Economic Affairs, Vol. **69**(Special Issue), pp. 43-51, February 2024
DOI: 10.46852/0424-2513.1.2024.6

AESSRA

Review Paper

The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats

Serhii Lysenko[1*], Natalia Bobro[2], Kateryna Korsunova[3], Oleksandra Vasylchyshyn[4] and Yehor Tatarchenko[5]

[1]Institute of Security, Interregional Academy of Personal Management, Kyiv, Ukraine
[2]Department of Economics, Finance and Accounting, European University, Kyiv, Ukraine
[3]Department of International Economic Relations, Simon Kuznets Kharkiv National University of Economics Kharkiv, Kharkiv, Ukraine
[4]Department of Security and Law Enforcement, West Ukrainian National University, Ternopil, Ukraine
[5]Volodymyr Dahl East Ukrainian National University, Kyiv, Ukraine

*Corresponding author: crimeconsult@ukr.net (**ORCID ID:** 0000-0002-7050-5536)

Received: 21-10-2023 **Revised:** 29-01-2024 **Accepted:** 07-02-2024

ABSTRACT

The trend of increasing attacks on information systems is gaining momentum globally. Traditional means of counteracting cyberattacks are currently unable to withstand the current situation. Therefore, AI-based technologies are seen as an effective solution to the problem. The study aims to provide a comprehensive substantiation of applying artificial intelligence tools in the cybersecurity system to automate the protection and timely detection of threats. The research was carried out using general scientific methods of cognition: logical and structural analysis, induction and deduction, comparison, abstraction, specification, generalization, and formalization. The article proves that AI technologies allow the implementation of highly effective solutions, efficiently and quickly identify cyberattacks, choose the optimal response to security incidents, assess their consequences, and determine the way to respond in a real-time manner. It is established that artificial intelligence systems play a key role in improving information security protocols while eliminating the risks of the human factor. The authors considered the main types of AI technologies used in the cybersecurity system. The paper emphasizes the high efficiency of decision-making with the help of artificial intelligence technologies in terms of threat identification, risk prevention, and protection automation. The authors have highlighted the risks and challenges of using artificial intelligence in information security systems. It is proved that the use of AI capabilities in cybersecurity actualizes the strategy of the concept of integrated formation of effective counteractions to external and internal threats. The practical value of research findings lies in the possibility of their use when actualizing the role of AI technologies in the formation of an effective cybersecurity system, given their apparent advantages and possible shortcomings.

HIGHLIGHTS

- Artificial intelligence has become an indispensable force in bolstering information security, with its ability to effectively analyze and identify threats, transforming the landscape of digital security protocols.
- The integration of artificial intelligence in cybersecurity not only enhances threat detection, incident response, and preventive measures but also presents challenges such as the potential misuse of AI by cybercriminals, highlighting the critical need for ongoing research and innovation in the field.

Keywords: Information security, artificial intelligence methods, decision support system, identification, analytics, data security

How to cite this article: Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O. and Tatarchenko, Y. (2024). The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats. *Econ. Aff.*, **69**(Special Issue): 43-51.

Source of Support: None; **Conflict of Interest:** None

In the era of technology-driven society, the convergence of artificial intelligence and cybersecurity is at the forefront of innovative searches. These two significant spheres of influence, acting in synergy, allow for the transformation of the basis of digital security.

Many scientific studies by both Ukrainian and foreign scholars have been devoted to the application of AI technologies and information security issues. They focus mainly on the intersection of cybersecurity and artificial intelligence (Karchevskyi *et al.* 2023), as well as on the theoretical and practical aspects of AI technologies application in cybersecurity (Saienko, 2023). The most comprehensive studies of the recent period are the studies by Neretin O. and Kharchenko V. (2022). They present the concept and typical features of information security by analyzing vulnerabilities, attacks, and countermeasures involving AI tools.

Some modern studies analyze the capabilities of AI tools in the field of information security (Sukaylo *et al.* 2023). Several scholars (Skitsko *et al.* 2023) have highlighted typical threats and risks that accompany the active use of AI systems in cyber defense.

However, given the viewpoints of the aforementioned authors, it should be noted that in the context of the constant dynamic impact of external and internal factors, there is a lack of research on artificial intelligence in the field of information security as a priority promising component of cyber defense. Many aspects of the studied issues remain understudied and require further research.

