The Relationship Between Artificial Intelligence and Critical Infrastructure Development: Bibliometric Analysis

Nataliia Trushkina
Research Center for Industrial Problems of Development of the National Academy of Sciences of Ukraine, Inzhenernyi Lane 1a, 61165 Kharkiv, Ukraine
nata_tru@ukr.net

Keywords: Critical Infrastructure, Critical Infrastructure Development, Artificial Intelligence, Cyber Threat, Cybersecurity, Information Security, Digital Space, Strategic Management, Risk Management, Digital Transformation, Information System, Information Technology, Bibliometric Analysis.

Abstract: Currently, the priority direction of the national economy in the world's countries is the formation of an appropriate system of protection and security of critical infrastructure, which is able to quickly respond to exogenous and endogenous threats and risks and flexibly adapt to new operating conditions using digital technologies and information systems. At the same time, in the last decade, the role of artificial intelligence as a powerful tool in the management system for the development of critical infrastructure will grow. Therefore, the purpose of this article is to identify the relationship between artificial intelligence and the development of critical infrastructure by characterizing the evolution of key patterns of scientific publications on this problem. To achieve this goal, a relevant sample of scientific articles was formed based on identifying periods of publication activity and bibliometric analysis of keyword matches to identify promising areas of research in this area. The formed sample of publications for the study includes 606 documents indexed by the international scientometric database Scopus for the period 2011-2025. Bibliometric analysis and visualization of its results were carried out using the VOSviewer software product. Based on the visualization maps, seven clusters were identified and characterized by the content coincidence of keywords in the publications and five stages of the evolutionary development of artificial intelligence technologies for the effective functioning of critical infrastructure. Based on the analysis of empirical data, the exponential growth of the number of publications on the selected issues was confirmed (the annual growth rate of the number of scientific papers on this topic is 23.5% for 2011-2024). The results of the analysis can be used in further research to substantiate and develop an algorithm of actions for rapid response to crisis phenomena and adaptation of the functioning of critical infrastructure facilities to new global challenges.

1 INTRODUCTION

In today's dynamic environment, the development of critical infrastructure is becoming an integral part of the national economy of the world's countries. This is due to the fact that disruption of the operation of critical infrastructure facilities (energy, agro-industrial, transport, telecommunications, information networks, energy and water supply systems, etc.) can lead to significant economic losses. It should be noted that these systems are very vulnerable to various threats – from climatic and geological hazards to industrial accidents, terrorist attacks, cyber threats, armed conflicts and military actions, which can cause a cascading negative impact on different levels of management.

In this regard, there is an extremely urgent need to search and apply innovative and management approaches, smart technologies, information and intellectual systems, qualitatively new methods, tools and mechanisms for ensuring the development of critical infrastructure facilities. One of these mechanisms is digital transformation, which becomes the basis for achieving the outlined goals of sustainable development of critical infrastructure in the context of global changes [1; 2; 3]. It is worth emphasizing that the rethinking of the principles of functioning of critical infrastructure facilities and fundamental changes in their activities occur

through the creation of an appropriate ecosystem of artificial intelligence. According to Statista [4], the volume of the global artificial intelligence market increased from 93.3 to 184 billion dollars in 2020-2024, or by 97.2%. It is predicted that this growth will continue – the value of this indicator will be 243.7 billion dollars in 2025, 415.6 billion dollars in 2027, and 826.7 billion dollars in 2030 [4]. That is, the growth rate of the global artificial intelligence market will be 24.4% in 2020-2030.

According to AIPRM experts [5], the volume of public investment in artificial intelligence in the United States amounted to 328.5 billion dollars in 2019-2023. This is 195.8 billion dollars more than in China (132.7 billion), which took second place in the same period. The United Kingdom takes third place in the ranking with a value of this indicator of 25.5 billion dollars, which is 92.2% less than in the United States. India takes fourth place (16.1 billion), and Canada takes fifth place (12.5 billion dollars). In terms of "share of investment in artificial intelligence as a percentage of GDP," Singapore ranks first (15%), followed by Sweden (14.1%), the United States (12.9%), Estonia (10.9%), and the United Kingdom (8.3%) [5].

A study conducted in October 2024 by consulting firm PwC [6] found that 49% of global technology leaders indicated that artificial intelligence was fully integrated into their companies' core business strategy. The survey found that 63% of the most effective companies are increasing their cloud budgets to leverage Generative Artificial Intelligence (GenAI). And 34% of companies say that sustainability considerations are driving the expected budget increase. At the same time, 67% of successful companies are already realizing the value of using GenAI for innovative products and services. In addition, 73% of executives emphasize that they plan to use generative artificial intelligence in the future to make changes to their company's business model [6].

According to S. Ghimire [7], in the ever-changing landscape of critical infrastructure development, artificial intelligence is a transformative force that helps to achieve unprecedented efficiency, resilience, and innovation. By continuously monitoring the health of infrastructure components, artificial intelligence systems can predict maintenance needs, optimize repair schedules, and extend the life of critical assets. This proactive approach not only reduces costs, but also increases the reliability and security of infrastructure networks, making the development of critical infrastructure more sustainable.

As noted in the 2024 Workshop Report "Securing Critical Infrastructure in the Age of AI" by the Center for Security and Emerging Technology [8], the introduction of artificial intelligence can lead to the creation of more efficient systems, improved business operations, and better tools for detecting and responding to cyber threats. At the same time, artificial intelligence systems can cause new cyber threats [9], which suppliers of critical infrastructure facilities must deal with. And, first of all, it is necessary to assess the potential risks associated with the use of artificial intelligence in the involved sectors of critical infrastructure, which will allow monitoring and diagnosing the level of vulnerability of the system to critical failures, physical attacks and cyberattacks [8].

According to D. M. Gerstein & E. N. Leidy [10], artificial intelligence must be used to ensure national security and monitor critical infrastructure systems. However, a study conducted by NATO to monitor the ability of AI to protect critical infrastructure from cyberattacks found that AI can operate without human intervention, help identify patterns of cyberattacks on critical infrastructure and network activity, and detect malicious software to improve decision-making on defensive responses, while warning that many government agencies are neglecting critical infrastructure security, failing to implement most of the recommendations for its protection since 2010 [11].

Therefore, it is particularly relevant to substantiate the directions for ensuring cybersecurity and increasing the resilience of critical infrastructure facilities, as well as to study the relationship between artificial intelligence and the critical infrastructure development.

2 LITERATURE REVIEW

Various aspects of the development of critical infrastructure, substantiation of the conceptual foundations of modernization and theoretical and methodological approaches to increasing the efficiency of functioning in various sectors of the economy are among the scientific interests of many leading foreign scientists (C. Baudrit et al. [12]; S. Bruno, M. De Fino & F. Fatiguso [13]; D. Buhalis et al. [14]; C. Cath [15]; K. Dick et al. [16];

R. Doshi, N. Apthorpe & N. Feamster [17]; S. Feng et al. [18]; F. Filgueiras [19]; F. Santoso & A. Finn [20]; A. C. Serban & M. D. Lytras [21]; F. van der Vlist, A. Helmond & F. Ferrari [22] and others).

At the same time, paying tribute to the scientific achievements of scientists in the study of the selected issues, it should be noted that some issues of the development of critical infrastructure require further development and finding ways to solve them. And especially the solution of this problem is becoming more relevant due to the emergence of new challenges associated with the digital transformation of strategic sectors of the economy and the intensive use of artificial intelligence technologies.

Thus, this problem determined the purpose of this article, which is to identify the relationship between artificial intelligence and the development of critical infrastructure based on the characteristics of the evolution of key patterns of scientific publications on the selected topic.

3 METHODOLOGY

The theoretical and methodological basis of the study is the provisions of institutional theory, in particular the paradigm of evolutionary development; theories of systems, globalization, transaction costs, infrastructure; concepts of strategic management, national, information and cybersecurity, sustainable development. The study is based on systemic, structural-functional, linguistic, synergistic and logical-semantic approaches.

The information base of the study is analytical materials of AIPRM, Center for Security and Emerging Technology, CSO, Frost & Sullivan Institute, Homeland Security Operational Analysis Center, PwC, Statista, which highlight the results of surveys and statistical analysis on the problems of the impact of artificial intelligence on the management of the development of critical infrastructure.

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

The study selected bibliometric analysis as a method that reveals the connection between artificial intelligence and the development of critical infrastructure. This type of analysis is based on the mathematical theory of graphs, clustering methods and scientific visualization, which makes it widely applicable in various fields of science [1].

Based on the structuring of a large volume of metadata of scientific publications, bibliometric analysis allows us to identify the essence of the subject area and its conceptual foundations and to substantiate the evolution of the research area [1]. The research methodology includes such main stages as data collection and analysis, selection of a visualization tool, graphical representation of the identified connections and interpretation of the results obtained.

This was implemented using the software product VOSviewer v.1.6.19. The functionality of this program involves creating keyword visualization maps based on compatibility data, maps of authors or countries based on the number of citations, etc. [3]. In addition, network visualization maps in VOSviewer are displayed in several ways (for example, by content criterion, by publication period) [1].

An important stage of bibliometric analysis, which ensures its quality, is the selection of a data source and the form of a relevant sample of publications. The Scopus database was chosen as a data source due to the breadth of its coverage of such subject areas as computer science; engineering; social sciences; energy; decision sciences; environmental sciences; business, management and accounting; economics, econometrics and finance, etc. To form the data sample, the chronology of the release of 642 publications was first determined for the search query “Artificial Intelligence” (or AI) and “Critical Infrastructure Development” for the years 1990-2025, and then the period of publication activity of the topic under study, namely from 2011 to 2025. Secondly, the sample was limited by the stage of publication, that is, only published works were taken. The key categories for selecting scientific publications were the title, abstract and keywords for them. Therefore, the studied sample of publications included 606 works that met the above criteria, published in the period 2011-2025 and indexed by the Scopus database.

4 RESULTS

Quantitative analysis of the formed sample of scientific works showed an exponential growth of research in the context of the relationship between artificial intelligence and the development of critical

infrastructure during the period 2011-2025 (Fig. 1). On average, the growth rate of the number of publications was 23.5% for 2011-2024. At the same time, it can be assumed that by the end of 2025 there will also be a trend of significant growth in the number of publications on the specified topic compared to previous years. According to preliminary estimates, the annual growth rate of the number of publications for 2011-2025 will be 10.7%.

As the analysis shows, the following keywords are mostly used in the publications: Artificial Intelligence (364 documents), Machine Learning (92), Internet of Things (58), Decision-Making (54), Decision Support Systems (52), Sustainable Development (49), Critical Infrastructures (41), Cybersecurity (40), Network Security (33), Risk Assessment (28), Learning Systems (28), Big Data (24), Climate Change (23), Blockchain (23), Automation (23), Sustainability (22), Smart City (22), Information Management (21), Learning Algorithms (20), Investments (20), 5G Mobile Communication Systems (20), Risk Management (19), Digital Storage (19), AI (19), Cost Effectiveness (17), Infrastructure (15 documents) etc.

In addition, it is advisable to study the geographical structure of scientific works on the development of critical infrastructure using artificial intelligence technologies (Fig. 2). According to the geographical structure, the leaders are countries such as United States (134 documents), India (79), China (61), United Kingdom (52), Italy (36), Germany (26), South Africa (24), Spain (23), Saudi Arabia (22), Canada (21), France (17), Malaysia (17), Netherlands (15 documents).

However, the overwhelming number of publications by researchers from India, Canada, China, and Italy is inferior in terms of citation level to the USA, Great Britain, and France. Thus, each article by scientists from the USA, Great Britain, and France is cited on average 20 times. This is more than 4 times the value of this parameter for representatives from India (on average 5 times), 1.5 times for scientists from Canada (on average 13 times), 1.3 times for China and Italy (on average 15 times).

In our opinion, it is important to determine the most cited works devoted to the study of the impact of artificial intelligence on the development of critical infrastructure (Table 1). According to the data in Table 1, the work of D. Buhalis et al. [14], published in 2019, has the largest number of citations. And to date, this work has 636 citations. This work is devoted to the study of technological changes (Internet of Things, autonomous devices, advanced analytical capabilities (artificial intelligence), virtual and augmented reality), which create a smart environment that transforms industry structures and processes of critical infrastructure facilities.

The second place is taken by the publication of the authors R. Doshi, N. Apthorpe, N. Feamster [17], which considers new methods for automatic detection of consumer traffic of IoT attacks on critical information infrastructure.

In third place is the publication by C. Cath [15], which has been cited 279 times. In this article, the author pays attention to the ethical, legal and technical possibilities of artificial intelligence, as well as the risks and challenges of its application in various areas of economic activity.

Table 2 shows the Top 5 journals with the largest number of publications on artificial intelligence and critical infrastructure development, indexed in the international scientometric database Scopus. The largest number of articles was published in the journal “Lecture Notes in Computer Science including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics”. The first article on the topic was published in 2008 and is devoted to the study of the issue of developing adaptive software to be used in high-level reliability systems, such as critical infrastructure management and protection systems [23].

Among universities and scientific institutions whose researchers have studied the impact of artificial intelligence on the development of critical infrastructure, the leading position is occupied by University of Johannesburg (10 documents), Southeast University (6), Tsinghua University (6), Virginia Polytechnic Institute and State University (6), Stanford University (5), National Technical University Kharkiv Polytechnic Institute (5), ETH Zürich (5), University of Cambridge (5), Virginia Tech College of Engineering (5 documents).

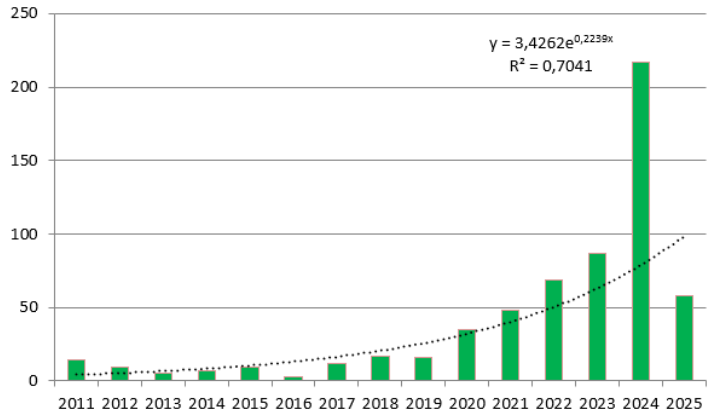

Figure 1: Dynamics of publications on artificial intelligence and critical infrastructure development for 2011-2025.

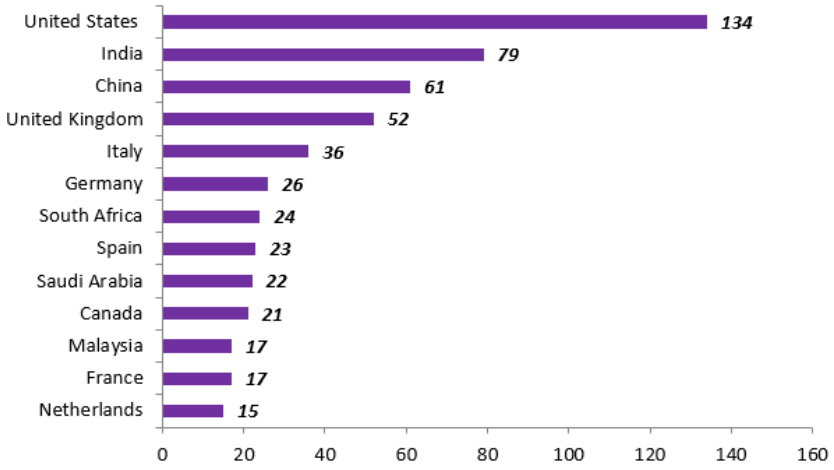

Figure 2: Geographic structure of scientific publications search query “artificial intelligence” and “critical infrastructure development”.

Table 1: Ranking of scientific papers by number of citations [13; 14; 15; 17; 18].

Title	Author(s)	Year	Source	Number of citations
Technological disruptions in services: lessons from tourism and hospitality	D. Buhalis et al.	2019	Journal of Service Management	636
Machine learning DDoS detection for consumer internet of things devices	R. Doshi, N. Apthorpe, N. Feamster	2018	2018 IEEE Symposium on Security and Privacy Workshops	602
Governing artificial intelligence: Ethical, legal and technical opportunities and challenges	C. Cath	2018	Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences	279
Dense reinforcement learning for safety validation of autonomous vehicles	S. Feng et al.	2023	Nature	240
Historic Building Information Modelling: performance assessment for diagnosis-aided information modelling and management	S. Bruno, M. De Fino, F. Fatiguso	2018	Automation in Construction	224

Table 2: Top 5 journals with the largest number of publications on the selected research topic, indexed in the scientometric database Scopus.

Journal Title	Indexing Period	Publisher	Field of Knowledge	Cite Score 2023	SJR 2023	SNIP 2023	Number of Articles
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	from 1973 to the present	Springer Nature	Computer Science: General Computer Science; Mathematics: Theoretical Computer Science	2.6	0.606	0.590	16
Lecture Notes in Networks and Systems	from 2016 to the present	Springer Nature	Computer Science: Signal Processing; Engineering: Control and Systems Engineering; Computer Science: Computer Networks and Communications	0.9	0.171	0.282	11
Sustainability (Switzerland)	from 2009 to the present	Multidisciplinary Digital Publishing Institute (MDPI)	Social Sciences: Geography, Planning and Development; Computer Science: Computer Networks and Communications, Hardware and Architecture; Environmental Science: Management, Monitoring, Policy and Law; Energy: Renewable Energy, Sustainability and the Environment etc.	6.8	0.672	1.086	10
ACM International Conference Proceeding Series	1993, from 1996 to 1997, from 1999 to 2023	-	Computer Science: Computer Networks and Communications, Computer Vision and Pattern Recognition, Software, Human-Computer Interaction	1.5	0.253	0.233	9
IEEE Access	from 2013 to the present	IEEE	Engineering: General Engineering; Computer Science: General Computer Science; Materials Science: General Materials Science	9.8	0.960	1.440	8

The institutions that most fund research by scientists on critical infrastructure development problems using artificial intelligence tools include the following: European Commission (22 documents), National Natural Science Foundation of China (20), UK Research and Innovation (17), National Science Foundation (15), Ministry of Science and Technology of the People's Republic of China (14), Horizon 2020 Framework Programme (12), U.S. Department of Defense (7), Horizon 2020 (6), U.S. Department of Energy (6 documents).

The ranking of scientific papers by document type is given in Table 3. As we can see, scientists mostly test the obtained research results during conferences of various levels and highlight them in scientific articles.

Table 3: Number and share of scientific publications by document type.

Type of publication	Number of publications	Share of publications, %
Conference Paper	248	38.6
Article	224	34.9
Review	74	11.5
Book Chapter	60	9.3
Conference Review	15	2.3
Book	13	2.0

Most scientific papers devoted to identifying the impact of artificial intelligence on the development of critical infrastructure are published in the following fields of knowledge: Computer Science (342 documents), Engineering (296), Social Sciences (115), Energy (81), Mathematics (80), Environmental Science (72), Medicine (52), Decision Sciences (49), Business, Management and Accounting (46 documents) (Table 4). All this indicates the multifaceted and multidisciplinary nature of the chosen research topic.

Table 4: Share of scientific publications by key fields of knowledge.

Field of knowledge	Share of scientific publications, %
Computer Science	24.8
Engineering	21.4
Social Sciences	8.3
Energy	5.9
Mathematics	5.8
Environmental Science	5.2
Medicine	3.8
Decision Sciences	3.6
Business, Management and Accounting	3.2

Based on the results of the analysis of the coincidences and closeness of the relationship between the keywords of the selected sample of publications, network visualization maps were constructed (Fig. 3 and Fig. 4), and 7 clusters on the studied topic were identified and characterized (Fig. 3).

The first cluster (red colour, Fig. 3) contains the largest number of terms (namely 48 positions), among which the following can be mentioned: “artificial intelligence”, “decision support system”, “information technology”, “decision-making”, “risk management”, “information systems”, “infrastructure development”, “disasters”, “project management”, “critical challenges”, “critical success factor”, “telecommunication networks”. It is worth noting the keyword “Artificial Intelligence”, the frequency of its co-use in the studied sample is 364, and the strength of the connection is 1945.

The second cluster (46 concepts, green colour. Fig. 3) combines such terms as “AI”, “climate change”, “cost effectiveness”, “digital technologies’, “energy policy”, “energy management”, “Industry 4.0”, “IoT”, “machine learning”, “renewable energy”, “smart city”, “smart grid”, “strategic planning”, “sustainable development”. In this cluster, the keyword “Internet of Things” has the highest frequency – the ratio is 58, while the strength of the association is 393.

The third cluster (45 elements, blue colour, Fig. 3) describes the connection between artificial intelligence and the critical infrastructure development with the following terms: “5G mobile communication system”, “artificial intelligence technologies”, “blockchain”, “cybersecurity”, “national security”, “network security”, “security systems”. The main keyword in this cluster is “Cybersecurity”, the frequency of its co-use in the studied sample of scientific publications is 40, and the strength of the association is 290.

The fourth cluster (41 elements, yellow colour, Fig. 3) is associated with the following categories: “algorithms”, “Big Data”, “data analysis”, “diagnosis”, “industrialization”, “infrastructure”. The keyword “Human” has the highest frequency of co-use – 49, while the strength of the association is 424.

The fifth cluster (41 elements, purple colour, Fig. 3) covers the following categories: “anomaly detection”, “cloud computing”, “cloud platforms”, “deep learning”, “digital storage”, “digital transformation”, “digitalization”, “intelligent systems”, “life cycle”, “predictive analytics”, “real time systems”, “transport infrastructure”. The frequency of co-use of the main keyword “Machine Learning” in this cluster is 92, and the strength of association is 604.

The sixth cluster (38 elements, turquoise colour, Fig. 3) is associated with the concepts of critical infrastructure, critical infrastructure protection, risk analysis, digital twin, generative AI, risk assessment, AI systems. The seventh cluster (16 categories, orange colour, Fig. 3) includes such concepts as automation, computer crime, cyber physical system, damage detection etc.

Therefore, based on the constructed terminological map of categories and the most significant keywords identified related to artificial

intelligence issues in critical infrastructure development management, it can be stated that the areas under study are multidimensional and interdependent, since there are numerous connections between terms, as well as their high prevalence in research.

According to the results of bibliometric analysis in the evolutionary and temporal dimensions, it can be stated that in the development of scientific research related to the development of critical infrastructure using artificial intelligence tools, five most significant stages can be distinguished (Fig. 4).

The first stage of development was observed until 2016, when most publications considered general issues of forming networks and decision support systems using data analysis technologies.

In the second stage, which lasted from 2016 to 2018, the focus of the scientists' research shifted to the terms “critical infrastructure”, “information management”, “decision-making”.

From 2018 to 2020, that is, in the third of the selected stages, the dominant key terms were “artificial intelligence”, “robotics”, and “metadata”. The fourth stage (from 2020 to 2022) is characterized by the predominance of the terms – “Big Data”, “human”, “intrusion detection systems”.

The last, fifth stage began from 2022 to 2024. According to the results of its analysis, it can be stated that the main terms in the study were: “cybersecurity”, “cyber threats”, “smart grid”, “machine learning”, “IoT”, “blockchain”, “denial-of-service attack” and others.

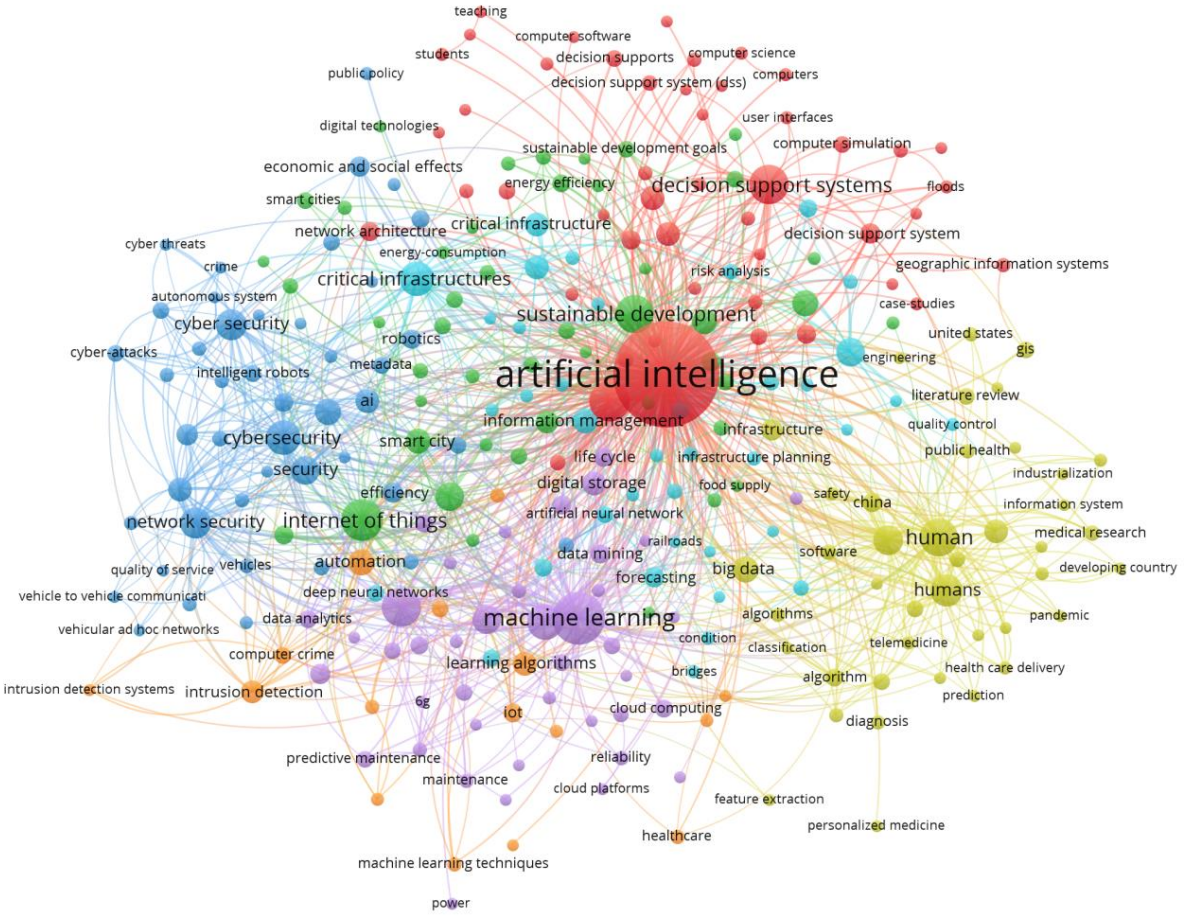

Figure 3: Visualization map of bibliometric analysis of publications that highlight the impact of artificial intelligence on the development of critical infrastructure (content aspect).

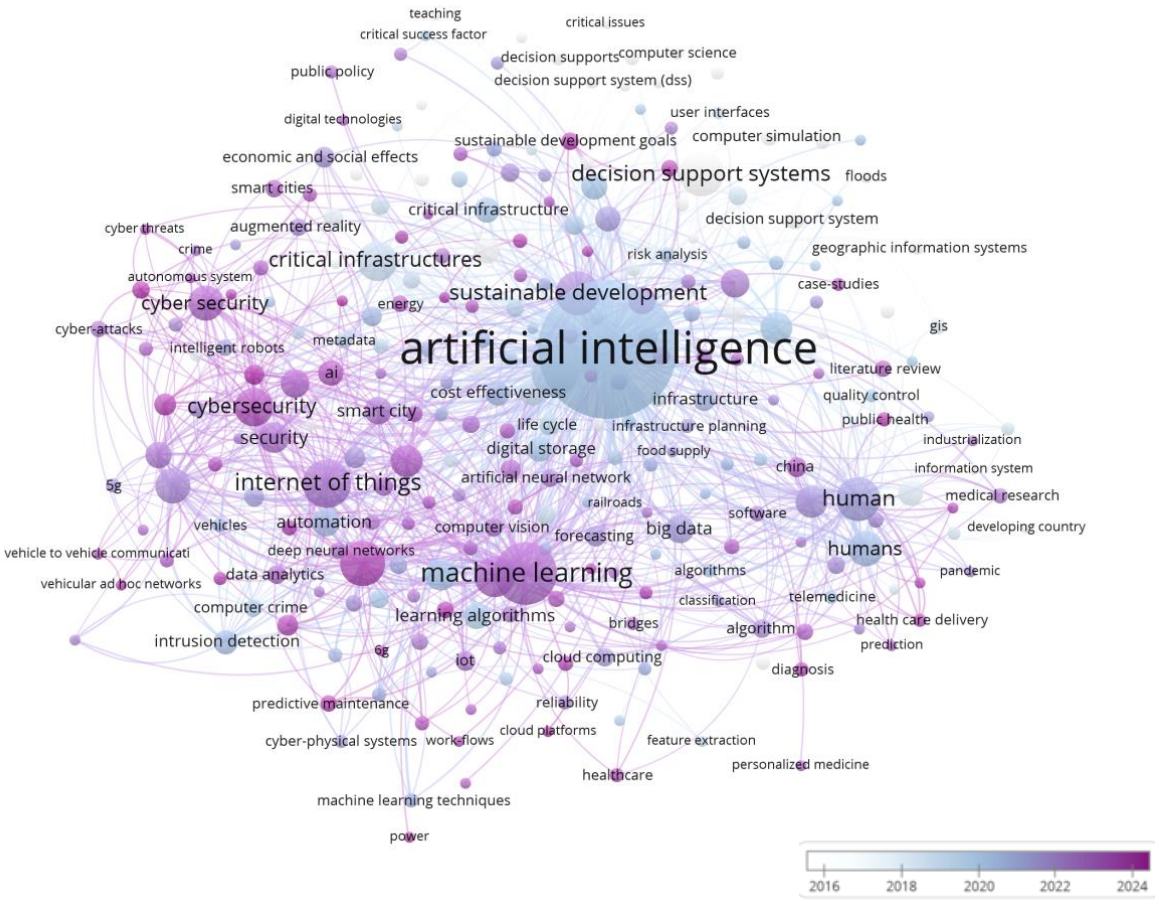

Figure 4: Visualization map of bibliometric analysis of publications that highlight the impact of artificial intelligence on the development of critical infrastructure (evolutionary and temporal aspects).

Thus, summing up the above, we can trace a change in emphasis in scientific publications, caused by the development and improvement of information technologies (from the already traditional ones: “Internet”, “software”, “information systems”, common at the first – third stages (Fig. 4) to the increasing importance of artificial intelligence tools at the fourth – fifth stages. The widespread use of modern technologies has led to the emergence of new phenomena and areas of scientific research, such as “information security management”, “critical infrastructure development management”, “cybersecurity”, “artificial intelligence”, “machine learning”, etc., which determines the importance of simultaneous study of the subject area in the context of digital transformations.

5 CONCLUSIONS

Based on the purpose and results of the study, we can conclude that there is a high level of closeness between the concepts of “Artificial Intelligence” and “Critical Infrastructure Development”. Thus, empirical data showed an exponential growth of research in the context of the relationship between artificial intelligence and the development of critical infrastructure (the annual growth rate of the number of scientific papers on this topic is 23.5% for 2011-2024, and 10.7% for 2011-2025). Therefore, it can be assumed that, in accordance with the dialectical law, the accumulated quantitative changes will turn into qualitative ones, which will lead to the complementarity and mutual stimulation of these factors.

This article provides a bibliometric analysis of scientific publications indexed in the international scientometric database Scopus, which highlight aspects of the application of artificial intelligence technologies to improve the efficiency of the development of critical infrastructure. This analysis made it possible to identify current trends in publication activity on the selected research topic. Using the VOSviewer software, network visualization maps of keyword matches of publications indexed by the international scientometric database Scopus from 2011 to 2025 were created.

Based on the semantic correspondence of the keywords of the studied sample, seven clusters were identified and described, and the presence of five most significant stages of the development of scientific research dedicated to identifying the relationship between artificial intelligence and the development of critical infrastructure was established.

This, in turn, provides an opportunity to expand theoretical knowledge on managing the development of critical infrastructure as an object of economic research. In addition, it also gives impetus to the development of a modern methodology for the formation and implementation of a strategy for the protection and security of critical infrastructure objects using artificial intelligence technologies and information systems.

Prospects for further research are to substantiate the feasibility of applying an integrated approach to managing the risks of critical infrastructure development in a changing security environment.

REFERENCES

[1] A. Kwilinski, “The relationship between sustainable development and digital transformation: Bibliometric analysis,” Virtual Econ., vol. 6, no. 3, pp. 56–69, 2023, [Online]. Available: https://doi.org/10.34021/ve.2023.06.03(4).

[2] D. Pudryk et al., “Towards achieving sustainable development: Interactions between migration and education,” Forum Sci. Oecon., vol. 11, pp. 113–132, 2023, [Online]. Available: https://doi.org/10.23762/FSO_VOL11_NO1_6.

[3] V. Khaustova, M. Kyzym et al., “Digital transformation of energy infrastructure in the conditions of global changes: Bibliometric analysis,” in Proc. 12th Int. Conf. Appl. Innov. IT (ICAIIT), Koethen, Germany, Mar. 7, 2024, vol. 12, no. 1, pp. 135–142, [Online]. Available: http://dx.doi.org/10.25673/115664.

[4] Artificial intelligence (AI) market size worldwide from 2020 to 2030 (in billion U.S. dollars), Statista, Nov. 28, 2024, [Online]. Available: https://www.statista.com/forecasts/1474143/global-ai-market-size.

[5] AI Statistics 2024, AIPRM, [Online]. Available: https://www.aiprm.com/ai-statistics/.

[6] 2025 AI Business Predictions, PwC, 2025, [Online]. Available: https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-predictions.html.

[7] S. Ghimire, “The role of AI in infrastructure development of developed nations,” Frost & Sullivan Institute, Jan. 22, 2025, [Online]. Available: https://frostandsullivaninstitute.org/the-role-of-ai-in-infrastructure-development-of-developed-nations/.

[8] K. Crichton et al., Securing Critical Infrastructure in the Age of AI. Workshop Report, Center for Security and Emerging Technology, Oct. 2024, [Online]. Available: https://cset.georgetown.edu/wp-content/uploads/CSET-Securing-Critical-Infrastructure-in-the-Age-of-AI.pdf.

[9] A. Kwilinski and N. Trushkina, “Impact of cyber risks and threats on the critical infrastructure development: Visualization of scientific research,” in Proc. 12th Int. Conf. Appl. Innov. IT (ICAIIT), vol. 12, no. 2, pp. 107–119, 2024, [Online]. Available: http://dx.doi.org/10.25673/118123.

[10] D. M. Gerstein and E. N. Leidy, Emerging Technology and Risk Analysis Artificial Intelligence and Critical Infrastructure, Homeland Security Operational Analysis Center, 2024, [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2800/RRA2873-1/RAND_RRA2873-1.pdf.

[11] M. Hill, “NATO tests AI’s ability to protect critical infrastructure against cyberattacks,” CSO, Jan. 5, 2023, [Online]. Available: https://www.csoonline.com/article/574281/nato-tests-ai-s-ability-to-protect-critical-infrastructure-against-cyberattacks.html.

[12] C. Baudrit et al., “Artificial intelligence and non-destructive testing data to assess concrete sustainability of civil engineering infrastructures,” Materials, vol. 18, no. 4, p. 826, 2025, [Online]. Available: https://doi.org/10.3390/ma18040826.

[13] S. Bruno, M. De Fino, and F. Fatiguso, “Historic Building Information Modelling: Performance assessment for diagnosis-aided information modelling and management,” Autom. Constr., vol. 86, pp. 256–276, 2018, [Online]. Available: https://doi.org/10.1016/j.autcon.2017.11.009.

[14] D. Buhalis et al., “Technological disruptions in services: Lessons from tourism and hospitality,” J. Serv. Manag., vol. 30, no. 4, pp. 484–506, 2019, [Online]. Available: https://doi.org/10.1108/JOSM-12-2018-0398.

[15] C. Cath, “Governing artificial intelligence: Ethical, legal and technical opportunities and challenges,” Philos. Trans. A Math. Phys. Eng. Sci., vol. 376, no. 2133, p. 20180080, 2018, [Online]. Available: https://doi.org/10.1098/rsta.2018.0080.

[16] K. Dick et al., “Deep learning for critical infrastructure resilience,” J. Infrastruct. Syst., vol. 25, no. 2, p. 05019003, 2019, [Online]. Available:

https://doi.org/10.1061/(ASCE)IS.1943-555X.0000477.

[17] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," in Proc. 2018 IEEE Symp. Secur. Priv. Workshops, pp. 29–35, 2018, [Online]. Available: https://doi.org/10.1109/SPW.2018.00013.

[18] S. Feng et al., "Dense reinforcement learning for safety validation of autonomous vehicles," Nature, vol. 615, no. 7953, pp. 620–627, 2023, [Online]. Available: https://doi.org/10.1038/s41586-023-05732-2.

[19] F. Filgueiras, "Artificial intelligence governance challenges in Latin America: Infrastructure, decolonization and new dependency," Reforma y Democracia, no. 87, pp. 44–70, 2023, [Online]. Available: https://doi.org/10.69733/clad.ryd.n87.a3.

[20] F. Santoso and A. Finn, "An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures," IEEE Trans. Serv. Comput., vol. 17, no. 3, pp. 1293–1311, 2024, [Online]. Available: https://doi.org/10.1109/TSC.2023.3331083.

[21] A. C. Serban and M. D. Lytras, "Artificial intelligence for smart renewable energy sector in Europe – Smart energy infrastructures for next generation smart cities," IEEE Access, vol. 8, pp. 77364–77377, 2020, [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2990123.

[22] F. van der Vlist, A. Helmond, and F. Ferrari, "Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence," Big Data Soc., vol. 11, no. 1, 2024, [Online]. Available: https://doi.org/10.1177/20539517241232630.

[23] H. J. Goldsby, B. H. C. Cheng, and J. Zhang, "AMOEBA-RT: Run-time verification of adaptive software," Lect. Notes Comput. Sci., vol. 5002, pp. 212–224, 2008, [Online]. Available: https://doi.org/10.1007/978-3-540-69073-3_23.