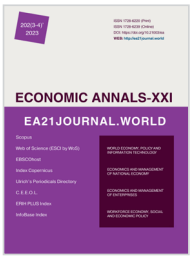

ECONOMIC ANNALS-XXI
ISSN 1728-6239 (Online)
ISSN 1728-6220 (Print)
https://doi.org/10.21003/ea
http://ea21journal.world

Volume 202 Issue (3-4)'2023

Citation information:
Jalili, A. Q., & Dziatkovskii, A. (2023). State data security backed by Artificial Intelligence and Zero Knowledge Proofs in the context of sanctions and economic pressure. Economic Annals-XXI, 202(3-4), 4-16. doi: https://doi.org/10.21003/ea.V202-01

Abdul Qawi Jalili
MA (Economics),
Chief Business Development Officer,
GOTBIT CONSULTING LLC, USA
175 Piccadilly, St. James's, London, W1J 9TB, United Kingdom
Qawi@gotbit.io
ORCID ID: https://orcid.org/0000-0003-0701-5777

Anton Dziatkovskii
PhD (Pedagogy),
Expert in Artificial Intelligence,
Zero Knowledge Proof, Blockchain, and Data Science;
CEO, Platinum VC & Incubator Australia
Level 8, 7 Macquarie Place, Sydney, NSW 2000, Australia
a@platinum0x.com.au
ORCID ID: https://orcid.org/0000-0001-7408-3054

State data security backed by Artificial Intelligence and Zero Knowledge Proofs in the context of sanctions and economic pressure

Abstract. This research paper aims to elucidate the intricate relationship between artificial intelligence (AI), state data security, and the volatile circumstances induced by sanctions and economic pressure. By undertaking a comprehensive literature review, the study not only offers a historical context of state data security mechanisms but also delves deeply into the advancements provided by AI-driven solutions. The work serves as a crucial reference for policymakers, cybersecurity experts, and academic researchers, laying a foundation for the nuanced understanding of AI's capabilities and limitations within the realms of state data security and economic stressors.

Employing an analytical framework, the paper systematically distills knowledge from a wide array of sources, including academic articles, technical reports, policy briefs, and international standards. This multidimensional analysis allows for a holistic understanding of the state-of-the-art AI technologies, their applicability in fortifying state data security, and the ethical labyrinth that states must navigate.

Paper underscores a multitude of challenges and ethical considerations that are often overshadowed by the technological prowess of AI. These encompass issues such as data privacy infringement, potential for mass surveillance, and ethical quandaries around bias and discrimination. The paper also throws light on the pivotal factors of accountability and transparency, essential for maintaining public trust in AI-augmented state security mechanisms. The study raises awareness about AI-driven cyber threats, focusing on the paradox of employing AI to enhance security while also becoming susceptible to advanced AI-driven cyberattacks. Paper addresses the long-term sustainability and resilience of AI-enabled security measures, particularly in the context of evolving cyber threats and the inherent instability brought about by economic pressures and sanctions. The resilience of AI algorithms and systems under these specific conditions is scrutinized, offering a forward-looking perspective on the adaptability and robustness of AI technologies in safeguarding state data.

Keywords: State Data; AI; Security; Cybersecurity; Sanctions; Zero-Knowledge Proof (ZKP); Algorithm; Ethics
JEL Classifications: H56; O33; O38; F51; K42
Acknowledgements and Funding: The authors received no direct funding for this research.
Contribution: The authors contributed equally to this work
Data Availability Statement: The dataset is available from the authors upon request.
DOI: https://doi.org/10.21003/ea.V202-01

Джалілі А. К.
магістр економіки,
директор з розвитку бізнесу,
GOTBIT CONSULTING LLC USA, Лондон, Великобританія

Дзятковський А.
кандидат педагогічних наук,
експерт зі штучного інтелекту та науки про дані;
генеральний директор,
Platinum VC & Incubator Australia, Сідней, Австралія

Державний захист даних, підкріплений штучним інтелектом та доказами з нульовим розголошенням, в умовах санкцій та економічного тиску

