Ewa Maria Włodyka*

Cyber Security as A Research Subject: Quantitative and Qualitative Analysis of Data in Scopus Database Covering in 2020–2024

Abstract

Modern society is increasingly reliant on digital technologies, thus bringing with it not only opportunities but also threats. This is particularly relevant for the area of the public sector, which by definition serves citizens. This particularity is consists in citizens frequently optionally rather than obligatory entrusting their data via ICT systems. In this context, cyber security is becoming a key research area, and this research is essential for understanding and effectively responding to increasingly complex cyber threats. This study aims to conduct a quantitative and qualitative analysis (within a selected range) of cyber security data for the period of 2020–2024 for the data published in the Scopus repository database.

Key words: cyber security, public administration, e-government, analysis

*   Ewa Maria Włodyka, PhD, Faculty of Humanities, Koszalin University of Technology, e-mail: ewa.wlodyka@tu.koszalin.pl, ORCID: 0000-0002-8229-342X.

Introduction

E-government is a common form of performing public tasks, from the international level to the local level. IT systems are widely used not only by private entities (including entrepreneurs) but also by public authorities, and they are used not only for faster communication (including one over long distances) but also for the implementation of tasks, including those of fundamental importance for the state and its institutions[1]. In fulfilling their responsibilities, it is particularly important for public entities to handle incidents understood as taking action to identify, record, analyse, classify, prioritise, mitigate and resolve incidents[2]. This shows how often attention is paid to the practical aspects of cyber security research findings, not only in the public sector area. What are the characteristics of research carried out in the field of cyber security (RQ1)? With the research question posed in this manner, no research hypothesis was considered.

The study was carried out using a quantitative analysis of research results (in a variety of forms, not limited merely to research papers) published in the Scopus repository database[3]. The study was conducted for data published between 2020 (inclusive) and 20 March 2024. The use of the key word: „cybersecurity" by the authors of the study was used as a variable. In the next step, a qualitative analysis of the research results of selected research paper[4], which is also included in the Scopus database, was carried out.

Quantitative analysis

A search for the key word of „cybersecurity" in the Scopus database yielded 68 077 documents (with no distinction made into the forms, i.e. a research paper or a monograph or a chapter).

---

1 M. Karpiuk, *Crisis management vs. cyber threat*, „Sicurezza, Terrorismo e Società" 2022, no. 2, p. 121.
2 Idem, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2, p. 57.
3 *Scopus – Document search results. Signed in*, https://www.scopus.com/results/results.uri?sort=plf-f&src=p&st1=cybersecurity&sid=723f28a7f23eb40acbe0eb2b25de1fac&sot=b&sdt=cl&sl=28&s=ALL%28cybersecurity%29&origin=resultslist&editSaveSearch=&sessionSearchId=723f28a7f23eb40acbe0eb2b25de1fac&limit=10 [access: 24.03.2024].
**4** M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Table 1. Key word of „cybersecurity" in Scopus database for 2020–2024

No.	Date of publication	Number of items	Highest number of publications
1.	2024	4289	
2.	2023	22632	X
3.	2022	17516	
4.	2021	13598	
5.	2020	10042	

Source: Author's own work, based on: *Scopus...*

The year 2024 saw the lowest number of publications, but the figure of 4289 as at 23 March represents 42% of the entire year 2020, which was the first year considered in the study below, and was also the year with the lowest number of publications.
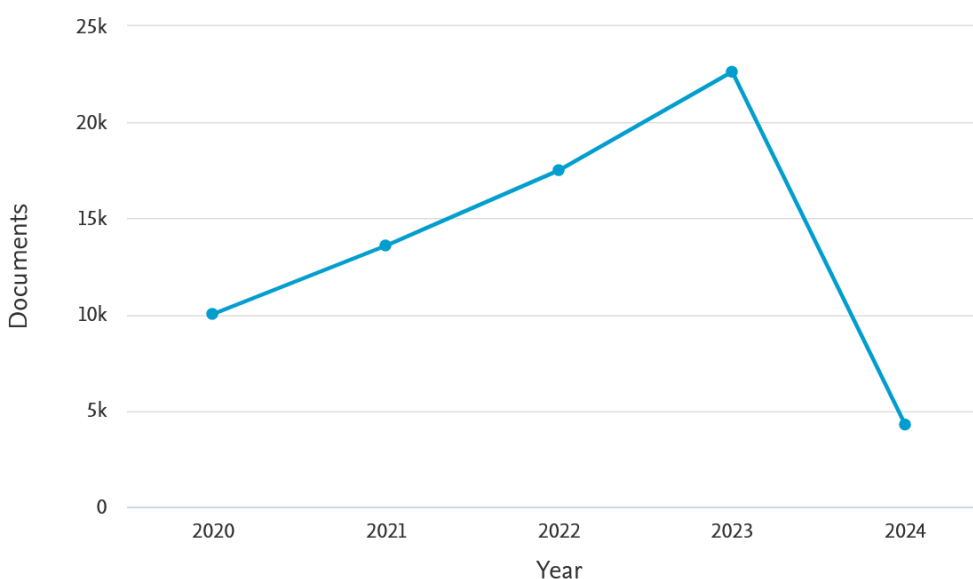
Source: compiled with visualisation tools available in the Scopus database [access: 24.03.2024].