The article aims to analyze the role of artificial intelligence in cybersecurity, including in terms of threat identification and the formation of automated defense systems.

Literature Review

A solid scientific and theoretical basis has been formed in the field of artificial intelligence technologies in the cyber defense system. It includes scientific publications in professional journals, dissertations, monographs, and the results of theoretical and practical developments in this field.

The scientific and methodological basis of the studied issues is formed by researchers who have focused on the functional tools of AI, as well as on the problems of protecting information data from unauthorized access (Sarker *et al.* 2020).

In particular, scientists have thoroughly developed the principles of a threat identification system (Abbas *et al.* 2019; Sarker *et al.* 2021). Also, they have developed an algorithm for detecting, evaluating, and compensating malicious attacks in nonlinear cyber-physical systems (Farivar *et al.* 2020). Various studies have highlighted the possibilities of automating protective measures through AI (Tan *et al.* 2022; Shaukat *et al.* 2020). The issues of ethical use of AI with respect to confidential data are studied in the studies of certain scientists (Kanimozhi *et al.* 2019). Some economic aspects of using machine learning and AI technologies in cybersecurity are focused on by several modern scholars (Wan *et al.* 2022; Cheatham *et al.* 2019).

It should be noted that the results of the scientific research of the aforementioned authors do not sufficiently analyze the feasibility of using in the context of automated data protection and rapid threat identification. This enables the formation of a comprehensive concept of cybersecurity, quick response to new challenges, and the development of a complex of preventive protection against cyberattacks. In this regard, the search for an optimal model for using AI capabilities in the information security system is a promising direction of research.

MATERIALS AND METHODS

While working on this article, a set of general scientific research methods was applied. In particular, the authors used the methods of analysis, synthesis, abstraction, induction and deduction, comparison, specification, and formalization. The theoretical and methodological basis of the current study is made up of relevant publications in professional journals, manuals, materials of scientific conferences and dissertation research, monographs, and conclusions of practical and analytical developments of modern scholars.

The research was carried out under the principles of systematic analysis and complexity. Such principles allowed us to analyze the research object as a system with a corresponding set of interconnections.

The methods of analysis and synthesis were used to identify the factors of functioning of the process under study, its defining elements, and vectors of influence.

The method of comparison was employed to identify the specific characteristics of AI technologies in terms of cybersecurity, compared to traditional approaches to the implementation of information security policy.

The method of abstraction was used to formulate theoretical generalizations, identify the main concepts and categories, and draw conclusions about the feasibility of using AI tools in cybersecurity.

The formalization method was used to identify priority vectors for the involvement of AI technologies in cybersecurity algorithms, as well as in the process of structuring the functionality, principles, priorities, and limitations of the object under study.

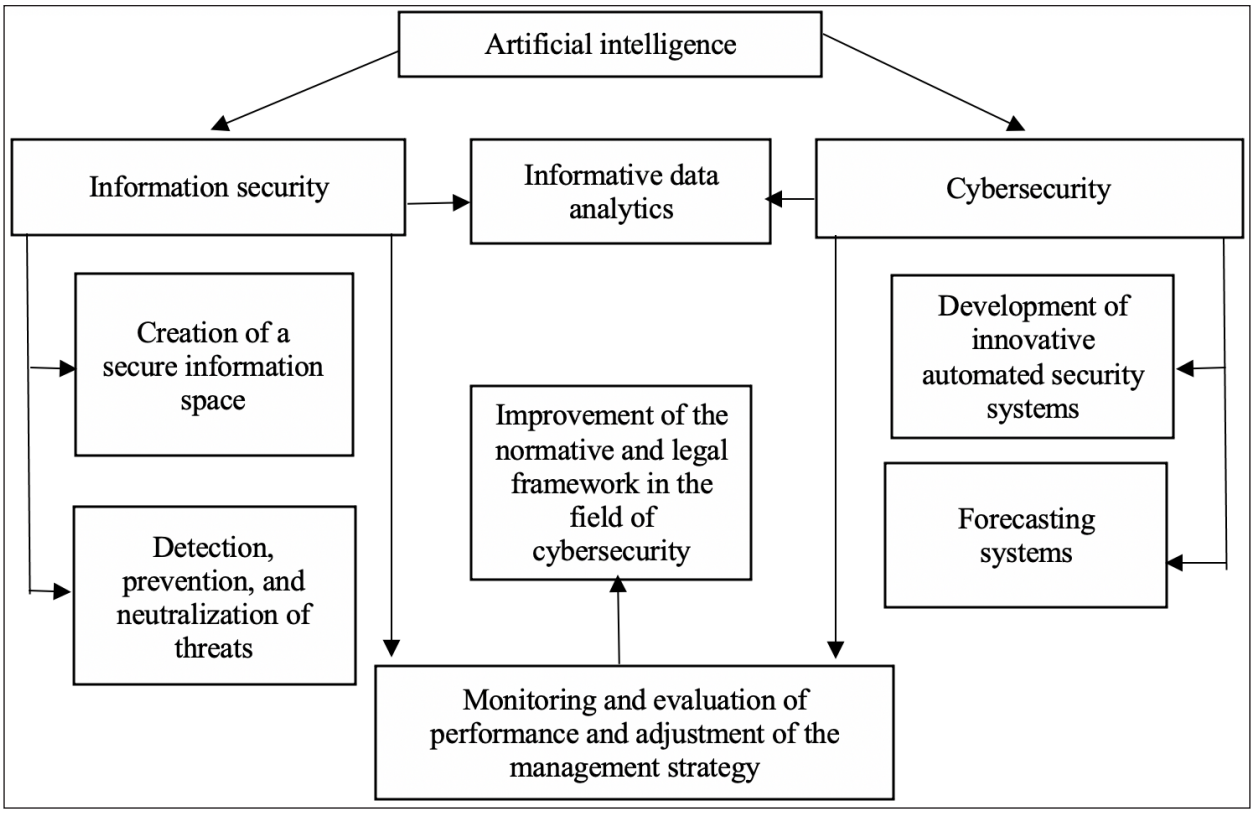
The deductive method was applied to identify proposals for the implementation of the concept of using artificial intelligence capabilities as an effective tool for information security policy. The inductive method was used to formulate prognostic directions for the development of the studied process.

The method of concretization was employed to prove the feasibility and effectiveness of the systematic, integrated use of artificial intelligence technologies and tools in cybersecurity policy to automate protection and identify potential threats.

RESULTS

The introduction of artificial intelligence-based tools and methods in cybersecurity operations is now positioned as a relevant strategy. It is a compulsory necessity to counter cyberattacks that are becoming even more unpredictable (Prasad *et al.* 2020). This trend is confirmed by statistics that show that by 2025, 63% of organizations plan to integrate AI. Moreover, 69% of them believe that it is only possible to respond effectively to cyber threats with the help of AI (Alhayani *et al.* 2021).

The growing importance of artificial intelligence in cybersecurity strategy indicates its significant potential in optimizing threat detection, response time, and overall resilience to hostile intrusions. Today, AI-powered tools are widely used to identify, monitor, and effectively respond to cyberattacks (Fig. 1). At the same time, they are characterized by significant levels of speed and accuracy.



Source: *The authors.*

Fig. 1: The potential of AI technologies in cyber defense

Cybersecurity solutions with AI capabilities help to identify anomalous activity and other suspicious actions with appropriate notification of the management system. In addition, AI should be used to analyze web traffic to detect malicious activities. It prevents malicious code from entering the information system, as well as notices and blocks identified malicious requests (Singh *et al.* 2020). AI helps to create strong passwords and encryption keys, as well as to record suspicious users' activity.

Systems based on artificial intelligence tools are considered to be effective tools for detecting and responding to phishing attacks and other types of social engineering. They are also used to identify and respond to denial of service attacks (Fatemidokht *et al.* 2021). At the same time, the source and type of attack are determined, as well as ways of minimizing damage. In addition, as practice shows, AI-based technologies should be used to detect and neutralize zero-day exploits. In other words, they are focused on previously unknown software vulnerabilities (Zhang *et al.* 2022).

The current level of technological development necessitates the search for innovative capabilities of AI tools. Intrusion detection systems (IDS) based on artificial intelligence use advanced algorithms to identify anomalous behavior. It results in a more reliable and comprehensive security solution (Taddeo *et al.* 2019). The purpose of such systems is to detect malicious activity and promptly notify security specialists about potential threats.

The advantages of artificial intelligence-based IDSs include the ability to identify specific innovative threats that are not available to traditional IDSs (e.g., zero-day attacks), as well as the function of real-time analytics of known amounts of information for effective and efficient threat detection (Ansari *et al.* 2022). AI-based IDSs can dynamically learn from the data they accumulate, adjusting the underlying identification algorithms. By automating the identification and analysis of potential threats, AI-based IDSs reduce the workload of security specialists. They free up resources to create a preventive defense system (Soni, 2020).

Such a concept of operation allows AI-based IDSs to work proactively and detect new threats before they can cause any damage. In general, AI-based intrusion detection systems provide a comprehensive solution to information security.

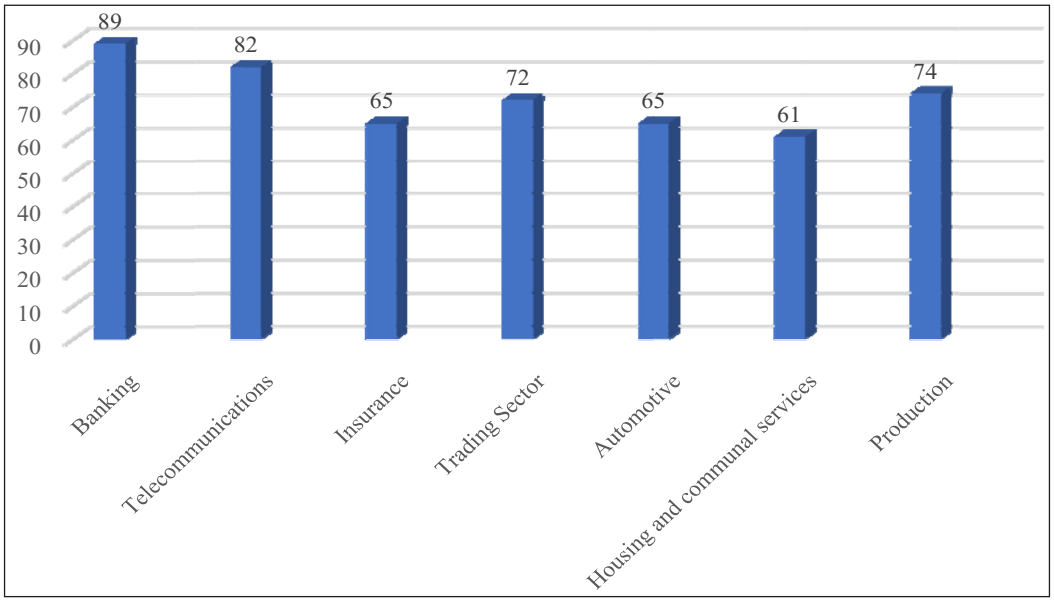
Another critical issue in today's technocratic world is the need for data loss prevention (DLP) to optimize cybersecurity. Such solutions enable organizations to identify, manage, and optimally protect informative data from accidental or malicious loss on time (Geluvaraj *et al.* 2019). AI-powered DLP solutions combine advanced analytics, machine learning, and natural language processing to identify patterns and anomalies in data sets, as well as provide proactive warnings of potential data loss or risk of misuse. The use of AI-based DLP solutions opens up the following opportunities:

- to detect the use of confidential data for unauthorized purposes;
- to prevent data transfer to unauthorized destinations;
- to control the actions of users who have access to confidential information;
- to warn organizations about potential data leaks (Mishra *et al.* 2023).

Among the positive effects of using AI-enabled DLP solutions are high speed of response to threats, minimization of information security management costs, reduction of the risk of data loss or unauthorized use, and time savings for regular monitoring and security audits. Due to the ability to quickly identify threats and notify the organization of potential data loss or misuse, AI-based DLP solutions are considered an essential tool for optimizing cybersecurity.

According to Capgemini's assessment, if by 2019 the AI toolkit was used for cybersecurity issues by 20% of organizations, then in 2023, AI capabilities would be used to improve cybersecurity by more than 77%. Today, most of the leading companies of the developed countries of the world see the possibilities of artificial intelligence as an irreplaceable protection against cyber threats (Fig. 2).

The latest area of AI application is to improve the cybersecurity of cloud providers by automating the analysis and detection of potential threats, tracking anomalies in information data and traffic patterns, and predictive security based on the analysis of data from previous security incidents. Such prerequisites enable cloud providers to take preventive measures to prevent and mitigate risks. By leveraging the power of artificial intelligence, they are able to



Source: *Author's development based on statistical data (Capgemini, 2023).*

Fig. 2: Share of organizations in the global community that use AI capabilities to protect cyber security

optimally control and manage user access to informative data and resources. This guarantees selective access to sensitive data. An additional positive bonus is the increased accuracy and speed of security checks, as well as the analytics of log data to identify potential security issues.

As a result, cloud providers can quickly identify and eliminate potential threats, minimizing the risk of data breaches. It should be noted that the application of artificial intelligence and machine learning for cloud security is rapidly gaining momentum. This creates a secure environment for data storage and access (Alrfai *et al.* 2023).

The global trend of digital transformation of various sectors in public life is driving the need for encryption of sensitive data and the latest protection strategies. Encryption methods involving AI capabilities create an opportunity to protect data during transmission, for example, when sending data between two different networks (Kuppa *et al.* 2020). In addition to encryption, AI can be used to identify patterns in data that may indicate a potential threat using specific data analytics. AI is also used to develop secure authentication methods, such as biometric authentication (Mishra *et al.* 2023). This form of authentication requires the use of the user's physical characteristics (fingerprints or face identification) to gain access to secure systems.

However, despite the significant advantages and innovative capabilities of AI in cybersecurity, there are certain risks and disadvantages of using AI in information security systems. First of all, hackers can use AI capabilities to automate the process of finding and exploiting vulnerabilities in networks and applications by scanning large amounts of data in a short time frame and identifying security weaknesses. In addition, there is a rise in social engineering. Artificial intelligence can be utilized to create personalized phishing messages and fraudulent campaigns that optimally adapt to legitimate requests and messages. AI can significantly increase the effectiveness of brute-force attacks by guessing passwords and keys faster than traditional programs (Wiafe *et al.* 2020).

In addition, it is likely that AI will be used to develop hard-to-detect malware that can easily bypass threat detection systems and antivirus programs. AI allows hackers to hide the location and source of an attack. This significantly complicates the process of detecting and prosecuting them by cyber police.

AI can be used for criminal purposes to analyze data about a potential victim to accurately target the attack and choose the best time to implement it to maximize damage or avoid detection.

The relevance of the aforesaid risks of utilizing AI capabilities for criminal cyber purposes necessitates

the progressive and innovative development of means and methods of protection against cyber threats. AI-based systems should promptly notify of dangers, recognize new types of malware, and protect critical information data.

It should be noted that machine learning requires sets of informative data. In some cases, such data may be collected, accumulated, and used in violation of data privacy axioms. Consequently, it is necessary to anticipate this kind of problem and solve it preventively. Another potential pitfall may be AI-based systems that make access to the original data virtually impossible after the training is completed. The anonymization of informative data points is positioned as a method that currently requires deeper study to avoid distortion of program logic.

It is also obvious that there is a shortage of experts in artificial intelligence-based cybersecurity. The effectiveness of network security tools will increase significantly if there are qualified employees who can effectively maintain and configure them, performing a management function. Therefore, teams of specialists will remain an integral part of cybersecurity departments in the future, as critical thinking and creativity are consistently significant components of the decision-making system, which is not typical for AI tools.

In the future, the cybersecurity industry will improve innovative approaches involving AI to optimize the cybersecurity system. First of all, it is advisable to apply a multi-level approach to information security, introduce advanced training methods to understand the innovative complexity of modern threats and improve monitoring, detection, and response to threats using AI tools. This approach will allow for more effective counteraction to threats, including in the preventive vector of protection.

DISCUSSION

Many modern scientists are working on the application of artificial intelligence capabilities in the field of cyber defense. According to researchers in relevant scientific areas (Andraško *et al.* 2021; Kuzlu *et al.* 2021), the analytics of the interaction of traditional basic approaches to information security and AI technologies allows a wide range of multifactorial synergy concepts. This includes the introduction of automatic systems for the protection and prevention of cyber threats.

Based on the research findings of Zeadally S., Adi E., Baig Z. and Khan I. (2020), AI technologies in cybersecurity are considered to be a complex dynamic system that is successful in the synergy of technological, intellectual, and innovative vectors.

A study by Bécue A., Praça I. and Gama J. (2021) draws attention to the need to automate the creation of machine learning algorithms using AI that can identify various cybersecurity issues, including spam, threat websites, third-party applications, and shared data.

According to some scholars (Samtani *et al.* 2020), this concept should mitigate the risks of using AI for pattern recognition and biometric authentication, which increases the security of access to systems.

Some scientific papers consider the possibility of using AI technologies to monitor and analyze security events, detect anomalies, and quickly identify threats (Capuano *et al.* 2022). The scientific research results are similar to this study's conclusions in terms of the feasibility of using AI tools to analyze known amounts of data and traffic in real time and automatically detect abnormal behavior or suspicious activity.

Research by modern scientists shows that the ability of AI systems to predict risks is vital, as they can predict the potential time of a breach, estimate predictive losses, and choose ways to compensate them, taking into account the inventory of IT assets and determining the level of threat (Rawat et al., 2022).

According to experts, such an approach to forecasting based on AI analytics is positioned as an effective means of strengthening an organization's cybersecurity by automating the protection of areas where systems and devices are particularly vulnerable.

The results of modern scientific research by Kalarani (2021) show a trend of using AI capabilities to detect phishing emails and fraudulent schemes, as well as to identify false requests for money transfers or fraudulent transactions. In addition, according to scientists, AI provides an opportunity to automate numerous cybersecurity tasks. This allows analysts and security specialists to focus on more complex and strategic aspects of work (Kilincer *et al.* 2021).

Such conclusions are identical to the results of the current study and require further research into the functionality of AI in the field of cybersecurity.

According to Alqahtani, H., Sarker, I., Kalim, A., Minhaz Hossain, S., Ikhlaq, S., & Hossain, S. (2020), the ability to quickly comprehend various IT trends using machine learning algorithms and change its algorithms according to the latest data or information is a key feature of the artificial intelligence.

In a similar vein, artificial intelligence in cybersecurity is used for complex data networks that can quickly detect security threats and destroy them without human intervention. In addition, scientists consider the advantage of using artificial intelligence in cybersecurity by minimizing the need for human error, significantly reducing the possibility of error (Dash *et al.* 2022). At the same time, some scientists (Mosteanu, 2020) emphasize that AI in cybersecurity does not take over the entire functionality of information security experts. It only optimizes the process of identifying threats and quickly eliminating dangerous actions on the network.

Thus, the scientific position of most scientists today reflects the findings of this study. The authors consider AI technologies to be a formative force for a strong alliance between humans and machines that optimizes social processes, eliminates cybersecurity threats, and is focused on preventive information security protection. Today, we can predict the growing role of AI tools in the digital transformation of society. This approach will significantly improve the level of information security and contribute to the formation of an effective convergence of artificial intelligence and cybersecurity.

CONCLUSION

Artificial intelligence has become an essential part of the information security implementation system. It offers effective critical analysis and efficient threat identification.

The study examines the possibilities, aspects, and priorities of using artificial intelligence technologies in the cybersecurity system. It also highlights the benefits and risks of AI in information security. Based on the research outcomes, it was found that artificial intelligence in the field of security can identify risk priorities, quickly detect malware on the network, direct incident response, and prevent possible attacks before they occur.

The study revealed how artificial intelligence systems play a key role in improving information security protocols while eliminating the risks of the human factor. In addition, the authors have identified the dangers and challenges of using artificial intelligence in information security systems. The most significant risks and challenges include the possibility of cybercriminals using the potential of AI and the threat of unauthorized information leakage.

The article analyzes the main types of AI technologies used in the cybersecurity system. In addition, the authors substantiated the high efficiency of decision support systems using artificial intelligence technologies, as well as risk prevention and security automation. It is obvious that AI can create adaptive security systems that can respond quickly and effectively to changing threats and attacks in real time. At the same time, such systems can automatically adjust security rules and policies to protect networks and data more effectively.

Therefore, the combination of artificial intelligence and cybersecurity capabilities opens up the possibility of a paradigm shift in digital security. As a result of the development of such a symbiotic relationship, unprecedented opportunities to counter cyber threats are emerging. The high analytical accuracy of AI technologies, in synergy with their rapid response to new challenges, places them as the driving force behind the forward-looking cybersecurity of the future.

REFERENCES

Abbas, N., Ahmed, T. and Shah, S. 2019. Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, **121**: 1189–1211. https://doi.org/10.1007/s11192-019-03222-9

Alhayani, B., Mohammed, H., Chaloob, I. and Ahmed, J. 2021. WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.02.531.

Alqahtani, H., Sarker, I., Kalim, A., Minhaz Hossain, S., Ikhlaq, S. and Hossain, S. 2020. Cyber Intrusion Detection Using Machine Learning Classification Techniques. *Communications in Computer and Information Science*, 1235. https://doi.org/10.1007/978-981-15-6648-6_10

Alrfai, M., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M. and Almaiah, M. 2023. The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security. *Cogent Social Sciences*, **9**(2).

Andraško, J., Mesarčík, M. and Hamuľák, O. 2021. The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. *AI & Soc.*, **36**: 623–636.

Ansari, M., Dash, B., Sharma, P. and Yathiraju, N. 2022. The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *Int. J. Adv. Res. in Computer and Communication Engineering*. https://ssrn.com/abstract=4323317 Last Accessed in 14th July,2023

Bécue, A., Praça, I. and Gama, J. 2021. Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. *Artif. Intell. Rev.*, **54**: 3849–3886.

Capuano, N., Fenza, G., Loia, V. and Stanzione, C. 2022. Explainable Artificial Intelligence in Cybersecurity: A Survey. *IEEE Access*, **10**: 93575–93600.

Cheatham, B., Javanmardian, K. and Samandari, H. 2019. Confronting the risks of artificial intelligence. *McKinsey Quarterly*, **2**(38): 1-9. Last Accessed on 13th March, 2023.

Dash, B., Ansari, M., Sharma, P. and Azad, A. 2022. Threats and Opportunities with AI-Based Cyber Security Intrusion Detection: A Review. *Int. J. Software Engineering App (IJSEA)*, **13**(5).

Farivar, F., Haghighi, M., Jolfaei, A. and Alazab, M. 2020 . Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. *IEEE Transactions on Industrial Informatics*, **16**(4): 2716–2725.

Fatemidokht, H., Rafsanjani, M., Gupta, B. and Hsu, C. 2021. Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms With UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*, **22**(7): 4757–4769.

Geluvaraj, B. and Satwik, P. 2019 . The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. *Lecture Notes on Data Engineering and Communications Technologies*, **15**. Springer, Singapore. https://doi.org/10.1007/978-981-10-8681-6_67

Hurzhii, S. 2023. Specifics of using artificial intelligence in cybersecurity. *Information and the Law*, (47). https://doi.org/10.37750/2616-6798.2023.4(47).291669

Kalarani, D. 2021 . Empowering Artificial Intelligence and Cyber Security Challenges in Smart Manufacturing. *Turkish J. Comp. and Math. Educ.*, **12**(6): 150–160. Last Accessed on 17th March, 2023.

Kanimozhi, V. and Jacob, T. 2019. Artificial Intelligence based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 using Cloud Computing. *2019 International Conference on Communication and Signal Processing (ICCSP),* Chennai, India. 33-36. https://doi.org/10.1109/ICCSP.2019.8698029

Karchevskyi, M. and Radutniy, O. 2023. Artificial intelligence in Ukrainian traditional categories of criminal law. *Herald of the Association of Criminal Law of Ukraine*, **1**(19).

Kilincer, I., Ertam, F. and Sengur, A. 2021. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*, **188**: 1389–1286.

Kuppa, A. and Le-Khac, N.2020. Black Box Attacks on Explainable Artificial Intelligence (XAI) methods in Cyber Security. *International Joint Conference on Neural Networks (IJCNN), Glasgow*, UK. 1–8. https://doi.org/10.1109/IJCNN48605.2020.9206780

Kuzlu, M., Fair, C. and Guler, O. 2021. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discov Internet Things*, **1**(7).

Mishra, A., Tripathi, N., Vaqur, M. and Sharma, S. 2023. International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). 1685–1690. https://doi.org/10.1109/ICSCDS56580.2023.10104702

Mosteanu, N. 2020. Artificial Intelligence and cyber security a – face to face with cyberattack – a Maltese case of risk management approach. *Ecoforum J.*, **9**(2). Last Accessed on 6th May, 2023.

Neretin, O. and Kharchenko, V. 2022. Ensurance of artificial intelligence systems cyber security: analysis of vulnerabilities, attacks, and countermeasures. *Information systems and networks*, 12. https://science.lpnu.ua/sites/default/files/journal-paper/2023/jan/29738/221029maket-9-24.pdf. Last Accessed on 24th June, 2023.

Paul, P.K., Kayyali, M., Das, N., Chatterjee, R. and Saavedra, R. 2023. Artificial Intelligence and Smart Society: Educational Applications, Emergences and Issues – A Scientific Review. *Int. J. App. Sci. Eng.,* **11**(1).

Prasad, R. and Rohokale, V. 2020. Artificial Intelligence and Machine Learning in Cyber Security. *In:* Cyber Security: The Lifeline of Information and Communication Technology. *Springer Series in Wireless Technology*. Springer, Cham. https://doi.org/10.1007/978-3-030-31703-4_16

Rawat, B., Gangodkar, D., Talukdar, V., Saxena, K., Kaur, C. and Singh, S. 2022. The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality. *5th International Conference on Contemporary Computing and Informatics (IC3I),* Uttar Pradesh, India. 247-250. https://doi.org/10.1109/IC3I56241.2022.10072877

Saienko, D. 2023. The main areas of artificial intelligence technologies application in cybersecurity. *International Scientific and Practical Conference "Countering Cybercrime and Human Trafficking,"* Vinnytsia, 158–160. https://dspace.univd.edu.ua/handle/123456789/17501 Last Accessed on 23rd October, 2023.

Samtani, S., Kantarcioglu, M. and Chen, H. 2020. Trailblazing the Artificial Intelligence for Cybersecurity Discipline: A Multi-Disciplinary Research Roadmap. *ACM Trans. Manage. Inf. Syst.*, **11**(4).

Sarker, I., Abushark, Y., Alsolami, F. and Khan, A. 2020. IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. *Symmetry*, **12**(5).

Sarker, I., Furhad, M. and Nowrozy, R. 2021. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling, and Research Directions. *SN Comput. Sci.*, **2**(173).

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. and Xu, M. 2020. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*, **8**: 222310–222354.

Singh, S., Rathore, S. and Park, J. 2020. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. *Future Generation Computer Systems*, **110**: 721–743.

Skitsko, O., Skladannyi, P., Shyrshov, R., Humeniuk, M. and Vorokhob, M. 2023. Threats and risks of the use of artificial intelligence. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique"*, **2**(22): 6–18.

Soni, V. 2020. Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. http://dx.doi.org/10.2139/ssrn.3624487

Sukaylo, I. and Korshun, N. 2022. The influence of nlu and generative ai on the development of cyber defense systems. *Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique"*, **2**(18): 187–196.

Taddeo, M., McCutcheon, T. and Floridi, L. 2019. Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nat. Mach. Intell.*, **1**: 557–560.

Tan, L., Yu, K., Ming, F., Cheng, X. and Srivastava, G. 2022. Secure and Resilient Artificial Intelligence of Things: A HoneyNet Approach for Threat Detection and Situational Awareness. *IEEE Consumer Electronics Magazine*, **11**(3): 69–78.

Wan, H., Liu, G. and Zhang, L. 2022. Research on the Application of Artificial Intelligence in Computer Network Technology. *Proceedings of the 2021 5th International Conference on Electronic Information Technology and Computer Engineering (EITCE '21)*. 704–707. https://doi.org/10.1145/3501409.3501536

Wiafe, F., Koranteng, N., Obeng, E., Assyne, N., Wiafe, A. and Gulliver, S. 2020. Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access*, **8**: 146598–146612.

Zeadally, S., Adi, E., Baig, Z. and Khan, I. 2020. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access*, **8**: 23817–23837.

Zhang, Z., Ning, H. and Shi, F. 2022. Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artif. Intell. Rev.*, **55**: 1029–1053.