Cybersecurity in higher education: a bibliometric review

Jhon Richard Orosco-Fabian*
Universidad Nacional del Centro del Perú, Tarma, Perú https://orcid.org/0000-0001-9035-706X jorosco@uncp.edu.pe

Cite as: Orosco-Fabian J. (2024). Cybersecurity in higher education: a bibliometric review. *Revista Digital de Investigación en Docencia Universitaria, 18(2)*, e1933. https://doi.org/10.19083/ridu.2024.1933

Received: 20/05/2024. **Revised:** 9/07/2024. **Published**: 30/07/2024.

Abstract

Introduction: ICTs have impacted all sectors of society, especially in higher education, where students are trained to enter the labor market, but will be mediated by these technologies and at the same time exposed to cybersecurity issues. Objective: The aim of the study was to analyze the scientific production on cybersecurity in higher education using bibliometric methods. **Method:** Bibliometrics was used in the study. The research design was non-experimental of longitudinal type in the quantitative route and interpretative hermeneutic in the qualitative route. Datawrapper, VOSviewer and Bibliometrix were used for data analysis and presentation. **Results:** The results reveal that cybersecurity in higher education is a growing field since 2003, with exponential growth since 2018, led by authors from Finland, Saudi Arabia and the United States, in specialized journals such as IEEE Security and Privacy. **Discussion:** scientific mapping identified cybersecurity, cyber threats, cybersecurity awareness, cybersecurity breach, information security and General Data Protection Regulation (GDPR) as central topics, revealing emphasis on studying cybersecurity education. A fertile field of study regarding cybersecurity in higher education is evident.

Keywords: Cybersecurity; Digital security; Information security; Privacy; Higher education.

Ciberseguridad en educación superior: una revisión bibliométrica

Resumen

Introducción: Las TIC han impactado en todos los sectores de la sociedad, sobre todo en educación superior, donde el estudiantado se forma para la inserción al mercado laboral, pero que será mediado por estas tecnologías y a la vez expuestos a aspectos de ciberseguridad. **Objetivo:** El objetivo del estudio fue analizar la producción científica sobre ciberseguridad en educación superior mediante métodos bibliométricos. **Método:** En el estudio se utilizó la bibliometría. El diseño de investigación fue no experimental de tipo longitudinal en la ruta cuantitativa y hermenéutico interpretativo en la ruta cualitativa. Para el análisis y presentación de datos se usó Datawrapper, VOSviewer y Bibliometrix. **Resultados:** Los resultados revelan que la ciberseguridad en educación superior es un campo en expansión desde 2003, con crecimiento exponencial desde 2018, liderado por autores de Finlandia, Arabia Saudita y Estados Unidos, en revistas especializadas como IEEE Security and Privacy. **Discusión:** El mapeo científico identificó a la ciberseguridad, ciberamenazas, conciencia en ciberseguridad, violación de la ciberseguridad, seguridad de la información y Reglamento General de Protección de Datos (GDPR) como temas centrales, revelando el énfasis en estudiar la educación en ciberseguridad. Se evidencia un campo fértil de estudio en cuanto a la ciberseguridad en la educación superior.

Palabras clave: Ciberseguridad; Seguridad digital; Seguridad de la información; Privacidad; Educación superior.

***Correspondence:**
Jhon Richard Orosco-Fabian
jorosco@uncp.edu.pe

Introduction

In the current context, as a result of the impact of Information and Communication Technologies (ICTs), society is becoming increasingly dependent on cyberspace. Its daily use has normalized that any activity is mediated by technology to such an extent that most people consider, for example, that the internet is a safe environment, when, in reality, daily cyber-attacks, hacks, security breaches, etc. occur (De Bruijn & Janssen, 2017).

Everyone is exposed to threats that exist on the network (Medina-Rodriguez et al., 2020), either directly or indirectly. Moreover, since it is not possible to detect their origin because cyberspace is not based in any country, cybersecurity has become a global concern (Ospina & Sanabria, 2020; De Bruijn & Janssen, 2017). In recent years, there were cyber incidents associated with alleged cyberattacks to Russia (during the celebration of the World Cup); to Venezuela (electrical infrastructure); theft of intellectual property and information on COVID-19 vaccines; and unauthorized access to the Zoom videoconferencing platform in order to obtain information, infiltrate data, and boycott virtual meetings (Ospina & Sanabria, 2020), among others that happen on a daily basis. The extent is such that, "the world requires between 2.5 and 3.5 million new professionals in the field of cybersecurity" (Mitxelena, 2020, pp. 195-196).

In view of these problems, there is a need to prevent attacks and/or threats and to implement and maintain a secure virtual environment in order to generate trust regarding the information processed on the network. This is known as cybersecurity, information technology security, or electronic information security, which refers the set of procedures and tools implemented to protect digital information generated and processed through servers, computers, mobile devices, networks, and electronic systems (Medina-Rodríguez et al., 2020).

In the context of higher education, cybersecurity is also a concern in three areas. First, there is a lack of professionals trained in cybersecurity, so there is a need to redesign curricula of professional programs related to information systems (Towhidi & Pridmore, 2023) or create professional programs in cybersecurity, in order to meet the needs of the current context (Sudha et al., 2023). Second, there are concerns of being a victim of cyberattacks that violate information systems (Hobbs, 2023; Md Alimul et al., 2023; Njoku et al., 2023); there are already cases of this (Piazza et al., 2023) and only few studies on the level of cybersecurity preparedness from the socio-technical aspect (Hakiem et al., 2023).