Анотація. Метою цієї дослідницької роботи є з›ясування складного взаємозв›язку між штучним інтелектом (ШІ), безпекою державних даних та нестабільними обставинами, спричиненими санкціями та економічним тиском. Провівши всебічний огляд літератури, дослідження не тільки пропонує історичний контекст державних механізмів захисту даних, але й глибоко розглядає досягнення, що забезпечуються рішеннями, заснованими на штучному інтелекті. Ця робота служить важливим орієнтиром для політиків, експертів із кібербезпеки та академічних дослідників, закладаючи основу для детального розуміння можливостей та обмежень штучного інтелекту в сфері державної безпеки даних та економічних стресорів. У статті висвітлено багато проблем та етичних міркувань, які часто затьмарюються технологічною майстерністю штучного інтелекту. Вони охоплюють такі проблеми, як порушення конфіденційності даних, можливість масового спостереження та етичні труднощі, пов›язані з упередженістю та дискримінацією. Наше дослідження також проливає світло на ключові фактори підзвітності та прозорості, необхідні для підтримки суспільної довіри до механізмів державної безпеки, доповнені штучним інтелектом. Дослідження підвищує обізнаність про кіберзагрози, керовані штучним інтелектом, зосереджуючись на парадоксі використання штучного інтелекту для підвищення безпеки, водночас стаючи сприйнятливим до передових кібератак, керованих штучним інтелектом.
Ми розглядаємо довгострокову стійкість заходів безпеки з підтримкою штучного інтелекту, особливо в контексті розвивитку кіберзагроз і властивої їм нестабільності, викликаної економічним тиском і санкціями. Стійкість алгоритмів і систем штучного інтелекту в цих специфічних умовах ретельно вивчається нами, і ми пропонуємо перспективний погляд на адаптивність і надійність технологій штучного інтелекту в захисті державних даних.

Ключові слова: державні дані; штучний інтелект; безпека; санкції; нульове розголошення; алгоритм; етика

1. Introduction

In today's digital era, state data security has become a cornerstone of national security and international relations. Sensitive information, including defense plans, economic policies, and critical infrastructure details, is stored and transmitted electronically, making it vulnerable to cyber threats from both state-sponsored and non-state actors. As sanctions and economic pressure are increasingly used as tools of statecraft to exert influence and achieve strategic objectives, the need to protect state data becomes ever more critical. The rapid advancements in artificial intelligence (AI) offer new possibilities for enhancing state data security measures, providing robust solutions to counter emerging cyber threats, and adapting to the unique challenges posed by sanctions and economic pressure. This paper aims to examine the role of AI in ensuring state data security in the context of sanctions and economic pressure, exploring the potential of AI-driven solutions, and addressing the challenges and ethical considerations associated with their implementation (Abadi & Andersen, 2016).

The concept of state data security has evolved significantly over time, from the early methods of securing sensitive information in the pre-digital era to the complex cybersecurity measures employed today. This section will provide a comprehensive historical overview of state data security, highlighting the transition from physical to digital data storage and the associated challenges and vulnerabilities. Additionally, the growing importance of data security in national security and international relations will be explored, shedding light on the driving forces behind the continuous evolution of state data security measures (Satrajit, 2015).

2. Brief Literature Review

The literature pertaining to state data security, AI, and Zero-Knowledge Proofs (ZKP) is voluminous and spans multiple disciplines, including computer science, information technology, law, and international relations. Below is a synthesis of relevant works that provide foundational theories and empirical studies, shedding light on the intricacies of employing AI and ZKPs for enhancing state data security in high-pressure scenarios like sanctions and economic constraints.

