Chapter

Bibliometric Analysis of Cyber Threat and Cyber Attack Literature: Exploring the Higher Education Context

Nazahah Rahim

Abstract

In nearly all procedures involving students and faculty, higher education organizations make substantial use of computers and the internet. Little is known on the progress and development of literature on cyber threats and cyber attacks in this sector. This chapter fills this gap by examining the trends of literature on cyber threats and cyber attacks focusing on the higher education. Bibliometric analysis through Scopus database was employed to offer research ideas and trigger debates. Analyzed parameters include the number of document types, publications, authorship, citation, and subject areas, as well as the topographical dispersion of published research. The earliest publication could be seen in the year 2003, and since then 606 papers were published. The majority of publications were conference papers but merely 8.42% of those were open access. The results indicate that publications hit a plateau in 2018, with English becoming the main publication language. The most prominent country that has contributed to the literature is the United States. Nonetheless, the majority of the publications were contained by the subject area of Computer Science, hence it is relatively challenging to trace the progress in education context. This chapter presents a groundwork providing insights for others to probe into the topic further.

Keywords: bibliometric, cyber attack, cyber threat, higher education, university

1. Introduction

The global population exceeds seven billion humans, and as of February 2019, there were over four billion internet users worldwide (Internet World Stats). Asia accounts for almost two billion of these internet users. From 2000 to 2018, internet use in Asian countries increased at a pace of 1,704% (Internet World Stats). Malaysia, for example, a nation in the Asian region, experienced 880 percent rise from 2006 to 2017, as well as a rise in the number of internet users from 2.5 million to 24.5 million citizens [1]. This trend shows that people across the globe are widely accessing internet capabilities in their everyday lives; as more and more people invest in cyber space to conduct their daily activities, cyber protection is critical.

One aspect adding to this effect is the advancement in information and communication technology (ICT), which provides consumers with unique resources and

possibilities. Although ICT and its technology have made substantial strides, the cyber space is still far from protected, as it is prone to cyber breaches and cyber-attacks. For example, despite Malaysia's strong commitment to cyber protection and ranking third among 193 countries worldwide, there were 6,274 cases of cyber-attacks reported in 2017 [2]. This demonstrates that cyberspace cannot be completely protected; therefore, concern regarding cyber protection is critical given the increasing dependency on information systems and the internet. Again, considering Malaysia as an example, a report by Microsoft, an acclaimed technology firm, revealed that the possible economic loss due to cyber threats would reach a stunning USD12.2 billion, which is equal to more than 4 percent of Malaysia's total GDP of USD296 billion [3]. Additionally, the analysis discovered that a large-sized organization in Malaysia would suffer a USD22.8 million economic loss, which is 630 times greater than the average economic loss for a medium-sized organization [3]. While cyber protection is a serious concern, a massive amount of information and information is still exchanged globally through the cyber space. This is true not just for companies, but also for other industries, such as higher education.

Cyber protection is an appealing concern due to the supremacy and rapid development of computing systems and internet capabilities. Higher education is one of the industries under pressure. There have been reports of universities being subjected to cyber assaults in which their data are hacked. Users in institutions of higher education access information through portable devices that enable them to be highly mobile. This familiarity with networking enables them to connect to the network at any time and from any platform. As a consequence of the tradition of transparency and having free access to data and documents, security breaches and cyber-attacks at institutions of higher education are highly challenging to protect [4, 5].

Inadequate computer defense exposes higher education to risks, and the abundance of scholarly study data has transformed educational institutions into an enticing destination for cyber criminals [6]. This demonstrates that institutions of higher education, such as colleges and universities, are increasingly vulnerable to cyber security threats. They become insecure as a result of the open access and information-sharing ethos prevalent in the majority of universities. This is concerning for the higher education industry, as cyber-attacks such as hacking have the potential to halt research operations. Hackers distribute valuable knowledge obtained from universities, and hackers may quickly exchange data when it becomes an asset [6]. Universities' online systems are a prime subject for cyber security attacks like hacking [6]. It is because the network in operation at universities includes highly confidential personal details for students and faculty, as well as a wealth of scholarly intellectual property. The university community's tradition of accessible dialog and teamwork, which includes faculty, administrative personnel, researchers, and study organizations, makes the system much more susceptible to threats and assaults.

