Received Date: 17 August 2021 I Accepted Date: 10 January 2022

OPUS Journal of Society Research

RESEARCH ARTICLE

Cyber-Physical Systems and Cyber Security: A Bibliometric Analysis

Bülent Yıldız[1] **I Elham Hasan Younes Gejam**[2]

[1] Assit. Prof. Dr., Kastamonu University, Kastamonu/Turkey
ORCID: 0000-0002-5368-2805
E-Mail: dr.yildiz.bulent@gmail.com

[2] PhD. Std., Kastamonu University, Kastamonu/Turkey
ORCID: 0000-0002-0024-2910
E-Mail: elham.libya37@gmail.com

Corresponding Author: Bülent Yıldız

January 2022
Volume:19
Issue:45
DOI: 10.26466//opusjsr.1063227

Citation: Yıldız, B. ve Younes Gejam, E. H. (2022). Cyber-physical systems and cyber security: A bibliometric analysis . *OPUS– Journal of Society Research, 19*(45), 35-49.

Abstract

With the emergence of Industry 4.0, the use of advanced technologies has become widespread in both the manufacturing and service sectors. Among the most important of the advanced technologies used are cyber physical systems (CPS). Along with the use of technology, security has also become highly important. For this reason, along with CPSs, the issue of cyber security has also developed. For this purpose, in this study, bibliometric analysis of 827 studies published between 1999-2021 in the field of CPS and cyber security in journals scanned in Web of Science was performed. With the thematic evolution analysis, the change in the field has been revealed based on time. While the basic elements of cyber security issues were discussed in the period of 1999-2015, which was determined as the first period, issues such as smart grids and education were observed in the period of 2016-2019, which was determined as the second period. In the last period of 2020-2021, topics such as cloud computing, game theory and maritime cyber security have emerged. However, there are also CPSs and cyber security concepts that exist in all three periods. From this point of view, it can be concluded that the field of CPS and cyber security is not yet fully mature and more detailed studies are needed on basic issues, while interdisciplinary studies are expected to gain weight in the coming days, as it is a subject that has an impact on many different dimensions.

Key Words: *Cyber-Physical Systems, Cybersecurity, Bibliometric Analysis.*

Öz

Endüstri 4.0'ın ortaya çıkması ile beraber gerek imalat gerekse hizmet sektöründe ileri teknolojilerin kullanımı yaygınlaşmıştır. Kullanılan ileri teknolojilerden en önemlileri arasında da siber fiziksel sistemler (CPS) yer almaktadır. Teknoloji kullanımı ile beraber güvenlik unsura da yüksek derecede önemli hale gelmiştir. Bu nedenle CPS'ler ile beraber siber güvenlik konusu da gelişim göstermiştir. Bu amaçla bu çalışmada Web of Science da taranan dergilerde CPS'ler ve siber güvenlik alanında 1999-2021 yılları arasında yayımlanan 827 çalışmanın bibliometrik analizi yapılmıştır. Tematik evrim analiziyle birlikte alanda yaşanan değişim zamana dayalı olarak ortaya konulmuştur. İlk dönem olarak belirlenen 1999-2015 aralığında siber güvenlik konularının temel unsurları ele alınırken ikinci dönem olarak belirlenen 2016-2019 dönemine gelindiğinde akıllı şebekeler ve eğitim gibi konular gözlenmiştir. Son dönem olarak belirlenen 2020-2021 aralığında ise bulut bilişim, oyun teorisi ve denizcilik siber güvenliği gibi konular ortaya çıkmıştır. Bununla birlikte her üç dönemde de varlığını sürdüren CPS'ler ve siber güvenlik kavramları da mevcuttur. Buradan hareketle CPS ve siber güvenlik alanının henüz tam olarak olgunluğa erişmediği ve temel konular üzerinde daha detaylı çalışmalara ihtiyaç duyulduğu sonucuna varılabilirken aynı zamanda çok farklı boyutlar üzerinde etkisi olan bir konu olması hasebiyle disiplinler arası çalışmaların önümüzdeki günlerde ağırlık kazanması beklenen bir durumdur.

Anahtar Kelimeler: *Siber Fiziksel Sistemler, Siber Güvenlik, Bibliometrik Analiz*

Introduction

The effects of globalization have caused changes in the ways in which we obtain and process information and have helped to bring about new concepts like digitalization and innovation. The public has lost its interest in traditional industry practices, and Industry 4.0 has started to take effect. As a result of Industry 4.0, systems that include both digital and physical components have come into existence. A result of this is that cyber physical systems (CPS) are increasing in usage and applications can be found in a variety of different sectors including the airline industry, the infrastructure industry, and the manufacturing process (Brandman et al., 2020: 202). Complex systems include control, communication, and computing technologies, and CPSs are no exception. The term CPS is used to describe stem cells that have the ability to differentiate into multiple cell types, also known as "pluripotent stem cells" (Zhang et al., 2021; Tantawy et al., 2020). Security threats will inevitably increase for CPSs as they become more widely deployed. Attack of this kind can significantly degrade system performance and/or CPSs. Such attacks can cause considerable harm. Resistance to cyber attacks is therefore an important consideration when making CPSs (Kholidy, 2021, p.1). Although attacks against the manufacturing sector have been common in recent years, these attacks have mostly been the result of targeted phishing emails. An increase in the number of internet-connected devices creates new opportunities for cyberattacks via connected devices. Attacks are conducted with the aim of damaging critical infrastructure, affecting production, and stealing sensitive data about customers (Pandey et al., 2020, p.05).

Failure to detect cyber-physical attacks in production can result in significant damage. Poorly executed attacks may have a detrimental effect on the design, functionality, and quality of a product. In practice, this means errors in production systems are likely to occur. Due to this, it is possible that consumers are using faulty products, which could put human safety at risk. Use of the product can lead to premature deterioration of the product. distortions at the beginning of the design process have the potential to be extremely costly, especially to critical product components such as brakes, jet engines, or turbine blades (Elhabashy et al., 2019, p.922). Malicious attacks can have dangerous, widespread, and potentially catastrophic consequences on human life, productivity, and national security. Due to these concerns, CPS security experts are increasingly concerned about the possibility of a cyberattack (Walker-Roberts et al., 2020, p.2645).

As tech advances, the evolution of the supply chain reflects and expands on those concepts from Industry 4.0 such as the Internet of Things (IoT), additive manufacturing, virtual reality, artificial intelligence, and blockchain, which help to link supply chain partners. Cybersecurity countermeasures, however, are lagging behind digitizing supply chains. It has been suggested that supply chains unwittingly expand their exposure by dealing with multiple different parties without regard for risk (Ghadge et al., 2020, p.224).

Even with continuous security and protection efforts, these critical infrastructure components remain vulnerable to cyber attacks. These recently intensified complex attacks reveal the significance of conducting an ongoing risk assessment and management process (Tantawy et al., 2020, p.1).

