Research of Information Conflict between Humans and Artificial Intelligence in Information and Cybernetic Systems[⋆]

Svitlana Shevchenko[1,*,†], Yuliia Zhdanova[1,†], Olena Nehodenko[1,†], Svitlana Spasiteleva[1,†] and Vitalii Nehodenko[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

Abstract

Humanity is currently experiencing the fourth industrial revolution, the main characteristic of which is full automation of production in real-time, taking into account changing external conditions and internal influences. All this is connected with the introduction of innovations in the field of information technology, in particular artificial intelligence (AI), in the activities of various industries. AI is an integral part of modern cybersecurity systems. However, its use poses certain threats to ensuring the confidentiality, availability, and integrity of information. This paper is a logical continuation of scientific research aimed at studying information conflicts in modern society, namely: the information conflict between humans and AI in information and cybernetic systems. The main areas of use of AI in cyber security systems are substantiated and presented in this paper. Among them are automatic processing and analysis of security reports, traffic monitoring and analysis, intrusion detection, spam filtering, natural language processing and computer vision, threat forecasting, and others. As the results of practitioners show, the implementation of AI in security systems is a justified investment, as it provides more effective and proactive protection against cyber threats, reduces the risk of human error, and allows the automation of routine tasks. One of the results of the study is the consideration of the state and prospects for the use of AI in Ukraine's cybersecurity. Data interpolation methods have been used to predict the AI market in Ukrainian cybersecurity. The dynamics model is based on the Lagrange polynomial with an initial set of statistical data. As a result of the assessment, slow growth has been determined over the next two years. At the same time, the analysis of scientific sources allowed determining that in such systems based on AI, information conflicts arise between humans and AI at the stages of observation identification, analysis, and management. The paper describes the factors of the emergence of an information conflict between humans and AI. Among them is the lack of large and high-quality datasets for training AI; vulnerabilities of AI systems; offensive and/or competitive AI; and ethical aspects. Mathematical approaches to modeling the process of information conflict between humans and AI, which are based on the theory of differential equations, the theory of probability processes, and game theory, are proposed. It has been determined that the human mind plays a decisive role in this process. The approaches considered in this study can be used in the training of information and cybersecurity professionals.

Keywords

information conflict, artificial intelligence, cybersecurity, information system, cyber security system, factors of conflict

1. Introduction

Cyberattacks on information systems are increasing every year, becoming more sophisticated, complex, and targeted, and their potential targets are spreading to all sectors of society [1]. As a result, companies' financial and reputational losses are increasing significantly. At the same time, information security specialists are faced with a huge amount of routine work. This includes analyzing logs, preventing hacking attempts, investigating fraud, and more. In this regard, AI solutions that are capable of self-learning and adapting to new threats, providing more reliable

[⋆] *CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine*

[*] Corresponding author.

[†] These authors contributed equally.

s.shevchenko@kubg.edu.ua (S. Shevchenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova); o.nehodenko@kubg.edu.ua (O. Nehodenko); s.spasitielieva@kubg.edu.ua (S. Spasiteleva); v.nehodenko.asp@kubg.edu.ua (V. Nehodenko)

0000-0002-9736-8623 (S. Shevchenko); 0000-0002-9277-4972 (Y. Zhdanova); 0000-0001-6645-1566 (O. Nehodenko); 0000-0003-4993-6355 (S. Spasiteleva); 0000-0002-7678-9138 (V. Nehodenko)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-3991/paper22.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

information protection, are becoming increasingly relevant in cybersecurity systems. Implementing AI into security systems is not a cheap process, due to the need for significant investments in development, infrastructure, personnel, and integration. However, the use of AI is necessary to ensure the reliable protection of information systems, therefore, the cost of AI solutions in cybersecurity is growing, which confirms the importance of this process. According to analytical research [2] the global AI in cybersecurity market size is estimated at USD 24.82 billion in 2024 and is anticipated to reach around USD 146.52 billion by 2034, expanding at a CAGR of 19.43% between 2024 and 2034 (Fig. 1).