Higher education institutions make full use of information technology and the internet in nearly all of their operations. Higher education networks are linked to the virtual realm, but the cyber space remains insecure as a result of fraud and misconduct, posing cyber security risks. Cyber security refers to the process of safeguarding computer-related systems, such as software, hardware and electronic data, from fraud, destruction, disturbance, or subterfuge. Prior research has addressed a variety of topics associated with data security in general, though not directly to cyber-attacks and network security. Only recently have scholars recognized the importance of this problem in an educational or academic environment, particularly when universities begin to adopt online learning. As such, this chapter would examine the pattern of research undertaken in the field of cyber challenges

and cyber-attacks in higher education. Its aim is to investigate what is currently available and to explain the history of the literature, as well as to make recommendations for potential study.

This chapter is divided into the following sections: The following segment would discuss the literature review, accompanied by the methodology. The methodology segment details the methodology followed, including the source, dataset, data collection, and major research components. The results and discussion segment includes an overview of the data produced by the bibliometric studies, as well as a summary of the findings. Finally, the conclusion segment discusses the study's shortcomings, makes recommendations for potential studies, and makes several closing remarks.

2. Literature review

Cyber threats are the chances of malicious attempts to damage or disrupt a computer network or system and are called cyber-attacks when these possibilities turn into a genuine effort [7]. A cyber-attack can be initiated through viruses, worms, Trojan horses, rootkit, botnet, or spyware that interrupt the online system [8]. These attacks are executed to acquire unauthorized access to personal data, to destroy and steal sensitive information [9]. The terms cyber threat and cyber attack are often used interchangeably in the literature; however, the main difference between these two terms is like intention and actions. When a malicious program is developed with an intention to breach cyber security is called a cyber threat and when it is actually used for intrusion into the system is become the potential attack [10].

Cyber threats have mainly three types, i.e. malware, distributed denial of service (DDoS) attacks, and ransom-ware. Firstly, malware is the most common type of malicious program that can attack a computer system, but the victim must have to click on the link provided. This link is given on an email or web page, and hackers usually place this link under some attractive statement or image that forces the victim to click on it. Upon clicking, the malware downloads into the computer and accesses the system, after which it can delete important files and leak sensitive information [8]. Secondly, Secondly, Ransomware resembles malware in nature, but they do not need to click on a link to download it to the system but are automatically downloaded from an email or website. The ability to auto-download makes it more powerful and dangerous as compared to malware (Russell, 2017). Finally, DDoS attacks are not intended to gain access to the computer system, but to overload web traffic. This causes the website to temporarily shut down, and the company may be facing loss in terms of revenues and consumers [9].

With the robust increase in online activities in the last decade, many virtual networks are exposed to cyber-threats [11]. In this regard, mostly prior studies focused the banking and defense systems, but a little is known about the intensity of cyber threats and attacks in the context of higher education [10, 11]. Higher education institutions are increasingly using web-based portals, where all their educational resources and information (including academic results, students' personal records and e-library) are available [12]. Therefore, higher educational institutions are exposed to cyber-attacks due to the availability of sensitive information and data [13].

Mostly, past studies explored the recent digitization and development of web-based educational management systems in higher education institutes to gain ICT competence [14]. Utilization of cyber services not only develop a knowledge management system of higher educational institutes but also enhance their performance

[15]. This growing trend in e-learning systems adopted by higher education institutions highlights the serious concern for cyber security [16]. In line with this, [17, 18] highlighted the gaps in cyber security and stressed the development automated threat modeling system. Therefore, it is required to develop an effective cyber security system that can detect and prevent cyber-threats and attacks.

Specifically, in the context of cyber security, most of the research in higher education has been done in risk management frameworks and standards whereas, the least focus is given to the governance and cultural awareness [19]. Due to which cyber security has not been implemented in higher education institutions in its true spirit. In line with this, [18], highlighted that generally higher education institutions do not have independent central security services due to lack of resources. As a result, they have to out-source these services, which are insufficient for cyber security [19]. The main reason for this inadequacy is the unique nature of educational institutions' security systems, which is radically different from other institutions' security systems [20].

In addition, [21] argued that linking with a countywide firewall; the institutions can prevent cyber-attacks more effectively. When a network is linked to a national firewall, it filters all the incoming network stream that prevents cyber threats and attacks. One possible drawback of this process is that it reduces the pace of data transmission within the networks that cause in a long delay in system response and sometimes declines the request [22]. In order to smooth and quick data transmission, the threat modeling approach is preferred for cyber-attack prevention, that models the independent and exclusive security framework for a specific system [17]. But this is not possible without the special attention of the administration as it requires considerable resources in the form of a dedicated workforce and system [18].

Furthermore, [23] noted that awareness of the information security of higher education institution members (students, faculty, and employees) could play a vital in the prevention of cyber-attacks. They also assessed the information security awareness among the members of middle-east higher education institutes and found a low level of awareness among them. Similarly, [24] analyzed cyber security behavior among Malaysian students of higher education institutes and also found a low level of understanding about the subject among them. The findings of both studies are similar that indicate the need for a comprehensive training program of higher education institution members to enhance their understanding of information security [23].

