Artificial Intelligence in Cyberspace: Between Danger and Innovation[‡]

Submitted: 5 April 2024
Reviewed: 16 September 2024
Revised: 19 September 2024
Accepted: 20 September 2024

Mykhailo Dumchikov[*]
https://orcid.org/0000-0002-4244-2419
Olha Maletova[**]
https://orcid.org/0000-0002-2288-1393
Tetyana Mishchenko[***]
https://orcid.org/0000-0002-8801-0734
Yevheniia Lytvynenko[****]
https://orcid.org/0000-0002-4735-3722

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v17i1.53386

Abstract

[Purpose] The purpose of the article is to examine the impact of artificial intelligence on cybersecurity and to explore both the risks and the opportunities it presents. The article examines the primary forms of criminal use of AI in cyberspace, as well as develops effective methodologies for its application in the process of investigation, prevention, and analysis of these socially dangerous actions.

[Methodology/approach/design] The authors employed an interdisciplinary approach combining methods from legal science, economics, and information technology in their work. Numerous scientific works on AI's characteristics, its role in digitization, and its use in criminal investigations have been noted. These studies offer suggestions, particularly for law enforcement agencies, financial institutions, and cybersecurity organizations. However, they are mainly theoretical and overlook new cyber threats and techniques used by cybercriminals with AI. In contrast, the authors analyzed illegal activity websites and forums, including cyberspace, using AI capabilities. They used cognitive methods to

[‡] The work was carried out within the project "Corruption in the Context of Martial Law and Post-War Reconstruction: Optimal Resistance Model" (state registration number 0124U000556) and Jean Monnet Module 'EU EXPERIENCE ON THE PROTECTION OF PERSONAL DATA IN CYBERSPACE' 2023-2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE.

[*] Doctor of Juridical Sciences, Associate Professor, Associate Professor, Department of Criminal Legal Disciplines and Procedure, Sumy State University. E-mail: m.dumchykov@yur.sumdu.edu.ua.

[**] Doctor of Juridical Sciences, Associate Professor, Head of the Department of Criminal Legal Disciplines and Procedure, Ukraine, Sumy State University. E-mail: o.bondarenko@yur.sumdu.edu.ua.

[***] PhD in Law, Lecturer, Department of Criminal Legal Disciplines and Procedure, Sumy State University. E-mail: kpds@yur.sumdu.edu.ua.

[****] PhD in Law, Lecturer, Department of Criminal Legal Disciplines and Procedure, Sumy State University. E-mail: e.lytvynenko@yur.sumdu.edu.ua.

analyze how AI is used in cybercrimes, both as an auxiliary and primary tool. Content analysis methodology facilitated a systematic review of web content related to AI-enabled cybercrimes. The comparative-legal method compared AI-enabled cybercrimes to similar crimes without AI. Reviewing scientific articles, books, and conference proceedings helped understand AI, cybersecurity, and law enforcement. Case studies examined specific instances of AI in cybercrime, aiding in real-life prevention and investigation. The systematic method ensured a comprehensive examination of previous studies, identifying trends, challenges, and development prospects in AI and cybersecurity. By adopting this multifaceted and innovative approach, the authors were able to provide a more comprehensive and nuanced understanding of the emerging landscape of AI-assisted cybercrime. This research not only contributes to the academic discourse but also offers practical insights for law enforcement agencies, policymakers, and cybersecurity professionals working to combat these evolving threats.

[Findings] The utilization of AI in the realm of cybercrimes unveils new prospects for the criminals themselves, as well as offers opportunities for effective combat and investigation of these crimes through AI. It is emphasized that the application of AI in crime investigations aids in refining the processes of detection and analysis of cybercriminal activities, allowing for quicker identification of anomalies and response to them. However, despite AI's significant potential, its use necessitates a cautious approach and the development of ethical and legal standards. This is essential to avoid possible negative consequences and ensure balanced development in cybersecurity.

Keywords: Information Technology. Artificial intelligence. Cybercrime. Cybersecurity. Innovation in Cybersecurity.

INTRODUCTION

State security, national security, and defense, as well as the multilateral development of society depend on the advancement of high technologies. A specific phenomenon playing a crucial role in this process is artificial intelligence (AI).

The principles and algorithms behind AI remain largely unknown to most of the society. Essentially, AI is perceived as a sort of "magical black box" capable of understanding human natural language, musical descriptions, or graphical images and providing statistically accurate responses to user queries. Typically, users receiving outcomes from such systems do not grasp the origin of these responses or the methods used to solve the tasks. It's noteworthy that, unlike traditional computational and information-telecommunication technologies, AI introduces an element of unpredictability regarding its results and conclusions.

On the other hand, the lack of transparent methods for verifying the conclusions and recommendations offered by AI creates a source of uncertainty regarding their veracity and practical value. This effectively means that AI could become part of the arsenal in information warfare, aimed at disseminating dubious, unverified information and outright falsehoods. AI has the potential to become a powerful tool in information wars, crafting more convincing and targeted fake news, and automating its dissemination.

The use of AI by criminals in committing socially dangerous acts in cyberspace has effectively spawned a new era of cybercrime that is rapidly evolving. With AI, cybercriminals can craft persuasive phishing emails, scale their cyberattacks, train AI in social engineering skills for further use in cyber fraud, and much more.

At the same time, AI can also be employed in counter-cybercrime efforts and cybersecurity, enhancing the efficiency of cybersecurity professionals. Moreover, AI can assist in predicting potential attacks and developing defensive strategies against them. Automated monitoring and data analysis systems can detect unusual activity in information and telecommunication networks and systems, warning of potential threats. AI can be utilized to create a cybercrime prevention system that prevents possible attacks before they start.

STATE OF SCIENTIFIC DEVELOPMENT

In their scientific works, the issue of AI usage in general, and its role in combating socially dangerous actions in cyberspace, is examined. For instance, T. Kokotajlo, D. Long, M. Reith and R. Dill have focused on the trend of exploiting AI capabilities for the development of software aimed at conducting cyber wars at the national level (Kokotajlo, Long, Reith, Dill, Richard, 2021).

In their study, V. Petri and L. Martti explored the threats and risks associated with AI, alongside its potential in addressing cybersecurity challenges. The authors examined AI's impact across twelve critical areas of cybersecurity, presenting a condensed but comprehensive analysis of its role in enhancing digital security measures (Vahakainu, Lehto, 2019).