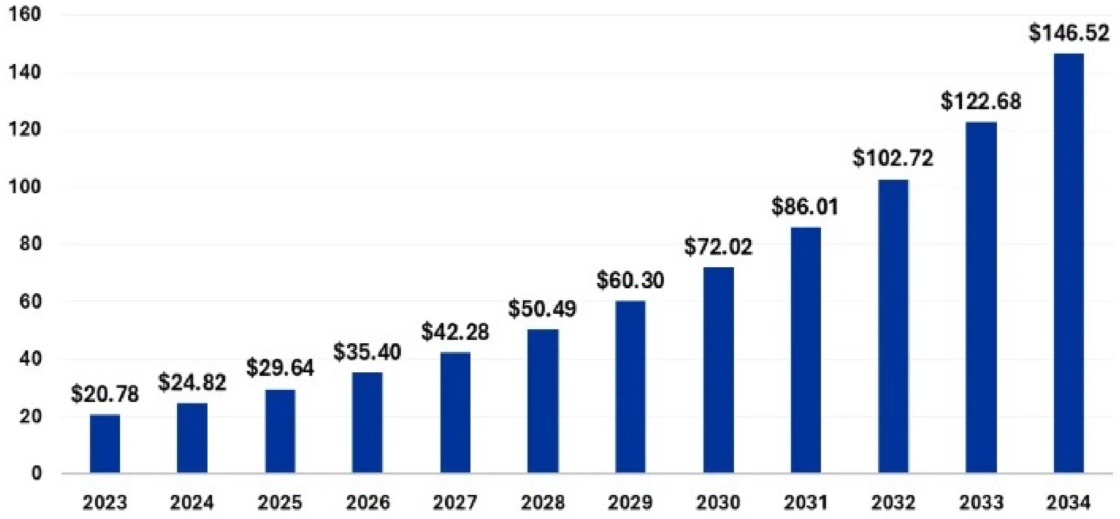

Figure 1: Artificial Intelligence In Cybersecurity Market Size 2023 to 2034 (USD Billion)

At the same time, the introduction of new technologies into information and cyber systems carries new risks in the field of ensuring the confidentiality, availability, and integrity of information. Hackers are also learning to use AI to increase their productivity. An information confrontation arises between those who want to dominate the information space, and control and manage the processes taking place in it [3, 4].

Information system conflict is related to the introduction or use of an information system that is perceived as inappropriate and as a threat to tasks, competencies, processes, values, and power relationships of individuals, groups, or organizations. IS conflicts are associated with resisting behaviors that express reservations in the face of pressure from change supporters seeking to alter the status quo by implementing an information system and related organizational changes [5].

The authors of articles [6–10], investigating the application of conflict theory in information and cyber security, proposed to consider this problem from three different perspectives: “subject-subject”, “object-object”, and “subject-object”. For each of these perspectives, the authors define the concept of “information conflict”. This study is the next stage of the analysis of applied aspects of conflict theory and is devoted to the problem of modeling information conflicts from the perspective of a “subject-object” between humans and AI.

2. Artificial intelligence is an integral part of modern cybersecurity systems

There is a wide range of interdisciplinary intersections between AI and cybersecurity. Scientists and practitioners in this field discuss and propose various solutions, focusing primarily on the benefits that companies receive after implementing AI into the information and cybernetic system of their business. The relevance and importance of this research are confirmed by a large base of achievements that are analyzed in review articles [11–16]. The results of these studies revealed that the first works on implementing AI in security systems were related precisely to detecting intrusions using AI, which allows the replacement of routine human work in this process. In this regard, various AI methods and algorithms have been developed for these purposes. In recent years, research has been conducted on the comprehensive implementation of AI in cybersecurity, highlighting the types of cyberattacks driven by AI, the motivations for these attacks, and outlining the range of ethical and legal aspects of AI cybersecurity.

2.1. Directions of application of artificial intelligence in cybersecurity

A review of the literature [11–26] and the results of experiments, for example, Table 1, 2, and 3, on the implementation of AI in information and cyber systems confirm the view that AI has great potential for improving information protection. Table 1 presents the results of the experiment on the implementation of AI in the network security system of financial services (FS) and healthcare (HS [19]. Accuracy of Threat Detection: In the financial services case study, the AI system achieved a 92% accuracy rate in detecting potential threats, up from 75% using the previous rule-based detection system. Similarly, the healthcare organization saw a jump in detection accuracy to 89% after implementing ML algorithms, compared to 68% under their older security framework. AI and ML systems significantly reduced the number of false positives—security alerts triggered by non-malicious activity. In the financial sector, false positives were reduced by 35%, from 300 alerts per day to 195. The healthcare provider reported a 28% reduction, decreasing from 260 to 187 daily false positives. This reduction allowed security teams to focus on real threats, improving overall efficiency.

By automating routine monitoring and alert-handling tasks, both organizations reduced the need for manual intervention in security operations, leading to cost savings.

- Financial Services: The company reduced the number of full-time security analysts required for manual threat monitoring from 10 to 6, resulting in annual savings of approximately US $200,000.
- Healthcare Provider: The healthcare organization saved around US $150,000 [19].