3. Methodology

A bibliometric analysis was conducted to ascertain the developments in the literature on cyber risks and cyber assaults. Due to the exploratory aspect of this research, bibliometric analysis is an efficient tool for detecting and examining the development of this research field. Although this research offers a foundational analysis, it adds to awareness and experience by being one of the first to analyze literature on cyber vulnerability and cyber assault in higher education since 2004. As of 25 July 2019, the list of publications was retrieved using the Scopus database search engine. Scopus (scopus.com) is an online library that stores the world's biggest collection of abstracts and citations to peer-reviewed literature. The index contains 1.4 billion citations extending all the way back to the 1970s and is an often-referenced source of other bibliometric research studies. Numerous forms of recorded evidence and articles were analyzed, including scientific journals, articles, books, and conference proceedings. Due to the chapter's primary emphasis on cyber

threat and attack, the following search words were used: cyber threat*, cyberthreat*, cyber-threat*, cyber attack*, cyberattack*, and cyber-attack*. The index was checked using these words in the following areas: title, keywords, and abstract. The online searching of these words resulted in 606 datasets, which were then analyzed further. The findings were then classified according to the number of articles, document formats, subject fields, authorship, and geographical distribution of countries contributing to the literature. The subsequent section discusses the analysis's findings, which are represented graphically and in organized views of the cited studies.

4. Results and discussion

This segment addresses the different methods of access and the amount of publications over time, the text types, the subject fields in which the papers were written, the most influential contributors, the countries where the study was conducted or the regional distribution of the articles, as well as the languages used.

4.1 Access types and number of publications

The data was initially analyzed depending on the type of access and the amount of publications. According to **Table 1**, 8.42 percent of documents released on the subject of cyber threats and cyber attacks were open access. This implies that it would be difficult for researchers to obtain and access materials, data, and information from sources such as journal articles, conference papers, and theses, so study outputs are not often freely available online. It is clear that the previous publications occurred in 2003 with two publications and remained a relatively unpublished subject until 2010, when the number of publications increased from fewer than ten per year to fourteen per year. Following the year, there is a reasonably constant growth in the number of publications. This may be due to increased interest in the topic. The most productive year was 2018, with a record of 144 (23.76 percent). **Table 2** and **Figure 1** outline the detailed statistics on the amount of literature written. Nevertheless, further examination of the papers, especially the title, demonstrated that very little research on higher education has been conducted.

4.2 Document types

Table 3 summarizes the document forms, with conference papers accounted for the bulk (54.29% of documents written before 2020), journal articles accounted for 32.67 percent, and book chapters accounting for 6.93 percent. The remaining documents included conference reviews, book reviews, articles in press, brief essays, editorials, notices, and erratum. Over a 17-year span, 329 conference papers on the subject of cyber threat and cyber attack have been published mostly as proceedings

Access type	Frequency	% (N = 606)
Open access	51	8.42
Other (non-open access)	555	91.58
Total	606	100%

Table 1.
Access type.

Publication Year	Frequency	% (N = 606)
2020	2	0.33
2019	65	10.73
2018	144	23.76
2017	99	16.34
2016	66	10.89
2015	47	7.76
2014	41	6.77
2013	51	8.42
2012	33	5.45
2011	17	2.81
2010	14	2.31
2009	8	1.32
2008	7	1.16
2007	2	0.33
2006	4	0.66
2005	3	0.50
2004	1	0.17
2003	2	0.33
Total	606	100%

Table 2.
Number of publications according to year.