Y. Harel, I. B. Gal, and Yu. Elovici highlighted that AI could be exploited for illicit activities on social networks, particularly in crafting sophisticated social engineering attacks. This includes identity impersonation and information manipulation to access personal data (Harel, Ben Gal, Elovici, 2017).

A. Ali Almazroi and N. Ayub proposed innovative approaches to combating financial fraud using AI capabilities. They specifically focused on the implementation of autoencoder techniques and the rapid identification of suspicious transaction patterns (Almazroi, Ayub, 2023).

In their scholarly work "Artificial Intelligence and Cybersecurity: Past, Present, and Future," T. Cong Truong,

I. Zelinka, J. Plucar, M. Čandík, and V. Šulc highlighted the challenges posed by automated cyber-attacks and identified AI's role in combating them. The authors noted that AI could manage bots for the automated creation of fake accounts, dissemination of spam, and execution of phishing attacks (Truong, Zelinka, Plucar, Čandík, Šulc, 2020).

S. Ismaeel Khalel and S. M. Khudher employed AI methodologies to discern the nature of cyber offenses and how they differ from traditional crimes not involving AI.Simulation results showed the capabilities of artificial intelligence to reach the target with high accuracy which helps grid operators of control center to better protect power system against threat of cyber-attack (Khalel, Khudher, 2022).

S. Samtani, H. Chen, M. Kantarcioglu, and B. Thuraisingham analyzed how AI can be applied in cyber threat intelligence. They demonstrated the feasibility of implementing a Cyber Threat Intelligence system—a data-driven process designed to identify emerging threats and key threat actors to facilitate effective cybersecurity decision-making (Samtani, Chen, Kantarcioglu, Thuraisingham, 2022).

Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and Kim-K. Raymond Choo investigated the application of AI in user access authentication, network situation awareness, monitoring of malicious behavior, and identification of anomalous traffic (Zhang, Ning, Shi, Farha, Yang Xu, Xu, Zhang, Choo, 2022).

A. João Gonçalves de Azambuja, P. Christian, S. Klaus, A. Reiner, S. Benjamin, and A. Vilson Ros conducted a comprehensive literature review to explore the impact of AI on cybercrime. They presented the scientific community with information crucial for developing protective measures against potential threats arising from AI's influence on cybersecurity (Azambuja, Gonçalves, Plesker, Schützer, Anderl, Schleich, Almeida, 2023).

N. Naeem Abbas, T. Ahmed, S. Habib Ullah Shah, M. Omar and Han Woo Park, first to provide an overall perspective of hotspots and trends in the research on AI in the cyber security domain (Abbas, Ahmed, Ullah Shah, Omar, Woo Park, 2019).

The approaches mentioned above regarding the establishment of AI's essence in cybersecurity provision and its use during cybercrime investigations highlight that the field remains largely unexplored. Furthermore, scientific works analyzing the impact of AI on the evolution of cybercrime and how cybercriminals utilize it in their activities are virtually nonexistent. Our research aims to elucidate how AI assists criminals in committing socially dangerous acts in cyberspace, with a particular focus on the methods of AI utilization in cybercrime perpetration. Simultaneously, we propose methods and ways of using AI in the prevention and investigation of crimes in this domain.

LEGAL REGULATION OF AI IN SPECIFIC COUNTRIES

It's worth emphasizing that countries worldwide are intensifying efforts to develop approaches to AI regulation, striving to account for its dynamic and multifaceted nature. However, as of early 2024, most nations still lack systematic legal regulation in this field. Currently, no country has enacted a specialized AI law. Nevertheless, several jurisdictions, such as China, Japan, Israel, the USA, and Canada, are already on the path to developing relevant legislation.

It's important to note that for many countries, the first step in AI regulation is launching national strategies or ethical policies, rather than immediately introducing laws. This cautious approach demonstrates governments' desire to maintain a delicate balance between supporting innovation and the need to control potential risks associated with technological development. This allows jurisdictions not only to ensure technological progress but also to protect society from unforeseen consequences of artificial intelligence use (IAPP Research and Insights, 2024).

In the context of the global trend towards AI regulation, some states are already implementing targeted measures aimed at regulating specific areas of AI use. For example, China demonstrates a clear example of this approach; in September 2023, a law aimed at regulating generative AI services came into effect in the country. This is an important step as it creates a legal framework for companies developing and offering AI tools capable of generating text, images, audio, and video.

The Chinese law has several key requirements, including mandatory safety assessments and obtaining administrative permits for service providers. This allows for controlling technologies at the implementation stage, which is important for minimizing risks associated with AI use. Of note is the requirement that these services align with socialist values, which are part of China's official ideology. This approach demonstrates the government's desire to maintain political stability and social control, even in the sphere of technological innovation.

Another important aspect of this regulation lies in protecting user rights. The law provides for preventing potential abuses, such as information manipulation or creating fake news. Additionally, the state emphasizes protection against user dependence on artificial intelligence, which is important given the potential social consequences of prolonged use of such technologies.

This case shows how countries can adapt their legal systems to specific challenges arising in the process of artificial intelligence development. While most states are taking initial steps in creating general strategies or ethical codes, China is going further by implementing regulation of specific technological sectors. This allows the government not only to ensure technological progress but also to use these tools to achieve its own political and social goals.

Compared to other countries that are still developing general national strategies in the AI field, China's approach demonstrates a more pragmatic and controlled regulatory model. However, this also underscores the dilemma between the desire for innovation and the need for strict control over technologies that may pose threats to privacy, security, and freedom of expression (Smirnov, 2023).

The concept of the AI law in the USA focuses on balancing technological progress and protecting civil rights, reflecting the unique approaches of the Western world to technology regulation. In the US, human rights and freedoms are prioritized, especially considering new risks that may arise from digital monitoring, mass data processing, and the implementation of algorithmic decisions. Therefore, the US approach to AI regulation has several key aspects.

1) Safeguards against risky or ineffective systems. The US aims to minimize threats that may arise from the implementation of AI technologies in critical areas such as healthcare, financial services, or public administration. The need for reliability and safety checks of algorithms is central to preventing harm caused by erroneous or incorrect decisions of AI systems.
2) Protection against algorithmic discrimination. The US recognizes that algorithms can reproduce and even amplify discrimination based on race, gender, age, or other characteristics. Therefore, legislation aims to ensure transparency and equality in AI application to avoid any biased decisions that may affect the rights of specific population groups.
3) Data security and privacy. One of the main threats in the AI field is the risk of privacy breaches using large volumes of personal data for algorithm training. At this stage, the US emphasizes the need for strict standards for data storage, processing, and transfer to minimize the risk of leaks and unauthorized access.
4) Openness regarding AI application and its impact. An important condition for protecting user rights is transparency in AI use. Legislators insist that companies inform consumers about the use of artificial intelligence in decision-making and how this may affect their rights and lives.
5) Possibility of human intervention in AI decision-making processes. In the US, it is considered critically important that humans can intervene in AI-driven processes, especially in cases where human rights or well-being depend on it. This means that

> automated systems should leave room for human correction or review of decisions to avoid situations where an algorithm can make an undesirable or erroneous decision without human control.