Table 1
Traditional vs AI/ML Security

Metric	FS		HS	
	Traditional Security	AI/ML Security	Traditional Security	AI/ML Security
Detection Accuracy	75 %	92%	68%	89%
False Positives	300	195	260	187
Threat Response Time	45 minutes	15 minutes	15 minutes	18 minutes

Table 2
Cost-effectiveness

Metric	Financial Services Savings	Healthcare Provider Savings
Full-Time Analysts (Pre-AI))	10	8
Full-Time Analysts (Post-AI)	6	5
Annual Savings in Labor Costs	US $200,000	US $150,000

Table 3
Comparison of pre and post-AI/ML integration cybersecurity metrics [24]

Metric	Before AI/ML Integration	After AI/ML Integration	Improvement (%)
Average Detection Time	48 hours	3 hours	93,75
False Positive Rate	20%	5%	75
Threat Response Time	24 hours	1 hour	95,83
Number of Undetected Attacks	50 per year	15 per year	70

AI, also known as machine intelligence, originated as a separate field of research in 1956 during the Dartmouth Seminar. There are two main views on what AI is:

- Scientific: AI is a science that seeks to understand the nature of intelligence and create intelligent machines capable of independent thinking and learning.
- Practical: AI is a set of methods and algorithms aimed at solving complex tasks that require human intellectual abilities, such as analyzing large amounts of data and making decisions based on them.

The field of cybersecurity is characterized by the practical aspect of AI [11].

It is not the purpose of this paper to go into too much detail about AI methods for improving traditional cybersecurity solutions. However, the main areas of application of this theory are worth considering for the following research questions.

An interesting proposal for the use of AI was the work [11]. The authors analyzed 91 articles and determined that making machines (computers) imitate human intellectual behavior, such as thinking, learning, reasoning, planning, etc. is possible due to the use of artificial neural networks, intelligent agent programs, artificial immune systems, genetic algorithms, and fuzzy sets, as well as their simultaneous use.

The study [12] presents the following approaches and architectures in the process of implementing AI in cybersecurity systems: artificial neural networks, expert systems, intelligent agents, quest, computer education, data collection, and constraint solving. The authors [17] recommend that companies apply AI in the following four areas to improve existing cybersecurity systems: automated protection, cognitive security, adversarial learning, and parallel and dynamic monitoring. Automated AI systems can be integrated into existing cybersecurity functions, which include creating more accurate login methods based on biometrics; detecting threats and malicious actions using predictive analytics; improving learning and analysis using natural language processing; securing conditional authentication and access; improving human analysis—from detecting malicious attacks to protecting endpoints; using automation to automate everyday security tasks; and eliminating zero-day vulnerabilities.

The study of scientific developments allowed us to summarize and present the areas of application of AI in information and cybersecurity systems (Fig. 2).

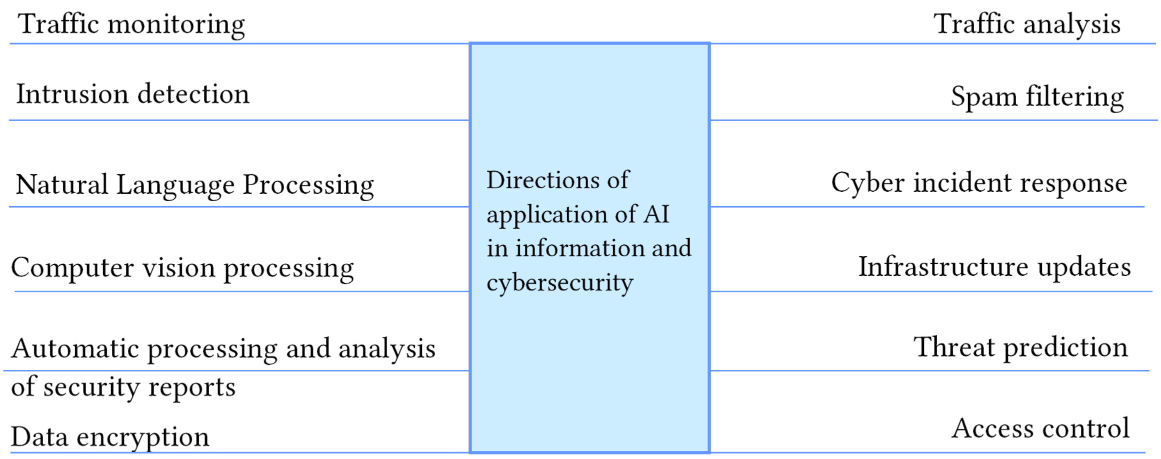
Traffic monitoring
Intrusion detection
Natural Language Processing
Computer vision processing
Automatic processing and analysis of security reports
Data encryption
Directions of application of AI in information and cybersecurity
Traffic analysis
Spam filtering
Cyber incident response
Infrastructure updates
Threat prediction
Access control

Figure 2: Directions of application of AI in information and cybersecurity

2.2. Artificial intelligence in cybersecurity in Ukraine

To promote the more active implementation of digital technologies in all spheres of the national economy, the Cabinet of Ministers of Ukraine approved the National Strategy for the Development of AI for the period 2021–2030 [27, 28]. At the beginning of 2020, Ukraine had the largest number of companies engaged in the development of AI in Eastern Europe, which indicates a high level of technological potential and innovative activity in the country.

The main task in the field of cybersecurity during the implementation of the state policy for the development of the AI industry is the protection of communication, information, and technological systems, information technologies, which are important for the continuity of the functioning of the state, society, and the safety of citizens. The use of AI technologies in ensuring information security is one of the factors that will contribute to ensuring national interests. In particular, monitoring social networks and online resources of electronic media using AI technologies makes it possible to identify systemic trends and problems, act proactively, and analyze the target audience [28].

AI in cybersecurity in Ukraine is at the stage of implementation and accumulation of initial experience. However, in recent years, it is cyber solutions (network and endpoint security) have dominated the Ukrainian market, which is due to the following objective factors [29, 30]:

- Increased frequency and scale of cyberattacks (the war increased the number and complexity of cyberattacks on information systems in Ukraine, which led to the rapid implementation of automated solutions).
- The need for immediate solutions.
- Shortage of personnel (as a result of military operations, there was an outflow of talent abroad, so the limited number of specialists prompted the use of automated solutions that require less human intervention).

Ukrainian science demonstrates significant interest in implementing AI methods in information and cyber systems [31–34].

The implementation of AI technologies requires large investments, which is why the development of AI in cybersecurity has slowed down since 2022.

Let us consider the forecast estimate of the size of AI in the cybersecurity market in Ukraine. According to reports [2, 35, 36] from 2021 to 2024, knowing the size of global AI and taking into account that the share of the Ukrainian market in cybersecurity is 0.07%, we will determine the size of AI in the cybersecurity market in Ukraine (Table 4).

Table 4
AI size in the cybersecurity market in the world and in Ukraine

Year	AI in the global cybersecurity market, USD billion	AI in the cybersecurity market in Ukraine, USD million
2021	14,9	10,43
2022	19,2	13,44
2023	22,49	15,743
2024	24,82	17,374

We will use interpolation based on the Lagrange polynomial. The initial stage is to determine the points that will be used in the calculations (Table 5)

Table 5
Interpolation of AI size based on Lagrangian polynomial

ix_if_iYear			
2021	0	0	10,43
2022	1	1	13,44
2023	2	2	15,743
2024	3	3	17,374

We get a third-degree polynomial:

$$L(x)=x(x-1)(x-2)(x-3)\times$$

$$\times\left(\frac{10{,}43}{-6x}+\frac{13{,}44}{2(x-1)}+\frac{15{,}743}{-2(x-2)}+\frac{17{,}374}{6(x-3)}\right),$$

$$L(x)=-1{,}74(x-1)(x-2)(x-3)+6{,}72x(x-2)(x-3)-$$

$$-7{,}87x(x-1)(x-3)+2{,}9x(x-1)(x-2)$$

According to the forecast results, we have: the size of AI in the Ukrainian cybersecurity market tends to grow: in 2025 it will be 18.432 USD million, and in 2026—18.848 USD million (Fig. 3.)

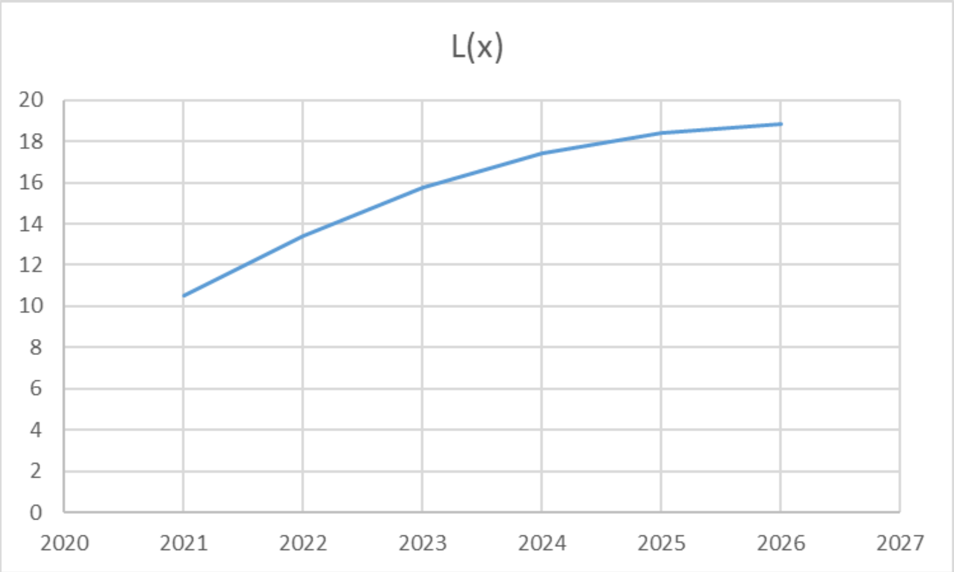

Figure 3: AI size forecast curve in the Ukrainian cybersecurity market

The slowdown in the growth rate of the AI market in cybersecurity systems is characterized by a decrease in donor funding and a personnel crisis in the context of martial law. Ukraine now has and is developing solutions that effectively use AI in the development of unmanned systems in the defense sector.

3. Challenges of implementing artificial intelligence in cybersecurity systems

3.1. Factors causing information conflict between humans and artificial intelligence

All of the above proves that AI does indeed demonstrate significant advantages over humans in many cybersecurity processes, especially when it comes to performing routine, templated work that requires speed and scalability. AI allows for the automation of processes, freeing people from monotonous work and allowing them to focus on more creative and complex problems.

However, trusting AI to perform cybersecurity tasks is "a double-edged sword: it can significantly improve cybersecurity practices, but it can also facilitate new forms of attacks on AI applications themselves, which can pose serious security and privacy threats" [37].

From a security perspective, the operation of AI technologies without human intervention raises concerns about their reliability [21]. Therefore, the scientific community is looking for effective solutions to prevent and overcome these threats.

Every day, scientists strive to develop new AI methods and algorithms to perform tasks that were previously only possible with human intelligence.

According to research [38], the technological process is occurring at an incredible speed and depth, which will lead to inevitable and radical changes in human life. The development of information technology is exponential, and it is obvious that humanity is approaching the point of technological singularity (Fig. 4). This is characterized by the fusion of biological and AI, where AI will play a key role, as well as the disappearance of the boundaries between the virtual and physical worlds.

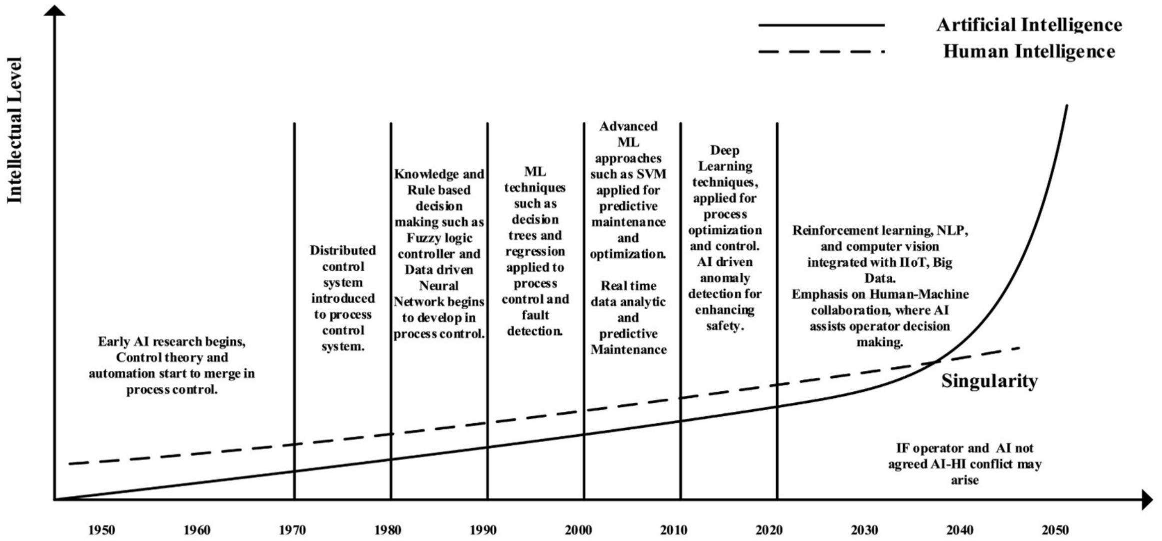

Figure 4: The intellectual level of HI and AI has been in the process of application for many years [21, 38]

As AI acquires more and more human-like skills, such as learning, pattern recognition, natural language processing, and decision-making, this growing similarity is leading to a new type of information conflict between AI and humans, particularly in security systems.

Information conflict between humans and AI is a state of relations between them in a situation where humans and AI have differences in the perception, interpretation, or use of information, which can lead to errors, misunderstandings, or even conflicting actions.

The conflict between humans and AI in the operation of an AI-based system can arise due to differences in observation, interpretation, and management actions [21].

We agree with the authors that humans and AI can interpret the same data or information differently. For example, a human analyst and an AI system receive data about unusual activity on the network, which includes an increase in the number of requests to a database server. A human, thanks to his experience and knowledge of typical user behavior, can identify this activity as a potential SQL injection attack. The analyst can take into account the time of day, the type of requests, the IP addresses from which the requests are coming, and other factors to conclude that this is indeed a hacking attempt. An AI system that has been trained on a large amount of network traffic data can classify this activity as "anomalous", but not necessarily as "malicious". If the algorithm has not seen enough examples of SQL injection attacks, it may miss this threat or classify it as a false alarm.

If a human and an AI perceive information in the same way, their conclusions may differ due to differences in training. For example, if an intrusion detection and prevention system incorrectly classifies legitimate activity as malicious, the results may be negative, as it will try to stop the action or change it. As a result, the AI may not act as human expects. Such discrepancies can lead to information conflicts, which negatively affect the confidentiality, availability, and integrity of information in AI-based systems. A person can think critically and analyze the context, which allows him to identify threats even by indirect signs. AI, on the other hand, relies on statistical patterns and patterns. If the algorithm has not seen enough examples of similar attacks, it may make a mistake in its classification. Thus, AI solutions rely on large data sets to train models and produce accurate results. This requires a huge amount of training, and accurately labeled data, which is often difficult to obtain in the cybersecurity field, which creates the first condition for the emergence of conflict between humans and AI.

The second factor that can cause conflict between AI and humans is the use by hackers of vulnerabilities in AI technologies, which can cause systems to act incorrectly. Cybercriminals are developing new attack methods aimed at bypassing AI-based security systems. One such method is to make minor changes to malware that allow it to remain undetected by AI. This calls into question the reliability of such systems, as they can miss real threats or generate false alarms. [24].

The authors [23] conducted a literature analysis and made a comparative characterization of the actions of AI: defensive AI, offensive AI, and competitive AI (Table 6).

Table 6
Key differences between defensive, offensive, and adversarial Al in cybersecurity

Defensive Al		Offensive Al		Adversarial Al	
Goal	Examples	Goal	Examples	Goal	Examples
Leverages Al techniques to protect computer systems and networks from attack	• Anti-malware • Intrusion detection systems (IDS)	Deploys Al techniques to attack computer systems and networks	• Developing new cyberattacks • Automating the exploitation of existing vulnerabilities	Maliciously exploits and/or attacks Al/ ML systems and data	• Poisoning training data • Manipulating input data

Cybercriminals use offensive AI or its subtype, adversarial AI, to carry out targeted attacks, forcing AI algorithms to misunderstand input data and react in a way that benefits the hacker.

This is the third factor that can cause conflict between humans and AI.

It is also important to note that there is another potential catalyst for conflict between humans and AI: ethical considerations. The use of AI to process and analyze information about humans raises ethical issues such as privacy, discrimination, and autonomy [23, 24, 39–42]. For example, AI requires access to users' data to effectively predict potential attacks or filter spam. However, this creates an invasion of privacy, known as the privacy paradox [22]. AI actions, such as restricting user access or selectively monitoring network activity, can significantly impact human rights to privacy and civil liberties. This raises important questions about the accountability, transparency, and impartiality of AI operations. It is necessary to develop clear rules for AI decision-making, define accountability for errors, and ensure that these systems are not biased or violate human rights. Ignoring these aspects can lead not only to technological and security issues but also to legal and reputational risks for organizations.

There is no doubt that the development of interaction between humans and AI will inevitably lead to the emergence of new information conflicts. Humanity will have to find ways to resolve these conflicts.

Cybersecurity experts believe that AI should not completely replace human decision-making. The most effective strategy is to integrate AI into decision-making processes, where humans will play a key role, using AI as a powerful tool [13].

3.2. Mathematical models for representing information conflict between humans and artificial intelligence

Mathematical models of information conflict between humans and AI help to better understand how information cooperation between humans and AI occurs, what factors influence the emergence of conflicts how these conflicts can develop, and what factors contribute to the formation of these conflicts. With the help of models, it is possible to predict possible conflict situations and their consequences, and as a result, manage them.

In modern science, modeling of information conflicts between humans and AI in information and cyber security systems remains underdeveloped. Existing developments are mostly point-based and relate to various specifications.

One approach to modeling information conflict between humans and AI is described in the study [21]. In an AI-driven process, humans develop algorithms based on historical data, and AI uses this knowledge and real-time sensor data to control operations. The human operator also monitors this data and controls the process, relying on their own experience, education, and AI data. According to the authors [21], such joint work between humans and AI can lead to conflicts due to differences in the observation process, the interpretation of data, and the choice of control actions. The mathematical approach to developing the model is based on probability theory (normal distribution of values and the three-sigma rule).

The original development of a mathematical model of information conflict between humans and AI is presented in [43]. Scientists have proposed a model for quantitative assessment of conflict risk, which includes methods of vector algebra and probability theory, and the Thomas-Kilman conflict mode tool is used to resolve the conflict.