Third, there is also the concern that both professors and students do not have basic skills in cybersecurity, especially those in professional programs that are not related to information systems (Beyari & Alrusaini, 2023), despite the fact that graduating students will join the labor market in a context increasingly mediated by technologies, where cybersecurity will be a necessary aspect. Therefore, curricular and extracurricular training on cybersecurity should be provided, and research in this field should be conducted (López et al., 2023).

The issue of cybersecurity has forced the governments of many countries to consider policies on cyberattack prevention (Toapanta et al., 2020). Also, addressing this global problem involves the incorporation of cybersecurity education, as public awareness is still rather limited (De Bruijn & Janssen, 2017). Being an emerging issue, it is necessary to know the scientific approach in the context of higher education in order to generate studies that allow understanding and proposing alternative solutions to this problem.

One of the gaps that this research seeks to bridge is the lack of specific knowledge about cybersecurity in education, which makes it difficult to understand the threats and vulnerabilities faced by higher education institutions. In addition, there is a lack of adequate policies and protocols for cybersecurity risk management in universities. This research can provide a basis for the development of effective standards and guidelines in this regard. A lack of cybersecurity training and awareness programs for the university community has also been identified.

Another significant gap is the insufficient space that cybersecurity has in university academic programs. This bibliometric review will highlight the need to include specific courses and modules on cybersecurity in various curricula. Likewise, several universities in the Peruvian context lack adequate technological infrastructure and the necessary resources to protect themselves against cyberattacks. Finally, there is a shortage of methods and tools to evaluate and determine the effectiveness of cybersecurity measures implemented in universities. Research could help develop criteria and methodologies for this evaluation.

Based on the above, the main question posed in the study asked what the level of scientific approach to cybersecurity in higher education over time is, and the specific questions asked a) how many studies have been published over the years, b) who the most active authors in the area are and what the most prominent journal is, c) what the main types of publications in the research on this topic are, d) From what areas of knowledge they have been researched, e) which institutions have funded these studies related to the phenomenon and which countries are most actively publishing, f) what has been the semantic development around the phenomenon under study, and g) what are the research trends regarding cybersecurity in higher education.

Method

Design

The study used bibliometrics, which is a discipline that uses quantitative and statistical methods for "the study of the size, growth, and distribution of scientific documents, as well as the study of the structure and dynamics of the groups that produce and consume science" (González, 1997, p. 212). This includes the formulation of research questions, the identification of databases, the elaboration of the search equation, the statistical and mathematical analysis of the metadata obtained, and the intersubjective analysis to identify the seminal contributions of the field of study, as well as the motor themes driving the creation of knowledge in the field.

The study is at the level of exploration and description of the process related to the scientific approach of the phenomenon studied. The research design is non-experimental of longitudinal type for the quantitative method and interpretative hermeneutic for the qualitative method.

Procedure

Based on the research questions, for an adequate selection of sources, the terms seguridad digital (digital security), *seguridad cibernética* (cyber security), *ciberseguridad* (cybersecurity), *peligros en internet* (dangers on the internet), *riesgos en internet* (risks on the Internet), *seguridad en línea* (online safety), *privacidad en línea* (online privacy), and *estafas en línea* (online scams) were used as fundamental criteria. On the other hand, given the context of the study in higher education, the following terms were used: *estudiantes universitarios* (university students), *educación superior* (higher education), *estudiantes de nivel universitario* (university level students) and *universidad* (university).

Based on these words, a translation into English was made, and the search equation was developed as follows: *TITLE(("Digital security" OR "Cyber security" OR "Cybersecurity" OR "Dangers on the internet" OR "Risks on the internet" OR "Online safety" OR "Online privacy" OR "Online scams") AND ("University students" OR "Higher education" OR "University level student" OR "University"))*.

This search equation was developed based on the research questions and was not limited to a specific timespan, because the objective was to address the evolution of the subject from its beginnings to the present, with the cutoff date for the study being October 2023. The Scopus database was chosen for its multidisciplinary approach and rigorous peer review system, resulting in 118 publications.

The inclusion criteria covered all publications the tittle of which included the keywords considered in the search equation. Therefore, scientific papers, reviews, conference papers, books, book chapters, papers on instruments, and editorials were included. All these sources

were considered because, being a topic of recent growth, it was necessary to analyze its presence in various publications to assess the relevance given.

Likewise, the criteria considered to extract the information to be analyzed from the Scopus database were the following: evolution of publications, authors, scientific journals, institutional affiliations, types of documents, areas of publication, sponsors, and countries.

Data Analysis

For the data analysis, once the information was found in the Scopus database, it was exported in comma separated values (CSV) format in order to perform mathematical and statistical analyses that allowed addressing the research questions. These data, subsequently, were analyzed with Bibliometrix (Aria & Cuccurullo, 2017) and VOSviewer (VOSViewer, 2023), which are specialized and free software. Likewise, the data were presented with the help of the Datawrapper application.

Results and Discussion

The results of the bibliometric mapping are presented below as an approximation to the state of the art of cybersecurity in higher education.

According to the data in Figure 1, the relevant scientific research on cybersecurity indexed in Scopus has mainly taken place in the last two decades, with a sustained growth between 2003 and 2023 (annual rate of 17.91%). This collection of 118 publications is distributed in 94 specialized journals, which shows that the topic has managed to position itself in academic circles focused on cybersecurity.

The production involves 359 authors, with an average of 3.24 coauthors per document and 18.64% international collaboration. This suggests an emerging but growing line of research, with contributions from various countries. The publications show a good level of updating, citing references that are only 3.13 years old in average.

In conclusion, the data shown in Figure 1 show that cybersecurity in higher education is an emerging line of research that is consolidating within cybersecurity studies. The steady growth over the last two decades, the publications in specialized journals, and the growing international collaboration suggest that a body of knowledge and an academic community focused on this topic is being established. However, it is important to note that the field is still in a developing phase.