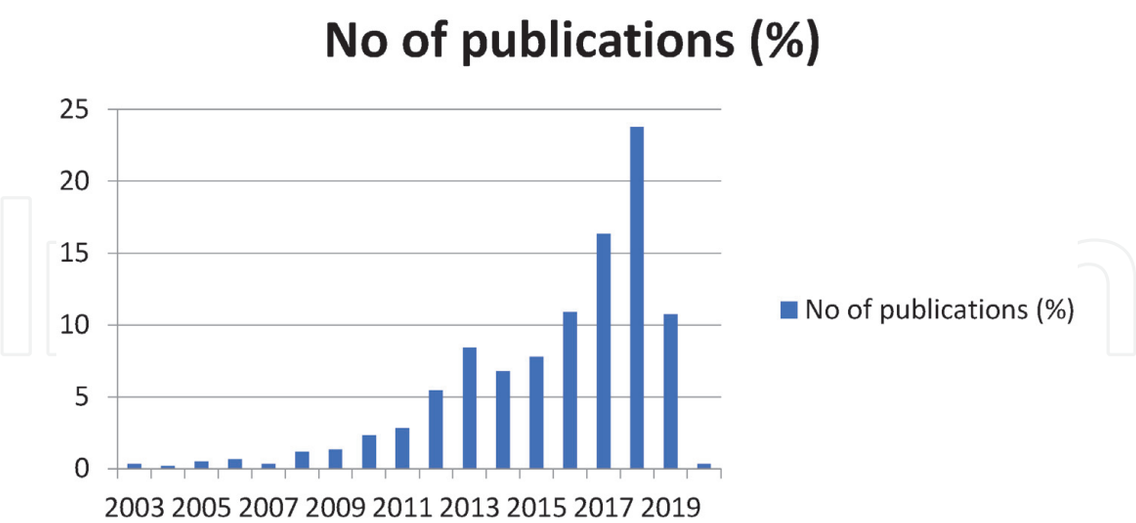

Figure 1.
The trend of publication from 2003 until 2020 (as at 25 July 2019).

in a variety of venues, including the European Conference On Information Warfare And Security Eccws, the ACM International Conference Proceeding Series, the Proceedings IEEE Military Communications Conference MILCOM, and the Proceedings Of The 12th International Conference On Cyber. Nonetheless, most scholars did not choose to report in specialized publications such as Advances in Intelligent Systems and Computing, Communications in Computer and Information Science, Computers and Security, and Computer Fraud and Security. This may be

Document Type	Frequency	% (N = 606)
Conference Paper	329	54.29
Article	198	32.67
Book Chapter	42	6.93
Review	17	2.81
Book	13	2.15
Short Survey	2	0.33
Editorial	1	0.17
Undefined	4	0.66
Total	606	100%

Table 3.
Document types.

that proceedings require less time to print than papers. Other variables include the expectations and criteria of journal publishers to ensure that their publications are comparable to existing and high-quality journals.

4.3 Subject areas

The subject areas of the publications published between 2003 and 2020 are depicted in **Figure 2** and **Table 4**. As a result of this analysis, 34.91 percent of documents released on cyber threats and cyber attacks fall under the area of Computer Science. This is accompanied by 25% in the field of Engineering and 7.19 percent in the field of Mathematics. Previous authors' works are also available in the fields of Social Sciences, Decision Science, and Energy. This indicates that the difficulty and multidisciplinary existence of the problem are important in a variety of fields. This is significant because the topic of cyber threats and attacks encompasses many subject fields, not just computer science, which examines the philosophy, experimentation, software, and engineering involved in the design and usage of machines, but also social sciences and humanities. This, though, makes it more difficult for prospective scholars to conduct literature searches centered on the education system.

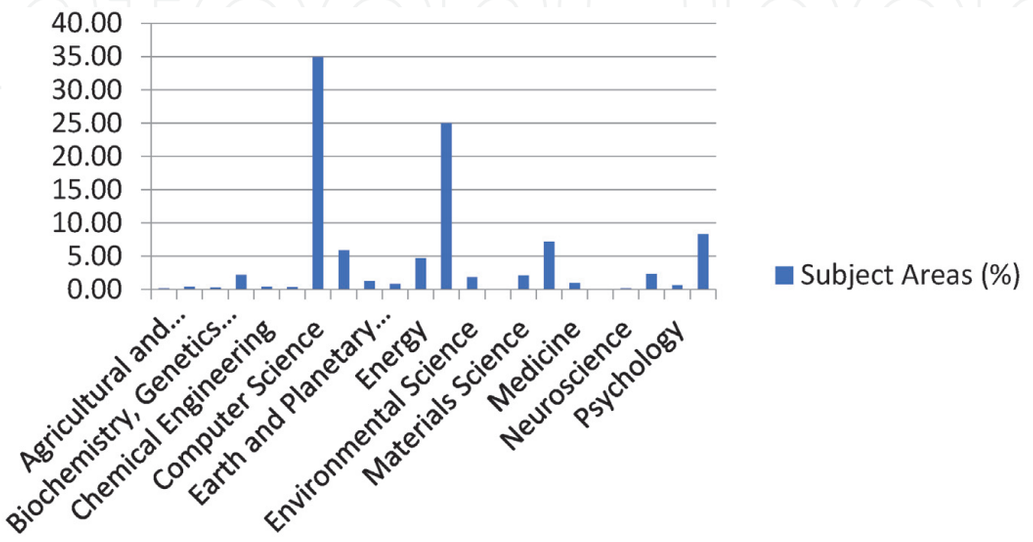

Figure 2.
Subject areas.