The use of advanced technology in the production processes of the enterprises and in the operational processes such as supply chain, logistics and financial systems has become very common today. Along with the use of advanced technology, it is also important to ensure the security of the data produced by these technologies. Emphasis has been made in the literature on the advantages of investing in technology for businesses. However, besides the advantages of technology, the security problems that may be experienced may turn these advantages into disadvantages. For this reason, it is necessary to take into account the issue of cyber security along with technology. For this purpose, in this study, CPS, one of the advanced technology applications, and cyber security were discussed and evaluated together.

Theoretical Framework

Cyber Physical Systems

CPSs are traditionally defined as computational integration with physical processes, where networks embedded in computing devices and integrated with feedback loops can monitor physical processes, intervene, control and support them when necessary. The most important paradigm of these defined processes is Industry 4.0 applications that take into account technologies such as big data analytics, decentralization, human-robot interactions, sensor and actuarial networks (Sreeram and Shimon, 2021, p.2-3). CPSs are complex and heterogeneous systems that include mechanical components, human activities and the surrounding environment, and have cyber components and physical processes such as sensors, computers, control centers and actuators that are seamlessly integrated (Pan et al., 2019). CPSs are physical systems and have features such as design, construction, and monitoring that are built into a central computing and communications core. To put it another way, CPSs allow us to interact with the physical world around us in ways we were not able to before the internet was created (Rajkumar et al., 2010, p.1).

CPSs are an important enabling factor for Industry 4.0, connecting various pieces of equipment, factories, products, suppliers, and customers. CPS technology has made physical devices with computers and networks that are used to expand functions more common in recent years (Zhang et al., 2021, p.1). As far as control systems go, CPS is complex networked systems with physical elements (like buildings and roads) mixed with computing elements (like computer networks). The fact that CPSs are everywhere affects nearly every aspect of our lives (Wu et al., 2016, p.2). Industrial sectors such as aerospace, defense, industrial automation, healthcare/medical equipment, and infrastructure have seen significant gains in competitiveness thanks to their innovations (Zhang et al., 2021, p.1). In order to manipulate a physical process, CPS utilizes various networking devices, hardware, and software components (Carter et al., 2019, p.1). It forms the basis for the development of a variety of areas, such as smart manufacturing, medicine, and infrastructures, as well as smart cities, vehicles, and wearable devices (Alguliyev et al., 2018, p.212). Also, CPSs include various factors such as industrial control systems, the Internet of Things, smart home devices, and smart objects, among others (Zegzhda, 2016). Many CPSs have both cyber and physical components and operations. By integrating physical systems with intelligent objects and services, this enhancement enables those physical systems to become even more effective (Akhuseyinoglu and Joshi, 2020:1).

Additionally, CPS is a concept that is related to cloud manufacturing. Cloud technology is a critical part of a company's service offering because it allows for a dynamic response to environmental changes. A critical feature of the conceptual architecture is the CPS, which can process large amounts of data and execute real-time functions. The CPS is rapidly making significant evolutionary leaps, and it is moving toward an infrastructure that is more dependent on the world around us, with quicker data processing and quicker control implementation. These technologies are going to increase the security and reliability of future designs. The cloud makes it easier for manufacturers to expand the cyber protection part of CPS and install it on the device (Mourtzis and Vlachou, 2016, p.713).

Ports can also be defined as locations where data flows from supply chain technology to the terminals and where human-computer interfaces are in place. The change from flow-based Industry 1.0 to intelligent network-based Industry 4.0 has also caused a CPS to be formed at port locations (Gunes et al., 2021, p.1).

Cyber Security

With more attention on cybersecurity over the past few years, it has become easier to understand how to apply the concept of security to all internet-related issues. Although network security stresses the protection of internal systems, protecting the overall network environment is just as important in cybersecurity. Such measures include real-time monitoring of suspicious entities or objects outside the network, identifying attack sources, and monitoring malicious applications (Chen et al., 2021, p.3).

Cyber-attacks have weaponized rapidly advancing technology by introducing undesired vulnerabilities because of complex integrated hardware, software, and firmware. Therefore, it becomes increasingly difficult for an organization to cope with the evolving threat environment (DiMase et al., 2015, p.292). Information systems consist of three parts as hardware, software and computer networks. Ensuring the security of these three components is a priority in the work against cyber attacks. A vulnerability that occurs in one of these three parts will affect all parts, as well as cause serious damage to companies that are attacked. For this reason, the needs of all parts should be evaluated separately when planning and working on cyber security (Ismail and Zainab, 2011).

We are currently living in the age of digitalization, where computer systems, networking hardware, and sensors are all in use together via networks. The desire to preserve safety is of utmost importance in this instance. A thorough attention to the requirements engineering process is essential for sound system development. In order to have a secure system, vulnerabilities must be taken into consideration (ur Rehman and Gruhn, 2018, p.1). Information leaks, denial-of-service (DoS) attacks, and sometimes other cyber actions related to national security or military matters are just some of the many ways that cyber attacks can be delivered. It is possible for cyber-physical attacks to lead to serious health and safety issues due to the damaging or deterioration of physical assets (Parn and Edwards, 2019, p.249). There are new technologies that are making an impact on cyber security, including autonomous technologies, the Internet of Things (IoT), artificial intelligence (AI), and blockchain (Raban and Hauptman, 2018).

Cyber attacks refer to organized attacks on the communication or information systems of government agencies, private companies or individual users for the purpose of attacking and decommissioning critical sectors, baiting, damaging with malicious software, social engineering, data theft and modification, stealing, deleting or publishing confidential information within Information Systems (Çakmak and Demir, 2009, p.29-30). Cyber attacks are also attacks made with computer codes that are used and developed to prevent information technology systems from working by affecting them physically or systemically (Rid and McBurney, 2012, p.7).

An access attack is a type of attack in which access is granted to the host computer's machine even though the attacker does not have permission to use it for the purpose of manipulating information. Reconnaissance attacks are defined as attacks that match the targeted systems in order to scan for any vulnerabilities in the machine in order to gather information about the machine. Phishing attacks are the act of sending erroneous messages to users through a variety of means such as e-mail, text messages, and other similar methods that appear to come from a legitimate source in order to deceive users and obtain sensitive and confidential information such as login passwords, credit card numbers, and other similar information (Kaur and Ramkumar, 2021, p.2-3). After gaining access to a botnet, a common attack method is to launch a denial of service (DoS) attack. These attacks are aimed at compromising the usability of critical systems and causing service interruptions. In the past, DoS attempts were network-based, and they were used to overload active nodes with rogue traffic, causing them to stop serving or begin behaving abnormally until they were overwhelmed themselves. The service levels of the receivers are lowered as a result of such attacks, which overwhelm the targets with fraudulent requests that can cause excessive delays. An important aspect of such service interruptions is the ability to differentiate between active and aggressive attacks and legitimate requests, as well as the ability to respond equally to all incoming messages (Arnaboldi et al., 2020, p.42). In computer programming terms, a Trojan is a type of program in which destructive functionality has been added in order to associate it with an already existing program. Defining account hijacking as the process by which hackers gain access to a specific individual's computer or email account, as well as other accounts associated with the service or computing device, and use them for their own purposes. In general, a virus can be defined as a piece of code that attaches itself to another program and runs alongside them when the program is activated by the user (Al-Mhiqani et al., 2018, p.2).

