of the Presidency of the Republic of Türkiye reveals the rules that state institutions will follow regarding cyber security, it offers recommendations for the private sector. In addition, the Digital transformation office provides services for Cyber Security and Information Security. It plays a guiding role for public institutions and organizations and the private sector in line with the published information security guide [27].

Today, cyberspace emerges as the fifth field of operation after land, air, sea, and space operations where activities are carried out for national security. Understanding the scope and impact of academic research on cybersecurity can be a guide on the precautions that individuals, companies, or public institutions and organizations, that is, all elements of the state, should take. In this context, bibliometric analysis is a widely used research method to determine the main research topics of the literature and the missing issues in the research. VOSviewer software is

software used to visualize keywords, co-citations, and relationship links between studies in the literature in biometric analysis [28].

In this study, a bibliometric analysis was conducted using the keywords "cyber security", "cyber-attacks and threats", "protection", "spam security", "data security", "network security", and "anomaly detection". As a result of this analysis, it was tried to reveal the development of the existing literature on cyber security, and it was stated which direction the research in this field was focused on.

This study aims to reveal the focal points of the basic research topics in the cybersecurity literature and the academic impacts of the research. The aim of the bibliometric analysis and visualization performed through the VOSviewer software is to determine which topics are generally examined in cybersecurity and which topics are not researched in the literature in light of current information. In this context, it is aimed to clarify the following topics.

- To reveal the importance of cybersecurity in terms of national security,
- To emphasize the impact of artificial intelligence, especially deep learning, on cybersecurity and research,
- To indicate the importance of international cooperation and regulations,
- To increase the orientation towards missing topics in academic research and to make the importance of cybersecurity more evident.

In the following sections of the article, evaluations will be made on Co-occurrence of Keywords, Citation Analysis of Authors, Co-Authorship Analysis, Bibliographic Coupling of Documents, Bibliographic Coupling of Institutions, Citation Analysis of Countries and general results and evaluations will be given on technological developments and emerging approaches, especially on national security.

## II. MATERIAL AND METHOD

The data in this study were obtained from the Web of Science (WoS) database using the VOSviewer software and the tools within this software.

A search was conducted in the Web of Science (WoS) database using the query: ("Cybersecurity" or "cyberattacks" or "cyber

protection" or "spam cybersecurity" or "data security" OR "network security" or "anomaly detection" or "cyber countermeasures") in the fields of title, abstract, and keywords. This search yielded 11,990 documents. The publications span the years 1994–2025, with the following distribution: 6,609 journal articles, 5,107 conference papers, 310 review articles, 226 early access publications, 26 book chapters, 21 edited works, 9 retracted articles, 6 data papers, and 3 letters. The dataset was analyzed based on citations, documents, authors, institutions, countries, and keywords. Only WoS-indexed studies were used as the data source. Within the scope of the study, 6606 articles were reached by selecting 2000 and later as the journal article and year restriction for analysis. When classified by discipline, the majority of publications were found to focus on electrical and electronic engineering (2,286), computer science and information systems (1,880), artificial intelligence (1,088), and telecommunications (929). The data were analyzed in VOSviewer, focusing on citation, text, author, institution, country, and keyword analyses, using WoS-indexed studies as the primary source.

**Co-occurrence of Keywords:** It was conducted to examine how frequently keywords are used together and which topics are at the forefront in this field.

**Citation Analysis of Authors:** It was conducted to determine which authors were cited the most in the field and who were the most influential authors in the field.

**Co-Authorship Analysis:** It was conducted to determine which authors collaborated and between which research groups the most common collaborations occurred.

**Bibliographic Coupling of Documents:** It was conducted to examine which documents use the same references and the thematic similarities between these documents.

**Co-Citation Analysis of Authors:** It was conducted to determine which authors are frequently cited together and what kind of a connection there is between these authors.

**Bibliographic Coupling of Institutions:** It was conducted to examine which studies different institutions are involved in together and which institutions interact the most.

**Citation Analysis of Countries:** It was conducted to examine which countries' studies are most cited and the impact of these countries on the field.

