Interdisciplinary Description of Complex Systems 22(3), 305-316, 2024

ON THE WAY TO UPDATING THE MEASUREMENT OF INFORMATION SECURITY AWARENESS – A LITERATURE ANALYSIS

Gerda Bak[1], László Berek[2,] *, Zoltán Som[3], Péter Ujhegyi[1] and József Répás[3]

[1]Óbuda University
Budapest, Hungary

[2]Óbuda University, University Library
Budapest, Hungary

[3]Gábor Dénes University
Budapest, Hungary

DOI: 10.7906/indecs.22.3.6
Regular article

Received: 20 May 2024.
Accepted: 16 June 2024.

ABSTRACT

Cybersecurity is crucial in the digital age, as organizations and individuals face increasing threats when using digital devices. The interdisciplinary nature of cybersecurity requires consolidation to meet the requirements of further theoretical and practical applications and international standards and regulations. This study reviews studies published between 1991 and 2022 in the field of cybersecurity and information security, examining trends and relevant publications and collaborations. The aim is to develop a modern, relevant, and up-to-date measurement method – named Security Awareness Measurement – by analysing security awareness measurements and questionnaires used in recent years. The study uses the Web of Science database, Zotero reference management program, VOSviewer software, Scopus database, and GoogleScholar databases for analysis.

KEY WORDS

cybersecurity, Information Security Awareness, Security Awareness Measurement, HAIS-Q, bibliometric analysis

CLASSIFICATION

JEL: D83, L86

*Corresponding author, η: berek.laszlo@uni-obuda.hu; +36 (1) 666-55976;
Óbuda University, Bécsi út 96/B, H – 1034 Budapest, Hungary

INTRODUCTION

Cybersecurity is critical in the digital age as both organisations and individuals face increasing threats when using their digital devices. Over the years, cybersecurity has evolved rapidly, going through different phases, resulting in many different approaches. These approaches sometimes overlap and sometimes exist in isolation, without bridges. However, the interdisciplinary nature of cybersecurity and its continued utility require their consolidation to meet the requirements of further theoretical and practical applications and international standards and regulations.

It is often discussed whether information security is the same as cybersecurity or whether cybersecurity is only a subset of information security [1]. Understanding the long-term implications and consequences of the ambiguity in meaning and terminology of the cybersecurity paradigm is crucial to its proper understanding and application [2]. The most used but differently defined terms are “information technology security”, “information security”, “information security”, “cybersecurity”, “digital security”, “internet security”, “electronic security”, “cybersecurity” or “cybersecurity”. In fact, all these terms are related to cybersecurity, but the terms are not necessarily synonymous [2, 3]. The lack of standardisation of terminology and concepts leads to ambiguity, despite some common points in the literature (e.g. technology, principles CIA – confidentiality, integrity, and availability).

For more than twenty years, the internet has played a major role in global communication and has become increasingly integrated into people’s lives. The internet of things (IOT) and the functioning of smart cities are also closely linked to the online environment, which raises deeper and deeper security questions for the research community today [4]. This is evidenced by its wide availability, high usage and some 3 billion users [5]. The global network provided by the Internet not only facilitates communication, but also generates billions of dollars annually for the world economy [6]. This is further reinforced by the fact that today, a large part of our economic, commercial, cultural, social, and governmental activities and interactions, including individuals, governmental organisations, and business organisations, take place in cyberspace.

Most media activity is moving online, most financial exchanges take place online and citizens spend a significant part of their time and activities interacting in this space [7]. The share of countries’ gross domestic product (GDP) derived from cyberspace businesses has increased significantly [8]. This means that citizens are connected and dependent on online space at many points, with the consequence that any instability, uncertainty, and challenge in this space has a direct impact on different aspects of citizens’ lives [9]. However, cyberspace has also presented governments with new security challenges (cyber warfare, cybercrime, cyber terrorism).

The lack of clear and standardised terminology also makes it difficult to prepare for different cases, both in terms of regulation and action. Therefore, until governments develop a clear definition of cyber-attack that is accepted and supported by the international community, it will certainly be very difficult for experts to deal with the complex and multiple dimensions and aspects of the issue and to provide legal advice and analysis [10]. The question therefore arises as to what cyber-attack is and, consequently, what can be considered cyber defence and information security and what are their characteristics [11].

The lack of a precise and comprehensive definition not only complicates legislation, but also leads to a diversity of interpretation and practice, and ultimately to sometimes contradictory legal conclusions. It is therefore very important and necessary to have an acceptable definition and to explain and adapt it.

In the present study, a review of the studies published between 1991 and 2022 in the field of cyber security and information security was conducted. Subsequently, trends were examined, and relevant publications and collaborations were identified. Finally, the conclusion of the article is presented.

In the next step of the literature review stage, a further qualitative analysis of the measurement methods of previous research will be carried out. The aim of the research conducted at Gábor Dénes University (Budapest, Hungary) is to develop a modern, relevant, and up-to-date measurement method. This requires a systematic review of the security awareness measurements and questionnaires used in recent years.

MATERIALS AND METHODS

The aim of this stage of the research is to prepare a questionnaire survey of users and citizens, exploring the evolution of the relevant literature in the field of cybersecurity. The literature review and analysis were conducted using the Web of Science (WoS) database, which was searched and analysed in fall 2023. The papers and their metadata have been collected, organized, and prepared for further analysis using the Zotero reference management software. For network analysis of publications, connections, and metadata, and for visualisation of the datasets, the VOSviewer software was used.

The Scopus database and GoogleScholar databases were also used for the analysis section on the use of the HAIS-Q questionnaire.

CRITERIA AND LIMITATIONS

As the first approach, the entire literature was examined, regardless of publication date. The search query was conducted on 15 November 2023.

SEARCH QUERY

The structure of the search query was started by mapping the relevant keywords most frequently used in the literature. The following search query was used to conduct the analysis. The provided search parameters returned close to one thousand results. These were further refined by using exclusion criteria. The aim of this research was to investigate and chart the existing literature, and only a few specific criteria were set to limit the scope of the study, such as language and publication date. (Language: English; date of publications:1991-2022)

Web of Science search query #1

> *TS=(awarene* AND cybersecurit* AND questionn*) OR TS=(awarene* AND cybersecurit* AND survey*) OR TS=(awarene* AND "information securit*" AND questionn*) OR TS=(awarene* AND "information securit*" AND survey*) OR TS=(awarene* AND "IT securit*" AND questionn*) OR TS=(awarene* AND "IT securit*" AND survey*) OR TS="Cybersecurity skill*" OR TS="Cybersecurity awareness" Or TS="Information security awareness" OR TS="Information security behaviour"*

The following keywords were used to build the CCL search term:

- cybersecurity,
- information security,
- IT security,
- Awareness,
- survey,
- questionnaire.

The search term has also been combined with other concrete keywords:

- “cybersecurity skill”,
- “cybersecurity awareness”,
- “information security awareness”,
- “information security behaviour”.

Our search query in WoS did not exclude conference proceedings or book chapters. All content indexed in WoS was included in the analysis.

OBJECTIVES

The following objectives have been identified.

The limiting criteria have resulted in a minimal reduction in the number of resulting publications, reducing the number of studies to 884. The primary aim of the survey was to provide a snapshot of the state of the field, including trends in recent years, prominent papers, and major authors. To do this, the following approach was adopted: to identify which countries dominate the field, how research on the topic has changed in recent years, and which journals are most frequently associated with the publication of research.

RESULTS

The increasing number of publications on the measurement of cybersecurity and information security awareness in the period under review shows the relevance of the topic, Figure 1.

Further analysis of the results also identified the main areas of research on the measurement of security awareness. The published research results were examined according to the WoS Categories of the publishing journal.

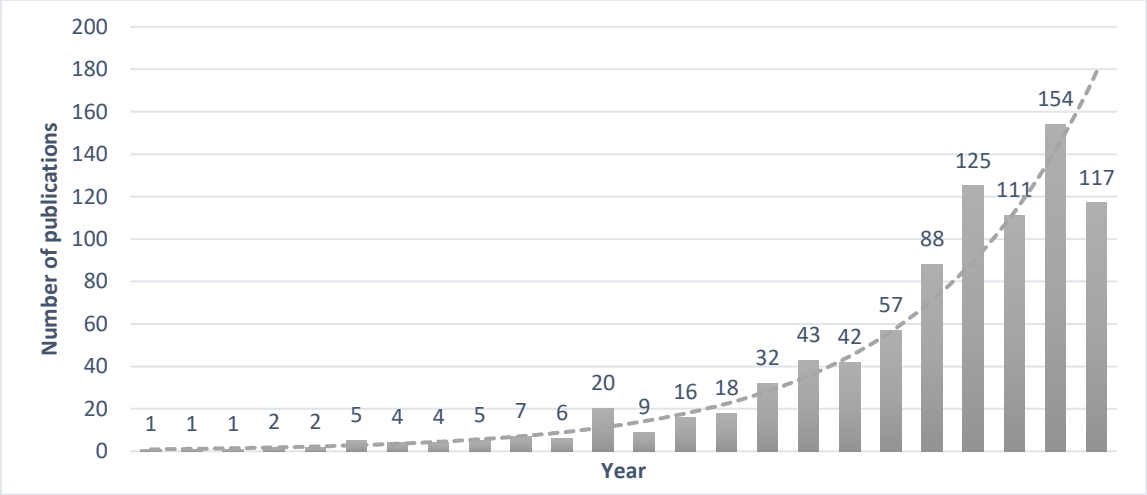

Figure 1. Number of publications (1991-2022), Web of Science.

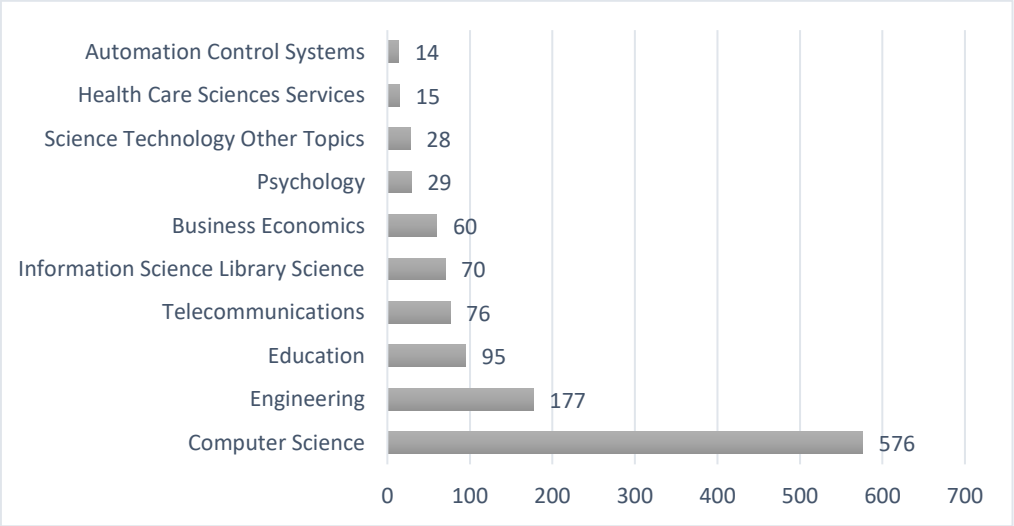

Figure 2. Number of publications (1991-2022), Web of Science.

Predictably, the majority of the papers were to the disciplines of engineering and computer science. It is important to mention that, at the same time, a large number of publications were published in journals classified in the social sciences by WoS.

AUTHOR COLLABORATIONS BY COUNTRY

Further, it was examined which countries have collaborations based on the studies. As a minimum requirement, three studies per country were set. Out of the 86 countries included in the sample, 59 countries meet the requirement, but only 56 countries have connections. The countries can be classified into 11 clusters, which indicates that the area is characterized by several smaller collaborations rather than a few large ones. The results are illustrated in Figure 3.

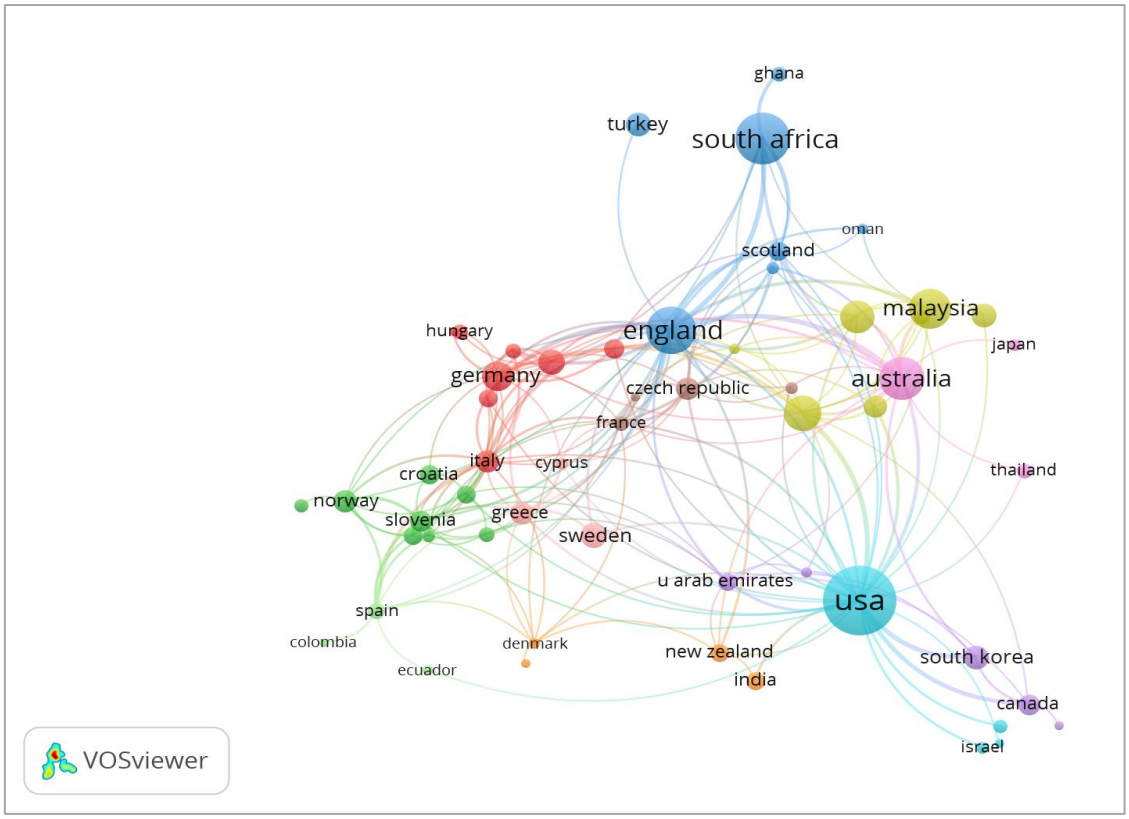

Figure 3. Author Collaborations by Country (1991-2022), VOSviewer.

In terms of collaborations, England ranks first with 77 studies and 1215 citations, which corresponds to a connection strength of 74. The United States follows in second place with 171 studies and 3305 citations, indicating a relatively well-embedded nation in this field. Australia comes next in terms of embeddedness (40), although it has 64 studies and 1330 citations. China is also worth mentioning, as it has 1463 citations and 45 studies included in the examined sample, but its weight in the field (26) is far behind the previously mentioned countries. Additionally, South Africa should be mentioned with 95 publications, 1138 citations, and a connection strength of 22.

CITATION RELATIONS

The papers with the greatest citation count were also analysed. The research paper was required to have a minimum of 4 citations. Out of the 868 papers in our database, only 365 fulfilled the basic threshold, and among them, only 289 showed a relationship. Figure 4 displays the outcome.

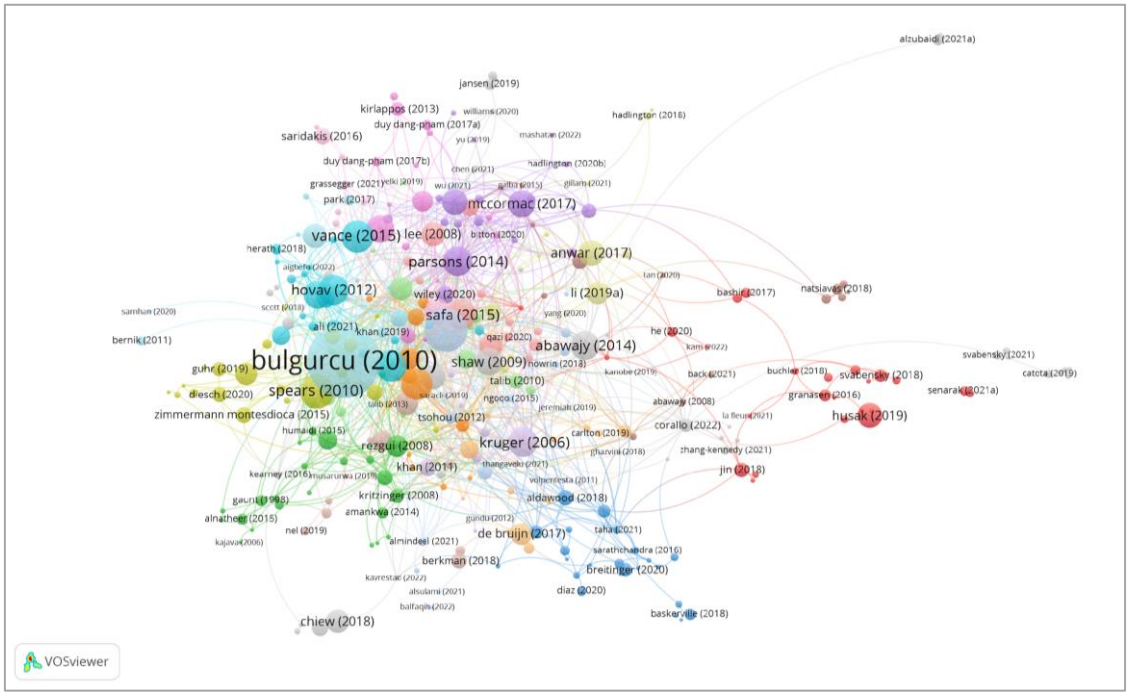

Figure 4. Citation relations (1991-2022), VOSviewer.

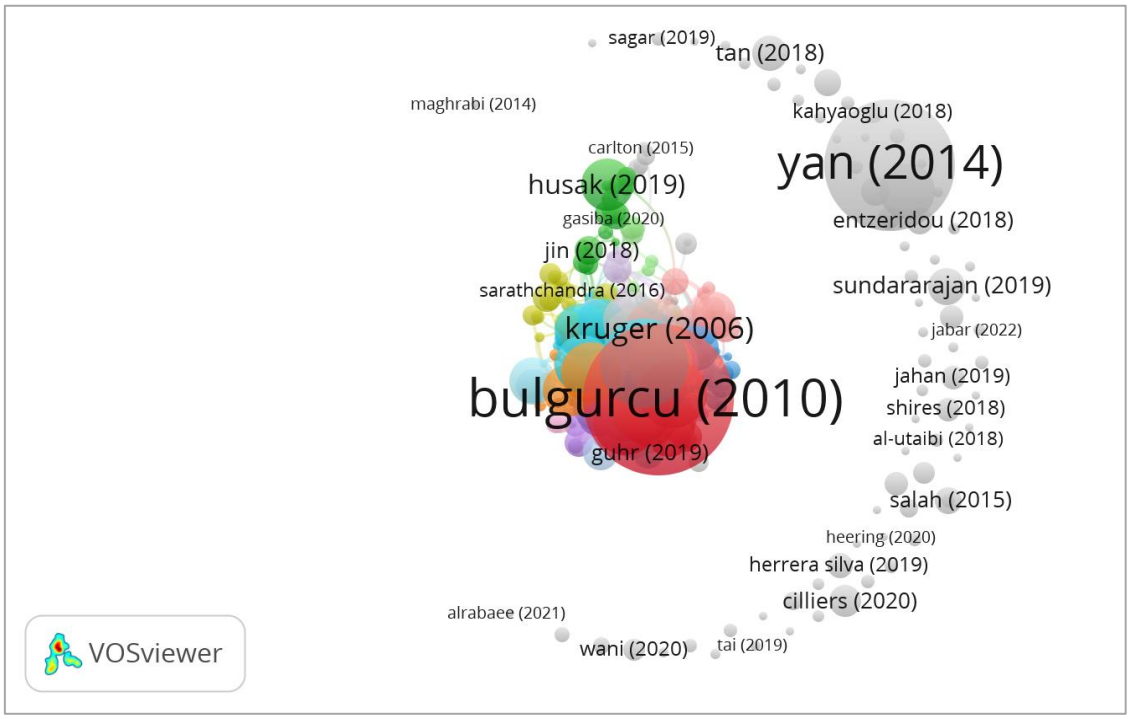

Figure 5. Citation network of researchers (1991-2022), VOSviewer.

The data shown in the figure indicates that the research conducted by Bulgurcu et al [12] has received a significant number of citations, namely 918 citations, and has a high link strength of 78. Following closely is the study by Parsons et al [13], which has received 154 citations and has a link strength of 45. Firstly, it is worth noting that one study in our database stands out significantly with 918 citations, which is quite exceptional in the field. Secondly, it is interesting to mention that the study conducted by Yan [14] holds the second position with 689 citations, but it is not directly related to the studies that serve as the foundation of our database. This was illustrated in Figure 5.

Researcher collaborations

A grand number of 2 224 authors have been identified in papers published in the subject of cybersecurity. Authors were required to have a minimum of two studies for the analysis. Out of the 314 authors, only 35 were determined to have a relationship, as shown in Figure 6. The 35 authors may be categorized into nine clusters, and the overall intensity of the connection among them is 105, resulting in 57 partnerships. The researchers who have made the most significant contributions are Steven Furnell, with 12 publications and 16 co-authors, Marianne Loock, with 11 papers and 5 co-authors, and Elmarie Kritzinger, with 9 papers and 6 co-authors. These findings indicate that the area is marked by several research groups, yet there is little cooperation between these groups.

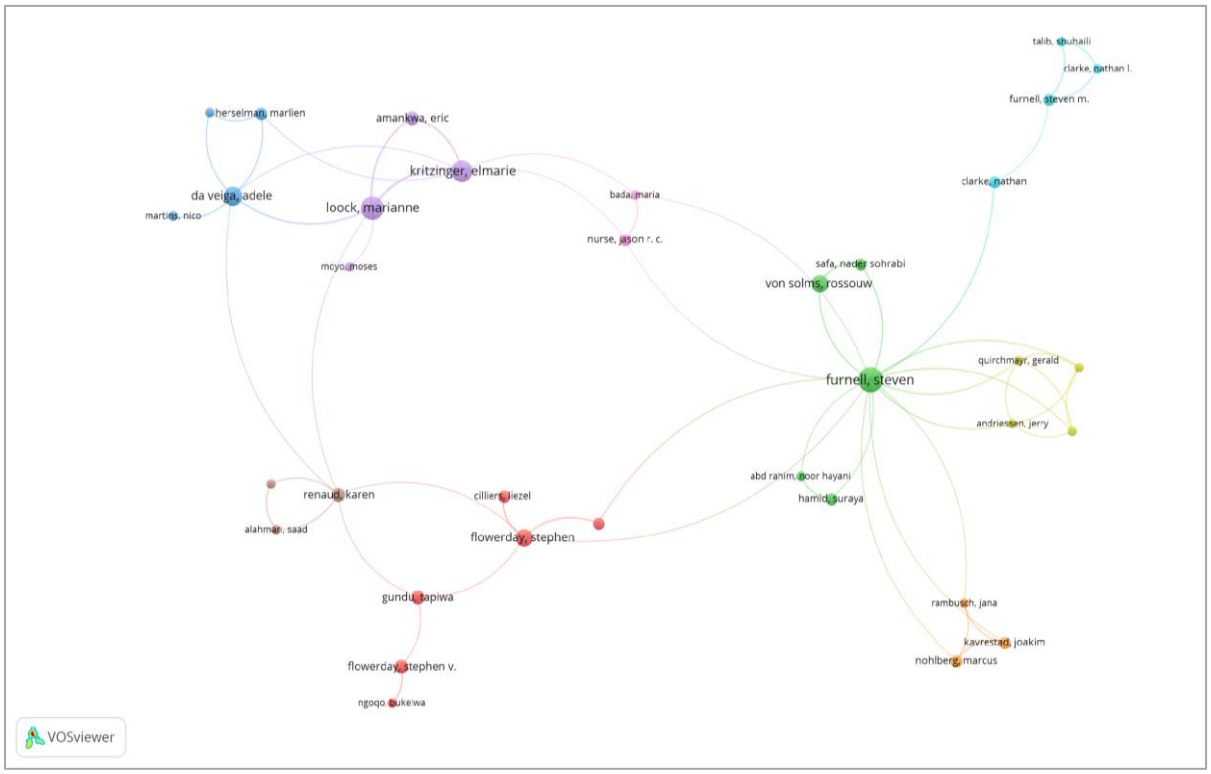

Figure 6. Researcher collaborations (1991-2022), VOSviewer.

KEYWORD ANALYSIS

An analysis of keywords and subject terms is crucial for research as it provides insights into the specific words and expressions used in a particular subject area, how they relate and evolution, and reveals the frequency with which certain terms are studied in scientific literature and how they connect with other terms.

The study of articles involves an examination of keyword use. The findings are shown in Figure 7. The analysis includes words that have a minimum frequency of 5 occurrences. Among a total of 2 219 words, only 102 keywords meet this criterion.

Each colour represents a cluster, with nodes and lines of various colours. The size of a node indicates the frequency of word/term pairs used together, indicating a stronger link. Moreover, the lines connecting the nodes represent the recurrence of the nodes in the same publication. As the distance between two nodes decreases, the frequency of two keywords appearing together increases.

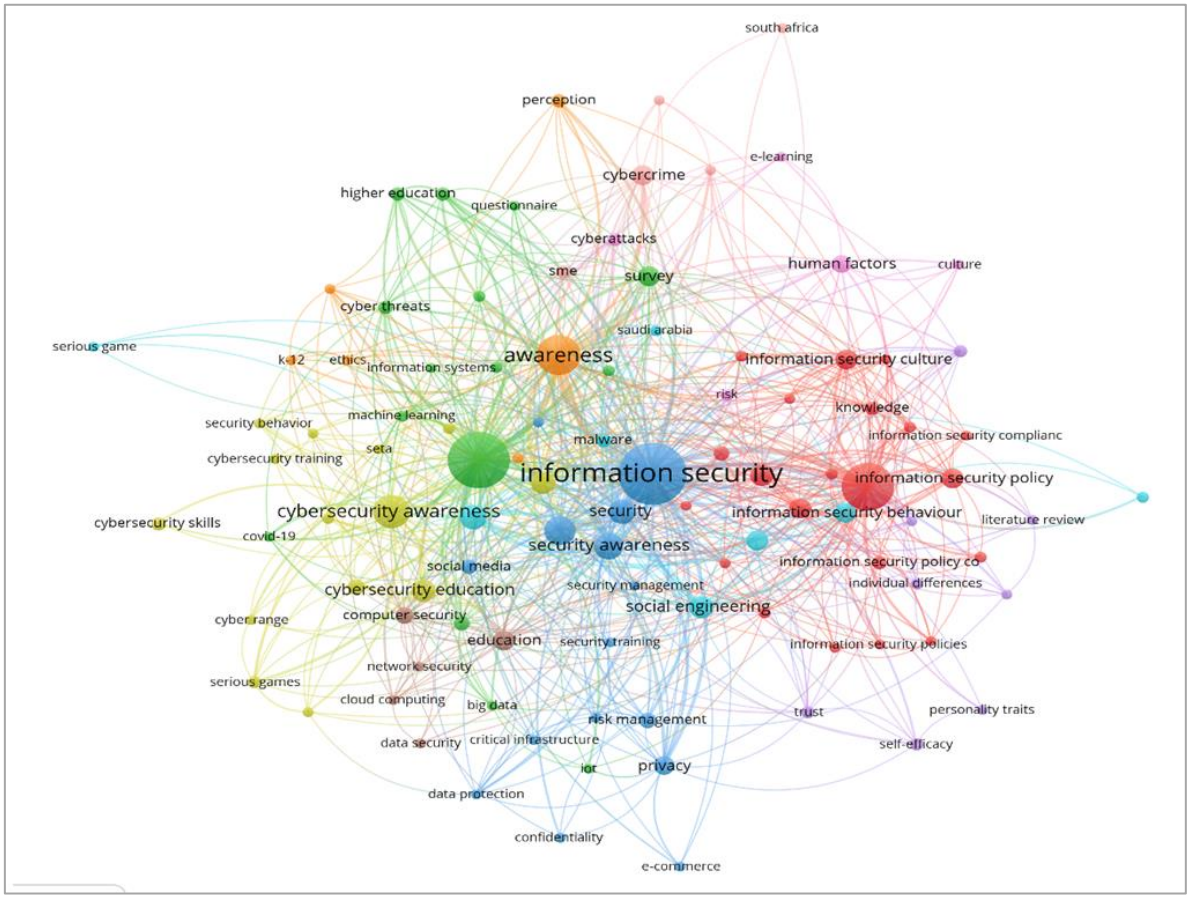

Figure 7. Keyword connections (1991-2022), VOSviewer.

Based on this premise, it can be said that "information security policy", "knowledge", "information security compliance", and "information security behaviour" are interconnected and tightly linked. The blue cluster is primarily characterized by "information security" and "information security awareness". This cluster is closely associated with "risk management", security policies, and security regulations: "policy". The yellow cluster consists of smaller but more precise phrases, such as "cybersecurity", "cybersecurity education", "machine learning", and "cybersecurity skills".

CITATION NETWORK OF JOURNALS

The citation relationship of publications and source journals was also examined, and a map of these is shown in Figure 9. The minimum criterion, in this case a minimum of 20 citations, was also applied in the analysis, with 162 out of 14 978 sources meeting this criterion.

The size of the clusters indicates the activity of the journal, i.e. the number of publications on the topic. The proximity of the clusters allows us to monitor the frequency of citations between journals, greater the proximity, greater the frequency. And the proximity of clusters between journals indicates the increased citation rate between them.

The source journals were grouped into 5 clusters, which showed a total of 9 886 links and 217 317 total link strengths between journals. Three major journals were identified from the analysis of the studies reviewed: Computer Security (1960 citations – 161 links), MIS Quarterly (993 citations – 158 links), Computer Human Behaviour (628 citations – 160 links).

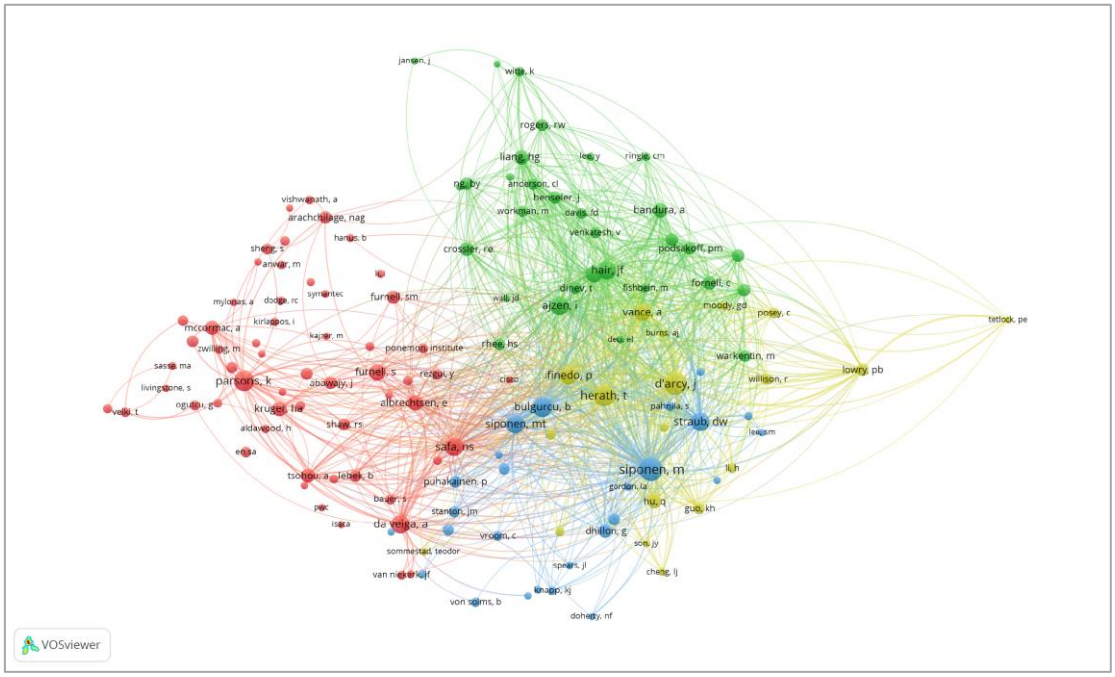

Figure 8. Keyword connections (1991-2022), VOSviewer.

MEASUREMENT METHODS IN PREVIOUS RESEARCH

The analysis of information security awareness measurement and measurement methods was not performed on our complete database. The 200 most cited publications were selected for the analysis. This was followed by a detailed screening of the full text and appendices. From these publications, papers were selected for which a specific questionnaire survey was conducted. A separate database of available questionnaires was created to facilitate further analysis. The top 25 most cited papers also included the three fundamental HAIS-Q studies using this method. [13, 15, 16].

From a detailed examination of the sample, it was identified that although the HAIS-Q questionnaire is not commonly used exclusively, the same cannot be said for other questionnaires. Out of the 200 most cited publications, only 9 references to HAIS-Q were found. Further searches on the HAIS-Q will be carried out to have a more complete picture of its use. As the set of 200 most cited publications is a restricted sample, due to its size and the limitations of the search term, separate targeted searches were conducted.

The first additional search was initiated in the Scopus database using the following search term:

> *(TITLE-ABS-KEY (hais-q) OR TITLE-ABS-KEY ("Human Aspects of Information Security Questionnaire"))*

The search returned 41 results, which is the number of publications with the term in their title, abstract or keywords. This was followed by a citation analysis of the 3 “basic” publications of HAIS-Q. The citations of the 3 publications returned 596 citations in the Scopus database.

The distribution of citations over time for the three publications [13, 15, 16] shows that the number of citations is increasing almost continuously. It is also worth mentioning that, out of a total of 596 citations, 119 publications cited one of the three journal articles in 2023.

In addition to Web of Science and Scopus, we also searched a wider database of publications, not necessarily in the most highly ranked journals. Although GoogleScholar also includes - at the data level – publications indexed by the two major scientific databases, it also includes lower ranked journals and conference proceedings. Based on GoogleScholar data, the number of citations for the three HAIS-Q articles in January 2024 was 1207.

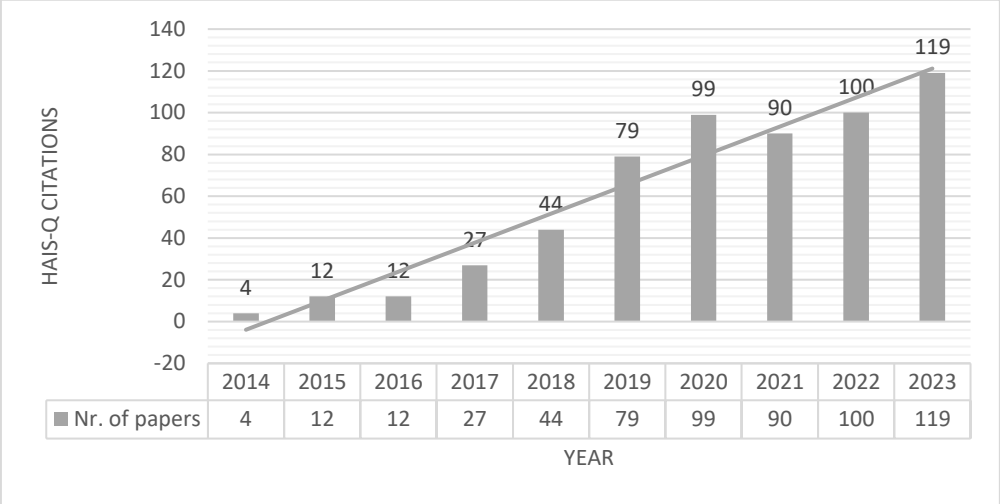

Figure 9. HAIS-Q citations (2014-2023), Scopus.

The findings from the three databases show that the HAIS-Q questionnaire is referred to and used much more frequently than the other questionnaires. After a detailed analysis of the questionnaire, the research team decided to further develop and revise the questionnaire. In the next stage of the research, the revised questionnaire, SAM including the new items, will be evaluated in pilot groups.

CONCLUSIONS

Due to the rapid advancement of technology, the rise of artificial intelligence, and the escalating occurrence and intensity of cyber-attacks, there is a growing number of scientific papers and research being conducted on this topic. Evaluating the quality of a substantial quantity of research publications and extracting significant information is of the highest importance. Scientific, professional, IT, and educational research are crucial in analysing cyber-attacks and developing strategies to limit their spread and improve cyber-defence. Considering its extensive prevalence and impact, cybercrime poses a substantial threat to national economies, resulting in concrete financial losses. Moreover, it has the capacity to erode the faith of a considerable portion of the population in IT services.

The aim of Gábor Dénes University is to develop a modern, relevant and up-to-date method for measuring cybersecurity awareness. This involves the analysis of security awareness measurements and questionnaires used in recent years. The research aims to prepare a questionnaire survey of users and citizens, exploring the evolution of relevant literature in cybersecurity. The HAIS-Q questionnaire is found to be more frequently used than other questionnaires. After a detailed analysis, the research team decided to further develop and revise the questionnaire. The revised questionnaire, *Security Awareness Measurement*, will be evaluated in pilot groups in the next stage of the research.

A further important objective of the research was to develop an appropriate methodology to measure information security awareness. The mapping, systematic review, and analysis of the literature in the selected areas also provides a direction for other stages of the research. In the next stage, the research group will examine the literature from the perspective of the following areas: identifying target groups; data collection methods; information security awareness parameters.

ACKNOWLEDGEMENT

The project was funded by the Thematic Excellence Programme (TKP) of the National Research, Development and Innovation Office, in the framework of the Information Security Complex Research Programme of Gábor Dénes University (Project ID: TKP2021-NVA-05).

REFERENCES

[1] von Solms, B. and von Solms, R.: *Cybersecurity and information security – what goes where?* Information and Computer Security **26**(1), 2-9, 2018, http://dx.doi.org/10.1108/ICS-04-2017-0025,

[2] Kianpour, M.; Kowalski, S.J. and Øverby, H.: *Systematically understanding cybersecurity economics: A survey.* Sustainability **13**(24), No. 13677, 2021, http://dx.doi.org/10.3390/su132413677,

[3] Althonayan, A. and Andronache, A.: *Shifting from Information Security towards a Cybersecurity Paradigm*. In: Proceedings of the 2018 10th International Conference on Information Management and Engineering. pp.68-79, 2018, http://dx.doi.org/10.1145/3285957.3285971,

[4] Simon, J. and Mester, Gy.: *Critical Overview of the Cloud-Based Internet of Things Pilot Platforms for Smart Cities.* Interdisciplinary Description of Complex Systems **16**(3-A), 397-407, 2018, http://dx.doi.org/10.7906/indecs.16.3.12,

[5] Tan, S., et al.: *Attack detection design for DC microgrid using eigenvalue assignment approach.* Energy Reports **7**(1), 469-476, 2021, http://dx.doi.org/10.1016/j.egyr.2021.01.045,

[6] Judge, M.A.; Manzoor, A.; Maple, C.; Rodrigues, J.J.P.C. and ul Islam, S.: *Price-based demand response for household load management with interval uncertainty*. Energy Reports **7**(2), 8493-8504, 2021, http://dx.doi.org/10.1016/j.egyr.2021.02.064,

[7] Priyadarshini, I.; Kumar, R.; Sharma, R.; Singh, P.K. and Satapathy, S.C.: *Identifying cyber insecurities in trustworthy space and energy sector for smart grids*. Computers & Electrical Engineering **93**, No. 107204. 2021, http://dx.doi.org/10.1016/j.compeleceng.2021.107204,

[8] Amir, M. and Givargis, T.: *Pareto optimal design space exploration of cyber-physical systems.* Internet of Things **12**, No. 100308, 2020, http://dx.doi.org/10.1016/j.iot.2020.100308,

[9] Li, N.; Tsigkanos, C.; Jin, Z.; Hu, Z. and Ghezzi, C.: *Early validation of cyber–physical space systems via multi-concerns integration.* Journal of Systems and Software **170**, No. 110742, 2020, http://dx.doi.org/10.1016/j.jss.2020.110742,

[10] Cao, J., et al.: *Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks.* Information Sciences **548**, 69-84, 2021, http://dx.doi.org/10.1016/j.ins.2020.09.046,

[11] Gupta Bhol, S.; Mohanty, J.R. and Kumar Pattnaik, P.: *Taxonomy of cyber security metrics to measure strength of cyber security*. Materials Today **80**(3), 2274-2279, 2023, http://dx.doi.org/10.1016/j.matpr.2021.06.228,

[12] Bulgurcu, B.; Cavusoglu, H. and Benbasat, I.: *Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness*. MIS Quarterly **34**(3), 523-548, 2010, http://dx.doi.org/10.2307/25750690,

[13] Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M. and Jerram, C.: *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q).* Computers & Security **42**, 165-176, 2014, http://dx.doi.org/10.1016/j.cose.2013.12.003,

[14] Yan, Z.; Zhang, P. and Vasilakos, A.V.: *A survey on trust management for Internet of Things.*
Journal of Network and Computer Applications **42**, 120-134, 2014,
http://dx.doi.org/10.1016/j.jnca.2014.01.014,

[15] Parsons, K., et al.: *The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies.*
Computers and Security **66**, 40-51, 2017,
http://dx.doi.org/10.1016/j.cose.2017.01.004,

[16] McCormac, A., et al.: *Individual differences and Information Security Awareness.*
Computers in Human Behavior **69**, 151-156, 2017,
http://dx.doi.org/10.1016/j.chb.2016.11.065.