Figure 2 shows the evolution of publications on cybersecurity, with a slow growth since 2003—showing little interest in the subject, but an exponential growth in publications since 2018, a trend that is in line with a similar study (Babilonia et al., 2023). The data allow us to argue that this topic has recently gained relevance because the COVID-19 pandemic forced a large part of the world population to acquire technological devices and be connected, which exposed them to risks related to cybersecurity. These results show the pertinence of the topic and its current importance, which indicates that the scientific and academic community is interested in further researching it.

Likewise, Figure 2 shows that, in terms of the authors who publish most frequently, the following stand out: Lehto Martti from the University of Jyväskylä (Jyvaskyla, Finland), Ragab Mahmud and Al-Malaise Al-Ghamdi Abdullah Saad from King Abdulaziz University (Jeddah, Saudi Arabia), Barnes K. T. from the Idaho National Laboratory (Idaho Falls, the United States), among others. And the most outstanding journal, considering the number of publications is IEEE Security and Privacy, which holds the top position of the IEEE Computer and Reliability Societies, a journal that publishes studies in English on security, privacy, and reliability of information technologies. The publication frequency of this journal is bimonthly, and article processing charges (APC) apply.

Figure 3 shows that there is diversity in terms of publication types, with the majority being published papers, followed by conference papers, which shows a fertile path for review work and instrument design. The studies come mainly from the fields of computer science, engineering ,and social sciences, which shows that cybersecurity is a concern of various areas of human knowledge because we live in an era influenced by technology.

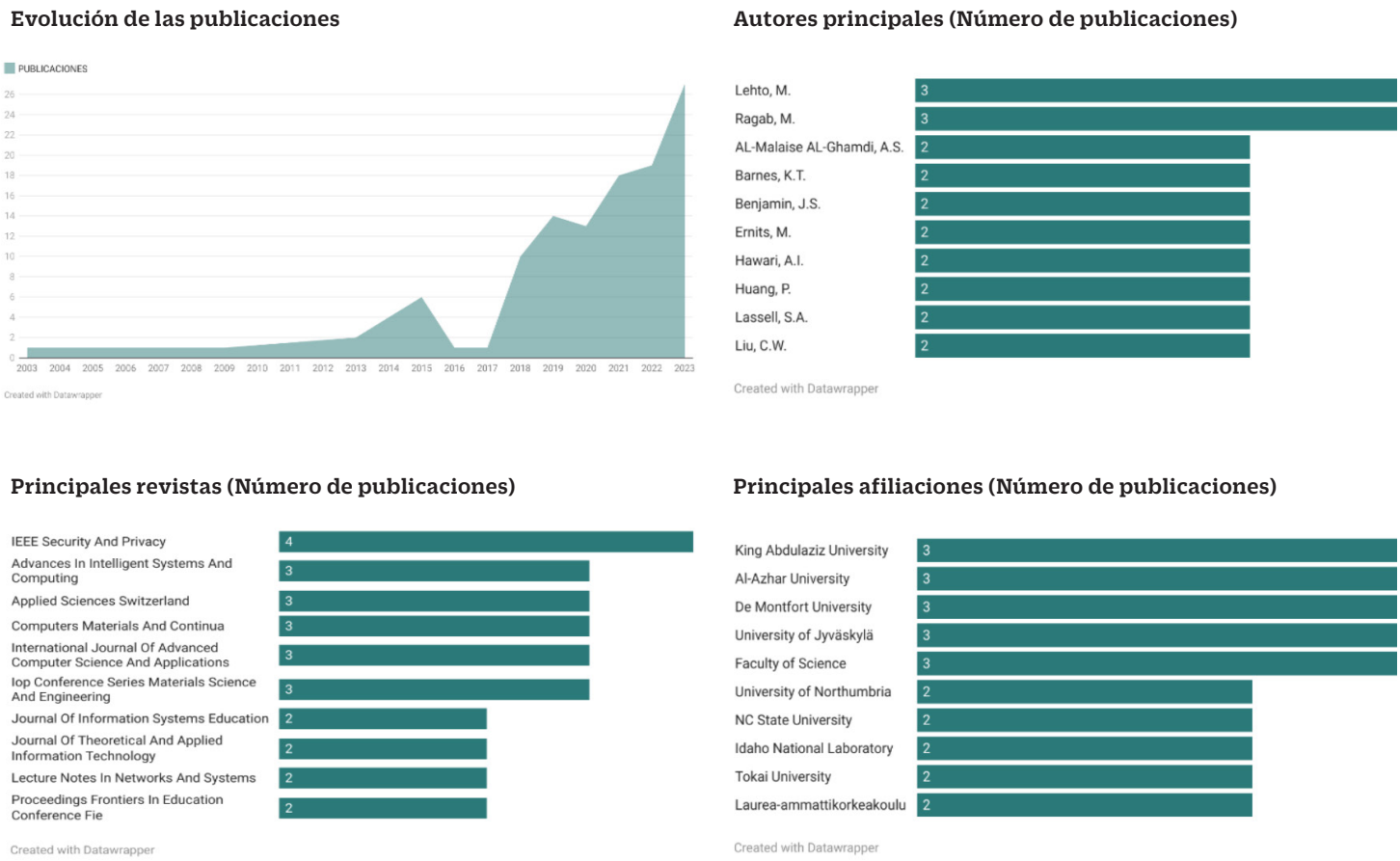
Figure 1

Summary of the Main Information of the Collection

Note. Collection summary prepared by Bibliometrix, based on metadata extracted from Scopus.