To develop models describing information conflict between humans and AI in information and cyber security systems, the following mathematical apparatus can be applied:

- Differential equations (to describe the dynamics of conflict development over time).
- Markov processes (to model random factors that may affect the conflict).
- Game theory with incomplete information (to determine optimal strategies for each party, taking into account the actions of the other party).
- Probabilistic models based on Bayes' theorem.

The effectiveness of human-AI conflict models will depend on the accuracy of parameter determination, historical data, and the adequacy of their application to specific cybersecurity situations.

Conclusions

The implementation of AI in cybersecurity systems is a complex and expensive process. However, with the constant increase in the number and complexity of cyberattacks, the use of AI is necessary to ensure the reliable protection of information systems. At the same time, the implementation of AI technologies in information and cyber systems has made the issue of ensuring information security more relevant. In particular, the use of AI can create new vulnerabilities and threats to main information security principles, such as confidentiality, availability, and integrity of information. This necessitates a cautious and balanced approach to the implementation of AI, taking into account potential risks and developing appropriate protection mechanisms. Cooperation and task allocation between humans and AI systems should, first and foremost, be determined by their mutual properties.

Despite the importance of human-AI collaboration in cybersecurity, the depth, and scope of this interaction, especially in critical and fundamental aspects, remain poorly understood. Effective use of AI in information security requires multidisciplinary research that takes into account aspects of psychology, cognitive science, and other fields.

In our opinion, the areas of further research are the development of mathematical models to manage information conflict between humans and AI in security systems.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] A. I. Jony, S. A. Hamim, Navigating the cyber threat landscape: A comprehensive analysis of attacks and security in the digital age, J. Inf. Technol. Cyber Secur. 1 (2024) 53–67. doi:10.30996/jitcs.9715

[2] Y. Kostiuk, et al., Models and algorithms for analyzing information risks during the security audit of personal data information system, in: 3rd International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 155–171.

[3] Y. Kostiuk, et al., A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps, in: 3rd International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 249–264.

[4] Artificial intelligence (AI) in cybersecurity market size, share, and trends 2024 to 2034. URL: https://www.precedenceresearch.com/artificial-intelligence-in-cybersecurity-market

[5] A. Boonstra, J. Vries, Information system conflicts: Causes and types, Int. J. Inf. Syst. Proj. Manag. 3 (2015) 5–20. doi:10.12821/ijispm030401

[6] S. Shevchenko, et al., Study of applied aspects of conflict theory in security systems, Cybersecure. Educ. Sci. Tech. 2(18) (2022) 150–162. doi:10.28925/2663-4023.2022.18.150162

[7] S. Shevchenko, et al., Conflict analysis in the "subject-to-subject" security system, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421, 2023, 56–66.

[8] S. Shevchenko, et al., Game theoretical approach to the modeling of conflicts in information security systems, Cybersecure. Educ. Sci. Tech. 2 (22) (2023) 168–178. doi:10.28925/2663-4023.2023.22.168178

[9] V. Astapenya, et al., Conflict model of radio engineering systems under the threat of electronic warfare, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 290–300.

[10] S. Shevchenko, et al., Conflicting subsystems in the information space: A study at the software and hardware levels, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 333–342.

[11] S. Dilek, H. Çakır, M. Aydın, Applications of artificial intelligence techniques to combating cyber crimes: A review, Int. J. Artif. Intell. Appl. 6(1) (2015) 21–39.

[12] R. Das, R. Sandhane, Artificial intelligence in cyber security, J. Physics: Conf. Series. 1964(4) (2021). doi:10.1088/1742-6596/1964/4/042072

[13] R. Kaur, D. Gabrijelčič, T. Klobučar, Artificial intelligence for cybersecurity: Literature review and future research directions, Inf. Fusion 97 (2023). doi:10.1016/j.inffus.2023.101804

[14] I. Jada, T. Mayayise, The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review, Data Inf. Manag. (2023) 100063. doi:10.1016/j.dim.2023.100063

[15] L. Ofusori, T. Bokaba, S. Mhlongo, Artificial intelligence in cybersecurity: A comprehensive review and future direction, Appl. Art. Intell. 38(1) (2024). doi:10.1080/08839514.2024.2439609

[16] A. H. Salem, et al., Advancing cybersecurity: a comprehensive review of AI-driven detection techniques, J. Big Data 11(105) (2024). doi:10.1186/s40537-024-00957-y

[17] M. N. O. Sadiku, O. I. Fagbohungbe, S. M. Musa, Artificial intelligence in cyber security, Int. J. Eng. Res. Adv. Technol. 06(05) (2020) 01–07. doi:10.31695/ijerat.2020.3612

[18] B. Alhayani, et al., Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry, in: Materials Today: Proceedings, 2021. doi:10.1016/j.matpr.2021.02.531

[19] T. Bashir, N. A. Al-Sammarraie, Revolutionizing network security with AI and machine learning solutions, Int. J. Comput. Appl. 186 (2024) 35–42. doi:10.5120/ijca2024924217

[20] S. Goel, et al., A neurosymbolic cognitive architecture framework for handling novelties in open worlds, Artif. Intell. 331 (2024) 104111. doi:10.1016/J.ARTINT.2024.104111

[21] R. Arunthavanathan, et al., Artificial intelligence—Human intelligence conflict and its impact on process system safety, Digit. Chem. Eng. 11 (2024). doi:10.1016/j.dche.2024.100151

[22] F. Li, Application and challenges of artificial intelligence in cybersecurity, Appl. Comput. Eng. 47 (2024) 262–268. doi:10.54254/2755-2721/47/20241480

[23] M. Malatji, A. Tolah, Artificial intelligence (AI) cybersecurity dimensions: A comprehensive framework for understanding adversarial and offensive AI, AI and Ethics, 2024. doi:10.1007/s43681-024-00427-4

[24] M. Roshanaei, M. R. Khan, N. N. Sylvester, Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions, J. Inf. Secur. 15 (2024) 320–339. doi:10.4236/jis.2024.153019

[25] O. Golubenko, et al., Research in the application of artificial intelligence in cybersecurity, ITSynergy (2) (2023) 71–81. doi:10.53920/ITS-2023-2-5

[26] A. Ilienko, et al., Prospects of integration of artificial intelligence into cybersecurity systems, Cybersecur. Educ. Sci. Tech. 1(25) (2024) 318–329. doi:10.28925/2663-4023.2024.25.318329

[27] A. V. Antonenko, et al., Classifications of machine learning application models in cyber security Taurida scientific herald, Series: Tech. Sci. 4 (2023) 11–22. doi:10.32782/tnv-tech.2023.4.2

[28] National strategy for the development of artificial intelligence in Ukraine 2021–2030, Kyiv: Ministry of Education and Science of Ukraine, National Academy of Sciences of Ukraine, 2021. URL: https://www.naiau.kiev.ua/images/news/img/2021/06/strategiya-110621.pdf

[29] Ukraine's AI ecosystem: Talents, companies, education. Saturday Team, 2024. URL: https://aihouse.org.ua/research/ai-ecosystem-of-ukraine-talent-companies-education/

[30] DataDriven, Overview of the cybersecurity market in Ukraine, 2025. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf

[31] S. Lysenko, et al., A cyberattacks detection technique based on evolutionary algorithms, in: 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, 127–132. doi:10.1109/DESSERT50317.2020.9125016

[32] O. E. Radutny, L. Yakuliavichene, Human rights through the prism of artificial intelligence, robotics and digital humans, Human rights in the context of digital transformation of society: monograph, Kharkiv: Yaroslav the Wise National University of Law, 2022, 19–41.

[33] V. A. Susukailo, Development of a model of a cybercrime investigation system for components of information systems infrastructure, PhD Thesis, Lviv Polytechnic National University of the Ministry of Education and Science of Ukraine, Lviv, 2024.

[34] V. Terziyan, O. Vitko, Explainable AI for Industry 4.0: Semantic representation of deep learning models, Proced. Comput. Sci. 200 (2022) 216–226. doi:10.1016/j.procs.2022.01.220

[35] Artificial intelligence in cybersecurity market outlook (2022 to 2032). URL: https://www.futuremarketinsights.com/reports/artificial-intelligence-in-cybersecurity-market

[36] Artificial intelligence in cybersecurity market by security type—Global forecast 2028. URL: https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-ai-cyber-security-market-220634996.html

[37] M. Taddeo, T. McCutcheon, L. Floridi, Trusting artificial intelligence in cybersecurity is a double-edged sword, Nature Mach. Intell. 1 (2019) 557–560.

[38] R. Kurzweil, The singularity is near, EthicsEmerg. Techn. (2014) 393–406. doi:10.1057/9781137349088_26

[39] D. Sontan, S. V. Samuel, The intersection of artificial intelligence and cybersecurity: Challenges and opportunities, World J. Adv. Res. Rev. 21 (2024) 1720–1736. doi:10.30574/wjarr.2024.21.2.0607

[40] J. E. H. Korteling, et al., Human- versus artificial intelligence, Front Artif. Intell. 4 (2021). doi:10.3389/frai.2021.622364

[41] G. Lima, et al., The conflict between people's urge to punish AI and legal systems, Frontiers in Robotics and AI. 8 (2021) 756242. doi:10.3389/frobt.2021.756242

[42] Md. F. Rafy, Artificial intelligence in cyber security (2024). doi:10.13140/RG.2.2.19552.66561

[43] H. Wen, F. Khan, A risk-based model for human-artificial intelligence conflict resolution in process systems, Digit. Chem. Eng. 13 (2024) 100194. doi:10.1016/j.dche.2024.100194