Document Type	Frequency*	% (N = 1140)
Agricultural and Biological Sciences	2	0.18
Arts and Humanities	5	0.44
Biochemistry, Genetics and Molecular Biology	3	0.26
Business, Management and Accounting	25	2.19
Chemical Engineering	5	0.44
Chemistry	4	0.35
Computer Science	398	34.91
Decision Sciences	67	5.88
Earth and Planetary Sciences	14	1.23
Economics, Econometrics and Finance	9	0.79
Energy	53	4.65
Engineering	285	25.00
Environmental Science	21	1.84
Health Professions	1	0.09
Materials Science	24	2.11
Mathematics	82	7.19
Medicine	11	0.96
Multidisciplinary	1	0.09
Neuroscience	2	0.18
Physics and Astronomy	26	2.28
Psychology	7	0.61
Social Sciences	95	8.33
Total	1140	100%

**Some documents were categorized under more than one subject area.*

Table 4.
Subject areas.

4.4 Authorship

The data collection method resulted in the development of 606 datasets, each of which was registered and published by 160 distinct writers. The datasets revealed information about the most prolific writers who have authored several research papers. According to the analysis in **Table 5**, there were two productive scholars who both reported six publications on cyber threats and cyber attacks. Bella Genge of Targu Mures University of Medicine, Pharmacy, Sciences, and Technology in

Author Name	Frequency
Genge, B.	6
Sengupta, S.	6
Chen, H.	5
Cho, H.	5
Haller, P.	5
Lakhno, V.	5
Samtani, S.	5
Debbabi, M.	4

Author Name	Frequency
Govindarasu, M.	4
Hwang, I.	4
Kim, N.	4
Kiss, I.	4
Lee, S.	4
Lehto, M.	4
Nunes, E.	4
Shakarian, P.	4
Ban, T.	3
Bou-Harb, E.	3
Chu, B.	3
Dolan, A.M.	3
Dondossola, G.	3
Eto, M.	3
Fergus, P.	3
Geers, K.	3
Graf, R.	3
Hurst, W.	3
Husari, G.	3
Joshi, A.	3
Kam, A.	3
Kamhoua, C.A.	3
Khanna, K.	3
Kiesling, T.	3
Kshetri, N.	3
Kwon, C.	3
Levy, Y.	3
Liu, E.C.	3
Merabti, M.	3
Panigrahi, B.K.	3
Ruane, K.A.	3
Simari, G.I.	3
Skopik, F.	3
Stevens, G.	3
Thompson, R.M.	3
Akhgar, B.	2
Al Hamar, J.	2
Al-Shaer, E.	2
Al-Shaer, E.	2
Alves, T.	2
Anwar, Z.	2
Arimatsu, T.	2
Ashok, A.	2
Assi, C.	2
Astatke, Y.	2
Au, H.	2
Awan, I.	2
Aydin, F.	2
Bagrodia, R.	2
Balitanas, M.O.	2
Betser, J.	2
Bracho, A.	2
Brenner, S.W.	2
Brooks, T.	2
Buch, J.P.	2
Campbell, R.J.	2
Canzian, L.	2
Castiglione, A.	2
Cheung-Blunden, V.	2
Choi, M.S.	2
Choo, K.K.R.	2

Author Name	Frequency
Choraś, M.	2
Chowdhury, A.	2
Ciancamerla, E.	2
Clark, R.M.	2
Cole, D.G.	2
Conti, M.	2
Dargahi, T.	2
Das, R.	2
Dawson, M.	2
Dean, R.	2
Dutt, V.	2
Dwivedi, A.	2
Ekstedt, M.	2
Eldridge, J.	2
Elliott, D.	2
Ewart, R.	2
Gamba, G.	2
Goncharova, L.L.	2
Grobler, M.	2
Ha, B.N.	2
Hassan, A.	2
Hein, C.	2
Henning, A.C.	2
Holsopple, J.	2
Hu, J.	2
Inoue, D.	2
Jalal, I.	2
Jaquire, V.	2
Jun, M.S.	2
Kalogeraki, E.M.	2
Kamhoua, C.	2
Kim, B.	2
Kim, K.	2
Kim, T.H.	2
Koike, H.	2
Kovacevic, A.	2
Kozik, R.	2
Kwiat, K.	2
Kwiat, K.A.	2
Lee, K.	2
Lee, K.	2
Lee, S.J.	2
Lee, S.W.	2
Lee, W.	2
Lee, Y.	2
Lim, I.H.	2
Linkov, I.	2
Liu, W.	2
Loukas, G.	2
Ma, Z.	2
Maccarone, L.T.	2
Magalhães, J.P.	2
McLorn, G.W.	2
Merino, X.	2
Minichino, M.	2
Moazzami, F.	2
Mokhtar, M.R.	2
Morris, T.	2
Musliner, D.J.	2
Nakao, K.	2
Nazir, S.	2