Figure 2

Evolution, Authors, Journals, and Affiliations



Note. Main bibliometric indicators related to the evolution of publications, authors, journals, and affiliations, based on Scopus metadata, processed in the app https://app.datawrapper.de/

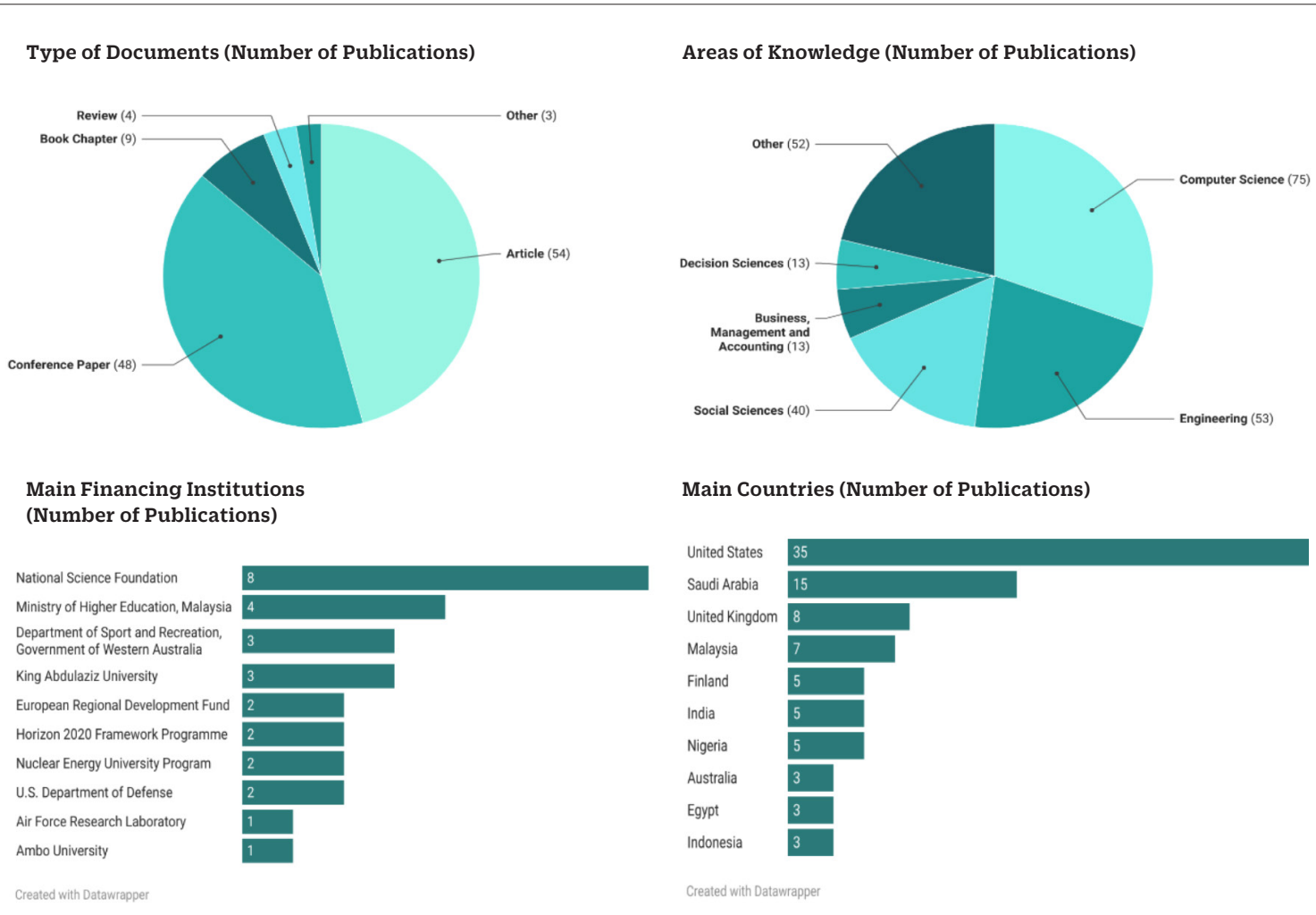
Also, in Figure 3, it is observed that the main institutions funding studies in this line of research are the National Science Foundation, which is an independent federal agency of the United States that supports colleges and universities to conduct basic research for curiosity and discovery; the Ministry of Higher Education of Malaysia; the Department of Sports and Recreation of the Government of Western Australia; and King Abdulaziz University. The most active countries in cybersecurity knowledge generation are the United States, Saudi Arabia, the United Kingdom, Malaysia, among others, a result concordant with that found by Babylon et al. (2023).

Figure 4 shows the semantic map generated from the analysis of keyword co-occurrences within the collection of publications. This visual representation highlights terms such as *cybersecurity, security, information security, internet security, cyber threats, cybersecurity awareness*, among others. These terms within the network, with preponderance in the size of the nodes and their relationships, allow identifying the main trends in research in this field. *Security, information security, and internet security* indicate that there is an emphasis on addressing cybersecurity within the field of higher education. *Cyber* threats shows interest in analyzing the risks to which one is exposed in the virtual context in relation to cybersecurity.