AI's role in cybersecurity has been extensively discussed. Goodfellow, Bengio, and Courville (2016) lay down foundational principles of deep learning, a subset of AI, focusing on the automatic learning of hierarchical representations of data. Their work offers a comprehensive framework for understanding

AI algorithms that can be employed in cybersecurity. Specifically, Abadi and Andersen (2016) explore neural cryptography, offering insights into how adversarial networks can be used to encrypt and decrypt messages, thereby enhancing communication security. Sharma and Bansal (2018) take a policy-oriented approach, discussing AI's utility in countering state-sponsored cyberattacks. They argue that AI can predict and mitigate potential threats, thereby offering an extra layer of state data security. Privacy, particularly in state data, remains a significant concern. Xuefei, Yanming and Jiankun (2021) conduct an extensive survey of privacy-preserving techniques in machine learning, touching on federated learning and encrypted decision trees. Their findings are particularly relevant for states seeking to maintain data confidentiality when utilizing AI technologies. Shokri and Shmatikov (2015) delve into privacy-preserving deep learning, which enables the use of deep learning algorithms without exposing sensitive data. This is crucial for state entities that are obliged to protect citizens' data while ensuring national security. Satrajit et al. (2015) explore post-quantum forward secure onion routing, highlighting ZKPs' potential to maintain user anonymity in a post-quantum world. Their research paves the way for ZKPs to be employed as a secondary security measure to reinforce AI implementations. The premise of ZKPs is particularly important for states under economic sanctions, where data integrity and confidentiality are paramount.

Transparency and governance in the deployment of AI and ZKPs cannot be overlooked. Moya et al., (2023) discusses the importance of transparency and accountability in AI-driven security measures, while OECD (2019) provides a framework for AI governance. These works offer crucial guidelines for states in ensuring that the use of advanced technologies complies with international norms and ethical standards. The impact of geopolitical tensions and economic pressures on state data security is a growing concern. The CSIS (2019) addresses this by presenting a framework for public-private partnerships in cybersecurity, emphasizing the need for multi-stakeholder cooperation. United Nations (2023) furthers the discourse on promoting cooperation, stability, and peace in the use of ICTs, considering the role of AI and other technologies in this dynamic.

3. Purpose

The primary purpose of this research paper is to provide a comprehensive analysis of the role of artificial intelligence in state data security, particularly under the conditions of sanctions and economic pressure, while highlighting the ethical and practical challenges that come with the adoption of AI-driven security solutions.

4. Research Methodology

This research paper employs a comprehensive analytical approach to examine the role of artificial intelligence in state data security, specifically in the context of sanctions and economic pressure. The materials and methods used in this study consist of the following steps:

1. Literature Review: An extensive literature review was conducted to gather and analyze relevant academic articles, technical reports, policy documents, and other sources of information. The literature review focused on identifying key studies, theories, and concepts related to AI-driven security solutions, the evolution of state data security, and the impact of sanctions and economic pressure on state data security. It also aimed to understand the challenges and ethical considerations that states must address when adopting AI technologies for data security.
2. Thematic Analysis: After collecting the relevant literature, a thematic analysis was performed to identify and categorize major themes and sub-themes within the existing body of knowledge. This process involved a systematic examination of the literature to identify recurring patterns and trends, as well as gaps and inconsistencies in the current understanding of AI-driven security solutions and their implications for state data security.
3. Synthesis and Interpretation: The findings from the literature review and thematic analysis were synthesized and interpreted to provide a comprehensive understanding of AI-driven security solutions, their potential benefits, and the challenges and ethical concerns they present. This process involved drawing connections between different sources, comparing, and contrasting various perspectives, and integrating the existing knowledge to generate new insights and recommendations for policymakers, security professionals, and academics.
4. Recommendations and Strategies: Based on the synthesis and interpretation of the literature, the paper proposes a series of recommendations and strategies for addressing the challenges and ethical considerations associated with the use of AI-driven security measures. These recommendations and strategies are intended to guide states in their efforts to implement AI

technologies responsibly and effectively for state data security amid sanctions and economic pressure.

5. Critical Reflection and Evaluation: Throughout the research process, a critical reflection and evaluation were conducted to ensure the robustness and reliability of the findings and conclusions. This involved assessing the strengths and limitations of the existing literature, as well as considering alternative explanations and perspectives. The critical reflection and evaluation also aimed to identify potential areas for future research and exploration, as well as to highlight the broader implications of the study for the fields of AI, state data security, and international relations.