In our opinion, this US approach underscores the desire to create a regulatory framework that simultaneously allows AI to develop and ensures civil rights at a high level. This reflects a balance between innovation and social responsibility, where privacy protection, transparency, and combating discrimination take center stage. While China directs its efforts towards socio-political control, the US emphasizes protecting citizens from possible abuses and errors by technologies (Shadska, 2024).

It's worth noting the EU's experience in AI regulation. In March 2023, the European Parliament adopted the AI Act, bringing the world's first specialized law in the AI field closer to reality. The draft Regulation establishing harmonized rules on AI was developed to implement the first unified legal framework for AI regulation within the EU. The AI Act proposes dividing AI systems into groups according to the potential risk they may pose to users and society: unacceptable risk, high risk, limited risk, and minimal risk.

AI systems with unacceptable risk pose an immediate threat to safety, life, and human rights and must be prohibited, including:

1) Social scoring systems;
2) Systems that perform real-time remote biometric identification for law enforcement purposes and are used for monitoring in public places, except in specific cases involving child abduction, terrorist threats, and individuals sentenced to more than 3 years of imprisonment.

AI systems used in critical infrastructure, education, employment, key public and private services, law enforcement agencies, migration services, and judicial bodies are recognized, according to the draft, as high-risk systems. These systems must meet certain requirements before they can be brought to market, namely: risk assessment and mitigation methods, high data quality, transparency, human control, and security.

AI systems with limited risk are only restricted by the transparency requirement: users should understand that they are communicating with a machine system, not a human. Most such AI systems, as well as systems without risk, can be used without legal restrictions.

The AI Act also provides for the establishment of a special EU AI Board, consisting of representatives from all member states, to assist in implementing regulations and imposing fines for violations. Fines for violations can reach 6% of the violating company's global turnover or 30 million euros, whichever is higher (Artificial Intelligence Act, 2024).

In addition to the Artificial Intelligence Act, the European Commission presented a draft AI Liability Directive, which plays an important role in shaping the legal framework for AI regulation in the European Union. This initiative aims to adapt civil liability rules to new challenges associated with the use of artificial intelligence and is expected to provide a reliable mechanism for protecting the rights of citizens and businesses facing potential harm from AI.

One of the key innovations proposed by the Directive is the introduction of the principle of strict liability for operators of high-risk AI systems defined in the AI Act. This means that operators of such systems will be liable for any damages or harm caused by their technologies, even if they acted without violations. This approach places the burden of responsibility on operators, as the risks associated with high-risk systems, such as systems in healthcare, transport, or justice, are significant, and even minor errors can have serious consequences.

For AI systems not considered high-risk, the traditional fault-based liability regime will apply. This means that to hold someone liable, it will be necessary to prove that the operator acted negligently or with malicious intent. This approach allows for balancing responsibility depending on the level of risk posed by a specific AI system.

The draft Directive is an important complement to the AI Act and aims to further improve the legal system regarding AI, giving users the opportunity to receive compensation in case of harm caused by artificial intelligence systems. This regulation also promotes increased transparency and trust in AI use, as operators will be interested in ensuring high quality and safety of their technologies to avoid potential lawsuits.

The European Union, by adopting such comprehensive legislative acts as the AI Act and the AI Liability Directive, clearly demonstrates its intentions to become a global leader in artificial intelligence regulation. Just as the General Data Protection Regulation (GDPR) set global standards in privacy and data protection, these new EU initiatives may have far-reaching impacts on global technology policy.

Like how GDPR established high standards for personal data protection, which are now considered by countries outside the EU, the AI Act may have a similar impact on artificial intelligence regulation on a global scale. This applies not only to EU member states but also to countries aspiring to integrate with the EU, such as Ukraine. Potential harmonization of Ukrainian legislation with EU norms in this field could be an important step towards EU accession and would raise standards of rights protection and security in Ukraine.

Given the EU's global influence in AI regulation, these legislative initiatives may serve as an example for other jurisdictions. As with GDPR, countries worldwide are likely to consider European regulatory approaches as a benchmark for shaping their own AI regulation strategies (AI Liability Directive, 2024).

AI: PROBLEMS AND PROSPECTS FOR DEVELOPMENT

In today's world, AI is applied across numerous facets of human life. However, it is important to note that the term "AI" is not entirely precise in contemporary usage. It is more commonly employed as an umbrella term for various technologies that endow computers and mechanisms with enhanced intellectual capabilities.

Modern AI systems encompass a variety of methods that expand the capabilities of information and telecommunication technologies. Among these techniques are machine learning, deep learning, big data processing, neural networks, cognitive computing, and others. In our view, modern AI systems should address the fundamental question: "What possibilities will arise if electronic computing machines are granted infinite computational power and access to unlimited data?"

The issue of job losses associated with the implementation of AI is actively researched both in the business community and academic circles. According to a study conducted by Oxford University, over 47% of American jobs could be at risk due to automation by the mid-2030s (Automation and the future of work – understanding the numbers, 2018)

According to the World Economic Forum, AI automation is projected to replace more than 90 million jobs by 2025 (Centre for Economic Policy Research, 2023).

Some figures are even more alarming. According to another report by McKinsey, AI-based robots could replace 30% of the current global workforce (McKinsey & Company, 2017).

According to AI expert and venture capitalist Kai-Fu Lee, within the next 10-15 years, 40% of jobs worldwide will be replaced by AI-based bots (Recurrent Ventures Inc, 2019).