TABLE I  
KEYWORDS AND RELATED DOCUMENTS

Keywords	1994-2025	2000-2025	Co-occurrence of Keywords	Cited
1.Cybersecurity 2.Cyberattacks 3.Cyber protection 4. Spam cybersecurity 5.Data security 6.Network security 7. Anomaly detection 8.Cyber countermeasures	<u>11990 documents.</u>  - Journal Article (6609), - Paper (5107), - Review (310), - Early View (226), - Book Chapter (26), - Edited Publication (21), - Withdrawn Publication (9), - Data paper (6) - Letter (3)	<u>6606 Journal Articles</u>  <u>Article Areas.</u> -Electrical and electronics engineering (2286), -Computer sciences and information systems (1880), -Artificial intelligence (1088), -Telecommunications (929).	1.Anomaly Detection, 2.Cybersecurity 3.Deep learning 4.Internet 5.Traing 5.Attacs 6.Network Security 7.Algorithm 8.Classification 9.Data security 10.Internet of things  (The order is from most to least.)	<u>The Most Cited Authors</u>  1.Quin Du (2085), 2.Wei Li (1433), 3.Liangpei Zhang (1417)



### III. RESULTS

The results section presents the analyses conducted with VOSviewer on the data obtained from the WoS database using the keywords "cybersecurity," "cyberattacks," "cyber protection," "spam cybersecurity," "data security," "network security," "anomaly detection," and "cyber countermeasures." In VOSviewer software, link strength represents the strength of the relationships between analyzed units (e.g. keywords, authors, articles). This relationship is usually related to the level of commonality between units.

**Link Strength Between Keywords:** It indicates how many times two keywords appear together in articles. For example, if the keywords "artificial intelligence" and "deep learning" appear together 50 times in an article, the link strength of these two words is calculated as 50.

**Article or Citation Link Strength:** It is calculated based on the citation or reference relationships of an article with other articles.

#### A. Co-Occurrence of Keywords

To examine the frequency of keyword co-occurrence and the prominent topics in the field, the dataset containing 18,059 keywords was filtered to include only those with a minimum occurrence of 25. This threshold resulted in the analysis of 225 keywords, revealing 5 clusters, 9,319 links, and a total link strength of 41,214. When the keywords in the articles obtained as a result of the keyword analysis were examined, it was seen that the words "anomaly detection", "cybersecurity", and "deep learning" were the most frequently used keywords. It is noteworthy that the word "deep learning" was not included in the words generated when determining the articles, but it was used as a keyword in the articles obtained as a result of the determined keywords." Notably, research in this field intensified after 2020, with "anomaly detection" and "cybersecurity" being frequently used terms from 2021 onwards. A temporal co-occurrence analysis of the keywords is presented in Figure 1.

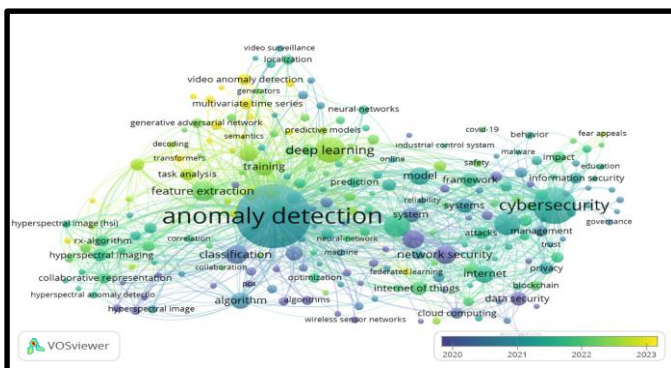


Fig. 1. Temporal Co-Occurrence Analysis of Keywords

#### B. Citation Analysis of Authors

This analysis was conducted to identify the most influential authors in the field and the citation relationships between their works to highlight the works with the greatest impact. Therefore, to identify the most cited authors and their impact on

the field, the dataset was filtered to include authors with at least 10 documents and 20 citations.

Out of 19,661 authors, 48 met these criteria and were analyzed, resulting in 5 clusters, 552 links, and a total link strength of 8,547. The analysis revealed that the top three most cited authors are Quin Du (2,085 citations), Wei Li (1,433 citations), and Liangpei Zhang (1,417 citations). The citation network analysis of these authors is presented in Figure 2.

