The Potential Threat of Artificial Intelligence Use in Cybercrime Activities: A Case Study of 2024 Regional Head Elections

Lytio Enggar Erlangga[1], Muhammad Syaroni Rofii[2], Eko Daryanto[3]
[1,2,3]Universitas Indonesia, Depok, Indonesia
Email: lytio.enggar@ui.ac.id

Abstract

The adoption of artificial intelligence (AI) has significantly increased in recent years, offering both opportunities and challenges. While AI enhances efficiency across various sectors, it also introduces new risks, particularly in the realm of cybercrime. This study explores the potential threats posed by AI-driven cybercrime activities in the context of the 2024 Regional Head Elections (Pilkada) in Indonesia. Using a qualitative method with literature review and document analysis, the research identifies three key threat domains: cybersecurity, physical security, and political security. AI enables cybercriminals to launch sophisticated and hard-to-detect attacks, such as phishing, misinformation campaigns, and distributed denial-of-service (DDoS) attacks. These threats could disrupt electoral processes, manipulate voter behaviour, and compromise the integrity of election outcomes. The study highlights how AI-driven attacks can also exploit Internet of Things (IoT) devices and spread deepfakes and political bots to influence public perception. With the rapid advancement of AI, traditional cybersecurity measures may struggle to keep pace, making it imperative for authorities and cybersecurity experts to strengthen monitoring and response capabilities. This research emphasizes the need for robust strategies to mitigate AI-driven cyber threats and safeguard the integrity of the electoral process in Indonesia.

Keywords: *Artificial Intelligence, Cybercrime, 2024 Regional Head Elections, Cybersecurity, Misinformation, Political Security.*

A. INTRODUCTION

The use of artificial intelligence (AI) has significantly increased over the past decade. According to a survey conducted by McKinsey (2022) in its report The State of AI in 2022 – and half decade in review, AI adoption has doubled from 2017 to 2022. In 2017, 20% of respondents reported utilizing AI in at least one business area, and this figure increased to 50% by 2022. This rise in AI adoption coincided with the average AI capabilities leveraged by organizations, such as natural language generation and computer vision, which doubled from 1.9% in 2018 to 3.8% in 2022. The most widely used AI capabilities are robotic process automation (39%), computer vision (34%), and natural language generation (33%).

The increasing trend in AI utilization can be a double-edged sword. On one hand, AI is widely employed to simplify human tasks in various domains, but on the other hand, it can be used for negative purposes, such as facilitating criminal activities in the cyber realm (Taddeo et al., 2019). The term "malicious use of AI" generally refers to actions that intentionally cause harmful consequences (Schneider & Breitinger, 2023). According to the report titled The Malicious Use of Artificial Intelligence:

Forecasting, Prevention, and Mitigation, the malicious use of AI poses threats in three key sectors: cybersecurity, physical security, and political security (Miles Brundage et al., 2018). AI's ability to analyse, process data, and make decisions can certainly enable cybercriminals to optimize their actions while evading detection. One of the main challenges in addressing the negative implications of AI use in cybercrime is that AI-based attacks are more difficult to detect and mitigate compared to traditional attacks. This is due to AI's adaptive nature and its ability to evolve over time, making traditional security measures less effective (Caldwell et al., 2020).

As the 2024 Regional Head Elections (Pilkada) in Indonesia approach, the potential misuse of AI in cybercrime has become a relevant issue. Elections are the cornerstone of democratic societies, and safeguarding the integrity of the electoral process is crucial. In the digital age, election-related cyberattacks—such as AI-driven disinformation campaigns, voter manipulation, and the hacking of election systems—can undermine the legitimacy of the elections. AI's ability to autonomously generate content and adapt to real-time data makes it a powerful tool for influencing political outcomes. Therefore, understanding and preparing for these threats is essential to ensuring a fair and transparent election process. This article aims to provide an overview of the potential threats posed by cybercriminals utilizing AI in cybercrime activities leading up to the 2024 Regional Head Elections, including threats in the realms of cybersecurity, physical security, and political security.