Workers with low income and low skills will be most affected by this change. As AI becomes smarter every day, even highly paid and highly skilled workers are becoming more vulnerable to job loss as companies gain significant profit from automating their operations. Indeed, today we can discuss numerous areas where AI can fully or partially replace human labor. Let's consider some of these:

1) AI systems, adept at recognizing images and analyzing large data sets, are revolutionizing medical diagnostics. Notably, Odesa has pioneered the BrainScan telemedicine project in Ukraine. Powered by AI, this system significantly speeds up the diagnosis of brain diseases or injuries, where timely intervention is crucial (Artificial intelligence has begun to be used in Ukrainian hospitals, 2023).
2) AI and Natural Language Processing systems are used for automated content creation, text translation, or even performing customer service tasks through chatbots (Botpres, 2023
3) The use of AI in autonomous vehicles, such as self-driving cars employing machine vision and navigation systems for road control, exemplifies its application. Presently, the U.S. Department of Defense intends to deploy thousands of AI-powered autonomous vehicles by 2026 to maintain pace with China (Dig Watch – Geneva Internet, 2023).
4) The use of AI in automated legal analysis, for example, involves systems utilized for examining legal documents and resolving legal issues. Docket Key, Bloomberg Law's proprietary docket filing classification system, employs AI models to identify and search up to 20 essential document types across all federal district court dockets, enabling users to find the exact filing they require, such as briefs, motions, etc. (Artificial Intelligence for Lawyers Explained, 2023)
5) It's noteworthy that one of the most critical directions in AI technology development today is the creation of cognitive intelligence systems and cognitive information-telecommunication technology. These systems can learn, understand the world around them, independently analyze, and make decisions based on this analysis. IBM, in collaboration with several universities and commissioned by the U.S. Department of Defense, is implementing one such project (Sumari, Ahmad, 2018).
6) According to forecasts by IDC, future expenses on cognitive and AI systems are expected to increase by 200% annually between 2024 and 2027. Expenditures are anticipated to reach 500 billion

USD, tripling the figure from 2024, when expenses amounted to 154 billion USD (IDC, 2023).

Current statistical data on AI also reveal that its software represents the largest and fastest-growing technological category, accounting for about 40% of all expenditures on cognitive functions and AI (Artificial Intelligence – Worldwide, 2023).

The development and integration of AI systems across all spheres of human activity serve as a catalyst not only for positive outcomes but also for the negative consequences of its application, including its use in committing socially dangerous acts.

THE USE OF AI TECHNOLOGIES IN THE COMMISSION OF CYBERCRIMES

The advancement in ChatGPT and other generative AI technologies poses threats not only to human jobs but also increases the risk of cyber threats. AI can aid cybercriminals in quickly creating malicious software, automating attacks, and enhancing the efficiency of fraud or social engineering attacks using deepfakes and synthesized voices mimicking human speech. The escalation of cyber threats becomes increasingly perilous, with AI playing a significant role in this process.

Criminals, being ruthless and inventive, unsurprisingly also exploit AI for their criminal objectives. There are numerous possibilities for the misuse of AI systems in illicit activities within cyberspace. One of the most dangerous aspects of AI system utilization is the potential to develop a cybercriminal AI based on the GPTJ model, an open-source AI language model developed by Eleuther AI. GPT-J operates similarly to OpenAI's GPT-3 in various zero-shot tasks and can even be adapted for code generation tasks (GPT-J, 2024).

Utilizing the GPTJ AI model, cybercriminals can automate various processes of their criminal activities, ranging from crafting phishing emails to training future cybercriminals. An example of using the GPTJ model for illicit activities is WormGPT. The advancement of generative AI technologies, such as WormGPT, opens new horizons not only in creativity and workflow optimization but also in cybercrime. Developed based on the open-source GPTJ model in 2021, WormGPT embodies the dual-use nature of technologies – on one hand, offering potential for innovation, and on the other, serving as a tool for cybercriminals (WormGPT Cybercrime Tool Heralds an Era of AI Malware vs. AI Defenses, 2023).

The AI system WormGPT markedly elevates the threat landscape by facilitating the automated generation of phishing emails and malware. It's essential to underline key aspects of this AI system's role in cybercrime.

Firstly, it lowers the barriers to entry into cybercrime, enabling even inexperienced perpetrators to conduct complex attacks effectively. A correctly configured AI system like WormGPT can act as a training ground for cybercriminals, thereby automating the learning process. Such an AI system can help quickly master the basics of "virology," allowing cybercriminals to create their own malware while simultaneously testing it against system vulnerabilities and antivirus detection.

Secondly, the automation of creating malware and phishing emails through advanced AI technologies, like WormGPT, significantly enhances the potential for widespread attacks while reducing the preparation time and effort required.

Thirdly, AI systems' ability to analyze phishing email content, such as WarmGPT, using diverse technologies and techniques, assists cybercriminals in bypassing anti-spam systems of email services. It's crucial to highlight experiments conducted by SlashNext, underscoring WormGPT's strategic capabilities in generating persuasive phishing emails that could deceptively appear as legitimate inquiries. This ability to create content that can fool even experienced users underscores the critical need for enhanced cybersecurity measures and the development of new methods for identifying and countering such threats (WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks, 2023).

The use of technologies like WormGPT poses significant ethical questions about the responsibility for AI development and usage, demanding collective efforts from the scientific community, developers, and legislators to establish regulatory frameworks ensuring safety and protection against malicious use. Technologies akin to WormGPT remind us of the dual nature of innovations - their capacity to serve humanity while also introducing new challenges and threats. The importance of a responsible approach to AI development and usage cannot be overstated, with information security and cybercrime prevention at stake.

In our view, it is important to delve deeper into the ability of AI systems to generate phishing emails and messages, clone voices, and create deepfakes for authenticating identities on various commercial platforms. "Today, fraudsters use grammatically impeccable messages, comparable to native speakers," states S. Ranjan, co-founder and CEO of the anti-fraud startup Sardine. According to him, the number of bank clients falling victim to criminal activities is increasing as "correspondence from fraudsters approaches perfection." A similar view is shared by an unnamed representative from the fraud prevention department of one of the

American digital banks, who highlights the high quality of phishing messages, complicating their detection (AI helps everyone, even fraudsters. How Artificial Intelligence Became Cybercriminals' New Weapon and Fueled $8 Billion in Scams, 2023).

It's noteworthy that in the era of generative AI development, it has become exceptionally easy for cybercriminals to create deceptive texts, audio, and video materials capable of misleading not only individuals but also specialized anti-fraud programs. Modern generative AI technologies can render even the most effective current anti-fraud methods, such as voice authentication and real-time checks (like matching a person's face image with their photograph in a database, i.e., biometrics), obsolete. According to a survey conducted by Deep Instinct among 650 cybersecurity professionals, the majority noted an increase in cybercrime, with 85% attributing this rise to the use of AI by fraudsters (Businesswire, 2023).