Cyber Security in Cyber Physical Systems

According to widely held belief, the CPS is considered to be an extremely well-isolated system that is invulnerable to outside attacks. Physical isolation has, however, been greatly reduced as a result of the Internet of Things and increased internet connectivity. A smarter control system that can protect itself from malicious attacks and establish multidisciplinary collaborations between information technology and process control is therefore required to supplement the CPS (Palleti et al., 2018, p.161).

The modern environment of digital manufacturing places a great emphasis on cyberphysical security. In this situation, a cyberattack can lead to faulty parts, IP theft, or infrastructure damage (Brandman et al., 2020, p.202). To date, the increase in IoT applications, such as smart cars and industrial control systems, has contributed to the prominence of CPSs such as these, and as a result, these systems have become a target for hackers (Geismann and Bodden, 2020, p.1). Although production systems are popular targets for cyberphysical attackers, there are many industries that make extensive use of them. Consider for example, the machined parts that are almost everywhere in the production business, all of which are vulnerable to attack (Brandman et al., 2020, p.203). It is possible that competitors may attack the cyber component of the CPS in an attempt to interfere with the physical processes. Because of this, it is essential to protect these systems from attempts to corrupt or subvert them, and to ensure that the integrity, functionality, and security of the systems are protected (Carter et al., 2019, p.1). CPS security security is only partially addressed by current IT security approaches. To give another example, channel encryption may in some cases limit the ability of unauthorized users to access it, but can be completely useless to malicious personnel and susceptible to decoding by a powerful attacker. Other issues with traditional IT security approaches include not accounting for physical devices' connections to cyber threats. When attempting to breach a cyber security system, an attacker is not only attacking the network, but also attacking the physical elements of the CPS (Wu et al., 2016, p.3). For a satisfactory level of protection, information security measures such as authentication, access control, and message integrity appear insufficient. To make matters worse, the security systems in place are neither reliant on underlying physical processes or control mechanisms, nor capable of protecting against insider attacks (Pasqualetti et al., 2013, p.1). In other words, the CPS device is vulnerable to various threats. Since heuristic attacks can hijack connected devices and turn them into email servers for mass spam, use them as botnets to execute DDoS (Distributed Denial of Service) attacks, or simply cause business process disruption (Walker-Roberts et al., 2020, p.2646), heuristic attacks can frequently hijack connected devices and turn them into email servers for mass spam, use them as botnets to execute DDoS (Distributed Denial of Service) attacks, or simply disrupt business processes (Walker-Roberts et al., 2020, p.2646).

An increase in the rate of cyberattacks targeting the CPS has occurred in recent years, with disastrous results. Code reuse attacks, malicious code injection attacks, and fake data injection attacks are extremely common in CPS, which are just a few of the myriad of potential attacks an attacker could be using. attacks on CPS industrial equipment can lead to a total blackout (Yaacoub et al., 2020, p.8).

Because system requirements are being translated into design, or during deployment and maintenance of cyber components, or when connecting any external USB device to workstations, it is possible for previously unknown vulnerabilities to be unintentionally incorporated into an attack vector. The tools attackers can use to launch attacks include sensors and communication networks, which means they can attack and compromise valuable targets (Tripathi et al., 2021, p.1).

Methodology

Articles on the subject have been compiled in the web of Science (WOS) database to perform bibliometric analysis of CPS and Cyber Security studies. Accordingly, articles in English language were searched by typing "TI= ("cyber*" AND "secur*")" and "TS= ("cyber physical system*") in the search section of the WoS database. While the titles of the articles were evaluated with TI, studies on cyber-physical systems were identified in the studies with TS. With the use of an asterisk (*) at the end of the search terms, the plural forms or different conjugations of the related search terms are also included in the search. The reason for searching in the title section is that although the concepts in question are included in the abstracts of the studies, they are sometimes not directly related to the subject. After this preliminary screening, the data set was manually controlled by the researcher and studies that were not directly related to the subject were excluded from the data set.

As the reason for choosing WoS as the database, it can be suggested that it is accepted as the most effective platform where scientific knowledge is shared today. Articles are currently the most effective tools in structuring and disseminating scientific knowledge. That's the reason why articles are covered in the search criteria. The reason for choosing English as the research language is that most of the published works are produced in this language and there are many opportunities for analysis in this language. The findings obtained as a result of the search are given in Table 1.

Table 1. General Information

Timespan	1999:2021
Documents	827
Average years from publication	3,98
Average citations per documents	14,7
Average citations per year per doc	2,571
Author's Keywords (DE)	2529
AUTHORS	
Authors	2202
Authors of single-authored documents	112
Authors of multi-authored documents	2090
Collaboration Index	2,94

According to Table 1, as of March 17th 2021, a total of 827 works on cyber security were produced between 1999-2021. The number of keywords in the relevant data set is 2529. Keywords are the summary of an article and express the concepts examined in the research. In this respect, the contents of the articles can be understood by examining the keywords. Another striking aspect of the data set is the low number of single-authored articles, and the high collaboration index.

In the following part, there are some findings showing the quantitative characteristics of the data set, and then there are content analyzes that show the subjectivity of the research. The Biblioshiny package of the R program was used for these analyses.

Number of Articles by Years

The number of articles published in a field is an important indicator of the development of the field. The change in the amount of studies compiled on CPS and cyber security over time is given in Figure 1.