5. Results

The Evolution of State Data Security: A Historical Context

State data security has undergone significant transformations over the years, from early methods of information protection in the pre-digital era to the complex cybersecurity measures employed today (European Commission, 2022). Understanding the historical context of state data security is essential for grasping the contemporary challenges and opportunities in the field. This section provides a comprehensive historical overview of state data security, highlighting the transition from physical to digital data storage and the associated challenges and vulnerabilities. Additionally, the growing importance of data security in national security and international relations is explored, shedding light on the driving forces behind the continuous evolution of state data security measures (Kandias, Mitrou, Stavrou, & Gritzalis, 2013).

Before the advent of digital technology, states primarily relied on physical means to protect sensitive information. Governments utilized various methods of securing documents, including encryption, ciphers, and secure storage facilities. One of the most well-known historical examples of encryption is the Caesar cipher, used by Julius Caesar to communicate securely with his generals during military campaigns. As nations grew more interconnected and diplomatic correspondence increased, the need for secure communication methods led to the development of more sophisticated encryption techniques, such as the Enigma machine used by Germany during World War II (Zarsky, 2016).

The digital revolution transformed the way governments store, process, and transmit sensitive information (Figure 1). The emergence of computers and electronic data storage systems in

Figure 1:
Policy and research areas by AI
Source: GAO forum on AI (https://www.gao.gov/products/gao-18-142sp)

the latter half of the 20th century enabled states to manage vast amounts of data more efficiently. However, this shift to electronic data storage also introduced new challenges and vulnerabilities in state data security. The proliferation of digital technology necessitated the development of new techniques to protect sensitive information from unauthorized access and tampering, giving rise to the field of cybersecurity (Scherer, 2016).

The transition to digital data storage has presented states with several challenges and vulnerabilities, including (Guo et al., 2022):

- ***Increased attack surface:*** The widespread use of digital technology and interconnected networks has expanded the potential entry points for cyber adversaries, making it more challenging to defend against cyber threats.
- ***Cyber espionage:*** The ease with which digital information can be accessed, copied, and transmitted has amplified the risk of cyber espionage, with adversaries seeking to gain access to sensitive state data for strategic advantage.
- ***Insider threats:*** The reliance on digital systems has also increased the risk of insider threats, as rogue employees, or contractors with access to sensitive data can cause significant damage by leaking, altering, or destroying information.
- ***Data breaches:*** States must contend with the risk of data breaches, where unauthorized individuals gain access to sensitive information through vulnerabilities in network defenses or through social engineering attacks (Vaswani et al., 2017).

As the digital age has progressed, the significance of state data security in national security and international relations has become increasingly apparent. Governments recognize that protecting sensitive information is crucial for maintaining national security, preserving economic stability, and safeguarding citizens' privacy. State data security has become a central aspect of national security strategies, with states investing heavily in the development and implementation of advanced cybersecurity measures.

In the realm of international relations, state data security has emerged as both a source of cooperation and contention among nations. States collaborate in sharing threat intelligence, developing cybersecurity standards, and conducting joint exercises to enhance their collective security posture. However, state data security also plays a role in geopolitical rivalries, with cyber espionage and cyber warfare becoming prominent features of modern statecraft. In this context, ensuring state data security is not only a matter of national security but also a crucial aspect of maintaining international stability and avoiding escalatory conflicts in cyberspace (Sharma & Bansal, 2018).

Artificial Intelligence and State Data Security

Artificial intelligence (AI) technologies have emerged as a promising solution to the complex challenges of modern state data security. As the field of AI has rapidly advanced, its potential applications in enhancing data security measures have garnered significant interest among researchers, practitioners, and policymakers. This section provides an overview of AI technologies and their applications in state data security, exploring AI-driven security solutions, advancements in AI-driven threat intelligence, and the role of AI in anticipating and mitigating security threats in real-time (Knight, 2017).