Author Name	Frequency
Niederl, J.	2
Nikolic, D.	2
Niu, X.	2
Nobles, C.	2
Noor, U.	2
Oksiuk, A.	2
Olsberg, R.	2
Omar, M.	2
Otero, C.	2
Palmieri, S.	2
Palomar, E.	2
Panguluri, S.	2
Papastergiou, S.	2
Park, J.	2
Park, M.	2
Patel, D.	2
Patel, S.	2
Patton, M.	2
Pena, J.	2
Polemi, N.	2
Pota, H.R.	2
Pourmirza, Z.	2
Pournouri, S.	2
Pozzobon, O.	2
Rahman, M.A.	2
Rahman, M.S.	2
Ramim, M.	2
Ridley, M.	2
Rob, R.	2
Undefined	1

Table 5.
Authors and their publications.

Romania and Sudipta Sengupta of Microsoft Research in Redmond, Washington, USA were the writers. Both scholars have amassed thousands of citations worldwide. Their research made significant contributions to information, experience, and philosophy, especially in the sense of cyber security concerns, but they remain underrepresented in the higher education sector.

4.5 Geographical distribution of publications

This division indicates the amount or percentage of papers written by writers from a certain region. The growing proportion of a country's international journals generates fresh opportunities for papers from that country to be seen by other scholars worldwide. Geographically, the bulk of publications (29.45%) originated in the United States of America. This may be attributed to the United States' plethora of resources and experience in the cyber threat and cyber assault domains. The United Kingdom comes in second with 6.69 percent and South Korea comes in third with 5.83 percent. As seen in **Table 6**, the majority of publications (600 papers) were written in English, while two were written in Ukrainian and the remaining in Polish, Russian, Portuguese, French, and Turkish. This specifically shows that writers from different countries have taken an interest in the research on cyber - attacks and cyber threats. Since 2003, researchers and scholars from more than 70 different nations have added to the body of knowledge on cyberattacks and cyber threats. **Table 7** lists all countries that led to the productivity of publications. The

Language	Frequency*	% (N = 607)
English	600	98.85
Ukraine	2	0.33
French	1	0.16
Polish	1	0.16
Portuguese	1	0.16
Russian	1	0.16
Turkish	1	0.16
Total	607	100%

One paper has been published in dual language.

Table 6.
Language used in the publications.

Publishing country	Frequency*	% (N = 703)
United States	207	29.45
United Kingdom	47	6.69
South Korea	41	5.83
India	35	4.98
Italy	21	2.99
Japan	21	2.99
China	18	2.56
Australia	16	2.28
Germany	16	2.28
France	14	1.99
Poland	14	1.99
Ukraine	14	1.99
Malaysia	13	1.85
South Africa	11	1.56
Canada	10	1.42
Finland	9	1.28
Russian Federation	9	1.28
Turkey	9	1.28
Pakistan	8	1.14
Saudi Arabia	8	1.14
Romania	7	1.00
Spain	7	1.00
Austria	6	0.85
Estonia	6	0.85
Portugal	6	0.85
Singapore	6	0.85
Israel	5	0.71
Netherlands	5	0.71
Denmark	4	0.57
Sweden	4	0.57
United Arab Emirates	4	0.57
Argentina	3	0.43
Greece	3	0.43
Ireland	3	0.43
Jordan	3	0.43
Kazakhstan	3	0.43
Norway	3	0.43
Qatar	3	0.43
Switzerland	3	0.43
Belgium	2	0.28
Bulgaria	2	0.28
Croatia	2	0.28
Hungary	2	0.28
Iraq	2	0.28

Publishing country	Frequency*	% (N = 703)
Montenegro	2	0.28
New Zealand	2	0.28
Serbia	2	0.28
Bahrain	1	0.14
Bangladesh	1	0.14
Bhutan	1	0.14
Botswana	1	0.14
Brazil	1	0.14
Colombia	1	0.14
Cyprus	1	0.14
Czech Republic	1	0.14
Ecuador	1	0.14
Hong Kong	1	0.14
Indonesia	1	0.14
Iran	1	0.14
Kuwait	1	0.14
Latvia	1	0.14
Lithuania	1	0.14
Macedonia	1	0.14
Malta	1	0.14
Mexico	1	0.14
Morocco	1	0.14
Nigeria	1	0.14
Slovenia	1	0.14
Taiwan	1	0.14
Viet Nam	1	0.14
Undefined	39	5.55
Total	703*	100%

**Some papers were published by more than one author.*

Table 7.
Countries contributed to the publication.