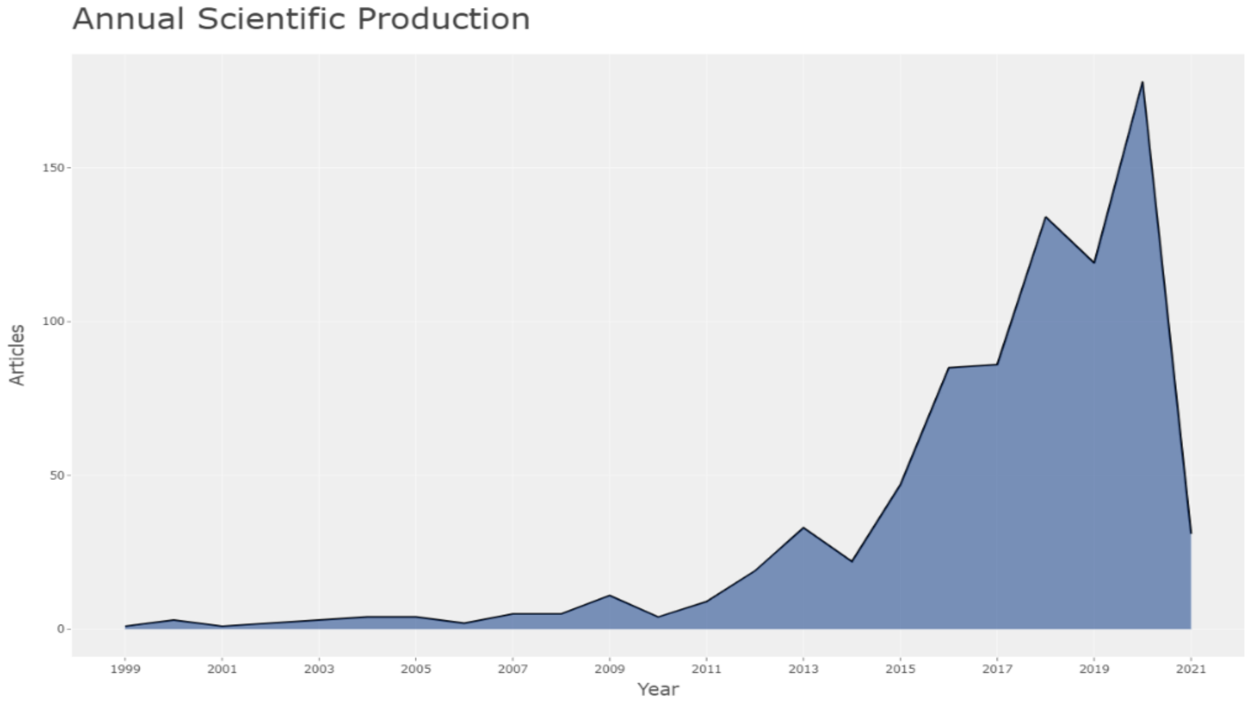

Figure 1. Distribution of Studies by Time

According to Figure 1, studies in the field of CPS and cyber security gained their first serious acceleration in 2009. In 2015 and after, it entered a serious upward trend. The number of studies on the subject between 1999 and 2009 is very few. It can be thought that the significant increase in the studies after 2015 is due to the fact that these years were the years when the use of technology started to become widespread with Industry 4.0. With the use of technology, ensuring the security of the technology used has also become important. Therefore, the increase in studies in which CPSs are evaluated together with cyber security has started to be seen after 2015.

Citation Numbers by Years

Figure 2 shows the levels of progress of citations to published works. The line around which the citation is shaped represents the normalization line. The reason why the number of citations made in some periods is below this line is that the citations made in these periods are at lower levels compared to the periods before and after them.

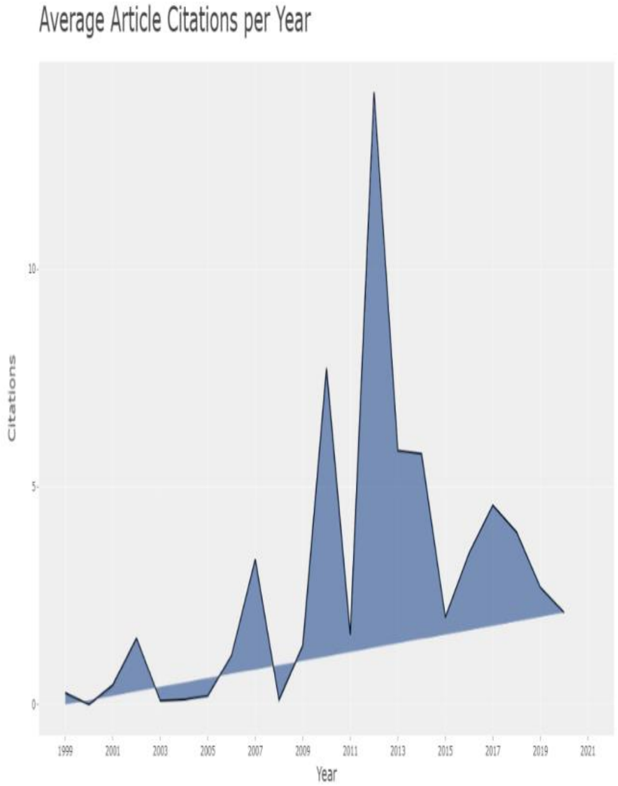

Figure 2. Citation Numbers by Years

Although the number of citations depends on the number of publications, they do not show complete linearity. Although the first period works reach a serious citation score with the increase in the number of publications, as the number of publications continues to increase, the citation line will become concave as new citations are distributed among the works.

Cross-Country Collaboration

The findings on cross-country collaboration are given in Figure 3. When the origins of the publications are examined, it is seen that China and the USA have the highest number of publications. In addition, in terms of the countries where the authors are located, it was observed that the most bilateral collaboration took place between China-Canada and China-USA.

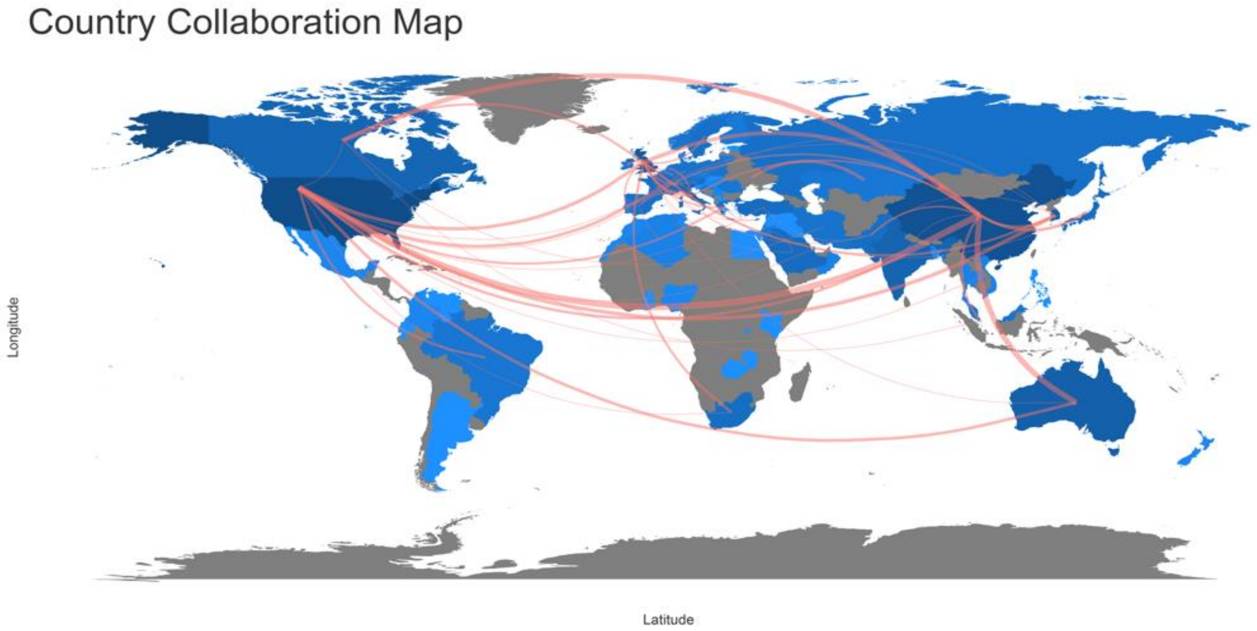

Figure 3. Cross-Country Collaboration

Although there exist studies on the subject in Turkey, it has been observed that there is a serious deficiency in international cooperation.

Universities by Number of Publications

The list of the top 20 universities in terms of their contributions to the field is given in Figure 4. According to this figure, the most active university in the field is Northeastern University in Massachusetts.