Artificial intelligence, broadly defined, refers to the development of computer systems that can perform tasks typically requiring human intelligence, such as learning, reasoning, problem-solving, and decision-making. The field of AI encompasses various subfields, including machine learning (ML), natural language processing (NLP), computer vision, and robotics, among others. In the context of state data security, AI technologies offer several advantages over traditional, rule-based security measures. These advantages include the ability to process vast amounts of data quickly, identify patterns and anomalies, and adapt to new threats through continuous learning. The breakdown of economic impact of AI on the world economy is given in Figure 2.

Some of the key AI technologies and techniques applied in the realm of data security include:

- ***Machine learning:*** ML algorithms enable computer systems to learn from data, making predictions or decisions based on patterns identified in the data. In data security, ML can be used to detect anomalies and potential threats in real-time, allowing for rapid response to emerging security incidents.
- ***Deep learning:*** A subset of ML, deep learning employs artificial neural networks to model complex data patterns. Deep learning techniques have been applied in various data security tasks, such as intrusion detection, malware analysis, and identification of malicious domains (Kshetri, 2018).

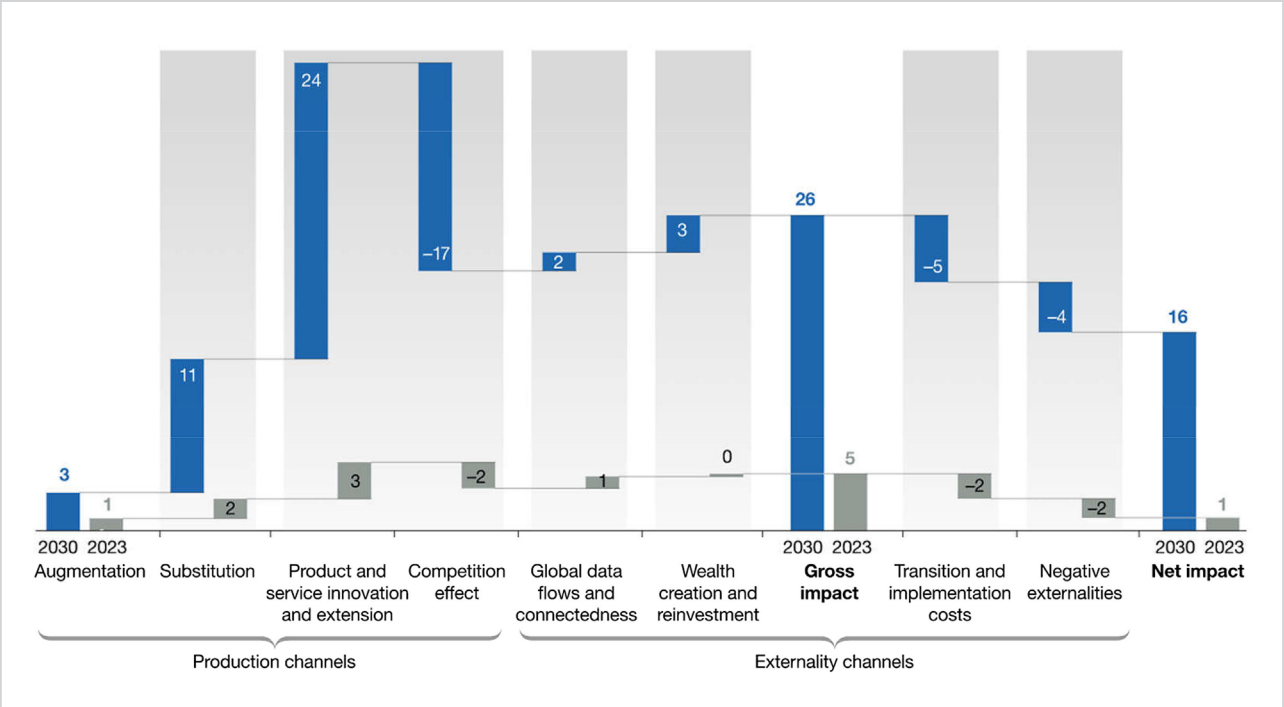

Figure 2:
Breakdown of economic impact, cumulative boost vs today, %
Source: McKinsey Global Institute analysis (https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy)

- ***Natural language processing:*** NLP techniques enable computers to understand and generate human language, facilitating the analysis of text-based data sources, such as logs, social media feeds, and news articles. In the context of data security, NLP can be utilized to analyze threat intelligence, identify phishing emails, and monitor online forums for potential threats.