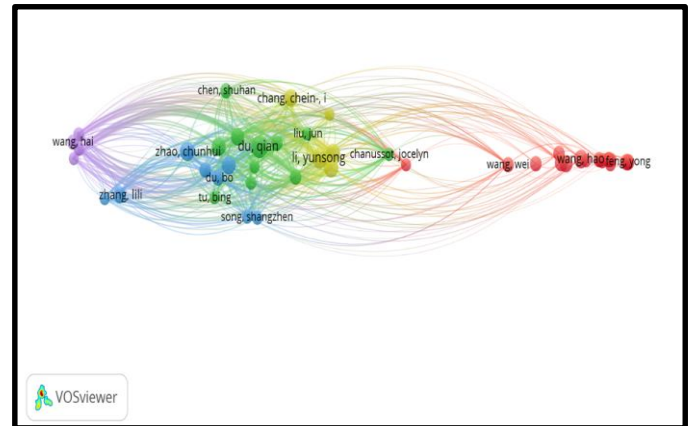


Fig. 2. Citation Analysis of Authors

#### C. Co-Authorship Analysis

To identify which authors collaborate and the most prevalent collaborations among research groups, a co-authorship analysis was conducted. From the dataset of 19,599 authors, a minimum citation threshold of 20 and a minimum of 5 publications were applied to highlight the most cited and active authors. This filtering yielded 299 authors, of whom the 183 most interconnected were analyzed.

The analysis revealed that these 183 authors formed 20 clusters, with 337 links and a total link strength of 1,061. Among them, Quin Du stood out with 26 publications and 2,085 citations. The top three authors in terms of publication count were Quin Du (26 publications), Yunsong Li (21 publications), and Weiying Xie (20 publications). Additionally, the collaborative paper by Quin Du and Wei Li, titled "Collaborative Representation for Hyperspectral Anomaly Detection," was noted to have received 508 citations. The co-authorship analysis is visualized in Figure 3.

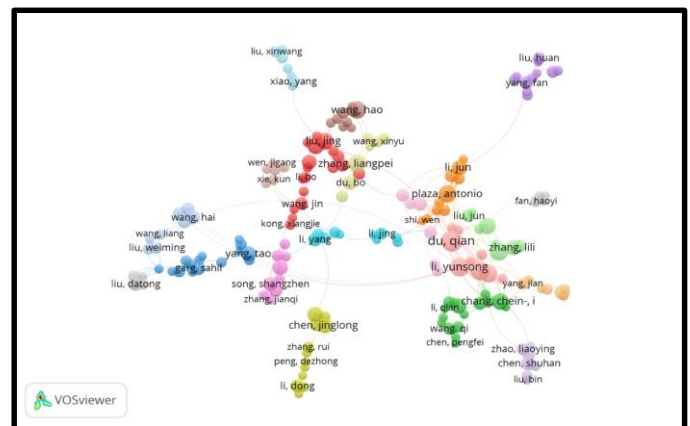


Fig. 3. Co-Authorship Analysis of Authors

#### D. Bibliographic Coupling of Documents

Bibliographic coupling analysis was conducted to examine which documents share the same references, thereby identifying thematic similarities and distinguishing the focal points of various studies. A minimum citation threshold of 25 was applied, resulting in the analysis of 1,000 documents. The analysis revealed 7 clusters with 47,978 links and a total link strength of 109,243.

The bibliometric coupling density visualization is presented in Figure 4, while the bibliographic coupling network analysis of documents is illustrated in Figure 5.

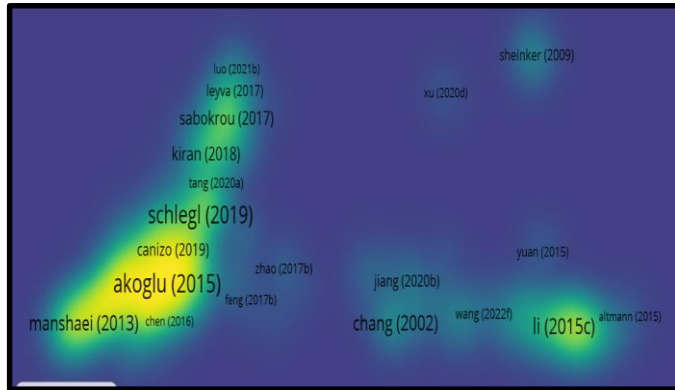


Fig. 4. Density Visualization of Bibliographic Coupling Among Documents

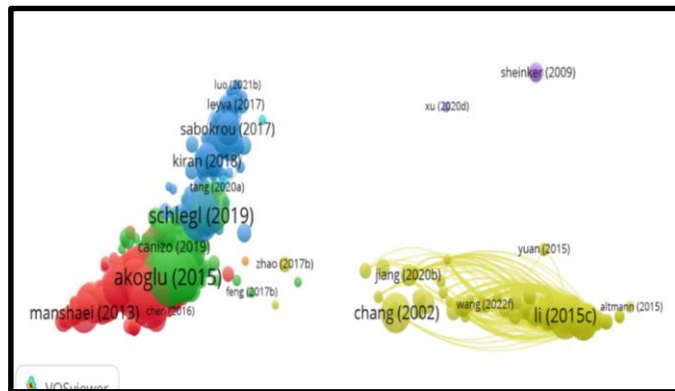


Fig. 5. Bibliographic Coupling Analysis of Documents

#### E. Co-Citation Analysis of Authors

A co-citation analysis of authors was conducted to determine how frequently authors are cited together, their interactions, and the thematic proximity of their work. Authors with a minimum of 30 citations were included in the analysis, resulting in a dataset of 1,058 authors.