The US Federal Trade Commission reported a record fraud loss of $8.8 billion last year, marking a 40% increase over 2021. Investment schemes were the most lucrative for criminals, while impersonation emerged as the most common fraud type, likely facilitated by AI advancements (FTC Consumer Response Center, 2022).

Criminals can train AI to mimic your communication style if you frequently share personal information online, enabling them to convincingly imitate your voice or writing to solicit money from relatives by claiming you are in distress. In the United States, there's a growing trend of targeting the elderly in fraud schemes, with cybercriminals often using landlines to mimic the voices of the victims' grandchildren or children. Victims report a high degree of similarity to the actual voices of their supposed relatives and note the thorough preparation of criminals who conduct detailed research into their targets' lives (CNBC, 2022)

This alarming phenomenon reflects not only the technical prowess of fraudsters in masterful imitation but also their ability to deeply analyze personal data and family relationships of their victims. Criminals utilize publicly available information, social networks, and other sources to gather data about their potential victims, allowing them to construct convincing narratives and emotionally manipulate the elderly. Additionally, the use of landline phones as a communication tool holds symbolic significance due to their prevalence among the older generation, thereby increasing this demographic group's vulnerability. Considering this, it is imperative to develop comprehensive countermeasures, including educational programs for the elderly aimed at enhancing their awareness of potential fraud schemes and teaching methods for their detection and prevention.

Cybercriminals are increasingly leveraging AI systems to circumvent anti-fraud measures developed by specialized companies. Identity verification organizations like Socure, Mitek, and Onfido have introduced "live checks" that require users to submit selfies or videos for comparison with existing images in the system. However, criminals familiar with this algorithm have adapted, using specialized software to create deceptive visual materials, complicating the process of authentic identity verification. Cybercriminals can acquire photographs of real documents, such as driver's licenses on the darknet, and then use accessible and cost-effective software to superimpose the face of a potential victim onto their own. This enables them not only to speak but also to simulate facial expressions using deepfake technology, effectively bypassing the "live check" procedure.

A journalist from 404media recently demonstrated a successful completion of the Know Your Customer (KYC) procedure on the cryptocurrency exchange OKX, using a service capable of generating counterfeit documents through AI (404 MEDIA, 2024).

According to information published by Cointelegraph, similar successful attempts to bypass identity verification procedures have been made on other platforms, including Kraken, Bybit, Bitget, Huobi, and PayPal (AI-generated fake IDs claimed to pass crypto exchange KYC are selling for $15, 2024).

The service named OnlyFake offers its services at a price of $15, highlighting the affordability and economic attractiveness of such tools for circumventing security systems. This case emphasizes not only the growing threat posed by AI systems in the context of financial security but also points to the need for enhanced control and verification measures on cryptocurrency exchanges and other financial platforms. Rick Song, CEO of Persona, a company specializing in combating fraud, noted a significant increase in the use of deepfakes to circumvent live checks, with some sectors experiencing up to a tenfold increase compared to last year. Fintech and crypto companies have been most affected (Forbes, 2022).

Fraud prevention experts express concern over deteriorating statistics among user verification service providers like Socure and Mitek. Socure disputes these concerns but admits delays in system updates by some clients could hinder fraud prevention efforts, revealing that three of its major bank clients missed four updates (Source Media, 2018).

Banking giants including JPMorgan, Bank of America, and Wells Fargo have refrained from commenting on fraud issues related to AI technologies. Meanwhile, a representative from Chime, the largest digital bank in the US, which previously faced serious fraud challenges, claims the company has not seen an increase in criminal schemes utilizing AI systems (Chime®., 2023).

These challenges require companies specializing in fraud prevention to continuously update and refine their technologies and verification methods to effectively counter the constantly evolving threats posed by AI.

Among other examples of the use of AI systems by cybercriminals, it is worth highlighting:

1) AI systems enable cybercriminals to rapidly create malicious software by automating and optimizing the malware development process. This allows for the generation of large volumes of malicious code quickly, challenging the effectiveness of antivirus programs and cyber defense mechanisms. Additionally, AI can identify vulnerabilities in software and automatically generate code to exploit these weaknesses, enhancing the efficiency of cyber-attacks and reducing the time needed to develop malicious programs.
2) AI systems facilitate automated targeted phishing by using natural language processing algorithms to create convincing phishing emails that are nearly indistinguishable from legitimate messages. This includes adapting the language, style, and content to a specific target audience, increasing the likelihood that the recipient will fall for the phishing attempt. With the ability to analyze large volumes of data on potential targets, criminals can scale their phishing campaigns, making them highly targeted and effective.
3) AI-enhanced botnets enable cybercriminals to evade detection and adapt their attacks in real-time. AI specialized systems, known as stressors, analyze network behavior and identify patterns that help botnets avoid standard defense mechanisms while coordinating distributed attacks with high precision and efficiency. This real-time adaptation significantly complicates the detection and neutralization of botnets.

Cybersecurity professionals are actively integrating AI to enhance cyber threat analysis, employing behavioral analysis for identifying potential dangers without solely relying on threat signatures, and automating processes for proactive attack detection. However, cybercriminals have a significant advantage in utilizing AI systems, particularly through adversarial machine learning techniques. These methods allow criminals to manipulate AI systems by inserting malicious data and exploiting weaknesses in algorithms, potentially leading to incorrect system conclusions.

Furthermore, cybercriminals can fabricate data and manipulate machine learning models, jeopardizing the reliability and accuracy of AI-based cybersecurity platforms. If they gain access to the training data, they can undermine the effectiveness of these systems, rendering them unreliable and inaccurate in threat detection.

PROSPECTS OF USING AI IN CRIME PREVENTION AND INVESTIGATION

Cybercrime has had an unprecedented impact across various industries, with damages projected to exceed $10 trillion by 2025 (BeInsure, 2024).

In the current era of digitalization, ensuring robust cybersecurity is critically important, more than ever, as business leaders strive to adapt to a constantly evolving environment. The impact of AI in cybersecurity is expected to significantly increase, becoming an increasingly essential element in this field. The market value of AI systems in cybersecurity is projected to reach $46.3 billion by 2027. Companies specializing in AI-powered cybersecurity offer significant advantages, providing organizations with crucial tools for effective cybersecurity management and enhancing adaptability to modern cyber threats (Artificial intelligence (AI) in cyber security market value worldwide from 2019 to 2027, 2022).