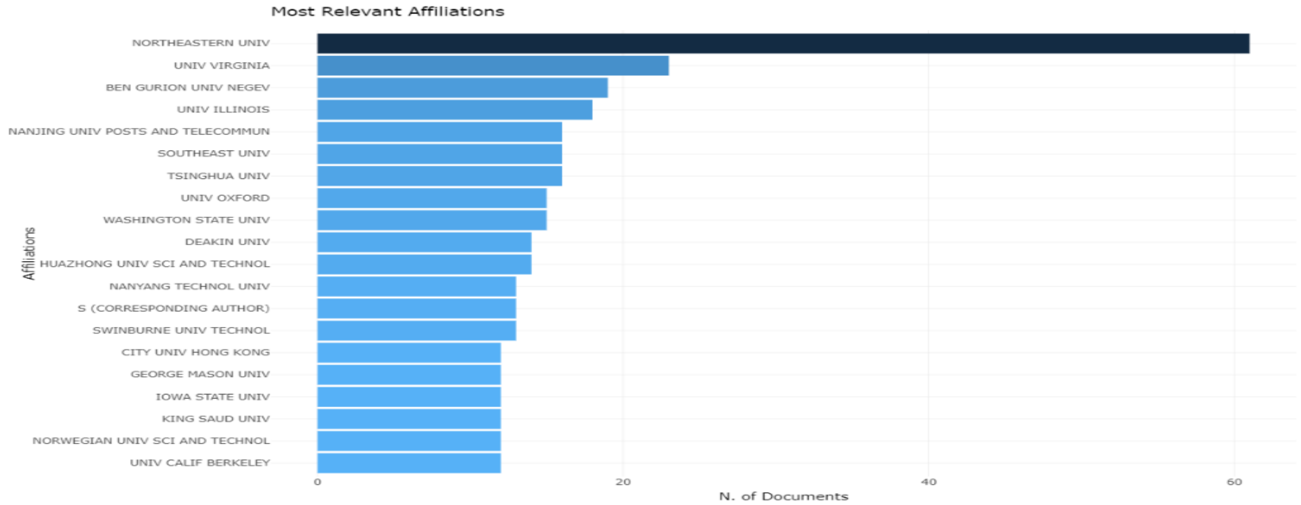

Figure 4. Universities by Number of Publications

The list includes universities of Chinese and US origin, as well as those from some European and Arab countries. However, it is noteworthy that there is no Turkish university among the top 20.

One of the most important issues to be examined about the development of a field is the activities of scientific journals related to the field. The ranking of the journals that include studies conducted in the context of CPSs and cyber security by their number of publications is given in Figure 5.

Journals by Number of Publications

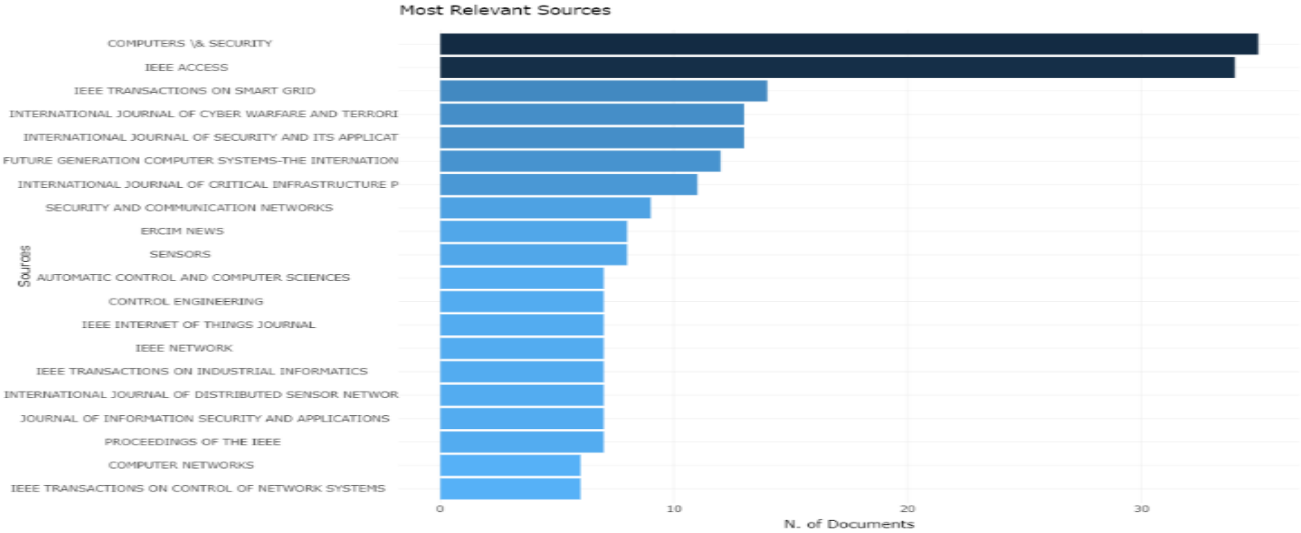

Figure 5. Journals by Number of Publications

According to Figure 5, Computers & Security is the journal with the highest number of publications in the field of CPS and cyber security, followed by IEEE Access. This is followed by IEEE Transactions on Smart Grid and International Journal of Cyber Warfare and Terrorism.

Journals by h-indexes

Apart from the number of publications, another issue that needs to be examined about the journals is how visible the published works are. As an indicator of this, it would be appropriate to examine the citations of the publications in the context of the journal. For this purpose, the h-indexes of the related data set on the basis of journals are given in Figure 6.

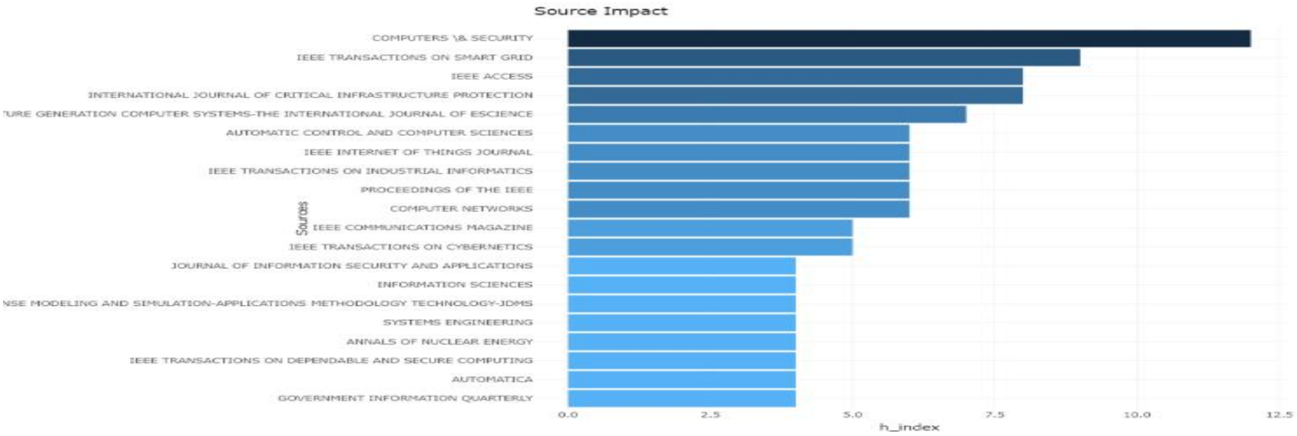

Figure 6. Journals by h-indexes

According to Figure 6, Computers & Security magazine ranks first in terms of h-index as well as in the number of publications. As of today, it can be said that it is the most influential journal in the related field. Except from the publication numbers, IEEE Transactions On Smart Grid magazine ranks second. In other words, it has more visibility with relatively less number of works.

Authors' Production Over The Time

Figure 7 lists authors who work in the field of CPS and cybersecurity by the number of works and intervals in which they produce. When the list is examined, it is seen that most of them consist of authors of Chinese origin. In terms of being a new field, the beginning years of the authors with the most studies do not go beyond 2011.

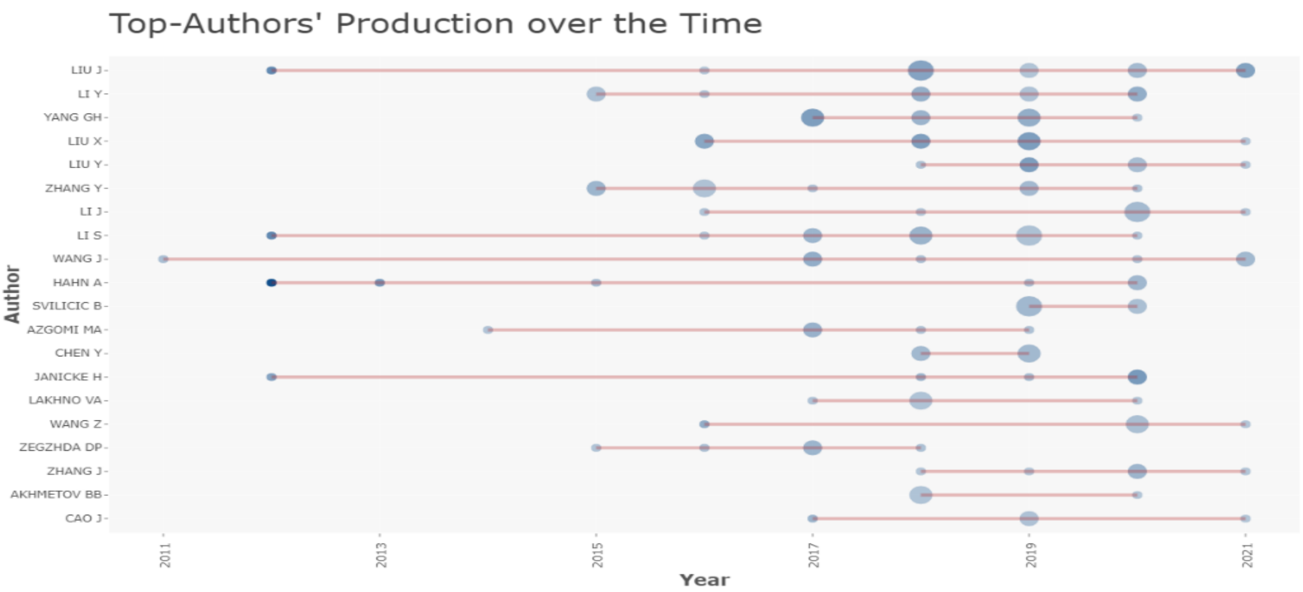

Figure 7. Authors' Production over the Time

Among the top twenty authors, Wang J. has the longest publication range. It is seen that the publication intervals became widespread in the related author set between the years 2017-2020.

Content Analysis

This section contains content analyzes applied to the keywords of works published in the field of CPS and cyber security between 1999-2021.

Factor Analysis

Factor analysis refers to the clustering of keywords in the dataset along the plane through multidimensional scaling. Since there has not been a similar study before, there is no prediction regarding the factors to be created. For this reason, the option of automatic creation of factors has been implemented. Factor analysis findings are given in Figure 8.

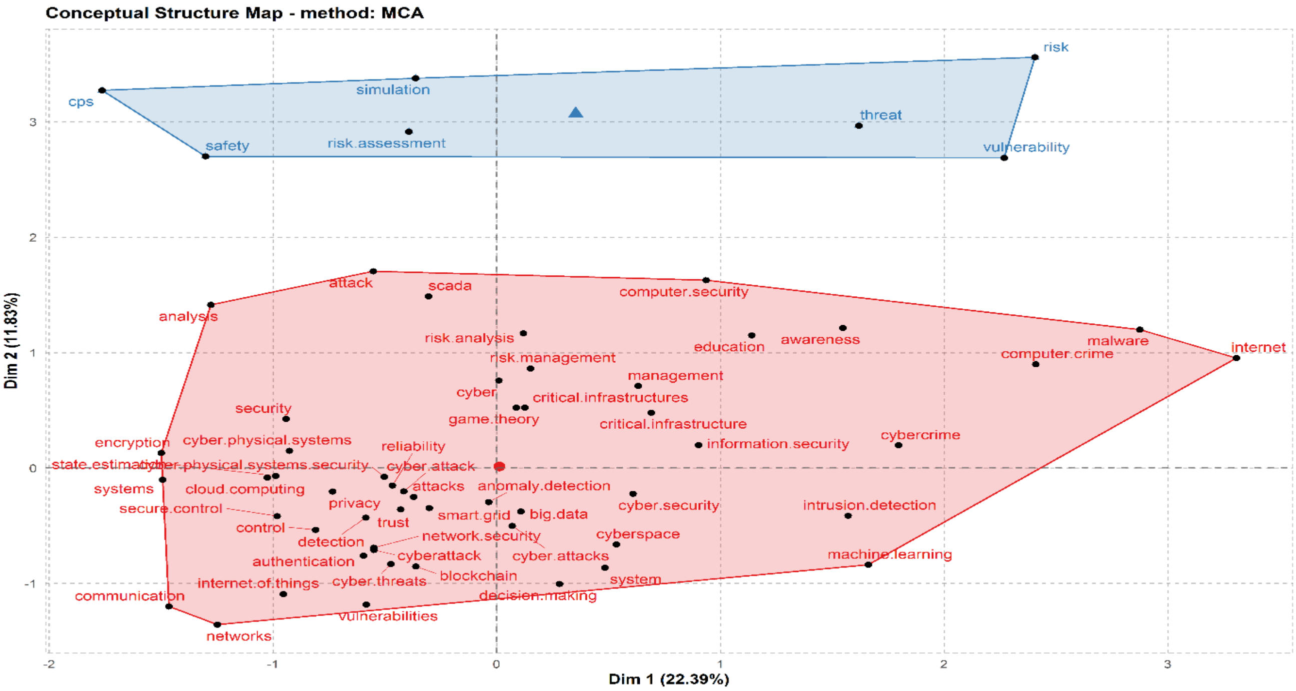

Figure 8. Results of the Factor Analysis

In the factor analysis, as the points representing the centers of the dimensions are approached, the centrality values of the related expressions in terms of area increase. “Cyber attack”, “anomaly detection”, “reliability” and “game theory” are the concepts closest to the center in the first dimension represented in red. In the second factor dimension given in blue, the most important concept was “risk assessment”.

Thematic Evolution Analysis

Thematic evolution analysis is an analysis method used to examine the interactions of the concepts in the analyzed data set at specified time intervals. In this way, it is possible to visualize the degree to which concepts have an impact on which concepts in ongoing periods. In the thematic evolution analysis in Figure 9, time intervals were adjusted to be as equal as possible according to the density of the number of publications, and the relevant periods were determined as 1999-2015, 2016-2019 and 2020-2021. The vertical sections of the concepts in Figure 9 show how frequently they were used in the relevant period, while the lines leading to the next period show which concepts they interacted with. The thickness of the lines represents the intensity of this interaction. In other words, the thicker a line is, the more intense a relationship exists between the two related concepts. The colors used in the lines are necessary for visual distinguishing.

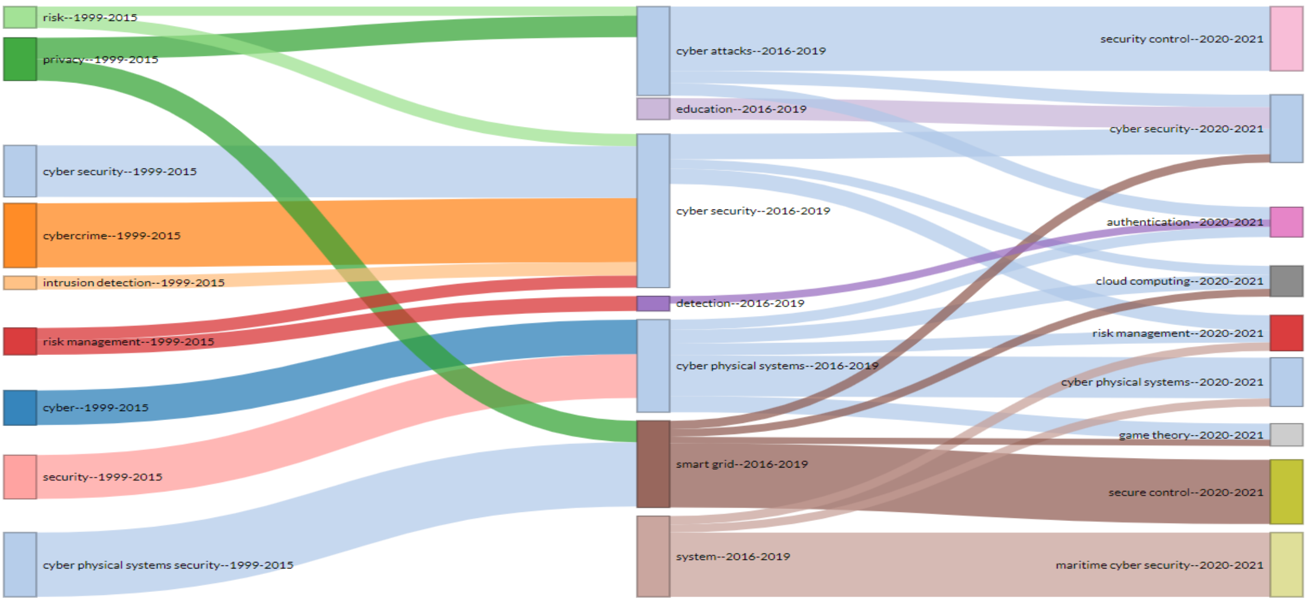
risk--1999-2015
privacy--1999-2015
cyber security--1999-2015
cybercrime--1999-2015
intrusion detection--1999-2015
risk management--1999-2015
cyber--1999-2015
security--1999-2015
cyber physical systems security--1999-2015
cyber attacks--2016-2019
education--2016-2019
cyber security--2016-2019
detection--2016-2019
cyber physical systems--2016-2019
smart grid--2016-2019
system--2016-2019
security control--2020-2021
cyber security--2020-2021
authentication--2020-2021
cloud computing--2020-2021
risk management--2020-2021
cyber physical systems--2020-2021
game theory--2020-2021
secure control--2020-2021
maritime cyber security--2020-2021

Figure 9. Thematic Evolution Analysis

According to Figure 9, where the change in cyber security is visualized, cyber physical systems maintain their importance in all three periods. While it is seen that the concepts examined in the first two periods mostly cover the subjects that will form the basis of the field, it has been observed that different disciplines such as "game theory", "maritime cyber security" and "cloud computing" have started to be examined gradually in the last period of 2020-2021.

Conclusion

With the increasing and facilitating use of electronic resources, CPS and cyber security have become much more important than ever before. The use of the internet environment in all kinds of activities has also brought risks that were not in question before. With the increasing use and possibilities, the issue of security has also become a separate problem. As a requirement of the nature of cyber activities, it is not possible to be aware of the problem before it arises. Therefore, in today's conditions, cyber security activities are always one step behind the problems. It does not seem possible to prevent this with only the activities to be carried out at the application level. Increasing the conceptual knowledge on the subject is a need in the field of CPSs and cyber security, as it is in every scientific knowledge community. It is important to examine the academic studies conducted for this purpose and to reveal the situation of the field, as it can shed light on the expected developments in the future.

This study involves bibliometric analysis of 827 studies which were conducted between 1999 and 2021 in the field of CPS and cyber security. In addition, it is a first, as far as it is known, within the scope of the field studied in terms of providing content analysis in the context of time as well as providing the citation information that the usual bibliometric studies have.

When the findings are examined, it has been observed that there has been a significant increase in the number of publications in the related field, especially in the last few years. Accordingly, the increase in the number of citations gained a serious momentum compared to the previous period. However, depending on the increasing number of publications, the number of citations per publication decreasingly grows. It is seen that the most effective names in cooperation between countries are the USA, China, Canada and Australia. When universities are ranked according to the studies on the subject, it is seen that Northeastern University of the USA takes the first place. The fact that no institution from our country could be included in this ranking indicates that there is a great deficiency in the subject. In the context of journals, Computers & Security, IEEE Access and IEEE Transactions On Smart Grid journals are decisive in the field, both in the number of publications and in terms of their h-index. Just like Universities, in terms of journals, there is no journal of Turkish origin that is among the top twenty. Considering the increasing importance of the subject, it would be beneficial for academic organizations that have serious effects on publication processes to examine and further understand the field in the context of Turkey, with activities such as special issues or call texts related to cyber security and CPSs. As a result of examining the studies in the field according to the authors, it was seen that the majority of the first twenty were of Chinese origin, as expected. It was observed that two basic categories were formed when automatic clustering was allowed in the factor analysis. While the larger category usually includes CPS infrastructure elements, the second and relatively small area includes the organizational reflections of cyber security applications. Finally, with the thematic evolution analysis, the change in the field was revealed based on time. While the basic elements of cyber security issues were discussed in the 1999-2015 period, which was determined as the first period, issues such as smart grids and education were observed in the second period. Recently, topics such as cloud computing, game theory and maritime cyber security have emerged. However, there are also CPSs and cyber security concepts that exist in all three periods. From this point of view, it can be concluded that the field of CPS and cyber security is not yet fully mature, and that more detailed studies are needed on basic issues, while interdisciplinary studies are expected to gain weight in the coming days, as it is a subject that has an impact on many different dimensions.