The analysis identified 6 clusters, with 186,504 links and a total link strength of 852,325. Prominent authors included D. P. Kingma, C. I. Chang, and N. R. Prasad. The density visualization of the co-citation analysis is presented in Figure 6, and the network visualization of the co-citation analysis is shown in Figure 7.

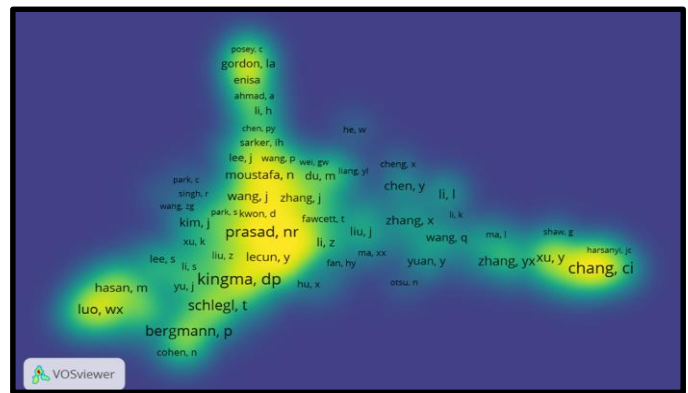


Fig 6. Density Visualization of Co-Citation Analysis Among Authors

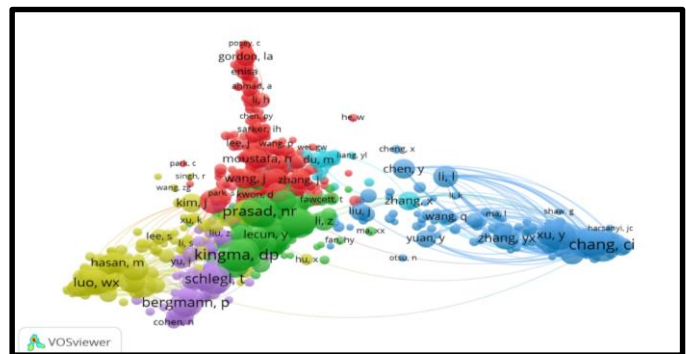


Fig. 7. Co-Citation Analysis of Authors

#### F. Bibliographic Coupling of Institutions

A bibliographic coupling analysis of institutions was conducted to examine which institutions collaborated on studies and identify the most interactive institutions. A minimum threshold of 20 documents and 20 citations was applied, resulting in the analysis of 71 institutions from an initial dataset of 5,361. The analysis identified 2 clusters with 2,484 links and a total link strength of 1,524,276. The Chinese Academy of Sciences emerged as the leading institution in terms of document and citation counts. The density visualization of institutional bibliographic coupling is presented in Figure 8.

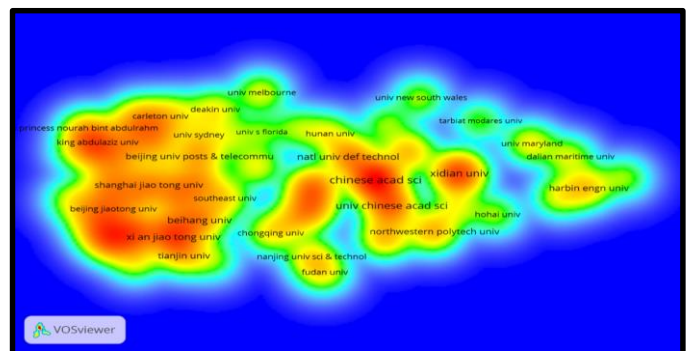


Fig 8. Density Visualization of Bibliographic Coupling Among Organizations

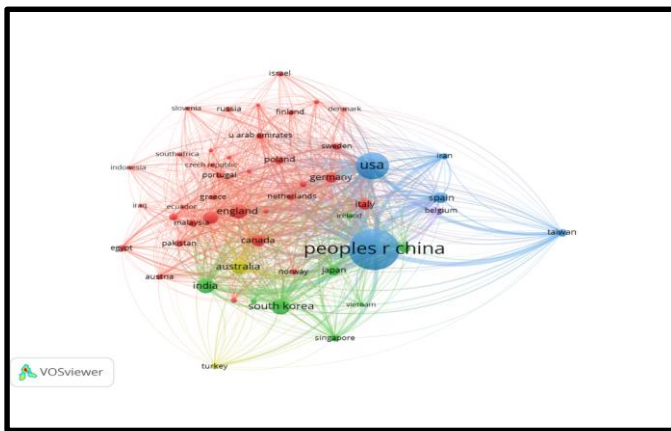


Fig. 9. Citation Analysis of Countries

#### G. Citation Analysis of Countries

With this analysis, we tried to explain cyber security interactions between countries and their research contributions. In this context, which country's academics. A minimum limit of 20 documents and 20 citations was applied to determine whether its cyber security studies were cited and their impact on cyber security. Among the 117 countries that make up the data set, 51 countries fell within the specified criteria and these 51 countries were included in the analysis. According to the number of research and citations, the People's Republic of China and the United States of America are in the first two places. The visual for the citation analysis of the countries is presented in Figure 9.

### IV. DISCUSSION

As a result of rapidly changing and developing technological developments, cyber security has become an area that needs to be evaluated multi-dimensionally with both the daily habits of users and the legal regulations of countries. Below are the results of the bibliometric analysis:

#### A. Co-occurrence of Keywords, Key Trends, and Focus Areas

The results revealed that concepts such as anomaly detection and deep learning in cybersecurity are fundamental topics in research and are mostly researched. These findings support the work of Torres et al. [23] on artificial intelligence-based security solutions. In particular, anomaly detection plays a critical role in determining threats to systems [29]. Ahmed et al. [30] showed that anomaly detection algorithms are very important for cybersecurity with low error rates. According to the bibliometric analysis results, it was shown that deep learning, which is not included in the search words, is frequently used in research in addition to anomaly detection. This reveals that artificial intelligence has an increasingly important place in cybersecurity applications and that its importance will increase in the future. Mahdavi et al. [31] also emphasized the importance of artificial intelligence-supported deep learning in modeling cyber threats in their study. This explains why deep learning, which emerged as a result of the analysis, is frequently included in research.

#### B. Author and Institution-Based Citation Analyses

The bibliometric analysis revealed that Quin Du, Wei Li, and Liangpei Zhang are leading researchers in this field, according to their citation numbers. Du's research on anomaly detection aligns with Ahmad et al. [30], who explored deep learning-based threat detection methods. Notably, Du's 2020 study, "Collaborative Representation for Hyperspectral Anomaly Detection," "provides an effective model for modern security systems. The leadership of the Chinese Academy of Sciences reflects national investments and strategic priorities in the field. China is seen to be increasing its emphasis on AI-enabled cybersecurity solutions in its academic output.

#### C. Global Collaborations and Regional Differences

China and the U.S. are identified as leaders in cybersecurity research, while other countries have also contributed significantly, with increasing interest in this field. For instance, in Türkiye, the Presidential Digital Transformation Office plays a guiding role in cybersecurity efforts [22,25]. Similarly, in the European Union, cybersecurity is closely tied to data protection regulations like GDPR [32]. Such regulatory approaches complement more technology-driven solutions in Asia and the Americas. The literature highlights that global collaborations provide stronger solutions to cybersecurity threats [8]. These collaborations not only enhance academic knowledge sharing but also lead to more effective industrial solutions.

#### D. Technological Developments and Emerging Approaches

AI technologies, particularly machine learning and deep learning, are regarded as the future of cybersecurity. Martínez Torres [23] explored the impact of deep learning algorithms on threat modeling and prediction, enhancing the proactive capabilities of anomaly detection systems. On the other hand, the literature draws attention to the ethical and legal challenges of AI-based approaches. The misuse of AI solutions could lead to privacy violations and discriminatory outcomes [33]. This highlights the importance of ethical considerations in cybersecurity research, a frequently discussed topic in the literature.

#### E. The Importance of Cyber Security for National Security

Today, cyber security has become an area that directly provides not only individual and corporate security but also national security. This power stands out as a critical requirement for law enforcement to be persistent and permanent against cyber threats. Cybersecurity has become a part of national security in the modern world. Ensuring the distribution of critical infrastructures, digital assets, information systems and permanence of images in cyberspace has become one of their most important tasks. This structural law enforcement force must have sufficient capabilities and operational individuals against cyber threats and should be at the center of national security. Cybersecurity training for law enforcement should not only be limited to preventing and controlling individual crimes but should also aim to increase resilience against organized attacks targeting infrastructure and digital infrastructure. This training should include topics such as developing proactive defense equipment against new-generation threats, supporting



national and international cooperation, and using threat detection technologies effectively. Consisting of the field of cyber security, it will enable law enforcement forces not only to respond to current attacks but also to be trained to anticipate potential threats, thus playing a key role in protecting national security.

Training for law enforcement personnel to recognize cyber threats and develop intervention strategies has become an issue emphasized by law enforcement agencies around the world, as well as in Türkiye. [34].

Intervention methods should be constantly applied in the light of exercises and scenarios to enable law enforcement cyber security personnel to intervene faster and more effectively by improving their abilities to respond to potential attacks [35].

#### F. Comparisons with Literature and Identified Gaps

The analysis reveals gaps in the literature and opportunities for future research. For example, although it is stated in the literature that small and medium-sized enterprises (SMEs) are more vulnerable to cybersecurity threats, it is evaluated that this issue has not been addressed much in the analysis [36]. The analysis draws attention to the fact that research is concentrated in countries considered to be technologically advanced, such as China and the United States of America, while cybersecurity research in developing countries is scarce. It is evaluated that this may be due to resource constraints [36]. As cyberspace becomes the fifth operational domain, new attacks by state-sponsored actors or terrorist groups can be expected to pose significant threats to national security. The question of whether cyberattacks should be considered within the framework of cyberwarfare in terms of national security requires a detailed examination.

#### G. Main Results and Global Assessment

Although the word "deep learning" was not among the words produced when determining the articles, it was observed that it was mostly used as a keyword in articles about cybersecurity. This shows that artificial intelligence and its sub-branches are effectively used in the protection of cyberspace.

In the field of cyber security, it is evaluated that China-based research is intensifying and China is increasingly placing more emphasis on artificial intelligence-supported cyber security solutions and has begun to take on a leading role in this field.

In Türkiye, the Presidency Digital Transformation Office is seen to be carrying out binding and guiding studies on cybersecurity in national and international areas, such as European Union Data Protection Regulations, and states have developed necessary preventive measures in this regard.

In addition to the use of artificial intelligence-supported technologies in cyber security, it is seen that issues regarding the ethical use of these technologies have begun to be addressed in a significant way.

Cyberspace is the fifth field of activity where activities aimed at national security are carried out after land, air, sea and space operations, and necessary measures must be taken for national security from the individual to the state.

Cyber-attacks are considered within the framework of cyber warfare in terms of national security, and it is evaluated that these attacks can be carried out by aggressive states or terrorist

elements and that it is necessary to be prepared against these attacks.

## V. CONCLUSION

Cybersecurity has become a constantly evolving field affected by technological, ethical and regulatory dimensions driven by the increasing prevalence of digitalization. In this study, academic research was evaluated through a bibliometric analysis using VOSviewer based on the keywords whose location details are given in Table I. The evaluations based on the results obtained in this context are given below.

Artificial intelligence, and its sub-branch deep learning algorithms, are popularly used today to detect and prevent cyber-attacks. Anomaly detection and neutralization of cyber-attacks as a result of this detection are frequently mentioned in the literature [37]. These useful algorithms and cybersecurity technologies are very important for identifying threats such as zero-day attacks. The use of these technologies creates high costs for institutions and the need for personnel requiring technical expertise. This creates a need for solutions that are accessible to everyone. While searching for solutions that are accessible to everyone, critical infrastructures and national security should be taken into consideration. As a result of the analysis made with keywords, it is seen that the words "deep learning", "internet", "training", "attacks", "network", "security", "algorithm", "classification", "Data security", "Internet of things" are the most frequently used words in the detected articles after the words "anomaly detection" and "cybersecurity". It has been evaluated that the developments in the field of artificial intelligence are increasing their impact in the field of cyber security in a similar way [38].

Developments in artificial intelligence are transforming cybersecurity into a global issue today. International cooperation is very important in analyzing cyber threats, investigating their consequences, and developing useful applications [8]. In addition to the fact that the People's Republic of China and the United States lead the world in cybersecurity research, interest in cybersecurity is increasing at the national level. Although structures such as the European Union have regulatory approaches to cybersecurity, they are also changing their cybersecurity approaches in parallel with technological developments in Asia and America. Security needs to be ensured in all areas of cyberspace and defense mechanisms against attacks need to be developed. Therefore, as in Türkiye, the measures to be taken should be determined and a national policy should be developed [24, 27]. No matter how much national policies are developed, the importance of international cooperation towards cyberspace, which has become a global problem and can be used by cyber terrorists, should not be forgotten.

The increasing use of artificial intelligence in cybersecurity offers significant advantages to users, while it has become a concern for all states of the world at national and international levels. This has also brought ethical and legal challenges [39]. Regulations such as the European Union's General Data Protection Regulation (GDPR) aim to increase measures to strengthen data security while emphasizing the privacy of personal or corporate data in the use of artificial intelligence.

Therefore, legislators, government institutions and academics should work together on cybersecurity, taking into account ethical sensitivities.

While studies on changing perception of cybersecurity and the ethical issues that come with it continue around the world, cybersecurity vulnerabilities emerge in developing countries due to many problems and financial resources. Therefore, developing countries should be supported by international funds and collaborations involving projects to improve their cybersecurity infrastructure. It has been observed that small and medium-sized enterprises operating in developing countries are sensitive to cybersecurity threats and that there is a lack of research in this area and that it is a subject that has not yet been sufficiently researched [36].

Cybersecurity is vulnerable to small businesses, either individually or institutionally, and the concept of cybercrime emerges when they do not take sufficient measures in the field of cybersecurity. The concept of cybercrime has become a strategic priority for all modern law enforcement agencies and all units working for national security, as in Türkiye, which is responsible for public security [24,27].

The rapid growth of digitalization has led to cyberattacks posing serious threats to individual rights and public order [27]. Institutions responsible for ensuring national security and public order should develop and implement more effective measures against cyber threats [8].

In addition to cyberattacks that individuals and businesses will be exposed to, basic infrastructures such as energy, water, transportation, and finance are primary targets for cyberattacks that will affect the entire society [24,27]. AI-powered detection systems and cybersecurity solutions play an important role in continuously monitoring these infrastructures and preventing potential breaches [29,37,39]. Therefore, States should integrate National Cyber Defense Strategies, regulatory frameworks, international cooperation, and the development of national technologies [8,24,27]. Such strategies should focus on preventing cyber-attacks and accelerating post-incident recovery processes.

Law enforcement and national security agencies should continuously update threat models to address the dynamic nature of cyber threats. Artificial intelligence and machine learning-enabled detection systems offer innovative approaches to counter these evolving challenges [27]. National security policies should include international collaborations to address global cyber threats. Organizations such as NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE) provide effective frameworks for such collaborations [40].

## References

[1] Mas-Tur, A., Kraus, S., Brandtner, M., Ewert, R., & Kürsten, W. (2020). Advances in management research: a bibliometric overview of the Review of Managerial Science. *Review of Managerial Science*, 14(5), 933-958.  
 [2] Mistar, J., Setiakarnawijaya, Y., Dewi, P. C. P., Paramita, D. P., Aqobah, Q. J., & Akbar, M. A. (2023). Systematic Literature Review: Research on Martial Arts Competition Using Vos Viewers in the 2018-2022 Google Scholar Database. *Gladi: Jurnal Ilmu Keolahragaan*, 14(02), 221-228.

[3] Van Eck, N. J. & Waltman, L. (2023). VOSviewer manual for VOSviewer version 1.6.20. Universiteit Leiden: CWTS.  
 [4] Vosviewer (2025). <https://www.vosviewer.com/features/examples>. Access Date: January 18, 2025  
 [5] Dereli, A. B. (2024). Vosviewer ile Bibliyometrik Analiz. *Communicata*, (28), 1-7  
 [6] Zawish, M., Dharejo, F. A., Khowaja, S. A., Raza, S., Davy, S., Dev, K., & Bellavista, P. (2024). AI and 6G into the metaverse: Fundamentals, challenges, and future research trends. *IEEE Open Journal of the Communications Society*, 5, 730-778.  
 [7] Khan, L. U., Yaqoob, I., Imran, M., Han, Z., & Hong, C. S. (2020). 6G wireless systems: A vision, architectural elements, and future directions. *IEEE Access*, 8, 147029-147044.  
 [8] Kshetri, N., & Kshetri, N. (2016). Cybersecurity in National Security and International Relations. *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, 53-74.  
 [9] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, 4(10).  
 [10] Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*.  
 [11] Caviglione, L., Wendzel, S., Mileva, A., & Vrhovec, S. (2021). Guest Editorial: Multidisciplinary Solutions to Modern Cybersecurity Challenges. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 12(4), 1-3.  
 [12] Borrett, M., Carter, R., & Wespi, A. (2014). How is cyber threat evolving and what do organizations need to consider? *Journal of business continuity & emergency planning*, 7(2), 163-171.  
 [13] Ulsch, M. (2014). *Cyber threat!: how to manage the growing risk of cyber attacks*. John Wiley & Sons.  
 [14] Mallikarjunan, K. N., Muthupriya, K., & Shalinie, S. M. (2016, January). A survey of distributed denial of service attack. In 2016 10th International Conference on Intelligent Systems and Control (ISCO) (pp. 1-6). IEEE.  
 [15] Hasan, M. K., Habib, A. A., Islam, S., Safie, N., Abdullah, S. N. H. S., & Pandey, B. (2023). DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Reports*, 9, 1318-1326.  
 [16] Solomon, A., Walker, E., Kensington, J., Drummond, M., Hall, R., & Blackwell, G. (2024). A new autonomous multi-layered cognitive detection mechanism for ransomware attacks.  
 [17] Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In *Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15*(pp. 63-72). Springer Berlin Heidelberg.  
 [18] Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 9(4), e1306.  
 [19] Chua, Y. T., Parkin, S., Edwards, M., Oliveira, D., Schiffner, S., Tyson, G., & Hutchings, A. (2019, November). Identifying unintended harms of cybersecurity countermeasures. In 2019 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-15). IEEE.  
 [20] Volini, A. G. (2020). A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues. *J. Intell. Prop. L.*, 28, 291.  
 [21] Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods, and challenges. *Digital Communications and Networks*, 8(4), 422-435.  
 [22] Maddireddy, B. R., & Maddireddy, B. R. (2024). Neural Network Architectures in Cybersecurity: Optimizing Anomaly Detection and Prevention. *International Journal of Advanced Engineering Technologies and Innovations*, 1(2), 238-266.  
 [23] Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, 10(10), 2823-2836.  
 [24] Siber Güvenlik (n.d.). Dijital Dönüşüm Ofisi. <https://cbddo.gov.tr/siber-guvenlik/>  
 [25] National Cybersecurity Strategy (2023). White House. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>  
 [26] Anagnostakis, D. (2021). The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. *Journal of Cyber Policy*, 6(2), 243-261  
 [27] Siber Güvenlik (n.d.). Dijital Dönüşüm Ofisi. [https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg\\_rehber.pdf](https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf)



- [28] Orduña-Malea, E., & Costas, R. (2021). Link-based approach to study scientific software usage: The case of VOSviewer. *Scientometrics*, 126(9), 8153-8186.
- [29] Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON\_IoT datasets. *Sustainable Cities and Society*, 72, 102994.
- [30] Ahmad, R., Alsmadi, I., Alhamdani, W., & Tawalbeh, L. A. (2023). Zero-day attack detection: a systematic literature review. *Artificial Intelligence Review*, 56(10), 10733-10811.
- [31] Mahdavi, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. *Neurocomputing*, 347, 149-176.
- [32] Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705.
- [33] Abdullahi, M., Alhussian, H., Aziz, N., Abdulkadir, S. J., Alwadain, A., Muazu, A. A., & Bala, A. (2024). Comparison and investigation of AI-based approaches for cyberattack detection in cyber-physical systems. *IEEE Access*.
- [34] Baadel, S., Thabtah, F., & Lu, J. (2021). Cybersecurity awareness: A critical analysis of education and law enforcement methods. *Informatica*, 45(3).
- [35] Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*, 7(1), tyab005.
- [36] Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, 50, 100592.
- [37] Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International Conference on Computer Networks and Communication Technologies: ICCNCT 2018* (pp. 739-747). Springer Singapore.
- [38] Muhammad, G., Pratama, A. R., Shaloom, C., & Cassandra, C. (2023, November). Cybersecurity Awareness Literature Review: A Bibliometric Analysis. In *2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS)* (pp. 195-199). IEEE.
- [39] Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. *Legal Issues in the Digital Age*, (2), 78-121.
- [40] Štrucl, D. (2022). Comparative study on the cyber defense of NATO Member States. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

## BIOGRAPHIES



**Vedat Yilmaz** obtained his BSc degree in system engineering from the military academy in 2004. I completed Digital Communication Electronics Training at Hacettepe University in 2006. My master's degree in Management and Organization at Selçuk University in 2007 and my PhD in Biomechanics at Hacettepe University in 2022. Additionally, I received training on Principles of Communication from Cranfield University, Cyber Security from METU, and Training on Terrorists' Use of Cyberspace from the Center of Excellence in Combating Terrorism.

I managed many technology projects within the Gendarmerie General Command. Currently, I continue my studies in cyber security, artificial intelligence applications in cyber crimes, security technologies, and cybercrime.