United States of America (USA) came in first place with 207 (29.45 percent) documents, led by the United Kingdom (UK) with 47 (6.69%) documents and South Korea with 41 documents (5.83%).

The bibliometric analysis suggests that publications from more than 70 countries around the globe have contributed to the area. Researchers, including scholars from developed and developing countries, demonstrated an appetite and zeal for generating literature in the area of cyber attack and cyber threat.

5. Conclusions

The analysis provided in this chapter is aimed at increasing public awareness and interest in cyber threats and cyber attacks studies, especially among higher education institutions. Its aim is to investigate what is available and to explain its evolution over time, with the goal of igniting additional debates on the subject. As a result of the findings above, it is evident that there is a dearth of literature on cyber vulnerabilities and cyber attacks affecting higher education. Thus, much effort should be exerted in terms of this study, such as undertaking studies within the framework of higher education itself, as the effect of cybersecurity is felt worldwide, not only in one area, but in a variety of industries, including higher education. While the authorship and global distribution of the literature on cyber attacks and cyber threats indicate that the United States has the most publications and impact in

terms of authorship, research focused on developing countries remain scarce. The majority of writers in this field come from developed countries such as the United Kingdom and South Korea. This means that additional research from researchers and scholars in developing countries is needed.

A further consequence is the usability problem, in which it is difficult to access information or literature pertaining to research on cyberattacks and cyber threats, given that the majority of published works are password-protected (non-open access). The majority of highly published articles were conference papers, such as proceedings, which lack the depth of data and facts included in complete papers. Additional investigation through prolonged study projects is necessary to fully comprehend the reasoning behind this problem and to comfortably apply it to related studies.

This paper was inspired by two observations: first, cyber attacks and cyber threats challenges have remained a contentious subject in the literature in recent years but are still uncommon in higher education; and second, handling this challenge in the higher education sector is difficult. Despite this, there is no consensus in the literature regarding progress in this field, particularly in higher education. This chapter began by indicating that there was a lack of clarification about the current extent of improvement achieved in the area of cyber threats and cyber attacks on higher education.

The aim of this paper is to examine the patterns and advances in this field using bibliometric analysis of written documents accessed from an online database. This article conducts a bibliometric analysis in order to achieve a better understanding of the cyber attack and cyber threats literature's dynamics, historical review, predictions, and contributions. The findings indicate that the literature on this subject began in 2003 and has continued to grow, with the peak of publications occurring in 2018 with a total of 144 publications, up from 99 in 2017. It is estimated that the overall number of publications will rise in 2021, since there are publications that have not yet been indexed by Scopus and therefore are not included in the datasets for this analysis as of 25 July 2019. However, there is also a lack of understanding about the patterns and advancements in the field of higher education.

This analysis has some drawbacks due to the database used. Thus, prospective scholars should be aware of these limits. To begin, even though Scopus is one of the largest directories, it does not archive all journals and names, and so publications in these journals might have been overlooked. Second, this review narrows the attention on malware attacks and cyber challenges based on the titles, abstracts, and keywords of the documents. Thus, all other elements of the literature that are relevant to the subject but are not specifically classified under these requirements were omitted, including the journal title, abstract, and keywords. Thirdly, since the database is continuously modified, the cumulative number of publications and other details collected are only accurate at the time of the scan. The data collection phase began on 25 July 2019, and as a result, the data used in subsequent evaluations were focused on this date.

Amid these drawbacks, this research is one of the first to analyze a variety of bibliometric indices of literature in the field of cyber threats and cyber attacks. This research aims to lay the foundation for future discussions on the subject of handling cyber threats and cyber attacks in higher education. The results should be able to inform future researchers on how to expand the subject. Future scholars are encouraged to pursue textual study, which would undoubtedly uncover additional and important results. It is because this research used basic search terms, including article titles, abstracts, and keywords, which are all accessible electronically via the Scopus website, rather than searching through entire articles or complete records. The data is gathered using a single database - Scopus. Although Scopus is the largest

abstract and citation archive for peer-reviewed literature, including scientific journals, books, and conference proceedings, prospective research could include additional databases to obtain full and detailed findings on the published works of writers worldwide on the subject of cyber attacks and cyber threats. Comparative studies are often recommended in order to ascertain the parallels and discrepancies between findings obtained from various databases. Additionally, future studies may wish to use a range of research techniques, such as interviews, group discussions, surveys, or other approaches, in order to gather evidence and obtain rich information.