It is also evident in the study the need to generate awareness and education in

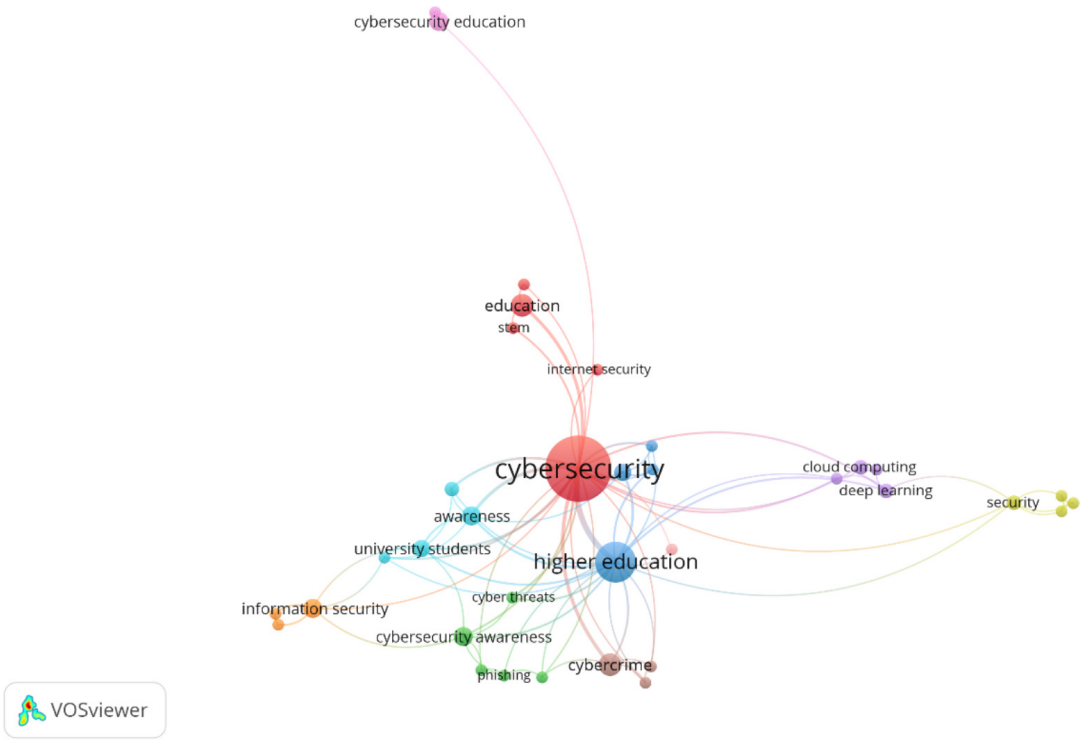
Figure 3

Types of Documents, Areas of Knowledge, Funding Institutions, and Countries



Note. Main bibliometric indicators related to type of publications, areas of knowledge, funding entities, and countries, based on Scopus metadata, processed in the app https://app.datawrapper.de/.

Figure 4
Semantic Map Related to Cybersecurity



Note. Visual map elaborated with VOSViewer, based on the keyword metadata of the collection extracted from Scopus on cybersecurity. Curation was done with the software thesaurus mechanism and similar terms were integrated (cybersecurity = cyber security and cyber; cybersecurity awareness = cyber security awareness; cybercrime = cybercrimes; higher education = higher education institution, higher education institutions, higher education students, educational institutes and university; education = pedagogy; university students = students).

cybersecurity, which denotes a concern of higher education institutions in developing digital skills of students in relation to cybersecurity to address this latent problem product of a technologized society. In conclusion, the research focuses on studying how cybersecurity manifests in higher education and seeking strategies to strengthen the digital skills of students to address the risks and problems related to cybersecurity.

The application of spectroscopy of the year of the reference mentioned in the collection of works on cybersecurity makes it possible to identify documents that have been consistently cited in subsequent research. By tracing the origin of these essential concepts, an insight into how knowledge in this area evolves and gets stablished is provided (Figure 5).

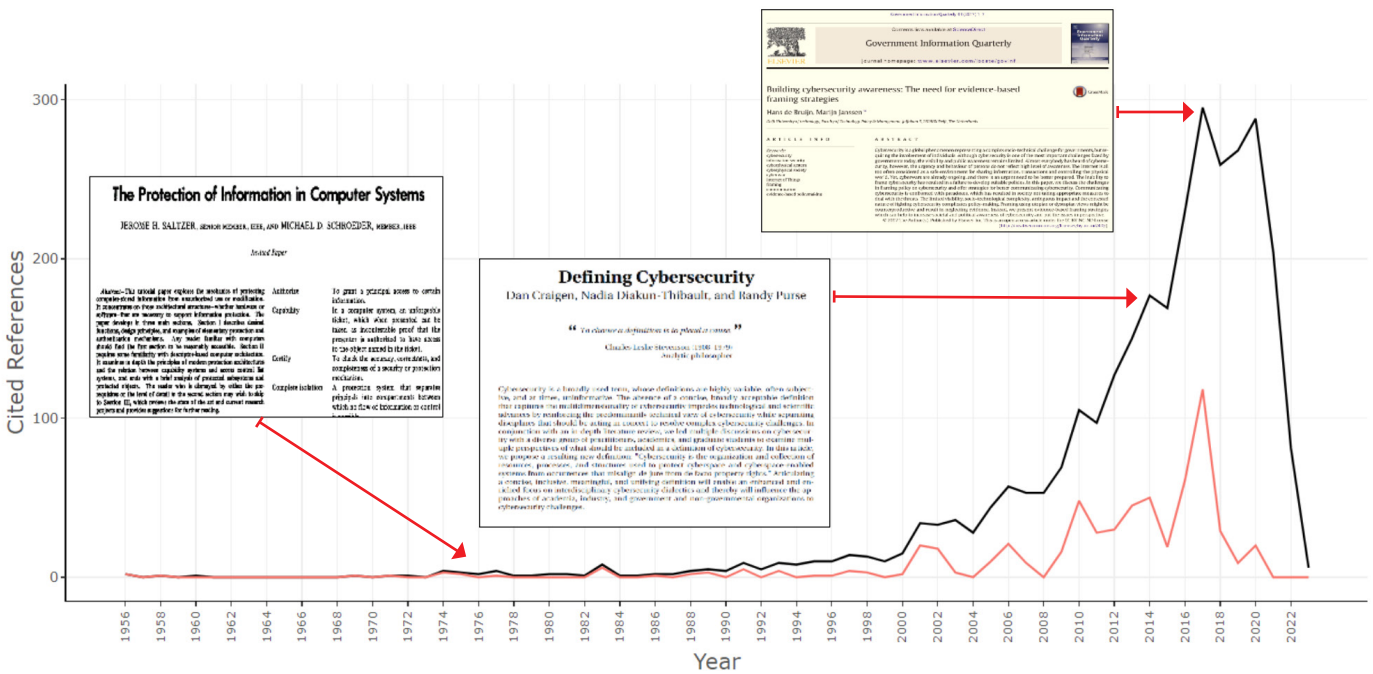
The Protection of Information in Computer Systems by Saltzer & Schroeder (1975) is considered one of the first works related to cybersecurity. The contribution of this work relates to the protection mechanisms to take into consideration regarding the information stored in a computer against unauthorized uses or modifications. It focuses on hardware and software architectural configurations that are important to ensure information security. Three important aspects are addressed: basic principles of information protection, descriptor-based protection systems, and the state of the art of the subject in question. In this last section, they show that, in those years, both manufacturers and customers did not attach much importance to the protection of information stored on computers.

They also point out that, between 1964 and 1974, research on the implementation of information protection architectures was carried out. They also mention the trends of that time in this area: certification of the accuracy of the designs and implementations of protection systems, invulnerability to single failures, restrictions on the use of information after its disclosure, encryption of information with secret keys, and improved authentication mechanisms. In conclusion, this paper makes evident the concern regarding the protection of information stored in computers by focusing on the structure of the software and hardware.

The paper by Craigen et al. (2014) represents an effort to define cybersecurity in an inclusive and unifying manner. The authors evidence that, before their study, there was no concise, broadly acceptable definition that captured the multidimensionality of cybersecurity. To fill this conceptual gap, they reviewed the literature from different areas of knowledge (computer science, engineering, politics studies, psychology, security studies, management, education, and sociology). They also deconstruct the term cybersecurity (*cyber- and security*) and show that the term cyber- evolved from the term *cybernetics* developed by Wiener (1948/1958) to the term *cyberspace* (Gibson, 1984) and from there became an accepted concept. The opposite happened with the term *security*, which has been difficult to define in a general sense. After deconstructing the term, the authors selected definitions on cybersecurity and analyzed

Figure 5

Spectroscopy of the Cited Reference Year



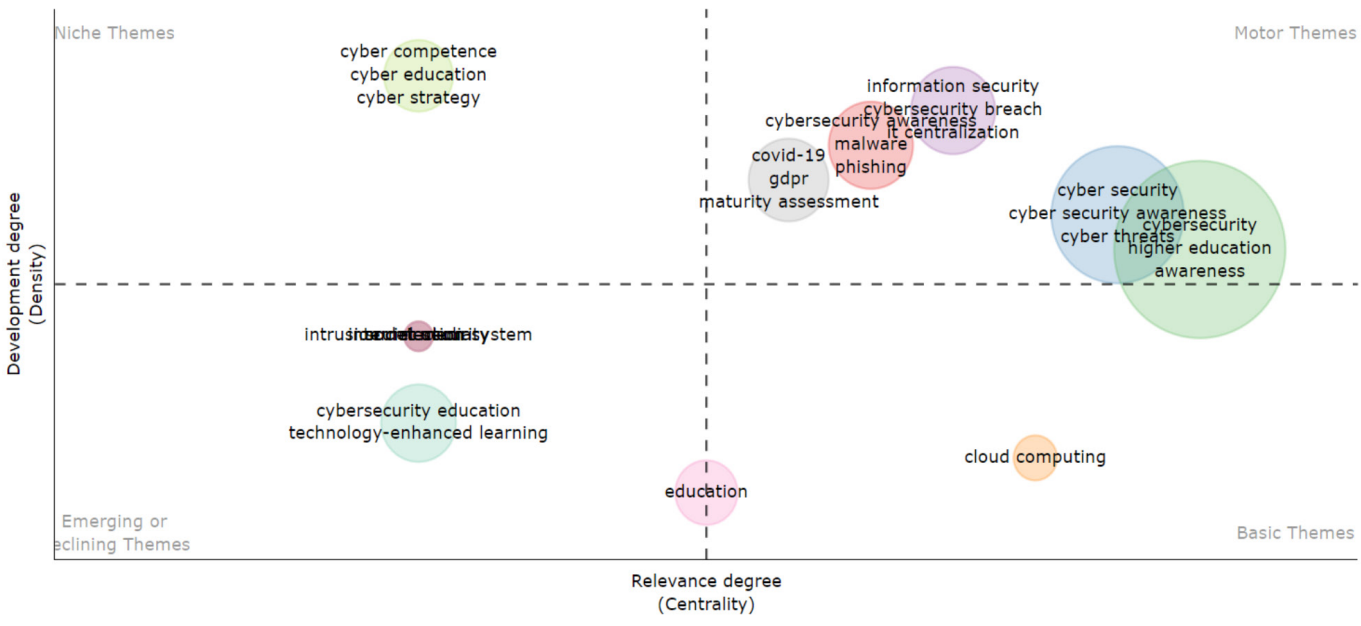
Note. The histogram in this figure was made with Bibliometrix and the process is as follows: i) All the papers that make up the bibliometric study sample are taken; ii) For each paper, the year of publication of all the references it cites is analyzed; iii) A histogram is constructed where the X axis represents the year of publication of the references (not of the paper) and the Y axis, the frequency with which these references are cited; iv) The peaks in the histogram represent highly influential works published in that year, which laid the conceptual and theoretical foundations of the field under study.

them. From there, they propose a holistic definition, assuming that cybersecurity is the organization and the set of resources, processes, and structures used to protect cyberspace and the systems enabled for this from events that are not respectful of property according to law and property rights in practice. In summary, the paper defines cybersecurity in a holistic manner so that it can be adopted by the various actors involved, which will allow a better understanding and collaboration to address the growing and complex threats in cyberspace.

The study by De Bruijn & Janssen (2017) represents the concern of researchers in raising awareness about cybersecurity, since, in the current context, as society is increasingly dependent on ICTs, it should be an important aspect for individuals, as well as public and private organizations. However, there is still little awareness about it because this topic falls in the domain of specialists and experts who are not trained to communicate to society in general. For this reason, there is a need to propose appropriate strategies to communicate this issue in a simple and understandable way. Based on the above, the authors identify the paradoxes that prevent the formulation of cybersecurity policies and the difficulty of communication in this area. Finally, they propose the message approach as a strategy to communicate cybersecurity-related problems, which should be evidence-based because a simple-message approach is considered ineffective. Based on the above, they propose six strategies to address cybersecurity: 1) Do not exacerbate cybersecurity; 2) make clear who the villains are; 3) give cybersecurity a face by putting the heroes in the spotlight; 4) link cybersecurity to values other than security only; 5) personalize the message for easy recognition; and 6) connect to other tangible and clear issues. In conclusion, this work deals with the strategies regarding raising awareness in cybersecurity, as it influences the need to generate competences in digital security of people and, especially, of future professionals who will be working in public or private institutions in a context mediated by ICTs.

Figure 6 shows the structural map, which allows analyzing the research trends regarding

Figure 6
Structural Map (Analysis of Research Trends)



Note. Figure elaborated with Bibliometrix, based on metadata extracted from Scopus, related to cybersecurity publications.

cybersecurity. This map places the concepts of information security, cybersecurity, cyber threats, cybersecurity awareness, cybersecurity breach, and General Data Protection Regulation (GDPR) in the Motor Themes quadrant, indicating that they are active lines of research within the field of cybersecurity. This is consistent with what is observed in the semantic map, where these terms are presented as central concepts and are strongly related to each other. Therefore, both maps evidence the central role of the study of cybersecurity in the context of higher education, which is why this line of research emphasizes the approach from different areas of human knowledge.

Likewise, the structural map (Figure 6) shows concepts on cybersecurity education and technology-enhanced learning in the Emerging Themes quadrant. This indicates that, given the cybersecurity problem, it is necessary to educate on this issue, which implies the development of digital competencies in cybersecurity. This is particularly important for higher education students, who will enter the labor market after completing their professional training and, regardless of their profession, will be immersed in the use of ICTs.

Finally, the study contributes to mapping and consolidating knowledge on cybersecurity in higher education. Likewise, the use of quantitative and qualitative methods allows for a comprehensive perspective, revealing trends through bibliometric indicators and synthesizing strategies and theoretical approaches through critical analysis. This methodological triangulation increases the reliability of the findings and highlights the identification of emerging areas and gaps in the literature that can guide future studies.

However, the study has the following limitations: a) Although the sample is broad, it does not cover all the scientific production on the topic in question; b) by relying on secondary sources, it fails to include unpublished research that could offer new perspectives; c) the qualitative analysis carried out depends on the author's intersubjective interpretation, making it necessary to empirically validate the strategies and theoretical models that have been identified; and d) by focusing on the academic literature, the knowledge of experts is not included.

Future research should conduct bibliometric studies including other databases, cross-sectional studies of both professors and students, and intervention studies to educate on cybersecurity competencies.

Conclusions

The evolution of publications on cybersecurity reveals a remarkable transformation over time. Until 2003, a gradual growth was observed, which evidenced little interest in this subject. However, from 2018 onwards, there has been a significant change with exponential growth in publications related to this field, which implies that the scientific approach in the current context is increasing because it is necessary.

From 2003 to 2023, 118 works have been published in 94 specialized journals, which shows that the topic has been positioning itself in academic circles focused on cybersecurity.

The most frequently published authors are Lehto Martti from the University of Jyväskylä (Jyvaskyla, Finland), Ragab Mahmud and Al-Malaise Al-Ghamdi Abdullah Saad from King Abdulaziz University (Jeddah, Saudi Arabia), and Barnes K. T. from the Idaho National Laboratory (Idaho Falls, the United States). And the journal that stands out the most is IEEE Security and Privacy, which holds the top position in the IEEE Computer and Reliability Societies.

The types of publication are diverse, the main form of publication being scientific papers, followed by conference papers, which constitutes a fertile path for review work and development of tools in cybersecurity.

The studies come mainly from the fields of computer science, engineering, and social sciences, which shows that cybersecurity is a concern of diverse areas of human knowledge because we live in an era with increasing influence of technology.

The main institutions funding studies in this line of research are the National Science

Foundation, which is an independent U.S. federal agency; the Malaysian Ministry of Higher Education; the Western Australian Government's Department of Sports and Recreation; and King Abdulaziz University. And the countries that are most active in cybersecurity knowledge generation are the United States, Saudi Arabia, the United Kingdom, and Malaysia.

There are seminal contributions to cybersecurity in higher education, the most important being the work of Saltzer & Schroeder (1975), who address the protection of information in computer systems; the work of Craigen et al. (2014), who make an effort to define cybersecurity in an inclusive and unifying way; and the work of De Bruijn & Janssen (2017), who focused on raising awareness of cybersecurity. From these works, key concepts around cybersecurity were introduced that allow the theoretical foundations to be laid: cybersecurity, security, information security, internet security, cyber threats, and cybersecurity awareness, among others.

Research trends in this area include information security, cybersecurity, cyber threats, cybersecurity awareness, cybersecurity breaches, regulation, etc.

References

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping análisis. *Journal of Informetrics, 11*(4), 959-975. https://doi.org/10.1016/j.joi.2017.08.007

Babilonia, A., Garcés-Giraldo, L. F., Valencia-Arias, A., Bermeo-Giraldo, M. C., Gómez-Bayona, L., Patiño-Vanegas, J. C., & Bao, R. (2023). Tendencias investigativas en ciberseguridad del Internet de las Cosas (IoT). *Revista Ibérica de Sistemas e Tecnologias de Informação,* (E62), 73-86. https://www.proquest.com/scholarly-journals/tendencias-investigativas-en-ciberseguridad-del/docview/2880949498/se-2

Beyari, H., & Alrusaini, O. (2023). The two-step cluster analysis of pre-COVID-19 experience and cybersecurity concerns about online education for academic staff in Saudi universities. *International Journal of Advanced and Applied SciencesOpen Access, 10*(3), 37-45. https://doi.org/10.21833/ijaas.2023.03.005

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. https://www.proquest.com/docview/1638205509

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*, 1-7. http://dx.doi.org/10.1016/j.giq.2017.02.007

González, L. (1997). Teoría de la ciencia, documentación y bibliometría. *Revista general de información y documentación,* 7(2), 201-214. https://dialnet.unirioja.es/servlet/articulo?codigo=170006

Gibson, W. (1984). *Neuromancer.* Titivillus. https://goo.su/o8zH

Hakiem, N., Afrizal, S., Shofi, I. M., Wardhani, L. K., Anggraini, N., Zulhuda, S., & Setiadi, Y. (2023). Assessing cybersecurity readiness among higher education institutions in indonesia using management perspectives. *ICIC Express Letters, 17*(10), 1151-1158. http://doi.org/10.24507/icicel.17.10.1151

Hobbs, J. (2023). Cybersecurity awareness in higher education: a comparative analysis of faculty and staff. *Issues in Information Systems, 24*(1), 159-169. https://doi.org/10.48009/1_iis_2023_114

López, A., Roque, R. V., Prieto, Ma. T. & Salazar, R. (2023). Cybersecurity among University Students from Generation Z: A Comparative Study of the Undergraduate Programs in Administration and Public Accounting in two Mexican Universities. Ciberseguridad entre estudiantes universitarios de la Generación Z: un estudio comparativo de las carreras de Licenciatura en Administración y Contaduría Pública en dos universidades mexicanas. *TEM JournalOpen Access, 12*(1), 503-511. https://doi.org/10.18421/TEM121-60

Md Alimul, H., Sultan, A., Alok, J., Khushboo, M., Binay M., Kailash, K., & Jabeen, N. (2023). Cybersecurity in Universities: An Evaluation Model. *SN Computer Science, 4*(5), Artículo 569. https://doi.org/10.1007/s42979-023-01984-x

Medina-Rodríguez, C. E., Casas-Valadez, M. A., Faz-Mendoza, Castañeda-Miranda, A., R., Gamboa-Rosales, N. K. & López-Robles, J. R. (2020). *The cyber security in the age of telework: A descriptive research framework through science mapping*. International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI), Sakheer, Bahrain. https://doi.org/10.1109/ICDABI51230.2020.9325633

Mitxelena, X. (2020). Euskadi 2025 - Sin ciberseguridad no hay futuro. *Ekonomiaz,* (98), 194-227. https://dialnet.unirioja.es/servlet/articulo?codigo=7694317

Njoku, N. S., Njoku, B. Ch., Chukwu, S. A., & Ravichandran, R. (2023). Fostering Cybersecurity in Institutional Repositories: A Case of Nigerian Universities. *African Journal of Library Archives and Information Science*, *33*(1), 1-21. https://www.ajol.info/index.php/ajlais/article/view/247643

Ospina, M. R., & Sanabria, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, *62*(2), 199-217. https://dialnet.unirioja.es/descarga/articulo/7667839.pdf

Piazza, A., Vasudevan, S., & Carr, M. (2023). Cybersecurity in UK Universities: mapping (or managing) threat intelligence sharing within the higher education sector. *Journal of Cybersecurity, 9*(1), Articul tyad019. https://doi.org/10.1093/cybsec/tyad019

Saltzer, J. H. & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of The IEEE, 63*(9), 1278-1308. https://doi.org/10.1109/PROC.1975.9939

Sudha, S. S., Sudha, S. S., Javaid, A. Y., Niyaz, Q., & Yang, X. (2023). *Examining the impact of early cybersecurity education in the selection of cybersecurity as a career among high school senior and university freshmen students*. ASEE Annual Conference and Exposition, Conference Proceedings, Baltimore. https://acortar.link/M6lvzj

Toapanta, S. M., Gaibor, G. S., & Mafla, L. E. (2020). Analysis of appropriate standards to solve cybersecurity problems in public organizations. *Association for Computing Machinery.* 4th International Conference on Information System and Data Mining (ICISDM '20). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3404663.3404678

Towhidi, G., & Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs. *Journal of Information Systems Education,* 34(1), 70 – 83. https://aisel.aisnet.org/jise/vol34/iss1/6

VOSViewer. (2023). *VOSviewer—Visualizing scientific landscapes.* VOSviewer. https://www.vosviewer.com//

Wiener, N. (1948/1958). *Cibernética y sociedad.* Sudamericana.