The adoption of AI technologies in cybersecurity offers significant potential to enhance organizational defines mechanisms and reduce the workload on professionals in the field. AI-based tools enable the automation of routine security procedures, freeing up expert resources to focus on critical tasks.

AI systems play a crucial role in monitoring and analyzing cybersecurity incidents, identifying anomalies, and optimizing the threat detection process. Machine learning algorithms, capable of recognizing malicious activity, allow professionals to concentrate their efforts on investigations and threat neutralization.

A successful example of AI systems implementation in cybersecurity is Bitdefender's experience. Specifically, the company's GravityZone eXtended Detection and Response (XDR) solution utilizes AI technologies for correlating and analytically reviewing vast volumes of security data collected from various sensors and information sources within an organization (AVDetection, 2023).

At the current stage of technological development, AI is actively used to automate processes of analysis and threat detection in the context of cybercrime investigations. Through machine learning methods, AI systems are capable of processing large datasets, including network traffic, server logs, email correspondence, and other information sources.

Additionally, generative AI systems can be employed to create user profiles and determine standard behavior patterns, enabling the detection of atypical activity and preventing potential cyberattacks before they occur. Overall, the automation of analysis and threat detection processes during cybercrime investigations significantly enhances the efficiency of cybersecurity professionals and provides a higher level of protection against cyberattacks.

It is worth highlighting the advantages and disadvantages of using AI systems in the investigation and prevention of cybercrimes.

Advantages of using AI in the fight against cybercrime	**Disadvantages of using AI in the fight against cybercrime**
Speed – the ability to process large volumes of data in real-time, enabling the swift identification and response to cyber threats.	**Limited understanding** – relying on the analysis of historical data, which can complicate the identification of new types of cyberattacks that differ from known patterns.
Precision – the capability, based on algorithms, to identify patterns and anomalies that may remain unnoticed by humans, thereby increasing the accuracy of cybercrime risk analysis.	**High cost** – the development and implementation of AI-based systems require substantial financial investments, including costs for development, maintenance, and electricity.
Scalability – adaptability to various network sizes, simplifying the work of law enforcement agencies with investigations of different scales.	**Privacy issues data** – the application of AI requires the collection of large amounts of information, raising concerns about privacy and the protection of personal data.

Table 1 - The advantages and disadvantages of using AI in the fight against cybercrime are developed by the authors.

AI has the potential to fundamentally transform cybercrime investigation methods through its ability to detect patterns and anomalies in large data volumes. However, the application's effectiveness is directly linked to the quality of the data analyzed and the precision of the algorithms developed. To optimize cybercrime investigation outcomes, law enforcement agencies must make significant investments in AI-based solution development and implementation. This encompasses not only financial contributions to technological advancements but also the creation of a proper database and the adaptation of algorithms to ensure high accuracy and effectiveness in the dynamically changing cyberspace. AI has enormous potential when it comes to cybercrime investigations. It can be used in a variety of ways, including:

Detection of anomalies. AI can analyze vast amounts of data, detecting anomalies that deviate from established norms, and identifying potential threats based on behavioral analyses and anomalies. User and Entity Behavior Analytics (UEBA) plays a crucial role in this process, focusing on the analysis of user and system behavior to identify insider attacks or compromised accounts (CrowdStrike, 2023).

Malware detection. Projects utilizing AI systems for surface defect detection or monitoring invasive species demonstrate AI's adaptability and effective analysis of specific tasks. This capability can be applied to identify malicious software by analyzing file characteristics, code patterns, and behavior (Saiwa, 2023).

Countering zero-day attacks. Research based on the UNSW-NB15 dataset highlights the importance of adapting to adversarial conditions, underscoring AI's capability in detecting malicious activities and software, thereby enabling effective defines against zero-day attacks (Bierbrauer, Kritzer, Chang Bastian, 2022).

Analysis of threats. The use of AI systems for threat analysis includes the automated collection of security information from various sources, including the dark web, ensuring the ability to detect new threats and provide valuable insights. Experiments with unsupervised and graph-based methods for anomaly detection demonstrate AI's capability for efficient identification of anomalous patterns (Bierbrauer, Kritzer, Chang Bastian, 2022).

Security analytics. Security analytics using AI systems involves analyzing large volumes of security data and incidents to identify trends and malicious activities. The effectiveness of this approach is demonstrated through projects that apply AI to specific tasks, such as defect detection or monitoring environmental threats (Saiwa, 2023).

In the context of cybersecurity evolution, the development of AI-based cybercrime prevention systems represents a cutting-edge direction in technological innovation. This methodology involves aggregating and analytically processing extensive datasets related to cyberattack incidents and identified vulnerabilities in defines systems. These data serve as a foundation for training machine learning algorithms designed to detect recurring behavioral patterns characteristic of such attacks. The application of these machine learning models not only allows for the analysis of the current cybersecurity state but also for the prediction of potential threats and the formulation of effective preventive response strategies. Cybersecurity professionals use these models to identify maximum possible risks and develop measures aimed at neutralizing these threats. Additionally, these systems are capable of automated monitoring and neutralization of cyberattacks in real-time. Thanks to machine learning algorithms that analyse user behavior and security mechanism parameters, the system can autonomously identify and respond to anomalies indicative of unauthorized cyber activity.

Undoubtedly, a cybercrime prevention system based on AI systems must meet certain requirements, in particular:

1) Network traffic monitoring – the integration of capabilities for comprehensive scanning of network activities to identify anomalies or potential threats signaling cyberattacks or other vulnerabilities.
2) Network activity visualization – the development of tools for graphically representing network flows enables quick identification of potential risk points and simplifies the threat identification process.
3) Risk analysis – applying AI for analytical assessment of threats and risks, allowing for the detection and classification of potential attack vectors.
4) Early warning – utilizing data analytics and machine learning to detect typical or new threats, aiming to initiate preventive measures.
5) Proactive protection – adapting security systems to changing threat conditions, providing a dynamic response to potential attacks.
6) Rapid incident investigation – effective incident management through analysis, reporting, and detailed investigation of situations, with the goal of developing response measures and enhancing network security.

In the context of strengthening cybersecurity measures, the implementation of AI in cybercrime prevention systems shows significant potential in detecting and countering cyberattacks. We have identified the following methodological approaches to the implementation of the analyzed systems.