B. LITERATURE REVIEW

1. Cybercrime Theory

Cybercrime is defined as criminal activities that involve computers or networks as tools, targets, or venues for crime. Cybercrime encompasses various activities, from data theft to system sabotage. In the context of elections, cyber threats are often aimed at manipulating election results, disrupting infrastructure, or spreading misinformation(Taddeo et al., 2019). AI-based cybercrime increases the complexity of such attacks since AI technology can accelerate, personalize, and autonomously modify attacks, making them more difficult to detect and counter (Caldwell et al., 2020).

2. Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) is the capacity of computer systems to perform tasks that typically require human intelligence, such as decision-making, problem-solving, and language comprehension. In cybersecurity, AI is used in two main ways: to enhance security by detecting and responding to threats and as a tool for attacks in the form of automated cyber-attacks. For example, AI can aid in personalized spear-phishing or continuously launching Distributed Denial of Service (DDoS) attacks. AI technology is also used to create deepfakes, which are manipulative videos or audio that can imitate someone's voice or face, often used to damage politicians' reputations or spread misinformation (Ahmed, 2022).

3. Public Opinion Manipulation through Disinformation

Public opinion manipulation is the process in which individuals or groups intentionally steer the masses' opinions on a particular issue by using false or misleading information. With AI, disinformation dissemination becomes more efficient and harder to detect. Bot and deepfake technology are two examples of AI applications that can effectively spread false narratives and manipulate public opinion (Bazarkina & Pashentsev, 2020). AI-driven bots can amplify false narratives or polarize society, creating an illusion of widespread support or dissatisfaction. Meanwhile, deepfakes allow malicious actors to create hyper-realistic but fake videos or audio, misleading the public and influencing perceptions of political candidates or issues (Veerasamy & Pieterse, 2022).

4. Election Security

Election security involves efforts to protect the integrity, accuracy, and confidentiality of the election process from various threats, both physical and digital. According to this theory, election security threats extend beyond election results manipulation to include any form of attack that could disrupt, intimidate, or influence voters. In the digital age, AI has become one of the primary threats to election security, as it can be used to disrupt election infrastructure, such as voting systems or voter monitoring (Deepak et al., 2023). These threats not only erode public trust in election outcomes but also destabilize political and democratic systems.

5. Cybersecurity Regulation and Policy

Cybersecurity regulation and policy theory includes guidelines and regulations that aim to protect information systems from external and internal threats. In the context of elections, strong policy enforcement and proactive security measures are essential to address the sophisticated threats posed by AI in cybercrime. Montasari (2023) emphasizes the importance of collaboration between the government and relevant agencies to establish a legal framework that can monitor and regulate AI use in political and electoral contexts. With clear regulations, the negative impact of deepfake and bot technology on political processes can be minimized, thus maintaining public trust in the electoral system.

C. METHOD

This study employs a qualitative method with a literature review and document analysis approach to understand the potential threats posed by artificial intelligence (AI) in cybercrime activities, particularly in the context of the 2024 Regional Head Elections in Indonesia. Data collection was conducted through a review of literature from scientific journals, research reports, and reliable publications relevant to the research theme. The selection of references focuses on topics related to cybersecurity, physical security, and political security impacted by AI, making it relevant to the context of AI threats in elections. Below is an overview of the key literature supporting this study:

Table 1. Overview of the Key Literature Supporting

No	Author	Year	Topic/Research Focus	Key Findings
1	Isabella Hansen, Darren J. Lim	2019	Doxing democracy: influencing elections via cyber voter interference	Explores state-sponsored cyber interference in elections and potential AI applications in voter manipulation.
2	Bülent Yener, Tsvi Gal	2019	Cybersecurity in the Era of Data Science: Examining New Adversarial Models	AI vulnerabilities lead to adversarial cybersecurity models, requiring advanced algorithms to mitigate election-related risks.
3	Pascal D. König, Georg Wenzelburger	2020	Opportunity for Renewal or Disruptive Force? How AI Alters Democratic Politics	AI can disrupt democratic processes through misinformation and automated disinformation, urging ethical and regulatory frameworks.
4	Uche Eme-Uche, Elechi Felix Aja, Chigozie Okonkwo	2020	Electoral Security and Voter Turnout in the 2019 Gubernatorial Election in Abia State	Security threats in elections can lower voter turnout, highlighting the need for reforms to secure voter confidence.
5	Darya Bazarkina, Evgeny Pashentsev	2020	Malicious Use of Artificial Intelligence	Stresses BRICS collaboration to regulate malicious AI use, addressing risks like deepfakes and phishing in elections.
6	Doowon Jeong	2020	Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues	Classifies AI crimes as tool or target-based, urging enhanced AI forensics for democratic integrity.
7	Ludovic Rheault, Andreea Musulan	2021	Efficient detection of online communities and social bot activity	Highlights AI's role in manipulating social media for election

No	Author	Year	Topic/Research Focus	Key Findings
			during electoral campaigns	influence, especially through bot detection.
8	HuYupeng, KuangWenxin, QinZheng, LiKenli, ZhangJiliang, GaoYansong, LiWenjia, LiKeqin	2021	Artificial Intelligence Security: Threats and Countermeasures	AI poses new cybersecurity risks in elections, like misinformation campaigns and automated attacks, necessitating stronger protocols.
9	Nektaria Kaloudi, Jingyue Li	2021	The AI-Based Cyber Threat Landscape: A Survey	AI-driven cyber threats in elections include targeted disinformation, phishing, and security vulnerabilities analysis.
10	Matyáš Boháček, Hany Farid	2022	Protecting world leaders against deep fakes using facial, gestural, and vocal mannerisms	Identity-based approach to distinguish leaders from deepfake imitators, protecting electoral integrity.
11	T. Blauth, Oskar Josef Gstrein, Andrej Zwitter	2022	Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI	Categorizes malicious AI uses, emphasizing collaboration to combat risks in cybersecurity and political integrity.
12	Yingjie Zeng	2022	AI Empowers Security Threats and Strategies for Cyber Attacks	AI-based systems pose threats to physical security by identifying vulnerabilities, with risks in deepfake misinformation and election manipulation.
13	Sarfraj Ahmed	2022	Impact of Deepfake Technology on Digital World Authenticity	Deepfake technology threatens public trust in political processes, with the rapid spread of misinformation.

No	Author	Year	Topic/Research Focus	Key Findings
14	Namosha Veerasamy, Heloise Pieterse	2022	Rising Above Misinformation and Deepfakes	Deepfakes, along with bots, amplify misinformation campaigns, harming democracy and trust in media.
15	Hina Shahzad, Furqan Rustam, Emmanuel Soriano Flores, Juan Luís Vidal Mazón, Isabel de la Torre Díez, Imran Ashraf	2022	A Review of Image Processing Techniques for Deepfakes	Deepfakes threaten political trust and can spread quickly on social media, complicating misinformation control.
16	Darya Bazarkina, Darya Matyashova	2022	"Smart" Psychological Operations in Social-Media: Security Challenges in China and Germany	Malicious AI applications, including bots and deepfakes, risk societal cohesion and democratic processes.
17	Mark Coeckelbergh	2022	Democracy, epistemic agency, and AI: political epistemology in times of artificial intelligence	AI, including deepfakes and bots, disrupts democratic knowledge foundations by undermining citizen trust in information.
18	P. Deepak, Stanley Simoes, Muiris MacCarthaigh	2023	AI and Core Electoral Processes: Mapping the Horizons	AI applications in voting booths raise privacy and security risks, with potential for misuse in surveillance and data exploitation.
19	S. R. Asiryan	2023	Use of AI During Elections, Threats to Voting Rights and Overcoming Them	Highlights the need for strong legal frameworks to mitigate AI misuse in elections, focusing on transparency and accountability.

No	Author	Year	Topic/Research Focus	Key Findings
20	Sandeep Singh Mankoo	2023	DeepFakes - The Digital Threat in the Real World	Deepfakes threaten election integrity by impersonating candidates, causing voter confusion and damaging democratic processes.
21	Reza Montasari	2023	Internet of Things and Artificial Intelligence in National Security	AI and IoT pose significant political security threats, including the use of deepfakes to manipulate public opinion.
22	Elina B. Urtaeva	2024	Opportunities and Threats of using Artificial Intelligence in Political Communications	The use of AI in political communications carries dual risks, notably deepfake proliferation and selective misinformation.

D. RESULT AND DISCUSSION

The use of artificial intelligence (AI) in cybercrime activities leading up to the 2024 Regional Head Elections (Pilkada) in Indonesia presents significant threats that impact cybersecurity, physical security, and political security. AI not only amplifies existing cyber threats but also introduces new, more sophisticated, and harder-to-detect forms of attacks. This technology enables cybercriminals to launch automated and highly precise attacks, often without the need for physical presence. These threats pose serious risks to the integrity of democratic processes, particularly in elections that involve many stakeholders and complex procedures. In this section, the analysis of AI threats is categorized into three subsections: cybersecurity threats, physical security threats, and political security threats.

1. Cybersecurity Threats

The rise of AI in cybersecurity threats marks a shift in both the sophistication and reach of cybercrime activities. AI technology enhances traditional methods of cyberattacks, such as phishing and DDoS, by automating and personalizing malicious actions at unprecedented scales. Kaloudi & Li (2021) highlight how AI-driven cyber

threats, including targeted disinformation and phishing, are particularly concerning for their potential to manipulate public opinion and compromise security infrastructure in elections. Attackers now have the ability to conduct thorough scans of systems for vulnerabilities autonomously, generating a continuous stream of malicious activities. These capabilities are critical during elections, where digital infrastructure—ranging from voter databases to voting machines—faces heightened risk from cyberattacks aiming to influence election outcomes. The precision of AI in gathering and analyzing information allows for crafting highly tailored phishing emails that mimic friends or colleagues, often making such attacks indistinguishable from legitimate communication (Rheault & Musulan, 2021).

Furthermore, the use of AI to streamline and amplify spear-phishing techniques makes these cyber threats even harder to detect and prevent. AI-powered systems can analyze public and social network data to identify high-value targets, selecting influential individuals or groups for attack. This level of analysis allows attackers to develop phishing messages that are uniquely relevant to their targets, which increases the likelihood of gaining unauthorized access to sensitive information or funds (Blauth et al., 2022). With automated attacks, AI systems can launch DDoS campaigns or other disruptions continuously, exhausting security resources and further exposing vulnerabilities within electoral systems. These cyberattacks underscore the need for advanced cybersecurity protocols capable of countering the growing complexity and adaptiveness of AI-driven threats, particularly during election periods when the integrity of democratic processes is at stake (Jeong, 2020).

2. Physical Security Threats

The increasing integration of AI with IoT devices has amplified physical security threats, especially within critical infrastructures, as these devices become an expanded surface for cyberattacks. Cybercriminals can exploit IoT vulnerabilities to deploy malware, disrupting essential services. According to Deepak et al. (2023), AI in IoT not only raises significant privacy and security concerns but also opens up potential misuse in surveillance, further complicating the physical security landscape. With millions of IoT devices projected to be online within the next five years, these interconnected systems in industrial equipment, energy grids, and public service infrastructure remain at risk for AI-driven attacks that can autonomously disrupt or manipulate physical operations without human intervention. Such technology can target core elements like power grids or voting infrastructure, underscoring the need for stringent security protocols.

In an electoral context, like the upcoming 2024 Pilkada, AI-driven threats pose particular risks for voting systems and critical infrastructure, as demonstrated by past incidents of targeted disruption. For instance, the infamous "Stuxnet" attack showcased how sophisticated malware infiltrated and manipulated industrial systems (Chung et al., 2019; Langner, 2011), reflecting the potential scale and precision of AI threats in undermining physical infrastructure. AI-driven attacks on IoT devices could lead to large-scale disruptions in physical election systems, such as vote

counting and data storage systems, or even tamper with surveillance technology around polling stations, as Asiryan (2023) notes the potential of AI to incite disturbances by exploiting system vulnerabilities. Given these potential threats, adopting strong, proactive security measures is essential to ensure the protection of physical and digital assets critical to the electoral process.

3. Political Security Threats

The rise of AI-driven bots and deepfake technology has introduced new dimensions to political security threats, posing serious risks to democratic processes. Bots, which are increasingly deployed in social media environments, play a crucial role in spreading misinformation at scale. According to Bazarkina & Matyashova (2022), the strategic use of bots in political communication enables malicious actors to create artificial consensus or amplify divisive narratives, leading to public polarization and erosion of trust in legitimate media sources. By continuously distributing hoaxes and misinformation, bots can manipulate public perception, affecting voter sentiment and influencing electoral outcomes. In the context of the 2024 elections in Indonesia, the use of AI-powered bots could distort the political landscape, making it difficult for voters to discern fact from fiction and potentially swaying their choices based on misleading narratives.

In addition to bots, deepfake technology has emerged as a potent tool for political manipulation, enabling the creation of hyper-realistic but fabricated media that can mislead the public and alter political narratives. Ahmed (2022) emphasizes that deepfakes have significant implications for the authenticity of digital content, as fabricated videos of political figures or events can rapidly spread on social media, leading to confusion and distrust. This form of AI-driven manipulation has already impacted international politics, where deepfakes have been used to portray political leaders in compromising situations or spread fake news. The implications of such technology for the 2024 elections in Indonesia are profound, as deepfakes could be used to undermine political candidates or even incite social unrest. Addressing these threats requires robust detection technologies and regulatory frameworks, as highlighted by Veerasamy & Pieterse (2022), to protect political security and maintain public trust in democratic institutions.

The threats posed by AI to cybersecurity, physical security, and political security are complex and require careful mitigation efforts and coordinated responses from various stakeholders. Governments, election authorities, and cybersecurity experts must work together to ensure that these threats are effectively addressed, maintaining the integrity and security of the election process.

E. CONCLUSION

This article aims to identify the potential threats posed by the use of artificial intelligence (AI) in cybercrime activities, particularly in the context of the 2024 Regional Head Elections (Pilkada). Through the analysis conducted on this topic, it is

evident that the utilization of AI in cybercrime presents significant challenges to the integrity and security of the electoral process.

First, cybercrime techniques supported by AI have the potential to undermine the integrity of elections by manipulating public opinion and influencing voter behaviour. With the capability to generate and disseminate large amounts of misinformation, AI can exploit vulnerabilities in social media platforms and spread false narratives to sway public opinion. This poses a serious threat to the democratic process and the legitimacy of election outcomes.

Second, AI can be used to compromise the security of electoral systems and infrastructure. Cybercriminals can leverage AI algorithms to launch sophisticated attacks such as phishing, ransomware, or distributed denial-of-service (DDoS), targeting critical components of the electoral infrastructure. Such attacks could disrupt the electoral process, compromise voter data, or even manipulate vote counts, leading to a loss of public trust and confidence in the electoral system.

Additionally, the rapid advancement of AI technology presents challenges in effectively detecting and responding to AI-based cyber threats. Traditional cybersecurity measures will find it difficult to keep up with the evolving tactics and capabilities of AI-driven cybercriminals. Therefore, it is crucial for governments, authorities responsible for conducting elections, and cybersecurity experts to enhance their capabilities to monitor, detect, and respond to AI-driven cybercrime activities.

REFERENCES

1. Ahmed, S. (2022). Impact of Deepfake Technology on Digital World Authenticity: A Review. *International Journal of Engineering and Management Research*, *12*(3), 78–84. https://doi.org/10.31033/ijemr.12.3.10
2. Asiryan, S. R. (2023). *Use of artificial intelligence during elections, practice, threats to the right to vote and ways to overcome them*. https://doi.org/10.24144/2307-3322.2023.77.2.2
3. Bazarkina, D., & Matyashova, D. (2022, April). "Smart" Psychological Operations in Social Media: Security Challenges in China and Germany. In *European Conference on Social-Media* (Vol. 9, No. 1, pp. 14-20). https://doi.org/10.34190/ecsm.9.1.174
4. Bazarkina, D., & Pashentsev, E. (2020). Malicious Use of Artificial Intelligence. *Russia in Global Affairs*, *18*(4), 154–177. https://doi.org/10.31278/1810-6374-2020-18-4-154-177
5. Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/ACCESS.2022.3191790
6. Boháček, M., & Farid, H. (2022). Protecting world leaders against deep fakes using facial, gestural, and vocal mannerisms. *Proceedings of the National Academy of Sciences*, *119*(48), e2216035119. https://doi.org/10.1073/pnas.2216035119
7. Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 14. https://doi.org/10.1186/s40163-020-00123-8

8. Chung, K., Li, X., Tang, P., Zhu, Z., Kalbarczyk, Z., Iyer, R. K., & Kesavadas, T. (2019). Smart Malware that Uses Leaked Control Data of Robotic Applications: The Case of Raven-II Surgical Robots. *22nd International Sym Posium on Research in Attacks, Intrusions and Defenses*, 337–351.
9. Coeckelbergh, M. (2022). Democracy, epistemic agency, and AI: political epistemology in times of artificial intelligence. *AI and Ethics*, 1–10. https://doi.org/10.1007/s43681-022-00239-4
10. Deepak, P., Simoes, S., & MacCarthaigh, M. (2023). AI and Core Electoral Processes: Mapping the Horizons. *arXiv.Org*, *abs/2302.03774*. https://doi.org/10.48550/arXiv.2302.03774
11. Eme-Uche, U., Aja, E. F., & Okonkwo, C. (2020). Electoral security and voter-turnout in the 2019 gubernatorial election in abia state: Interrogating the narratives. *IJASOS- International E-Journal of Advances in Social Sciences*, *6*(16), 80–92. https://doi.org/10.18769/IJASOS.616011
12. Hansen, I., & Lim, D. J. (2019). Doxing democracy: Influencing elections via cyber voter interference. *Contemporary Politics*, *25*(2), 150–171. https://doi.org/10.1080/13569775.2018.1493629
13. Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W., & Li, K. (2021). Artificial Intelligence Security: Threats and Countermeasures. *ACM Computing Surveys*, *55*, 1–36. https://doi.org/10.1145/3487890
14. Jeong, D. (2020). Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. *IEEE Access*, *8*, 184560–184574. https://doi.org/10.1109/ACCESS.2020.3029280
15. Kaloudi, N., & Li, J. (2021). The AI-Based Cyber Threat Landscape: A Survey. *ACM Computing Surveys*, *53*(1), 1–34. https://doi.org/10.1145/3372823
16. König, P. D., & Wenzelburger, G. (2020). Opportunity for renewal or disruptive force? How artificial intelligence alters democratic politics. *Government Information Quarterly*, *37*(3). https://doi.org/10.1016/J.GIQ.2020.101489
17. Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy Magazine*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67
18. Mankoo, S. S. (2023). DeepFakes- The Digital Threat in the Real World. *Gyan Management Journal*, *17*(1), 71–77. https://doi.org/10.48165/gmj.2022.17.1.8
19. McKinsey. (2022, December). *The State of AI in 2022 – and half decade in review*. QuantumBlack AI by McKinsey.
20. Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, & Ben Garfinkel. (2018, February). *The Malicious Use of Artificial Intelligence Forecasting, Prevention, and Mitigation*.
21. Montasari, R. (2023). Internet of Things and Artificial Intelligence in National Security: Applications and Issues. *Advances in Information Security*, 27–56. https://doi.org/10.1007/978-3-031-21920-7_3
22. Rheault, L., & Musulan, A. (2021). Efficient detection of online communities and social bot activity during electoral campaigns. *Journal of Information Technology & Politics*, *18*(3), 324–337. https://doi.org/10.1080/19331681.2021.1879705

23. Schneider, J., & Breitinger, F. (2023). Towards AI forensics: Did the artificial intelligence system do it? *Journal of Information Security and Applications*, *76*, 103517. https://doi.org/10.1016/j.jisa.2023.103517
24. Shahzad, H., Rustam, F., Flores, E. S., Mazón, J. L. V., Díez, I. de la T., & Ashraf, I. (2022). A Review of Image Processing Techniques for Deepfakes. *Sensors*, *22*(12), 4556–4556. https://doi.org/10.3390/s22124556
25. Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557–560. https://doi.org/10.1038/s42256-019-0109-1
26. Urtaeva, E. B. (2024). Opportunities and Threats of using Artificial Intelligence (AI) in Political Communications. *Obŝestvo: Politika, Èkonomika, Pravo*, *2*, 44–51. https://doi.org/10.24158/pep.2024.2.3
27. Veerasamy, N., & Pieterse, H. (2022). Rising Above Misinformation and Deepfakes. *Proceedings of the ... International Conference on Information Warfare and Security*, *17*(1), 340–348. https://doi.org/10.34190/iccws.17.1.25
28. Yener, B., & Gal, T. (2019). Cybersecurity in the Era of Data Science: Examining New Adversarial Models. *IEEE Security & Privacy*, *PP*, 1–1. https://doi.org/10.1109/MSEC.2019.2907097
29. Zeng, Y. (2022). AI Empowers Security Threats and Strategies for Cyber Attacks. *Procedia Computer Science*, *208*, 170–175. https://doi.org/10.1016/j.procs.2022.10.025