Graph 1. Number of scientific publications in the Scopus database with the key word „cybersecurity" for 2020–2024 in graphical format

What may be an implicit reason for the increase in publications in 2023 is the release to the public of the first generative artificial intelligence tool with such a widespread use, i.e. OpenAI's ChatGPT. Tools of this kind make it possible, in their rapidly developing forms, to generate not only new content, but they can also support the phenomenon of deepfake (generative image: e.g. Mindjournay, the so-called „sing-lips" voice or images, e.g. Sora). ChatGPT

was released in its basic free form in November 2023: could this contribute to this huge increase in cyber security research? Given the length of the research publication cycle and the geopolitical situation at the time, this surge can rather be traced back to Russia's attack on Ukraine in February 2022, although such an analysis deserves a separate study with appropriate geopolitical tools.

Table 2. Number of records obtained by subject area

No.	Name of scientific discipline [subject area] (according to Scopus)	Number of records obtained
1.	Computer Science	48 554
2.	Engineering	30 210
3.	Social Sciences	11 735
4.	Mathematics	11 327
5.	Decision Sciences	9 719
6.	Business, Management and Accounting	5 415
7.	Physics and Astronomy	5 027
8.	Energy	4 762
9.	Materials Science	3 605
10.	Medicine	3 359
11.	Economics, Econometrics and Finance	2 500
12.	Environmental Science	2 131
13.	Biochemistry, Genetics and Molecular Biology	1 423
14.	Chemistry	1 215
15.	Arts and Humanities	1 141
16.	Chemical Engineering	1 072
17.	Psychology	972
18.	Earth and Planetary Sciences	671
19.	Multidisciplinary	573
20.	Agricultural and Biological Sciences	495
21.	Health Professions	445
22.	Neuroscience	411
23.	Nursing	189
24.	Pharmacology, Toxicology and Pharmaceutics	119
25.	Immunology and Microbiology	74
26.	Dentistry	19
27.	Veterinary	7

Source: Author's own elaboration based on Scopus data.

The highest number of records can be noted in the area Computer Science, followed by Engineering. However, Social Science can be found as soon as on the third and fourth positions in the same place with mathematics. It is fairly surprising that it is not only exact sciences that are engaged in the study of cyber security, although they still account for less than 25% of the most represented discipline.
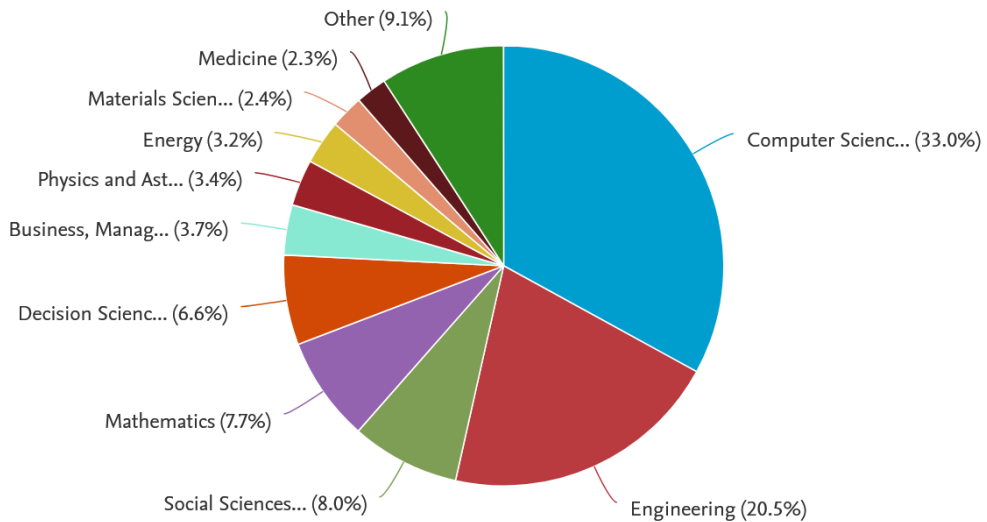
Source: https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=723f28a7f23e-b40acbe0eb2b25de1fac&sot=a&sdt=a&sl=56&s=ALL%28cybersecurity%29+AND+PUBYEAR+%3e+2019+AND+PUBYEAR+%3c+2025&origin=resultslist&count=10&analyzeResults=Analyze+results [access: 24.03.2024].
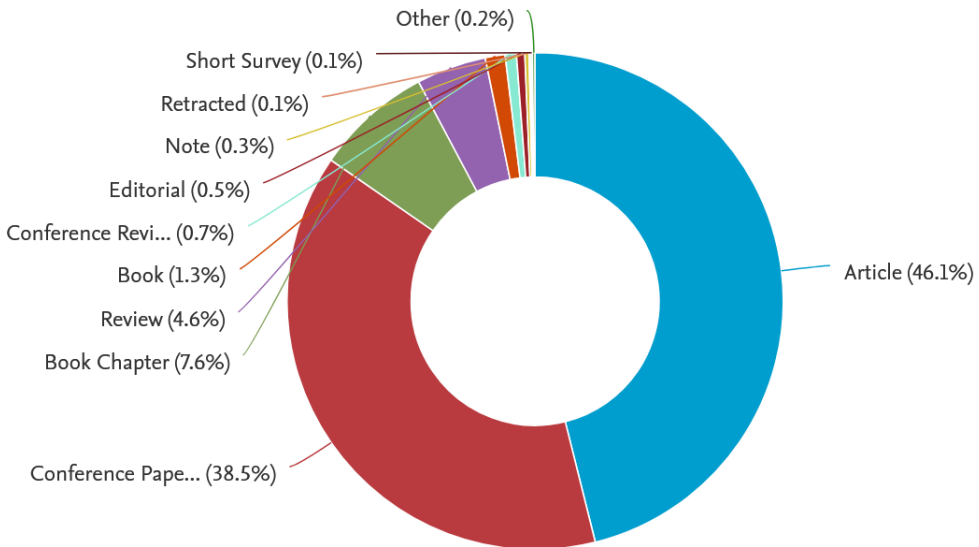
Graph 2. Records obtained by subject area – percentage breakdown

When analysing the type of research published, it most often took the form of research papers.

Table 3. Form of research result published in Scopus database in 2020–2024

No.	Form of research result published in Scopus database	Number of records obtained for 2020–2024
1.	Article	31 385
2.	Conference paper	26 225
3.	Book chapter	5 173
4.	Review	3 099
5.	Book	882
6.	Conference review	494
7.	Editorial	373
8.	Note	177
9.	Retracted	83
10.	Short survey	76
11.	Letter	53
12.	Erratum	30
13.	Data paper	27

Source: Author's own elaboration based on Scopus data.

Other (0.2%)
Short Survey (0.1%)
Retracted (0.1%)
Note (0.3%)
Editorial (0.5%)
Conference Revi... (0.7%)
Book (1.3%)
Review (4.6%)
Book Chapter (7.6%)
Conference Pape... (38.5%)
Article (46.1%)

Source: https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=723f28a7f23e-b40acbe0eb2b25de1fac&sot=a&sdt=a&sl=56&s=ALL%28cybersecurity%29+AND+PUBYEAR+%3e+2019+AND+PUBYEAR+%3c+2025&origin=resultslist&count=10&analyzeResults=Analyze+results [access: 24.03.2024].

Graph 3. Form of research result published in Scopus database in 2020–2024 – percentage breakdown

Conference papers come second, and data papers come last (less than 0,01%), which is not comforting given the trend in science towards data reuse. This is important not only for the quality of the research but also for the aspect of data acquisition most frequently funded by public funds.

The results obtained also included patents obtained by researchers, with the highest number recorded in 2023 (i.e. 2767, which is more than double that of the poorest year in this respect, i.e. 2020: 1086 patents). This may indicate an orientation of research in this area towards practical application, beyond the theoretical approach.

The most prolific author is Willy Susilo, Director of the Institute of Cybersecurity and Cryptology, with 159 papers co-authored in the aforementioned area[5].

5 *Willy Susilo*, https://sites.google.com/view/willy-susilo/ [access: 24.03.2024].

In terms of the most prolific of the affiliated institutions, the Chinese Academy of Science is on the first position with 598 papers.
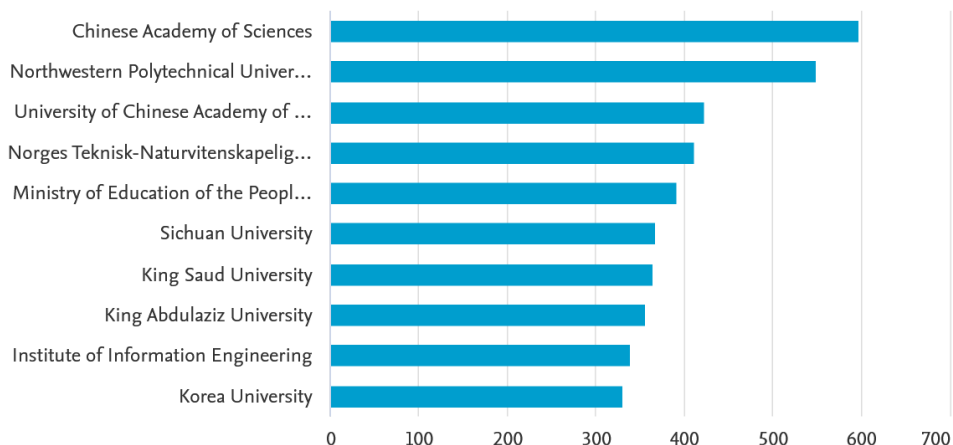
Source: https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=723f28a7f23e-b40acbe0eb2b25de1fac&sot=a&sdt=a&sl=56&s=ALL%28cybersecurity%29+AND+PUBYEAR+%3e+2019+AND+PUBYEAR+%3c+2025&origin=resultslist&count=10&analyzeResults=Analyze+results [access: 24.03.2024].

Graph 4. Form of research result made available in Scopus database in 2020–2024: percentages

In terms of the volume of research output, the United States is the leader in cybersecurity, with 1324 documents in the Scopus database (by comparison, China is on the second position with the number being lower by over 3000). What could be an interesting addition to this quantitative analysis is an examination of the inclusion of cyber security in the policies of both countries and their impact on the volume of research in this area, coupled with the translation of this research into implementation potential and practical application in the development of cybersecurity systems.
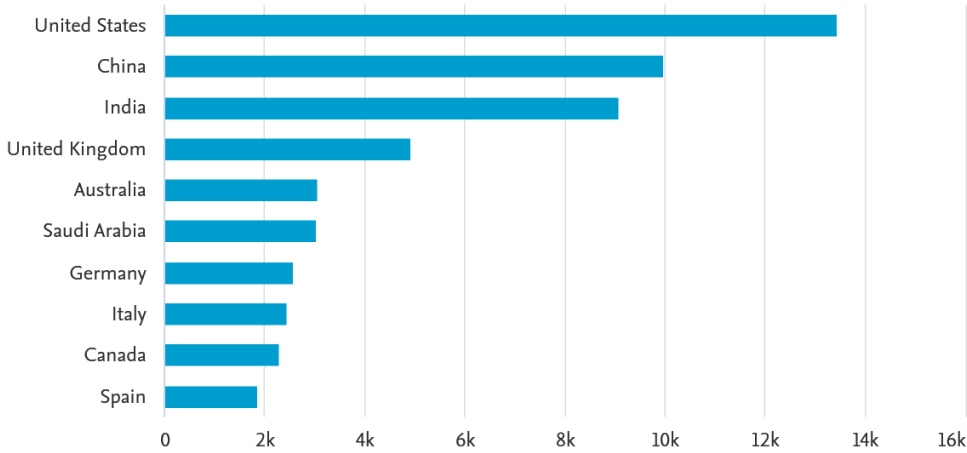
Graph 5. Number of studies on cybersecurity in research institutions in countries
publishing in Scopus database

According to the analysis of citations, out of more than 68000 records originally received, the tool available through the Scopus database which calculates the Hirsh index indicated less than 2000 records. 301 records were cited once only. 12 were cited a minimum of 12 times (hence, they have h-index = 12). The most cited record had 46 citations, and the subsequent one almost half as many, i.e. 25. A total of 175 records were cited from the aforementioned database, of which 44 only once. As many as 1995 research papers were not cited even once from this source selected for the calculation of the Hirsh index by the Scopus database.
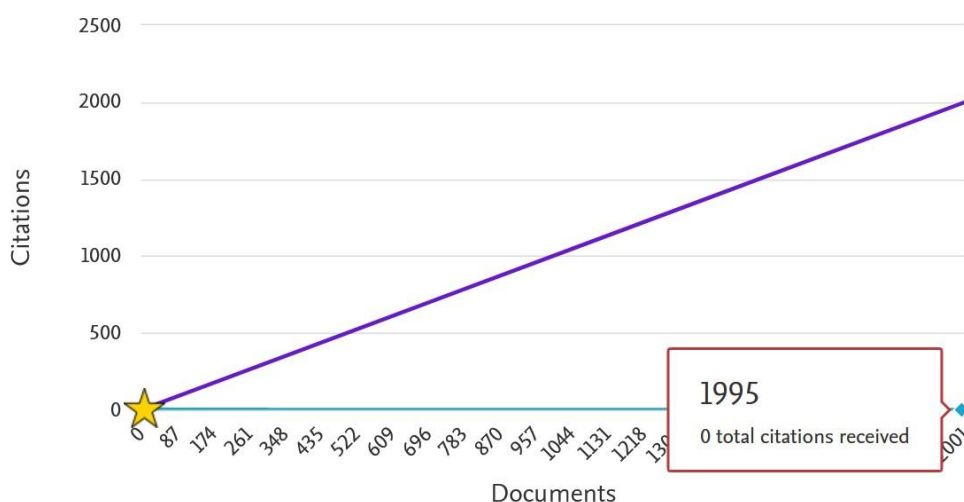
Source: compiled with visualisation tools available in the Scopus database [access: 24.03.2024].

Graph 6. Number of citations of research papers with the „cybersecurity" key word available in the Scopus database, published between 2020 and 2024

Cybersecurity as an element of public administration

In contemporary times, public administration around the world is more or less (depending on many factors related individual countries) integrated with cyberspace. E-government is a common form of performing public tasks. This hypothesis is no less obvious than the one that with the development of e-government, the threat in the form of cyber threats is increasing, especially at the level of local administration[6]. The purpose of the existence of local and regional governments is to meet the collective needs of their communities[7]. And this, in turn, implies the construction of cyber-security systems, including ones at local or central government levels. Cyber security is one of the tasks of both central and local governments, as well as of other entities which responsibility has been delegated to in this sphere[8]. Many tasks are performed
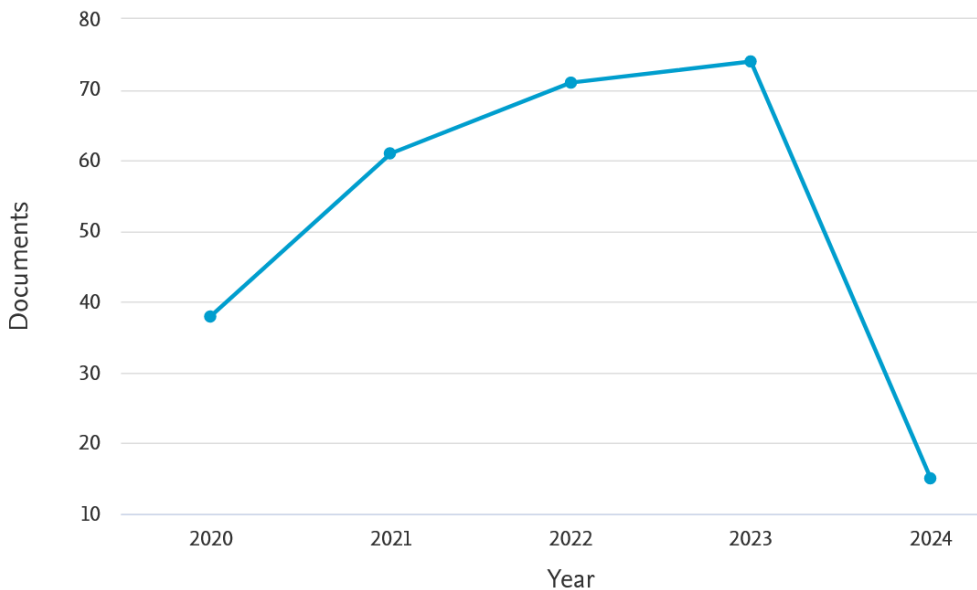
---

6 E.M. Włodyka, *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, no. 1, p. 202.
7 M. Czuryk, *Supporting the development of telecommunications services and networks through local and regionalgovernment bodies, and cybersecurity*, ibidem 2024, no. 1, p. 40.
8 M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, „Studia Iuridica Lublinensia" 2023, no. 2, p. 201.

using ICT systems that are exposed to external attacks and, therefore, they should meet appropriate security standards[9]. Cybersecurity occupies a special place in the public domain, and it is within this domain that planning is intended to ensure the coordination of activities in emergency situations[10].

A query of the availability in the Scopus database of papers indicating in their content the key words of „cybersecurity" and, at the same time, „administration" yielded the result of 259 papers resulting from research activities. Most (i.e. 74) were published in 2023.

Graph 7. Number of records received in searches for the key words
of „cybersecurity" and „administration"

---

9 W. Gizicki, *A Security Community: Poland and Her Visegrad Allies: The Czech Republic, Hungary and Slovakia*, Lublin 2013, p. 171.

10 M. Karpiuk, *Cybersecurity as an element...*, p. 45. See also: M. idem, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2.

When combining the key words of „cybersecurity" and „local government", we receive as few as 37 records in the Scopus database from the period of 2020–2024. The peak period is at the end of 2023, so one may speak of a slight research delay as regards a link between cybersecurity and local government in relation to the surge of publications in relation to the issue of cybersecurity.
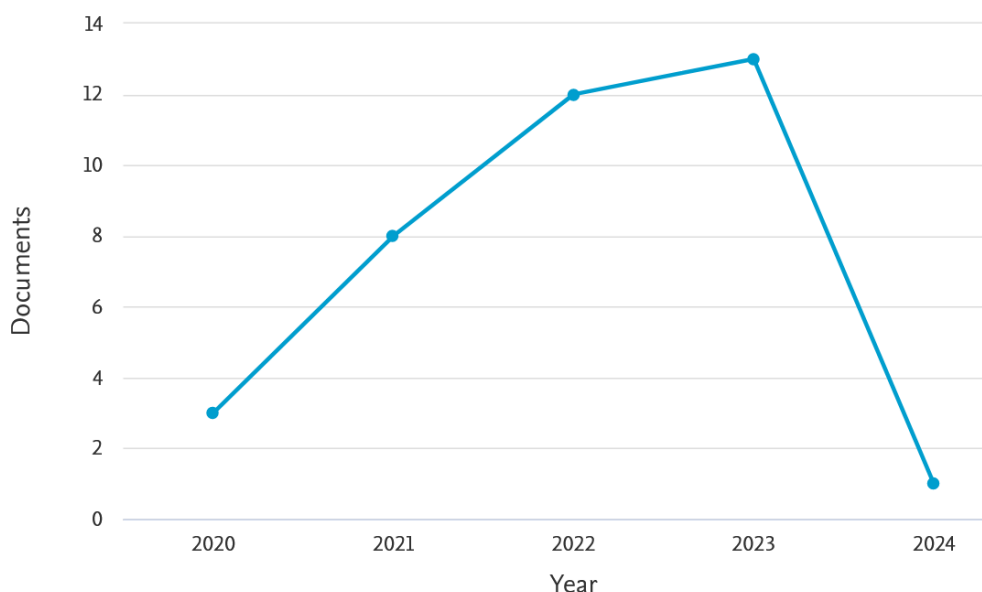

Source: https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=cca5e94f 52372dc49327916689d02e65&sot=a&sdt=a&sl=89&s=TITLE-ABS-KEY%28 %22cybersecurity%22+AND+%22localgovernment%22%29+AND+PUBYEAR+%3e +2019+AND+PUBYEAR+%3c+2025&origin=resultslist&count=10&analyzeResults =A nalyze+results [access: 24.03.2024].

Graph 8. Number of records received in searches for the key words of „cybersecurity" and „local government"

In addition, the analysis of the key words indicated shows little interdependence and interconnectedness and no common core indicating the local and regional specificity of the local government[11].

---

11 The citation correlation analysis for research papers containing the key words of „cybersecurity" and „local government" in the Scopus database published between 2020 and 2024 was performed using the VosWiever tool.
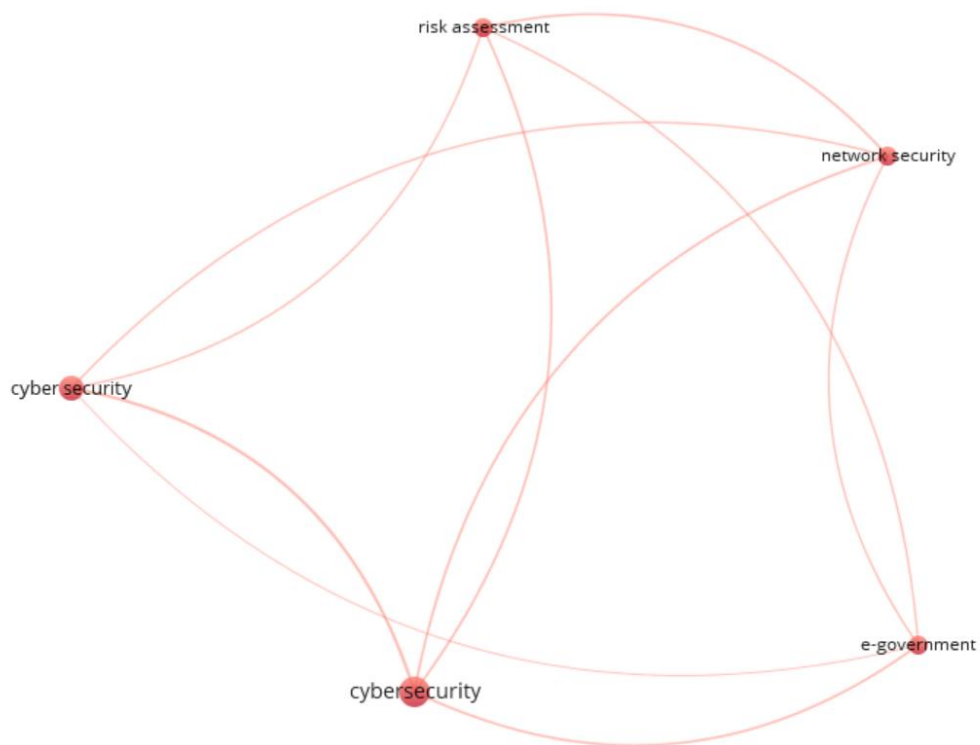
Source: Author's own indicated using VosWiever tool [access: 24.03.2024].

Graph 9. Citation correlation analysis for research papers containing the key words
of „cybersecurity" and „local government" in the Scopus database published between
2020 and 2024

At this point, one needs to move on to a qualitative analysis of the research article selected. The international legislator states that the local self-government means the right and capacity of local communities, within the limits of the law, to direct and manage an essential part of public affairs on their own responsibility and in the interests of their citizens[12]. At the same time, it should be emphasised that the manner which ICT tools are used in, like all other tools, depends on the user[13].

12   Art. 3 sec. 1 of the European Charter of Local Self-Government, drawn up in Strasbourg on October 15, 1985 (Journal of Laws of 1994, no. 124, item 607).
13   K. Kaczmarek, *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją*, „Cybersecurity and Law" 2021, no. 1, p. 71.

The Art. (P1) was selected for a qualitative analysis in the Scopus database while adhering to the criteria that have been used so far[14]. The local government's position in the Polish cybersecurity system[15] by Miroslaw Karpiuk: this article discusses the local government's position in the national cybersecurity system. It refers to the status of the local government administration in cyberspace, including duties and responsibilities ensuring cybersecurity in Poland. The local government is in the possession of the most extensive knowledge on the matters concerning a given (local or regional) community, also in relation to cybersecurity. In the case of Poland, the legislator has not awarded this entity with any special status. It is merely one of the many entities forming the national cybersecurity system. As part of its responsibilities, the local government is obliged to carry out a range of activities[16].

Conclusions

The research process resulted in the following answers based on the research question posed: The quantity of data published in the Scopus database in the years of 2020–2024 including the key word of „cybersecurity" has increased significantly since 2023. The reasons for the surge require a separate study. It was quite surprising to establish that it is not only exact sciences that are involved in research into cybersecurity, although they still account for less than 25% of the most represented discipline. What could form an interesting addition to this quantitative analysis is an examination of the approach to cybersecurity in the policies of China and the United States and its impact on the volume of research in this area. These countries are quantitatively leading in this area in relation to various categories.

In its practical dimension, cyber security as a research subject should take into account, similarly as in the case of the development of normative regulations for artificial intelligence for example, international cooperation and

---

14   Key words: „cybersecurity" and „local government" (additionally, the key words indicated by the Author included „confidential information", „information systems" and „telecommunication systems"); furthermore, the article had to be published between 2020 and 2024 and included in the Scopus database. This was the only article obtained in response to those search criteria.

15   M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 3, p. 610.

16   Ibidem, p. 620 and next.

participation of citizens (in the form of the third sector and the private sector that frequently act as contractors) in the formulation of legal regulations. The European Union has not yet developed any common standards to deal with the threats that cause such crises, instead leaving crisis management in the event of such emergency situations caused by cyber-attacks firmly to national legislation[17]. All the more, attention is to be paid to qualitative and quantitative analyses of research, its complementarity and mutual responsiveness with the legislator and public policy makers.

Incorporating a viewpoint from not only the hard sciences, but also the social sciences is crucial in addressing cybersecurity concerns. Educational and training programs play a significant role. Users connected to high-speed Internet must understand the processes that enhance cybersecurity, namely safeguarding against cyber threats. In this area, local and regional authorities play a vital role as supporters of the expansion of telecommunication services and networks[18].

It can be expected that 2024 will continue the upward trend in terms of the number of publications in the area of cyber security. It is noteworthy that cybersecurity is becoming a multidisciplinary issue, one that is going beyond exact sciences with an increase in the amount of research conducted on it, recognising the role of social sciences in the creation of security culture and pro-security attitudes at the stage of the human as part of the cyber security system.

Bibliography

Czuryk M., *Supporting the development of telecommunications services and networks through local and regionalgovernment bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Czuryk M., *The Legal Status of Digital Service Providers in The National Cybersecurity System*, „Cybersecurity and Law" 2024, no. 1.

Gizicki W., *A Security Community: Poland and Her Visegrad Allies: The Czech Republic, Hungary and Slovakia*, Lublin 2013.

Kaczmarek K., *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *Crisis Management vs. Cyber Threat*, „Sicurezza, Terrorismo e Società" 2022, no. 2.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

---

17 M. Karpiuk, *Crisis management...*, p. 113.

18 M. Czuryk, *Supporting the development of telecommunications services and networks through local and regionalgovernment bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2, p. 48.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2.

Scopus – Document search results. Signed in, https://www.scopus.com/results/results.uri?sort=plf-f&src=p&st1=cybersecurity&sid=723f28a7f23eb40acbe0eb2b25de1fac&sot=b&sdt=cl&sl=28&s=ALL%28cybersecurity%29&origin=resultslist&editSaveSearch =&sessionSearchId=723f28a7f23eb40acbe0eb 2b25de1fac&limit=10 [access: 24.03.2024].

Włodyka E.M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, no. 1.

Cyberbezpieczeństwo jako podmiot badań – analiza ilościowa i jakościowa danych w bazie Scopus w latach 2020–2024

Streszczenie

Współczesne społeczeństwo coraz bardziej opiera się na cyfrowych technologiach, które niosą ze sobą nie tylko szanse, lecz także zagrożenia. Jest to ważne zwłaszcza dla sektora publicznego, który z założenia pełni funkcję szczególną – służebną wobec obywateli. Polega ona nie na fakultatywnym, a obligatoryjnym powierzaniu swoich danych z wykorzystaniem systemów teleinformatycznych przez obywateli. W tym kontekście cyberbezpieczeństwo staje się głównym obszarem badawczym, a badania te są niezbędne do zrozumienia zagrożeń cybernetycznych oraz skutecznej reakcji na coraz bardziej złożone ich formy. Niniejsze badanie ma na celu przeprowadzenie analizy ilościowej i jakościowej (w wybranym zakresie) danych z dziedziny cyberbezpieczeństwa w latach 2020–2024 opublikowanych w bazie repetytorium Scopus.

Słowa kluczowe: cyberbezpieczeństwo, administracja publiczna, e-administracja, analiza