Acknowledgements

The author wishes to thank the Ministry of Education Malaysia for funding this study. The grant is coded as 13598.

Author details

Nazahah Rahim
Othman Yeop Abdullah Graduate School of Business (OYAGSB), Universiti Utara Malaysia, Malaysia

*Address all correspondence to: nazahah@uum.edu.my

References

[1] Povera, A. 2018. Internet users in Malaysia up from 2.5mil in 2006 to 24.5mil in 2017. Available at https://www.nst.com.my/news/nation/2018/02/331284/internet-users-malaysia-25mil-2006-245mil-2017

[2] Aruna, P. 2017. Combating cyber crimes. Available at https://www.thestar.com.my/business/business-news/2017/11/18/combating-cyber-crimes/

[3] Paramasivam, S. 2018. Cybersecurity threats to cost organizations in Malaysia US$12.2 billion in economic losses. Available at https://news.microsoft.com/en-my/2018/07/12/cybersecurity-threats-to-cost-organizations-in-malaysia-us12-2-billion-in-economic-losses/

[4] Ramim, M., and Y. Levy. 2006. Securing e-learning systems: a case of insider cyber attacks and novice IT management in a small university. Journal of Cases on Information Technology (JCIT). 8(4): 24–34.

[5] Davidson, P., and K. Hasledalen. 2014. Cyber threats to online education: a Delphi study. In ICMLG2014 Proceedings of the 2nd International Conference on Management, Leadership and Governance: ICMLG 2014 (p. 68). Academic Conferences Limited.

[6] Chabrow, E. 2015. China blamed for Penn State breach: Hackers remained undetected for more than two years. Available at http://www.databreachtoday.com/china-blamed-for-penn-state-breach-a-8230

[7] Abomhara, M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65–88.

[8] Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32(3), 183–196.

[9] Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system. Online Information Review, 41(2), 171–184. https://doi.org/10.1108/oir-12-2015-0394

[10] Awan, J. H., Memon, S., Memon, S., Pathan, K. T., & Arijo, N. H. (2018). Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities. Mehran University Research Journal of Engineering and Technology, 37(2), 359–366. https://doi.org/10.22581/muet1982.1802.12

[11] Loukas, G., Gan, D., & Vuong, T. (2013). A review of cyber threats and defence approaches in emergency management. Future Internet, 5(2), 205–236. https://doi.org/10.3390/fi5020205

[12] Pattanayak, S., Mohapatra, S., Mohanty, S., & Choudhury, T. (2019). Empowering of ICT-Based Education System Using Cloud Computing. Innovations in Computer Science and Engineering, 32, 113–120.

[13] Baygin, M., Yetis, H., Karakose, M., & Akin, E. (2016). An effect analysis of industry 4.0 to higher education. In 15th International Conference on Information Technology Based Higher Education and Training (ITHET) (pp. 1–4). IEEE. https://doi.org/10.1109/ITHET.2016.7760744

[14] Khwaldeh, S. M., Al-Hadid, I., Masa'deh, R., & Alrowwad, A. (2017). The Association between E-Services Web Portals Information Quality and ICT Competence in the Jordanian Universities. Asian Social Science, 13(3), 156. https://doi.org/10.5539/ass.v13n3p156

[15] Aulawi, H., Ramdhani, M. A., & Slamet, C. (2017). Functional Need Analysis of Knowledge Portal Design in Higher Education Institution. International Journal of Soft Computing, 12(2), 132–141.

[16] Arlitsch, K., & Edelman, A. (2014). Staying Safe: Cyber Security for People and Organizations. Journal of Library Administration, 54(1), 46–56. https://doi.org/10.1080/01930826.2014.893116

[17] Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. Computers and Security, 84, 53–69. https://doi.org/10.1016/j.cose.2019.03.010

[18] Chapman, J. (2019). HEPI Policy Note 12 - How safe is your data? Cyber-security in higher education. London, UK.

[19] Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers and Security, 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

[20] Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management, 29(6), 449–457. https://doi.org/10.1016/j.ijinfomgt.2010.06.001

[21] Sari, A. (2019). Turkish national cyber-firewall to mitigate countrywide cyber-attacks. Computers and Electrical Engineering, 73, 128–144. https://doi.org/10.1016/j.compeleceng.2018.11.008

[22] Russell, G. (2017). Resisting the persistent threat of cyber-attacks. Computer Fraud & Security, 2017(12), 7–11. https://doi.org/10.1016/S1361-3723(17)30107-0

[23] Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management, 15(1), 1–30.

[24] Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. Journal of Information Assurance & Cybersecurity, 2017, 1–13. https://doi.org/10.5171/2017.800299