Method	Description	The potential of AI applications	Observation itself
Data flow analysis	Deep analysis of network data to identify anomalies.	Machine learning algorithms can recognize illegal patterns of behavior	Requires constant updating of data to train models.

		that indicate cyber-attacks.	
Email monitoring and analysis	Automatic detection of phishing, spam, and viruses.	Using trained models to filter malicious messages.	Difficulty adapting to new phishing methods.
Continuation Of the Table 2			
Vulnerability modelling	Network analysis to identify potential weaknesses.	Predicting and simulating attacks to determine optimal defense strategies.	The importance of regularly updating models in view of new threats.
Blocking access	Automatic access restriction for potential threats.	Adaptive systems that quickly respond to changes in user or network behavior.	Risk of unjustified access restriction for legitimate users .
Attack handling	Localization and minimization of the consequences of cyber-attacks.	Automated incident response for fast resolution.	The need for constant updating of knowledge about new types of attacks.

Table 2 - The methodological approaches to implementing artificial intelligence in cybercrime prevention systems. Developed by the authors.

An important aspect of using AI systems in combating cybercrime is the expert component. In our view, the use of AI systems can enhance the efficiency of cybersecurity professionals. Since the cybersecurity systems themselves, built on AI, can automatically analyse a vast number of threats that may remain unnoticed by humans, cybersecurity professionals can focus on the most critical tasks and make informed decisions.

Optimizing the effectiveness of cyber security measures can be achieved through the implementation of the following strategies based on the application of AI:

1) The use of AI algorithms for automating the process of identifying potential vulnerabilities and anomalies in information systems allows cybersecurity experts to minimize the time spent on routine checks and focus on the development and implementation of protective mechanisms.
2) Using AI for training and developing the skills of cybersecurity professionals through the application of machine learning methods and data analysis to improve their competencies.

3) Monitoring employee activities to detect improper or dangerous actions, such as illegal file downloads or visiting suspicious websites.

These approaches not only enhance the overall efficiency of cybersecurity systems but also contribute to more effective resource use, optimization of specialists' working time, and increased protection of information systems against contemporary cyber threats.

CONCLUSIONS

The digital era and information technology face an unprecedented surge in cybercrime, presenting complex challenges in information security protection. The development and implementation of AI in cybersecurity open new perspectives for effective cybercrime countermeasures, threat identification and analysis automation, and strengthening of information system defenses. However, AI usage also imposes continuous learning and adaptation to the latest technologies on cybersecurity professionals, alongside the development and adherence to ethical and legal standards.

The application of AI in cybersecurity demonstrates significant potential for enhancing the efficiency of cybercrime investigations, anomaly detection automation, zero-day attack countermeasures, and preventive strategy development. Despite potential risks associated with cybercriminals using AI to sophisticate attacks and bypass security systems, integrating AI into cybersecurity strategies offers more intelligent, adaptive, and effective protection methods.

The practical value of this research lies in analyzing the methods and means of using AI systems in cybercriminal activities based on a comprehensive review of cybersecurity data. These approaches are valuable for the public and cybersecurity companies, as they assess the risks and possibilities of AI utilization by cybercriminals.

AI's practical implementation in cybersecurity enables organizations not only to significantly reduce data loss and financial damages from cyberattacks but also to increase overall adaptability and response to new cyber threats. This is achieved through automating routine tasks, freeing up specialists' time for strategic cybersecurity aspects and comprehensive defense mechanism development.

Moreover, AI aids in developing cybercrime prevention systems based on threat prediction and effective response strategy formation. This not only enhances the security level of information systems but also contributes to creating a more resilient digital environment.

Implementing AI in cybersecurity is crucial for training and skill development in the field, offering advanced methods and tools to enhance professional competencies. Thus, integrating AI into cybersecurity strategies not only improves technical security system enhancements but also fosters professional potential in the field, increasing the overall effectiveness of cybersecurity measures.

Therefore, introducing AI systems into cybersecurity is multifaceted, covering both the technical improvement of identifying and countering cyber threats and the professional development of specialists, impacting the resilience of information systems amid constantly evolving cyber threats.

REFERENCES

404 MEDIA. (2024, February 5). Inside the underground site where 'neural networks' churn out fake IDs. Available at: https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/

Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cybersecurity. *Scientometrics,* 121, 1189-1211. https://doi.org/10.1007/s11192-019-03222-9

AI helps everyone, even fraudsters. How Artificial Intelligence Became Cybercriminals' New Weapon and Fueled $8 Billion in Scams. (2023). Forbes. Available at: https://forbes.ua/innovations/shi-dopomagae-vsimi-navit-shakhrayam-yak-shtuchniy-intelekt-stimulyuvav-aferi-na-8-mlrd-19092023-16102

AI Liability Directive. (2024). Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496

AI-generated fake IDs claimed to pass crypto exchange KYC are selling for $15. (2024). Cointelegraph. Available at: Available at: https://cointelegraph.com/news/roblox-ai-translation-llm-metaverse-languages

Almazroi, A. A., & Ayub, N. (2023). Online Payment Fraud Detection Model Using Machine Learning Techniques. *IEEE Access,* 11, 137188-137203. https://doi.org/10.1109/ACCESS.2023.3339226

Artificial intelligence (AI) in cyber security market value worldwide from 2019 to 2027. (2022). Statista. Available at: Available at:

https://www.statista.com/statistics/1291380/ai-in-cyber-security-market-size/

Artificial Intelligence Act. (2024, March 13). High-level summary of the AI Act. Available at: https://artificialintelligenceact.eu/high-level-summary/

Artificial Intelligence for Lawyers Explained. (2023). Bloomberg law. Available at: https://pro.bloomberglaw.com/insights/technology/ai-in-legal-practice-explained/#whatAI

Artificial intelligence has begun to be used in Ukrainian hospitals. (2023). Information agency Union. Available at: https://www.unian.ua/health/v-ukrajinskih-likarnyah-pochali-vikoristovuvati-shtuchniy-intelekt-12390489.html

Automation and the future of work – understanding the numbers. (2018). Oxford Martin School. 13.04.2018. Available at: https://www.oxfordmartin.ox.ac.uk/blog/automation-and-the-future-of-work-understanding-the-numbers/

AVDetection. (2023). Extended Observability, Automated Detection, and Guided Response for the Entire Organization. Available at: https://avdetection.com/GravityZone-XDR.asp#:~:text=Bitdefender%20GravityZone%20XDR%20is%20a,endpoints%2C%20network%2C%20and%20cloud.

Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics,* 12(8), 1920. https://doi.org/10.3390/electronics12081920

BeInsure. (2024, January 2). Top 20 Cybercrime Predictions for 2024-2025. Available at: https://beinsure.com/cybercrime-predictions/

Bierbrauer, D. A., Kritzer, W., Chang, A., & Bastian, N. D. (2022). Cybersecurity Anomaly Detection in Adversarial *Environments*. Retrieved from https://ar5iv.labs.arxiv.org/html/2105.06742v1

Botpres. (2023, April 4). How does AI relate to natural language processing? Available at: https://botpress.com/blog/how-does-ai-relate-to-natural-language-processing

Businesswire. (2023, August 23). Deep Instinct Study Finds Significant Increase in Cybersecurity Attacks Fueled by Generative AI. Available at: https://www.businesswire.com/news/home/20230821068264/en/Deep-Instinct-Study-Finds-Significant-Increase-in-Cybersecurity-Attacks-Fueled-by-Generative-AI

Centre for Economic Policy Research. (2023, July 20). The impact of artificial intelligence on growth and employment. Available at:

https://cepr.org/voxeu/columns/impact-artificial-intelligence-growth-and-employment

Chime®. (2023, October 23). Reporting frauds and scams explained. Available at: https://www.chime.com/blog/fraud-vs-scams-what-you-need-to-know/

CNBC. (2022, April 2). FBI: 'Financial sextortion' of teens is a 'rapidly escalating threat.' How parents can protect their kids. Available at: https://www.cnbc.com/2024/02/01/fbi-financial-sextortion-of-kids-is-escalating-what-parents-can-do.html

CrowdStrike. (2023, September 7). What is AI-Powered Behavioral Analysis in Cybersecurity. Available at: https://www.crowdstrike.com/cybersecurity-101/secops/ai-powered-behavioral-analysis/

Dig Watch – Geneva Internet Platform. (2023, October 28). US military to deploy thousands of AI-enabled autonomous vehicles by 2026. Available at: https://dig.watch/updates/us-military-to-deploy-thousands-of-ai-enabled-autonomous-vehicles-by-2026

Forbes. (2022, July 2). Onslaught of deepfakes: How the maker of Photoshop is fighting a problem of its own making. Available at: https://forbes.ua/inside/nashestvie-dipfeykov-kak-adobe-boretsya-s-problemoy-kotoruyu-sama-porodila-01072022-6937

FTC Consumer Response Center. (2022, January 22). New data shows FTC received 2.8 million fraud reports from consumers in 2021 [Press release]. Available at: https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

Harel, Y., Ben Gal, I., & Elovici, Y. (2017). Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. *ACM Transactions on Intelligent Systems and Technology*, 8(4), 1–12. https://doi.org/10.1145/3057729

IAPP Research and Insights. (2024, January 21). Global AI Law and Policy Tracker. Available at: https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf

IDC. (2023, October 26). IDC FutureScape: Artificial Intelligence Will Reshape the IT Industry and the Way Businesses Operate. Available at: https://www.idc.com/getdoc.jsp?containerId=prUS51335823

Khalel, S. I., & Khudher, S. M. (2022). Cyber-Attacks Risk Mitigation on Power System via Artificial Intelligence Technique. *Paper presented at the 9th*

International Conference on Electrical and Electronics Engineering (ICEEE). https://doi.org/10.1109/ICEEE55327.2022.9772559

Kokotajlo, T., Long, D., Reith, M., & Dill, R. (2021). Artificial Intelligence Within Agile Software Development: Projected Impacts to Cyber Offense-Defense Balance. *In 3rd European Conference on the Impact of Artificial Intelligence and Robotics (ECIAIR)*, pp. 78-81. DOI: 10.34190/EAIR.21.030

McKinsey & Company. (2017, October 28). Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages. Available at: https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

Recurrent Ventures Inc. (2019, October 1). Former Google exec: AI will replace 40 percent of jobs in 15 years. Available at: https://futurism.com/the-byte/google-ai-jobs

Saiwa. (2023, December 11). Everything You Need to Know About Anomaly Detection in Cybersecurity. Available at: https://saiwa.ai/blog/anomaly-detection-in-cybersecurity/

Samtani, S., Chen, H., Kantarcioglu, M., & Thuraisingham, B. (2022). Explainable Artificial Intelligence for Cyber Threat Intelligence (XAI-CTI). *IEEE Transactions on Dependable and Secure Computing*, 19(4), 2149-2150. https://doi.org/10.1109/TDSC.2022.3168187

Shadska, U. (2024, February 15). Human rights in the era of artificial intelligence: challenges and legal regulation. Available at: https://www.scribd.com/document/705953643/ПРАВА-ЛЮДИНИ-В-ЕПОХУ-ШТУЧНОГО-ІНТЕЛЕКТУВИКЛИКИ-ТА-ПРАВОВЕ-РЕГУЛЮВАННЯ

Smirnov, I. (2023). Legal regulation of artificial intelligence: international experience and Ukrainian perspectives. Available at: https://biz.ligazakon.net/analitycs/223351_pravove-regulyuvannya-shtuchnogo-ntelektu-mzhnarodniy-dosvd-taukransk-perspektivi

Source Media. (2018). The problem with—and solution for—identity verification. Available at: https://www.socure.com/blog/the-problem-with-and-solution-for-identity-verification

Sumari A. D. W., Ahmad A. S. (2018). Cognitive Artificial Intelligence: Concept and Applications for Humankind. *Intelligent System.* DOI: 10.5772/intechopen.72764

Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial Intelligence and Cybersecurity: Past, Presence, and Future. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 351-363). *Advances in Intelligent Systems and Computing*, Volume 1056. https://doi.org/10.1007/978-981-15-0199-9_30

Vahakainu, P., & Lehto, M. (2019). Artificial Intelligence in the Cyber Security Environment. In 14th International Conference on Cyber Warfare and Security (ICCWS), pp. 431-440. Available at: ResearchGate: https://www.researchgate.net/publication/338223306_Artificial_intelligence_in_the_cyber_security_environment_Artificial_intelligence_in_the_cyber_security_environment

WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks. (2023). SlashNext. Available at: https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/

WormGPT Cybercrime Tool Heralds an Era of AI Malware vs. AI Defenses. (2023). Available at: Darkreading. https://www.darkreading.com/cyberattacks-data-breaches/wormgpt-cybercrime-tool-heralds-an-era-of-ai-malware-v-ai-defenses

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55, 1029–105. https://doi.org/10.1007/s10462-021-09976-0

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET