Impact of Cyber Risks and Threats on the Critical Infrastructure Development: Visualization of Scientific Research

Aleksy Kwilinski[1] and Nataliia Trushkina[2]
[1]The London Academy of Science and Business,
Unit 3, Office A, 1st Floor, 6-7 St Mary At Hill, London, EC3R 8EE, England
[2]Research Center for Industrial Problems of Development of the National Academy of Sciences of Ukraine,
1a Inzhenernyi Lane, 61165 Kharkiv, Ukraine
a.kwilinski@london-asb.co.uk, nata_tru@ukr.net

Keywords: National Economy, Critical Infrastructure, Cyber Risk, Cyber Threat, Cyberattack, Cyberwars, Cybersecurity, Cyber defense, Cyberspace, Digital Environment, Development Strategy, Bibliometric Analysis, Trend Analysis.

Abstract: In the global world, there is a constant dynamic process that leads to structural changes (economic, social, organizational, environmental, etc.) of objects and infrastructure networks in a multi-component spatial system. At this stage, the issue of transformation of economic systems through the transition of key elements of critical infrastructures to a qualitatively new level of development due to adaptation to risks and threats of the external environment is becoming particularly relevant. One of these risks is cyberattacks on important infrastructure facilities in the energy, IT, financial, transport sectors. According to the European Agency for Network and Information Security (ENISA), the number of cyberattacks on critical infrastructure in the EU increased in 2019-2020 by 2 times, or from 150 to 300. According to expert estimates, global losses from cyberattacks in 2020 amounted to approximately 945 billion dollars. In this regard, this study is devoted to the analysis of the impact of cyber risks and threats on the development of critical infrastructure using bibliometric and trend approaches. The purpose of the article is to identify the main directions of scientific research, assess the dynamics of publishing activity, as well as identify key trends and gaps in this field. As part of the study, a bibliometric analysis of the database of scientific publications was carried out to identify the most cited works and authors, as well as a trend analysis to identify changes in research topics. The results of the study will allow obtaining a holistic view of the current state and prospects for the development of research in the field of critical infrastructure development, taking into account cyber risks and threats, which can contribute to the formation of more effective strategies and policies of cybersecurity and the protection of critical infrastructure objects in the countries of the world.

1 INTRODUCTION

In modern society, cyberattacks on critical infrastructure are becoming an increasingly serious threat and risk to the development of national economies of the world. Therefore, the fact that reliable protection against cyberattacks actively affects the economic, political, defense and other components of the national security of states is undeniable. It is obvious that the disruption of the functioning of critical infrastructure facilities can lead to the appearance of risks, emergency situations and crisis phenomena of economic systems of various levels.

Therefore, cyber risks are considered the main global risk for strategic sectors of critical infrastructure. The type of information and communication technology risks that infrastructure objects are exposed to has not changed in recent years, but the frequency of cyber incidents and the scale of their impact on enterprise activity have increased. According to Cybersecurity Ventures [1], global annual costs of cybercrime will reach 9.5 trillion dollars in 2024. Global losses from cybercrime are predicted to grow 3.5 times over 2015-2025, or from 3 to 10.5 trillion dollars. Global spending on cybersecurity will increase to 1.75 trillion dollars by 2025 (for comparison: the volume of the global cybersecurity market was only 3.5 billion dollars in 2004 [2]).

Constant geopolitical tensions are one of the key factors focusing business leaders' attention on creating an effective cyber risk management strategy. According to the World Economic Forum's Global Security Outlook 2023 report [3], 74% of organizations indicated that global geopolitical instability has impacted their cyber strategy.

It should be noted that critical infrastructure businesses face an increased risk of disruption due to sophisticated cyber threats, from state-sponsored ransomware groups to supply chain vulnerabilities and new threats arising from ongoing geopolitical tensions.

Microsoft Digital Defense Report [4] showed that the number of cyberattacks targeting critical infrastructure had grown significantly and now accounts for 40% of all government attacks (20% in 2021). According to Verizon's 2023 Data Breach Report [5], the majority of attacks targeted government administrators, as well as organizations in the IT, finance, manufacturing, and professional services sectors.

In view of this, in the conditions that have developed today, it is important to ensure the appropriate level of security, including cybersecurity of critical infrastructure facilities. For this, it is necessary to substantiate conceptual provisions and develop practical recommendations for the formation of an appropriate secure information environment and the application of a risk-oriented approach to managing the development of critical infrastructure.

2 LITERATURE REVIEW

The analysis shows that most of the world's leading countries pay special attention to the formation and development of national cyber security systems and the protection of critical infrastructure facilities. Thus, in the European Union, the European Union Agency for Cybersecurity ENISA is the main body engaged in achieving a high common level of cybersecurity. ENISA developed a single pan-European concept of protection “Cyber Europe”, which was adopted in 2009 and is updated every two years. The basis of this concept is the safety and stability of objects of critical information infrastructure. The EU also ensured tactical actions and operational cooperation of countries at the pan-European level. In addition, the requirements for the protection of such important objects are determined by the national legislation of individual EU member states. Directive (EU) 2016/1148 of the European Parliament and the Council of July 6, 2016 “On measures to ensure a high general level of security of network and information systems on the territory of the Union” is of great importance in the European Union for protection against cyberattacks. NIS (The Security of Network and Information Systems) primarily concerns critical infrastructure companies and digital service providers (online marketplaces, online search engines, and cloud computing services).

On January 16, 2023, the New Cybersecurity Directive NIS 2 came into force, introducing mandatory information security measures and information security incident reporting requirements. Many companies in certain sectors will be subject to significant fines for failure to comply with these requirements. This Directive applies to organizations from the following sectors of critical importance for the economy: energy, transport, banking, financial market infrastructure, health care, drinking water supply, sewage systems, digital infrastructure, B2B management, IT services, public administration, and space research. Therefore, NIS 2 aims to improve the current state of cybersecurity in the EU by creating the necessary cyber crisis management framework, increasing the level of harmonization of security requirements and reporting obligations, as well as establishing a baseline level of cybersecurity risk management measures and reporting obligations in all critical sectors covered by the directive.

In the US, the organization that develops requirements in the field of cybersecurity is NIST – National Institute of Standards and Technology. For certain organizations in the USA, when building information systems, compliance with the requirements of the NIST Cybersecurity Framework is mandatory, in particular for objects of critical information infrastructure. This document appeared in 2014 and has been updated several times since then. In the United States of America, the Cybersecurity and Infrastructure Security Agency (CISA) deal with issues of cybersecurity in general and the protection of critical infrastructure. Facilitation of the broad exchange of critical infrastructure information between owners and operators of critical infrastructures and government agencies responsible for their protection is carried out in accordance with the Critical Infrastructure Information Act of November 25, 2002. In this regard, the country's vulnerability to terrorism is reduced.

In Singapore, attention is drawn to the Cybersecurity Act, which is the framework for protecting critical information infrastructure from cybersecurity threats, taking measures to prevent, manage and respond to cybersecurity threats and incidents of critical infrastructures. The Cybersecurity Agency of Singapore is also interested.

In the Republic of China, security measures for critical information infrastructure are entrusted to the state. The country adopted the Law on Cybersecurity, in which Critical Information Infrastructure is interpreted as public communications and information services, public administration, water supply, finance, public services, electronic management and other critical information infrastructure, which in case of its destruction, violation functionality or data loss may actually threaten national security, national welfare, people's livelihoods, or the public interest.

In India, there is an Information Technology Act (2008), according to which critical information infrastructure (Critical Information Infrastructure) computer resources, the failure or destruction of which will affect the national security, economy and social welfare of the nation (Article 70). The legislative document delineates the sector of telecommunications and information technologies. That is, information technologies are considered as an independent, critically important sector of the national infrastructure. According to the Information Technology Act, the National Critical Information Infrastructure Protection Center (NCIIPC) of India was established in 2014.

It is worth noting that not only at the government level, various aspects of increasing the level of cyber protection of critical infrastructure objects are being discussed, and appropriate methodological recommendations and practical techniques for combating cyberattacks on critical infrastructures are being developed.

In recent years, in the scientific and educational environment, they are also actively engaged in research and development on the chosen research topic. The study of various aspects of the development of infrastructure as a multifunctional system that ensures the functioning of economic systems is given considerable attention in the works of leading scientists (M. Blaiklock [6]; B. Frischmann [7]; G. Hedtkamp [8]; R. Jochimsen [9]; W. Rostow [10]; U. Simonis [11]; H. Singer [12]; A. Youngson [13] and others). Based on the generalization of the existing scientific approaches to the formulation of the term “infrastructure”, they are conditionally systematized according to the following groups: system; resource; mechanism; systemic economic category; a component of the economic system; complex of types of economic activity; part of the economy; appropriate conditions (institutional, economic, social, investment, financial, environmental [14; 15; 16]); a component of the environment; component of the spatial system.

In the scientific literature (R. Wróbel [17]; B. Rathnayaka et al. [18]; D. Rehak et al. [19]; L. Shen et al. [20]; C. Scholz et al. [21] and others), many interpretations of the concept of “critical infrastructure” are used from different positions, including cyber security in the national security system. Summarizing the existing scientific developments regarding the conceptual apparatus, it was established that scientists usually understand critical infrastructure as: a complex system; its key components or components; critical infrastructure facilities; network structure; physical structure; organizational structures; institutes; institutions; institutions; set of assets; object of administrative and legal protection; object of cyber protection; security direction; one of the security tasks of the state; a component of the national infrastructure; a set of objects, technologies, state and scientific structures; object of state administration; component of information security; an element of the national security system of the state or region.

The theoretical analysis shows that scientists (A. Coning, F. Mouton [22]; D. Decker, K. Rauhut [23]; A. Elmarady, K. Rahouma [24]; M. Komarov et al. [25]; M. Gazzan, F. Sheldon [26]; S.Venkatachary et al. [27]; A. Golgota, U. Cerma [28] – in chronological order) are focused on conducting thorough scientific research on the development of risk management tools for implementation in the operations of critical infrastructure facilities.

Researchers take a detailed look at the challenges associated with cybersecurity and cyberterrorism for critical infrastructures. The papers highlight the complexity of monitoring, managing, and measuring cybersecurity threats and discuss the critical need for analysis in this area, especially in the energy sector where command and control operations are performed in a networked environment. Despite effective risk management practices in the energy industry, it remains vulnerable to cyberterrorism, as evidenced by the Stuxnet attack. In addition, the economic consequences of cyberattacks on critical infrastructure are discussed, including the potential for significant financial losses and reputational damage. The authors provide practical advice on safeguards and defense mechanisms such as network segmentation, access control and encryption to help prevent cyberattacks. Scientists emphasize the need to continue developing effective risk management strategies and implementing appropriate measures to protect critical infrastructure objects from cyber threats. At the same time, scientists emphasize the creation of a digital security model in strategic sectors of critical infrastructure in various countries of the world.

Despite the wide range of scientific research on the chosen topic, the multifacetedness and debatable nature of certain issues require further development. Considering the above, it is relevant and necessary to analyse the impact of cyber risks and threats on the development of critical infrastructure using bibliometric and trend approaches.

3 METHODOLOGY

The theoretical and methodological basis of the study is the provisions of economic theory, institutional theory, theories of systems, network economy, digital economy, infrastructure, globalization, national interests of H. Morgenthau, possible conflicts of interest in the field of ensuring national stability according to J. Anderis, P. Martin-Breen, D. Chandler; concepts of information society, cyber and information security, sustainable development, strategic and energy management; models of national stability and development of the security environment.

The following general scientific methods were used in the research process: dialectical, historical, formal-logical, axiomatic, theory of logic and hypothetical-deductive, analysis and synthesis, induction and deduction, component analysis, trend analysis, bibliometric analysis, comparative analysis, analogy, classification, structural-logical generalization.

The information base of the research is statistical and analytical materials of Cybersecurity Ventures, Cybersecurity and Infrastructure Security Agency (CISA), The Cybersecurity Agency of Singapore, The European Agency for Network and Information Security (ENISA), Microsoft, the National Critical Information Infrastructure Protection Center (NCIIPC), Verizon, World Economic Forum (WEF), as well as legislative and regulatory documents the Critical Infrastructure Information Act of November 25, 2002; the Cybersecurity Directive NIS 2; the Cybersecurity Act of Singapore; Directive (EU) 2016/1148 of the European Parliament and the Council of July 6, 2016 “On measures to ensure a high general level of security of network and information systems on the territory of the Union”; Information Technology Act of India; the Law on Cybersecurity of China; the NIST Cybersecurity Framework; Pan-European concept of protection “Cyber Europe”.

4 RESEARCH RESULTS

Based on the bibliometric analysis, it was established that various aspects of ensuring the development of critical infrastructure, taking into account the impact of cyber risks and threats, are part of the long-term scientific interests of most leading foreign scientists. According to the title of articles, abstracts and keywords “Cyber risk”, “Critical infrastructure” or “Critical infrastructure facilities” in the international scientometric database Scopus, 1510 documents were found for the years 2002-2024.

As the analysis shows, these issues became especially relevant in the period from 2010. For 2010-2024, the number of scientific works increased from 24 to 134 or 5.6 times. During this period, the average growth rate was 13.1%. The following keywords are mostly used in publications: Cyber Security (521 documents), Risk Assessment (460), Network Security (446), Critical Infrastructures (424), Computer Crime (230), Risk Management (219), Cyber Attacks (213), Cyber Physical System (172), Security of Data (138), Industrial Control Systems (120), Risk Analysis (119), Internet of Things (111), Control Systems (97), SCADA Systems (93), Electric Power Transmission Networks (92), Risk Perception (91), Security

Systems (87), Cyber Threats (78), National Security (70), Resilience (69), Critical Infrastructure Protection (65) etc.

Among the most cited scientific works on the chosen subject, the following can be mentioned:

1) A. A. Cárdenas et al., "Attacks against process control systems: Risk assessment, detection, and response" [29] – the article examines how, using knowledge about the physical system under control, it is possible to detect computer attacks that change the behaviour of the target control system. By using knowledge about the physical system, it is possible to focus on the ultimate goal of the attack, rather than on specific mechanisms for exploiting vulnerabilities and hiding the attack. The authors analysed the protection and security of mechanisms, investigating the consequences of hidden attacks and ensuring that automatic mechanisms for responding to attacks do not lead the system to an unsafe state;

2) S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security" [30] – the article argues that industrial systems address security only partially, relying mostly on "isolated" networks and access-controlled environments. Monitoring and control systems, such as SCADA/DCS, are responsible for managing critical infrastructure that operates in environments where a false sense of security is common. The article explores the highly complex aspects of Stuxnet, the impact it may have on existing security considerations, and offers some thoughts on next-generation SCADA/DCS systems from a security perspective;

3) Y. Ashibani, and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions" [31] – an analysis of security problems at different levels of the architecture of cyber-physical systems (CPS), an assessment of risks and CPS protection methods is given;

4) H. Sandberg, S. Amin, and K. H. Johansson, "Cyber physical security in networked control systems: An introduction to the issue" [32] – hypothesized that cyber-physical security applications of networked control systems (NCS) range from large-scale industrial to critical infrastructures such as water supply, transportation, and power grids. NCS security naturally depends on the integration of cyber and physical dynamics, and the different ways in which they are affected by the actions of decision makers. Emphasis is placed on developing a principled approach to NCS cyber-physical security;

5) I. Stellios et al., "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services" [33] – the article states that for some sectors, such as industry, intelligent networks, transportation and healthcare, the importance of cyber-attacks using the Internet of Things is obvious, since IoT technologies are part of mission-critical server systems. Therefore, the purpose of this study is threefold: to assess IoT-enabled cyberattacks using a risk-like approach to demonstrate their current threat landscape; identification of hidden and subliminal ways of attacks on critical infrastructures and services supported by the Internet of Things; study of mitigation strategies for all areas of application;

6) A. Nicholson et al., "SCADA security in the light of cyber-warfare" [34] – the article reviews current research and provides a consistent overview of SCADA security threats, risks, and mitigation strategies;

7) P. A. S. Ralston, J. H. Graham, J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks" [35] – In the article, the authors emphasize that the growing dependence of critical infrastructure and industrial automation on interconnected physical and cyber control systems has led to a previously unforeseen cybersecurity threat to supervisory control and data acquisition (SCADA) and distributed control systems (DCS). This article provides a broad overview of cybersecurity and risk assessment for SCADA and DCS, introduces the major industry organizations and government groups working in the field, and provides a comprehensive review of the literature to date.

Key publications that publish works on the subject of cyber risks and threats to the functioning of critical infrastructure facilities include: Lecture Notes In Computer Science Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics (70 documents); IFIP Advances In Information And Communication Technology (40); ACM International Conference Proceeding Series (30); International Journal Of Critical Infrastructure Protection (23); Computers And Security (19 documents).

The main organizations dealing with the development of critical infrastructure in cyberspace are: Norges Teknisk-Naturvitenskapelige Universitet (28 documents); University of Piraeus (21); Austrian Institute of Technology (19); Pacific Northwest National Laboratory (18); University of Illinois

Urbana-Champaign (16); University of Jyväskylä (16); Sandia National Laboratories, New Mexico (14); Idaho National Laboratory (13); The George Washington University, Queensland University of Technology, University of Oxford (11 documents each); Virginia Polytechnic Institute and State University, The Grainger College of Engineering (10 documents each).

The results of the analysis show that most of the works on the studied issue are published by scientists from the United States (448 documents), United Kingdom (173), Italy (96), India (91), Germany (76), Greece (60), Norway (60), Australia (57), France (44), Spain (42), Canada (38), China (36), Sweden (35), Austria (33), Finland (28), Netherlands (28 documents), etc. In Ukraine, 26 documents were found based on the established search details.

By types of documents, works can be ranked as follows: 1st place is occupied by Conference Paper (790 documents or 52.3% of the total number of publications on the selected research topic); 2nd – Article (434 or 28.7%); 3rd – Book Chapter (145 or 9.6%); 4th – Conference Review (57 or 3.8%); 5th – Review (49 or 3.2%); 6th place – Book (29 documents or 1.9% of the total number of publications).

For the most part, scientific works on cyber risks and threats to critical infrastructure are published in the following fields of knowledge: Computer Science (953 documents or 30.6% of the total number of publications on this issue); Engineering (767 or 24.6%); Social Sciences (256 or 8.2%); Decision Sciences (231 or 7.4%); Energy (154 or 4.9%); Business, Management and Accounting (87 or 2.8%); Environmental Science (81 or 2.6%); Economics, Econometrics and Finance (42 documents). This shows that the researched topic is multidisciplinary and multifaceted.

The main sponsors that finance scientific publications on selected issues include the following: Horizon 2020 Framework Programme (75 documents); European Commission (64); National Science Foundation (52); U.S. Department of Energy (28); Engineering and Physical Sciences Research Council (22); U.S. Department of Homeland Security (18); Horizon 2020, National Natural Science Foundation of China (17 documents each); Norges Forskningsråd (15); Seventh Framework Programme (13); European Regional Development Fund (10 documents) etc.

As bibliometric analysis shows, in the international scientometric database Scopus there are 2,297 publications that contain the keywords “Cyber threat” and “Critical infrastructure”. The first publication on this topic appeared in 1997. Until 2005, publication activity was insignificant. And since 2005, scientists began to actively pay attention to this topic. For 2005-2024, the number of publications increased 26.5 times (from 10 to 265), and for 2015-2024 – 2.5 times (from 106 to 265).

Based on the analysis, it was established that the Scopus international scientometric database contains 3,537 publications that deal with various types of cyberattacks on critical infrastructure facilities. During 2005-2024, the number of such scientific works increased 17.3 times (from 18 to 312), during 2005-2015 – 8.6 times (from 18 to 155), during 2015-2024 – almost 2 times (from 155 to 312 documents).

Therefore, the analysis of publication activity confirmed that since 2010 there has been an increase in scientific interest in the study of the development of critical infrastructures in the context of global cyber risks and threats.

Further processing and analysis of bibliographic data was carried out using the VOSviewer software, which is a software tool for constructing and visualizing maps of bibliometric networks [36]. VOSviewer software was used to construct network maps of relationships between keywords based on bibliographic records from Scopus databases. The visual results of the obtained map of the bibliometric network are shown in *Figure 1*.

The map of the bibliometric network displays the frequency of use of terms by the size of the circle and the intensity of communication, and allows you to track variants of combinations of terms both within clusters and between them. The colour of the circle indicates that the keyword belongs to a certain cluster. The larger the diameter of the circle, the more often this term appears in scientific publications. Links on the map show the frequency of repetition of keywords in publications, while the smaller the distance between keywords, the stronger the connection between them [36].

According to *Figure 1* using the VOSviewer program, 785 keywords are systematized into 10 clusters, each of which symbolizes a separate direction of scientific research on the development of critical infrastructure, taking into account possible cyber risks and threats: the first cluster (red) contains 178 words, its share is 22.7% of the total number of key concepts; the second (green) – 149 words (or 19%); the third (blue) – 110 words (14%); fourth (yellow) – 94 words (11.9%); fifth (purple) – 84 words (10.7%); sixth (turquoise) – 54 words (6.9%); seventh (orange) – 37 words (4.7%); eighth (brown) – 33 words (4.2%); ninth (dark pink) – 28 words (3.6%); the tenth cluster (pale pink) includes 18 words, which is 2.3% of the total number of terms from the selected topic.

Let's consider the 4 main clusters in more detail. The grouped keywords in the first cluster indicate that scientists consider the security aspects of the development of critical infrastructure, that is, from the standpoint of different types of security. This cluster contains keywords such as critical infrastructure, critical infrastructure resilience, cyber conflict, cyber event, cyber insurance, cyber protection, cybercrime, cyber challenge, cybersecurity strategy, cyberspace, cyber threat, data protection, defense, economic security, national security, national infrastructure, national cybersecurity strategy, potential attack, potential cyber threat and others.

The second cluster is related to the search and definition of tools for minimizing risks and threats to the functioning of critical infrastructure facilities. This cluster includes the following concepts: behavioral research, budget control, compliance control, computer control system, control system analysis, control system security, critical infrastructure protection, critical infrastructure security, cyber physical security, cyber physical system, cyber physical threat, multi agent system, network security, networked control system, risk assessment, risk management, SCADA system, and security system.

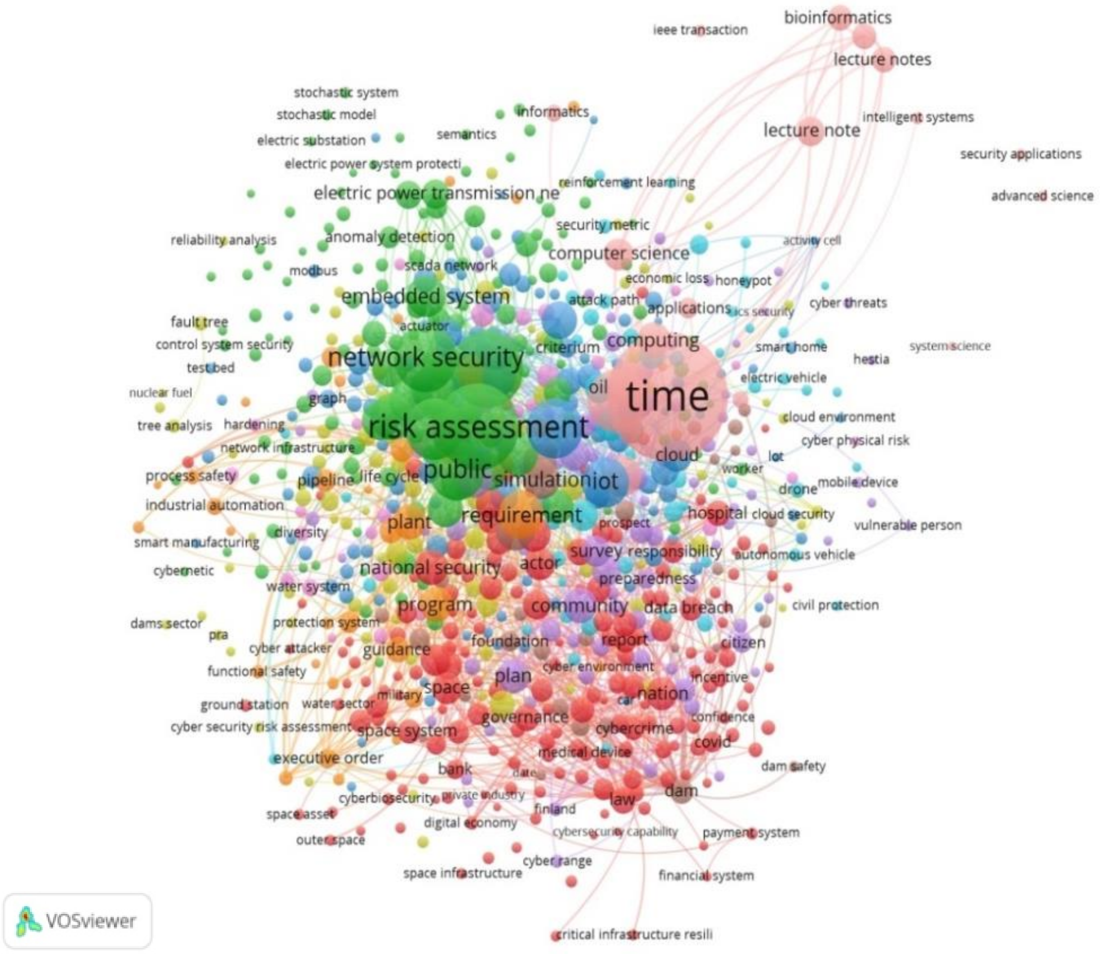


Figure 1: Network visualization of citations of articles on the impact of cyber risks on the critical infrastructure development, implemented using the VOSviewer tool[1].

[1] *Source:* built on the basis of data from the Scopus scientometrics database using the VOSviewer program.

The third cluster is related to the problems of forming a critical information infrastructure using modern information technologies and systems. The cluster includes Big Data, blockchain technology, cloud, cyberinfrastructure, diagnosis, IoT, industrial Internet, intelligent electronic device, machine learning, SCADA network.

The fourth cluster takes into account the processes of digital transformation of critical infrastructure. Emphasis is mostly placed on energy infrastructure. The cluster includes key terms such as communication protocol, critical energy infrastructure, defense strategy, digital instrumentation, digital technology, digital transformation, modernization, mathematical model, navigation, network environment, nuclear energy, safety critical system, security compliance, security risk assessment and others.

Thus, based on the results of the study, the following conclusions can be drawn:

1) The number of publications indexed in Scopus, whose titles, abstracts and keywords contain the terms “Cyber risk”, “Cyber threat”, “Cyberattack”, “Critical infrastructure”, “Critical infrastructure facilities”, “Critical infrastructure development” grows at an accelerated pace every year. Research on digital transformations of critical infrastructure has become increasingly popular since the 2000s. The key reason for the growing popularity of these scientific studies is the intensification of digitization processes and the introduction of digital technologies [37].
2) The term “critical infrastructure” has an interdisciplinary nature; it is used in studies of various branches of science, namely: it is found in publications on engineering, computer science, energy, ecology, social sciences, management, economics, decision science, etc.
3) Visualization of the network map of keywords based on bibliographic data made it possible to single out 10 clusters that characterize the priority areas of research: formation of a security environment, identification, adaptation, digitalization, development, cyber risk management, measures to reduce vulnerabilities and cyber threats, security, protection of critical infrastructure, development of a comprehensive national cyber security strategy.
4) The leaders in terms of the number of publications indexed in the international scientometric database Scopus are the USA, Great Britain, Italy, India, Germany, Canada, and China.

It should be noted that issues related to the definition of contextual and temporal patterns of the development of the views of scientists who investigate the impact of cyber risks and threats on the development of critical infrastructure in the countries of the world are gaining special relevance. For this, the toolkit of trend analysis is used – Google Trends.

Based on the trend analysis for the years 2004-2024, a high level of interest in the topics of “Critical Infrastructure” (on average 17 points) and “Cyber risk” (on average 13 points) was revealed worldwide (*Figures 2, 3*).

Looking back over time, we can see that in 2004, the popularity of the topic related to cyber risks was 0 points, and the development of critical infrastructure was 35 points. Since 2008, topics related to cybersecurity problems began to become popular, while the development of critical infrastructure began to decline. In 2012, the level of interest in both topics was 12 points. Since 2017, the level of interest in cyber risk management has been growing annually, while critical infrastructure has been shrinking. So, in 2019, the value of this indicator was 25 and 12 points, respectively; in 2023 – 47 and 24 points.

Queries are given points from 0 to 100, where 100 points means the location with the highest share of query popularity, 50 points - the location where the query popularity level is half as low as the first one. A score of 0 indicates a location for which there is insufficient data for the query in question. It is worth noting that the more points, the higher the proportion of relevant requests from all requests, and not their absolute number. Therefore, a small country, where queries with the words “Cyber risk” or “Critical infrastructure” make up 80% of all queries, will be assigned twice as many points as a large one, where only 40% of all queries contain this word.

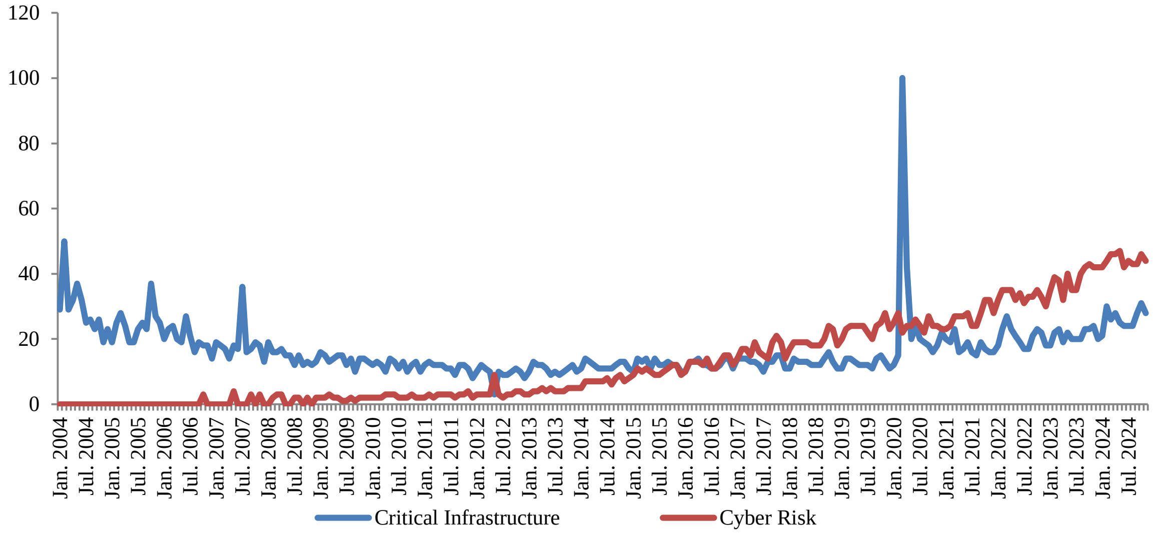
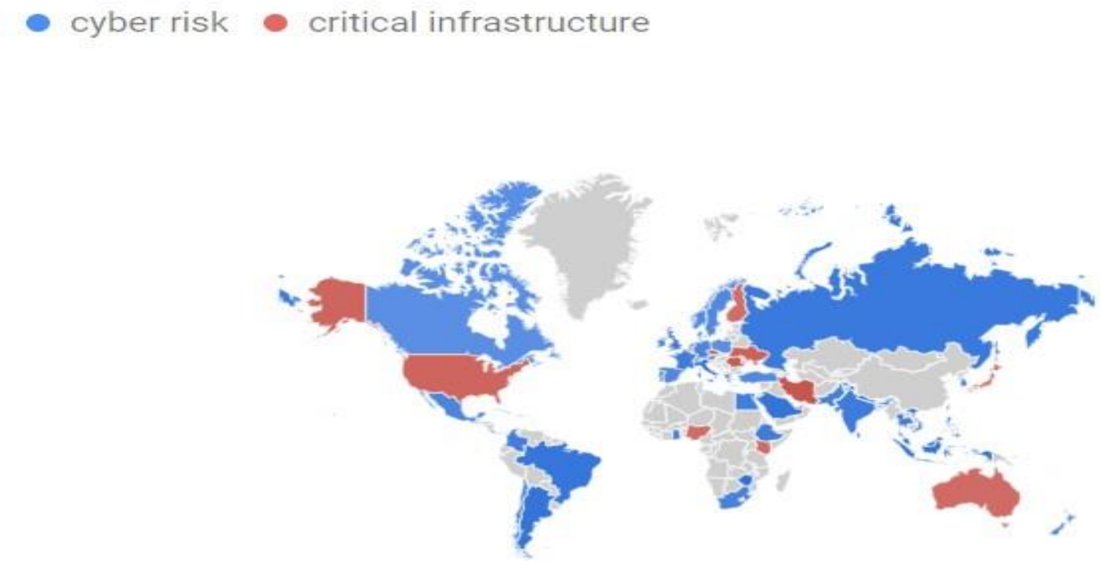


Figure 2: The dynamics of changes in search frequency in terms of the definitions of “Cyber risk” (blue colour) and “Critical Infrastructure” (red colour) in the world [3].



Note: the intensity of the colour depends on the percentage of requests.

Figure 3: Popularity of user searches for the topics “Cyber risk” and “Critical Infrastructure” in the world for the years 2004-2024 [4].

[3,4] *Source:* built using the Google Trends toolkit.

The topic, which is dedicated to the solution of urgent issues of the development of critical infrastructure, taking into account cyber threats and risks, has been updated again since 2022. This is due to the full-scale invasion of Russia on the territory of Ukraine and constant cyberattacks on critical infrastructure objects around the world.

Currently, in most countries of the world, in the last 20 years, the topics of cyber risks, threats, cyberattacks, cyberwars, cybersecurity, etc. are popular. In a number of countries, the share of requests for cyber risks exceeds 50% of the total number of requests in the respective country. For example, in Italy the value of this indicator is 81%, Switzerland – 77, Vietnam – 72, Korea and Great Britain – 71, France – 68, the Netherlands – 64, Portugal – 61, Germany – 59, Israel – 58, Spain – 56, Turkey – 55, Norway – 54, Canada and Poland – 50%. And in some countries, various aspects of development and implementation of critical infrastructure development strategies are gaining popularity and prevalence among sourcing. Thus, the level of popularity of the topic "Critical infrastructure development" in Finland and Japan is 51%, in Australia – 53, in the USA – 57, in Ukraine – 59, in the Czech Republic – 62, in Romania – 64% of the total number of requests in the respective country.

The following topics can be named among the leaders in terms of popularity: Cyber risk security (100 points); Cyber security (93); Cyber risk management (50); Risk management (49); Risk in Cyber security (35); Risk assessment (28); Cyber risk assessment (27); Risk management cyber security (26); Cyber risk insurance (17); Cyber insurance (15); Information security (14); Cyberattack (14); Cyber threat (13); Cybersecurity and Risk management (10 points).

The most common user search queries in countries around the world include: Critical infrastructure security (100 points); Critical infrastructure protection (85); Critical national infrastructure (64); Security of Critical infrastructure (51); Cybersecurity (36); Cybersecurity critical infrastructure (35); Critical infrastructure act (31); Critical infrastructure sectors (26); Critical infrastructure systems (25); Critical infrastructure definition (20); Critical information infrastructure protection (10 points).

The analysis shows that the subject of "Cyber threat" began to become more active since 2016. If in 2004 the level of popularity for this issue was 0 points, then in 2016 – 12, in 2017 – 15, in 2019 – 26, in 2022 – 39, in 2023 – 46 points. Users from Indonesia (84% of the total number of queries in the country), Malaysia (75%), Brazil (75%), Turkey (73%), Pakistan (72%), Korea (69%), Vietnam (69%), France (69%), Israel (69%), UK (67%), Portugal (60%), Italy (60%), Japan (57%), Poland (56%), Hungary (54%), Germany (54%), Canada (47%), USA (46%), Ukraine (45%), China (34%).

Since 2014, Cyberattack has become a popular search topic for users all over the world. The dynamics of popularity changed every year: in 2014, the level of interest was 14 points, in 2017 – 100, in 2020 – 40, in 2021 – 59, in 2023 – 61 points.

The leading countries in which users actively search for information on this issue include the following: The United Kingdom (94% of the total number of requests in the country), Pakistan and France (92%), Turkey (91%), Israel (90%), Canada, Switzerland, Sweden (87%), Germany (84%), USA and Japan (83%), Iran and Poland (80%), Republic of Korea (74%).

Among the leaders when searching for users using the keyword "Cyber threat" can be named Cyber security threat (100 points), Security threat (97), Threat intelligence (66), Cyber intelligence (63), Cyber threat intelligence (63 points). Popular queries on the subject of "Cyberattack" are Cybersecurity attack (100 points), Cyberattacks (54), Cyberattack types (17 points).

Thus, the study of trend patterns of publishing activity from the analysis of the relationship between the concepts of "Cyber risk" and "Critical infrastructure" proved the significant popularity of this issue in scientific circles, as well as its permanent growth.

At the same time, according to the results of the conducted trend analysis (based on the analysis of the dynamics of the number of publications on the researched topic, indexed by the Scopus scientometric database, for 2002–2024, the analysis of trends in user interest in this issue based on the Google Trends toolkit for the period 2004–2024 y.), as well as the generalization of existing conceptual developments in the scientific literature regarding the justification of national strategies for cybersecurity of critical infrastructure [22-28], it can be concluded that this problem is complex and multifaceted. It causes a synergistic effect on the national economy and is inextricably linked to ensuring information security in the national security system.

5 CONCLUSIONS

In today's conditions, the world is on the threshold of new challenges, as there is a growing trend of increasingly complex and large-scale attacks on critical infrastructure facilities. Therefore, cybersecurity of critical infrastructure is one of the priorities of national security in the countries of the world in the conditions of a changing information space.

At the same time, it is extremely important to diagnose the state of cybersecurity as an effective tool, the procedure of which should include the following stages: assessment of the state of cybersecurity according to the NIST Cybersecurity Framework; determination of the target state of cybersecurity; development of recommendations (high-level design, specifications of technical architecture, operational models of cybersecurity); development of a road map for the implementation of recommendations; cybersecurity reassessment.

Based on the results of cyber diagnostics, critical infrastructure objects must receive a comprehensive assessment of digital security; recommendations for increasing the level of cyber maturity and preparedness for cyber incidents.

Since the nature of cyberspace is changing rapidly, the countries of the world need to improve the mechanism of regulatory and legal provision of cyber protection of critical infrastructure and information systems of objects, as well as the structure and content of national cyber security strategies. It is necessary to implement a comprehensive and comprehensive approach to the development of critical infrastructure in cyberspace, which should take into account constant changes in the security segment.

In addition, the governments of most countries of the world should pay attention to the development or improvement of national cyber security strategies. This was confirmed by the results of the bibliometric analysis. This strategic document should be understood as defining the concept, common goals, principles and priorities that should guide the country in solving cybersecurity problems; a description of the steps, programs and initiatives (i.e. the “Roadmap”) that the country intends to take to protect its critical infrastructure (including information) and to improve security, protection and resilience.

Early definition of the concept, goals and priorities allows governments to comprehensively consider cybersecurity within the framework of their national digital ecosystem, rather than at the level of a separate economic sector, a single goal or a response to a specific risk – it allows them to act strategically. National cybersecurity strategy priorities vary from country to country, so one country's focus may be on addressing risks to critical infrastructure, while another may focus on protecting intellectual property, building trust in the online environment, or raising public awareness of issues of cybersecurity or a combination of these tasks. The strategy should emphasize the importance of protecting critical infrastructure from cyber risks and recommend a comprehensive approach to risk management in the risk management system.

Finally, in the process of developing a national cybersecurity strategy, the government's vision must be translated into a coherent and feasible policy that helps it achieve its goal. This includes not only the activities, programs, and initiatives that must be accomplished, but also the resources allocated to those efforts and how those resources are used. Also, during this process, the indicators that will be used to achieve the desired results within the established budgets and deadlines should be determined.

Prospects for further research are the substantiation of the National Cybersecurity Strategy of critical infrastructure in Ukraine and the need to apply a risk-oriented approach to managing the development of critical infrastructure, taking into account the best European practices and developing practical recommendations for their implementation.

REFERENCES

[1] 2023 Official Cybercrime Report. Cybersecurity Ventures. https://www.esentire.com/resources/library/2023-official-cybercrime-report.

[2] S. Morgan, “Top 10 Cybersecurity Predictions and Statistics For 2023”, Cybercrime Magazine, Dec. 10, 2022. https://cybersecurityventures.com/stats/.

[3] Global Cybersecurity Outlook 2023. World Economic Forum. Jan. 18, 2023. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

[4] Microsoft Digital Defense Report 2022. Microsoft. https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[5] 2023 Data Breach Investigations Report (DBIR). Verizon. June 6, 2023. https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf.

[6] M. Blaiklock, The infrastructure finance handbook: principles, practice and experience. London: Euromoney Books, 2014.

[7] B. M. Frischmann, Infrastructure: the social value of shared resources. New York: Oxford University Press, 2013.

[8] G. Hedtkamp, Die Bedeutungder Infrastruktur in makrookonomischer Sicht. Munchen: Osteuropa-Inst., 1996.

[9] R. Jochimsen, Theorie der Infrastruktur: Grundlagen der marktwirtschaftlichen Entwicklung. Tübingen: J.C.B. Mohr., 1966.

[10] W. W. Rostow, The Stages of Economic Growth. London: Cambridge University Press, 1962.

[11] U. E. Simonis, "Ecological Modernization of Industrial Society – Three Strategic Elements", In: F. Archibugi, P. Nijkamp (eds.), Economy and Ecology: Towards Sustainable Development. Volume 1: Economy & Environment. Dordrecht: Springer, pp. 119-137, 1989. https://doi.org/10.1007/978-94-015-7831-8_7.

[12] H. W. Singer, International Development: Growth and Change. New York: McGraw-Hill, 1964.

[13] A. Youngson, Overhead Capital: Study Development Economics. 1st ed. Edinburgh: Edinburgh University Press, 1967.

[14] H. Dzwigol, N. Trushkina, and A. Kwilinski, "The Organizational and Economic Mechanism of Implementing the Concept of Green Logistics", Virtual Econ., vol. 4(2), pp. 74-108, 2021. https://doi.org/10.34021/ve.2021.04.02(3).

[15] O. Hutsaliuk et al. "Factor-criteria assessment of greening prerequisites for transport infrastructure development in Ukraine", IOP Conf. Ser. Earth Environ. Sci., 1126(1), 012009, 2023. https://doi.org/ 10.1088/1755-1315/1126/1/012009.

[16] A. Kwilinski, and N. Trushkina, "Green Investments as Tools for Stimulating the Sustainable Financing of Logistics Systems Development", E3S Web of Conf., vol. 456, 01003, 2023. https://doi.org/10.1051/e3sconf/202345601003.

[17] R. Wróbel, "Dependencies of elements recognized as critical infrastructure of the state", Transp. Res. Proc., vol. 40, pp. 1625-1632, 2019. https://doi.org/10.1016/j.trpro.2019.07.225.

[18] B. Rathnayaka et al., "Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review", Int. J. Disast. Risk Re., vol. 78, 103123, 2022. https://doi.org/10.1016/j.ijdrr.2022.103123.

[19] D. Rehak et al., " Dynamic robustness modelling of electricity critical infrastructure elements as a part of energy security", Int. J. Elec. Power, vol. 136, 107700, 2022. https://doi.org/10.1016/j.ijepes.2021.107700.

[20] L. Shen, J. Li and W. Suo, "Risk response for critical infrastructures with multiple interdependent risks: A scenario-based extended CBR approach", Comput. Ind. Eng., vol. 174, 108766, 2022. https://doi.org/10.1016/ j.cie.2022.108766.

[21] C. Scholz, S. Schauer, and M. Latzenhofer, "The emergence of new critical infrastructures. Is the COVID-19 pandemic shifting our perspective on what critical infrastructures are?", Int. J. Disast. Risk Re., vol. 83, 103419, 2022. https://doi.org/10.1016/j.ijdrr.2022.103419.

[22] A. D. Coning and F. Mouton, "Bulk infrastructure management for facilities management", 2020 Resilience Week, RWS 2020, pp. 181-187, 92412622020, 2021. https://doi.org/10.1109/RWS50334.2020.9241262.

[23] D. K. Decker, and K. Rauhut, "Incentivizing Good Governance Beyond Regulatory Minimums: The Civil Nuclear Sector", J. Crit. Infrastruct. Policy, vol. 2, no. 2, pp. 19-43, 2021. https://doi.otrg/10.18278/jcip.2.2.3.

[24] A. A. Elmarady and K. Rahouma, "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment", IEEE Access, vol. 9, pp. 143997-144016, 2021. https://doi.org/10.1109/ACCESS.2021.3121230.

[25] M. Komarov et al., "Requirements for a taxonomy of cyber threats of critical infrastructure facilities and an analysis of existing approaches", In: Studies in Systems, Decision and Control, vol. 346. Berlin: Springer Science and Business Media Deutschland GmbH, pp. 189-205, 2021. https://doi.org/10.1007/978-3-030-69189-9_11.

[26] M. Gazzan and F. T. Sheldon, "Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems", Future Internet, vol. 15, iss. 4, 144, 2023. https://doi.org/10.3390/fi15040144.

[27] S. K. Venkatachary et al., "Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics – Comprehensive review", Int. J. Crit. Infrastruct. Prot., vol. 45, 100677, 2024. https://doi.org/10.1016/j.ijcip.2024.100677.

[28] A. Golgota and U. Cerma, "Securing Durres Port's Digital Transformation: Cybersecurity Strategy for Maritime Industry", 13th Mediterranean Conference on Embedded Computing, MECO 2024, 771, 2024. https://doi.org/10.1109/MECO62516.2024.10577771.

[29] A. A. Cárdenas et al., "Attacks against process control systems: Risk assessment, detection, and response", Proc. of the 6th International Symposium on Information, Computer and Communications Security, ASIACCS 2011, pp. 355-366, 2011. https://doi.org/10.1145/ 1966913.1966959.

[30] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security", 7th Annual Conf. of the IEEE Industrial Electronics Society, IECON 2011, pp. 4490-4494, 61200483, 2011. https://doi.org/10.1109/IECON.2011.6120048.

[31] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions", Comput. Secur., vol. 68, pp. 81-97, 2017. https://doi.org/10.1016/j.cose.2017.04.005.

[32] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue", IEEE Control Systems, vol. 35, iss. 1, pp. 20-23, 7011179, 2015. https://doi.org/10.1109/MCS.2014.2364708.

[33] I. Stellios et al., "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services", IEEE Communications Surveys and Tutorials, vol. 20, iss. 4, pp. 3453-3495, 8410404, 2018. https://doi.org/10.1109/COMST.2018.2855563.

[34] A. Nicholson et al., "SCADA security in the light of cyber-warfare", Comput. Secur., vol. 31, iss. 4, pp. 418-436, 2012. https://doi.org/10.1016/j.cose.2012.02.009.

[35] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks", ISA Transactions, vol. 46, iss. 4, pp. 583-594, 2007. https://doi.org/10.1016/j.isatra.2007.04.003.

[36] VOSviewer – Visualizing scientific landscapes. https://www.vosviewer.com.

[37] V. Khaustova, M. Kyzym, N. Trushkina, and M. Khaustov, "Digital transformation of energy infrastructure in the conditions of global changes: bibliometric analysis", Proc. of the 12th Int. Conf. on Applied Innovations in IT (Koethen, Germany, Match 7, 2024). Koethen: Anhalt University of Applied Sciences, vol. 12, iss. 1, pp. 135-142, 2024. http://dx.doi.org/ 10.25673/115664.