One of the findings observed in this research is the insufficiency of Turkish academics and institutions related to the field. Among the recommendations of the study is the inclusion of CPS and cyber security among the priority areas. Thus, by increasing the conceptual knowledge of both scientists and practitioners on cyber security, it will be possible to implement effective action plans in the face of possible problems, so they can establish CPSs in the most effective way and eliminate possible cyber security threats with the least damage.

Among the limitations of the study is the fact that the articles examined are in English, and the reason for this is that it is the language that is closest to being a global language today, and accordingly the majority of academic works are written in this language. It can be suggested that the works written in Turkish in the following periods should be subjected to a similar analysis. The reason for the selection of articles as a research element was that they were at the center of scientific knowledge production. In today's conditions, articles are the fastest and most common means of disseminating a new knowledge throughout the scientific community. Finally, although it is considered that scanning the subject in the Web of Science database creates a limitation, it has been preferred in terms of having the most comprehensive publication archive among the existing databases.

References

Akhuseyinoglu, N.B. and Joshi, J. (2020). A constraint and risk-aware approach to attribute-based access control for cyber-physical systems. *Computers & Security, 96*, 1-18.

Al-Mhiqani, M.N., Ahmad, R., Yassin, W., Hassan, A., Zainal Abidin, Z., Salih Ali, N. and Abdulkareem, K.H. (2018). Cyber-Security incidents: A review cases in cyber-physical systems. *(IJACSA) International Journal of Advanced Computer Science and Applications, 9*(1), 499-508.

Alguliyev, R., Imamverdiyev, Y. and Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry, 100*, 212–223.

Arnaboldi, L., Czekster, R.M. and Morisset, C. (2020). Modelling load-changing attacks in cyber-physical systems. *Electronic Notes in Theoretical Computer Science, 353*, 39–60

Brandman, J., Sturm, L., White, J. and Williams, C. (2020). A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems. *Journal of Manufacturing Systems, 56*, 202–212.

Carter, B., Adams, S., Bakirtzis, G., Sherburne, T., Beling, P., Horowitz, B. and Fleming, C.

(2019). A preliminary design-phase security methodology for cyber–physical systems. *Systems, 7*(21), 1-22.

Chen, D., Wawrzynski, P. and Lv, Z. (2021). Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society, 66*,1-12.

Çakmak, H. and Demir, C. K. (2009), *Siber dünyadaki tehdit ve kavramlar", suç, terör ve savaş üçgeninde siber dünya*, 1. Baskı İçinde (p.23-54), Ankara: Barış Platin Kitabevi.

DiMase, D., Collier, Z.A., Heffner, K. and Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environ Syst Decis*, *35*, 291–300

Elhabashy, A.E., Wells, L.J. and Camelio, J.A. (2019). Cyber-Physical security research efforts in manufacturing – a literature review. *Procedia Manufacturing, 34*, 921-931.

Geismann, J. and Bodden, E. (2020). A systematic literature review of model-driven security engineering for cyber–physical systems. *The Journal of Systems & Software, 169*, 1-17.

Ghadge, A., Weiß, M., Caldwell, N.D. and Wilding, R. (2020), Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management*, *25*(2), 223-240

Gunes, B., Kayisoglu, G. and Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security, 103*, 1-22

Ismail, R., and Zainab, A. (2011). Information systems security in special and public libraries: An assessment of status. *Malaysian Journal of Library & Information Science*, *16*(2), 45- 62.

Kaur, J. and Ramkumar, K.R. (2021). The recent trends in cyber security: A review. Journal of King Saud University – *Computer and Information Sciences,* 34(1), 1-16

Kholidy, H.A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. *Future Generation Computer Systems, 115,* 171–187

Mourtzis, D. and Vlachou, E. (2016). Cloud-based cyber-physical systems and quality of services. *The TQM Journal*, *28*(5), 704-733.

Palleti, V.R., Chong, T.Y. and Samavedham, L. (2018). A mechanistic fault detection and isolation approach using Kalmanfilter to improve the security of cyber physical systems. *Journal of Process Control, 68*, 160–170.

Pan, M., Wang, J., Errapotu, S. M., Zhang, X., Ding, J., and Han, Z. (2019). *Big data privacy preservation for cyber-physical systems.* Cham: Springer International Publishing. https://doi. org/10.1007/978-3-030-13370-2

Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128.

Parn, E.A. and Edwards, D. (2019). Cyber threats confronting the digital built environment Common data environment vulnerabilities and block chain deterrence. *Engineering, Construction and Architectural Management, 26*(2), 245-266

Pasqualetti, F., Dörfler, F. and Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control, 58*(11), 2715-2729.

Raban, Y. and Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight, 20*(4), 353-363.

Rajkumar, R., Lee, I., Sha, L., and Stankovic, J. (2010). *Cyber-physical systems. In S. Sapatnekar* (Ed.), Proceedings of the 47th Design Automation Conference on - DAC '10 (p.731). New York, New York, USA: ACM Press. https://doi.org/10.1145/1837274.1837461

Rid, T. and McBurney, P. (2012), Cyber-Weapons. *The RUSI Journal*, *157*(1), 6-13.

Sreeram, M. and Shimon, Y. N. (2021). Human-in-the-loop: role in cyber physical agricultural systems. *Internatıonal Journal of Computers Communıcatıons & Control*, 16(2), 1-20.

Tantawy, A., Abdelwahed, S., Erradi, A. and Shaban, K. (2020). Model-based risk assessment for cyber physical systems security. *Computers & Security, 96*, 1-15.

Tripathi, D., Singh, L.K., Tripathi, A.K. and Chaturvedi, A. (2021). Model based security verification of Cyber-Physical system based on Petrinet: A case study of nuclear power plant. *Annals of Nuclear Energy, 159*, 1-14.

ur Rehman, S. and Gruhn, V. (2018). An effective security requirements engineering framework for cyber-physical systems. *Technologies*, *6*(65),1-20

Walker-Roberts Hammoudeh, S.M., Aldabbas, O., Aydin, M. and Dehghantanha, A. (2020). Threats on the horizon: understanding security threats in the era of cyber-physical systems. *The Journal of Supercomputing, 76*, 2643–2664.

Wu, G., Sun, J. and Chen, J. (2016). A survey on the security of cyber-physical systems. *Control Theory and Technology*, *14*(1), 2–10.

Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab A. and Malli M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems, 77*, 1-33.

Zegzhda, D.P. (2016). Sustainability as a criterion for information security in cyber-physical systems. *Automatic Control and Computer Sciences*, *50*(8), 813–819.

Zhang, D., Wang, Q.G., Feng, G., Shi, Y. and Vasilakos, A.V. (2021). A survey on attack detection, estimation and control of industrial cyber–physical systems. *ISA Transactions*, 116, 1-16