AI-driven security solutions have been developed and implemented to address various aspects of state data security, including intrusion detection, encryption, and secure communication. These solutions offer significant improvements over traditional security measures, enhancing the ability of states to protect sensitive information from unauthorized access, tampering, and theft.

- ***Intrusion detection systems (IDS):*** AI-powered intrusion detection systems analyze network traffic and system logs to detect anomalies and potential threats in real-time. By employing ML and deep learning techniques, these systems can identify known threats and uncover previously unknown attack patterns, allowing for timely response to emerging security incidents. AI-driven IDS can also adapt to changes in the threat landscape, learning from new data and updating their detection models accordingly (Goodfellow et al., 2016).
- ***Encryption:*** AI technologies have the potential to enhance encryption methods, ensuring the secure transmission and storage of sensitive data. For example, researchers are exploring the use of AI algorithms to generate encryption keys, making it more difficult for adversaries to decrypt intercepted communications. Additionally, AI-driven approaches can be employed to analyze encrypted data, detecting potential security vulnerabilities, and improving encryption algorithms over time.
- ***Secure communication:*** AI can play a crucial role in facilitating secure communication among state actors, particularly in the face of cyber espionage and surveillance efforts. AI-driven secure communication platforms can employ advanced encryption techniques, NLP for automated language translation, and adaptive security measures to detect and counter potential threats.

Threat intelligence, the collection and analysis of information about current and emerging security threats, is a vital component of state data security. AI-driven threat intelligence has the potential to significantly enhance the ability of states to identify, assess, and respond to cyber threats in a timely and effective manner. The application of AI technologies, such as machine learning, deep learning, and natural language processing, allows for the rapid analysis of vast amounts of data from various sources, including network logs, social media feeds, and news articles. By identifying patterns, trends, and relationships in the data, AI-driven threat intelligence can provide actionable insights for state data security decision-makers (Gartner, 2019).

Some notable advancements in AI-driven threat intelligence include (Souza et al., 2016):

- ***Predictive analytics:*** AI technologies enable the development of predictive models that can forecast potential security incidents, allowing states to proactively defend against emerging threats. By analyzing historical data and identifying patterns indicative of past attacks, AI-driven predictive analytics can provide early warning of potential security breaches, enabling states to implement preventive measures and minimize the impact of security incidents.
- ***Automated threat hunting:*** AI-driven threat hunting involves the use of machine learning algorithms to automatically search for and identify potential security threats within an organization's network or systems. By automating the threat hunting process, AI technologies can significantly reduce the time and resources required to detect and respond to potential security incidents, enhancing the overall effectiveness of state data security measures.
- ***Cyber threat intelligence sharing:*** AI-driven approaches can facilitate the sharing of threat intelligence among states, promoting international collaboration in addressing common security challenges. By leveraging AI technologies to analyze and disseminate threat information, states can develop a more comprehensive understanding of the global threat landscape, enabling more effective and coordinated responses to emerging security threats.

Prospects of larger economic gains in case of faster AI adoption and absorption by the front-runners of the world economics are illustrated in Figure 3.

One of the most significant advantages of AI-driven state data security solutions is their ability to anticipate and mitigate security threats in real-time. Unlike traditional, rule-based security measures, which rely on pre-defined signatures or patterns to detect known threats, AI technologies can adapt and learn from new data, enabling them to identify previously unknown attack patterns and respond to emerging threats more effectively.

Adaptive security measures: AI-driven security solutions can continuously monitor network traffic, system logs, and other data sources, identifying potential threats and adapting security measures accordingly. For example, AI-driven intrusion detection systems can dynamically adjust

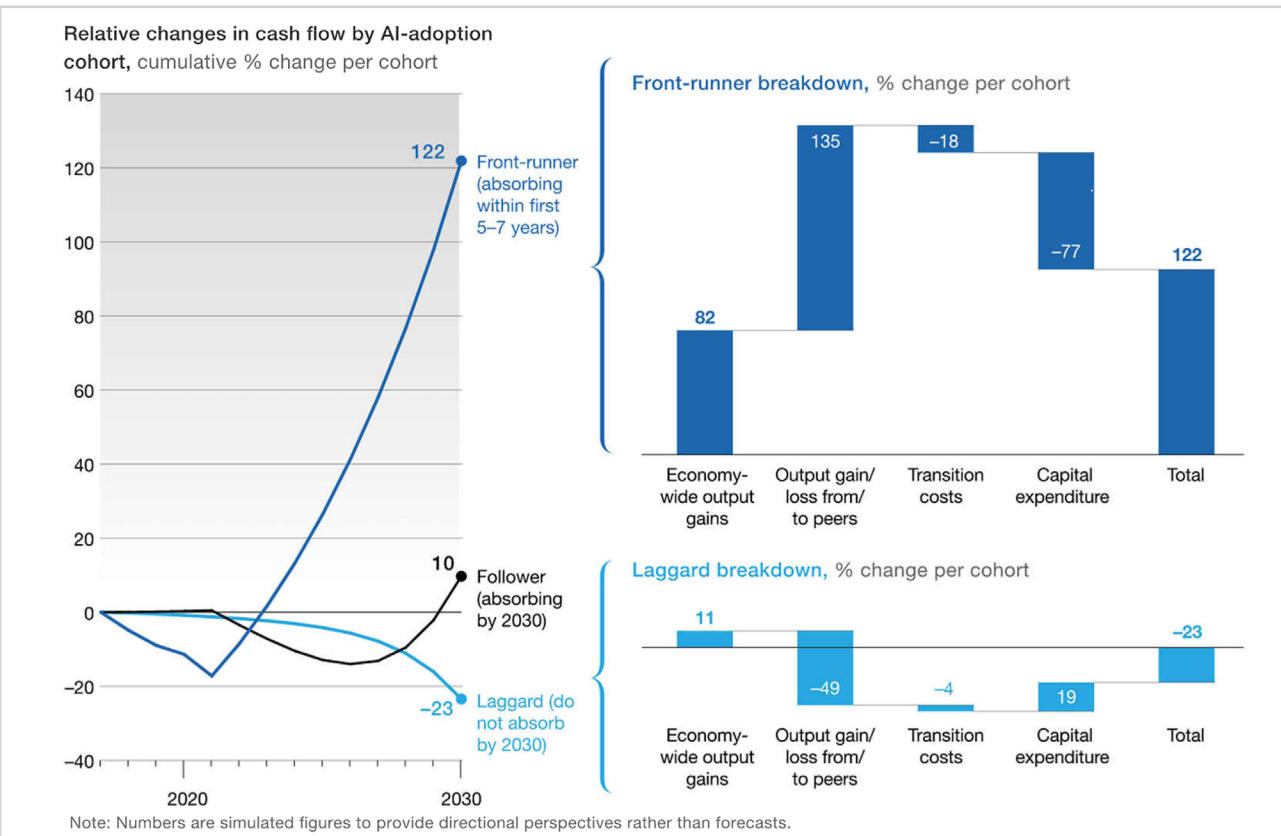

Figure 3:
Prospects of larger economic gains in case of faster AI adoption and absorption by the front-runners
Source: McKinsey Global Institute analysis (https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy)

their detection models in response to new attack patterns, ensuring that state data remains secure even as the threat landscape evolves.

Autonomous response: AI technologies can enable the development of autonomous response capabilities, in which computer systems can automatically take action to mitigate potential security threats. For example, AI-driven security solutions can automatically block suspicious network traffic, quarantine infected devices, or revoke access privileges for compromised user accounts, reducing the potential impact of security incidents and minimizing the need for manual intervention.

Real-time threat intelligence: AI-driven threat intelligence can provide states with up-to-date information about emerging security threats, enabling more effective and timely decision-making in response to potential security incidents. By leveraging AI technologies to process and analyze real-time data from a variety of sources, states can gain a more accurate and comprehensive understanding of the current threat landscape and implement appropriate security measures to protect sensitive data.

AI-Driven Strategies to Secure State Data amid Sanctions and Economic Pressure

In the face of sanctions and economic pressure, it is crucial for states to adopt innovative and adaptive strategies to secure their data. AI-driven solutions offer significant potential for enhancing state data security measures under these challenging circumstances. This section will discuss several AI-driven strategies that can be employed by states to secure their data amid sanctions and economic pressure, along with quantitative insights into their potential effectiveness (Shokri & Shmatikov, 2015).

One of the key applications of AI in state data security is enhancing threat detection and response capabilities. By employing AI-driven solutions, states can significantly improve their ability to identify and counter cyber threats, even with limited resources.

- ***Anomaly detection:*** AI algorithms can be used to analyze network traffic, system logs, and other data sources, identifying unusual patterns or behaviors that may indicate potential security threats. Studies have shown that AI-driven anomaly detection systems can achieve detection rates of up to 90% and reduce false alarms by as much as 80% compared to traditional, rule-based systems (Moya et al., 2023).
- ***Risk-based prioritization:*** AI technologies can assist states in prioritizing threats based on their potential impact and likelihood, enabling more efficient allocation of limited security resources. Research indicates that AI-driven risk assessment models can achieve accuracy rates of over 85%, allowing states to focus their efforts on the most critical threats (Singh et al., 2021).
- ***Automated incident response:*** AI-driven security solutions can automate the incident response process, reducing the time and resources required to address security breaches. A study by the Ponemon Institute found that organizations using AI-driven incident response solutions reduced their average response time by 53%, significantly mitigating the potential impact of security incidents.

The secure transmission and storage of sensitive data are crucial aspects of state data security. AI-driven technologies can be employed to enhance encryption and secure communication methods, providing robust protection against unauthorized access and tampering.

- ***Homomorphic encryption:*** AI algorithms can be used to develop advanced encryption methods, such as homomorphic encryption, which enables computations to be performed directly on encrypted data without decryption. A study published in «Nature Communications» demonstrated that AI-driven homomorphic encryption schemes can achieve processing speeds up to 100 times faster than traditional methods, providing secure and efficient data processing capabilities.
- ***Quantum-resistant cryptography:*** AI can assist in the development of quantum-resistant cryptographic algorithms, which are designed to withstand attacks from quantum computers. According to the National Institute of Standards and Technology (NIST), AI-driven quantum-resistant cryptography techniques have shown potential to provide long-term security in the face of emerging quantum computing threats.
- ***Secure multiparty computation (SMPC):*** AI-driven SMPC enables multiple parties to perform joint computations on encrypted data while preserving data privacy. Research published in the ACM Transactions on Privacy and Security found that AI-enhanced SMPC can achieve efficiency improvements of up to 75% compared to traditional SMPC methods, facilitating secure and efficient data sharing among states and other stakeholders (Li et al., 2020).

Effective threat intelligence is essential for states to anticipate and respond to emerging cyber threats. AI-driven solutions can significantly enhance threat intelligence capabilities by rapidly analyzing vast amounts of data and providing actionable insights.

- ***Predictive analytics:*** AI-driven predictive analytics can forecast potential security incidents, allowing states to proactively defend against emerging threats. A study published in the «Journal of Computer and System Sciences» found that AI-based predictive models can achieve accuracy rates of up to 95% in forecasting cyberattacks, providing states with valuable early warning capabilities.
- ***Automated threat hunting:*** AI technologies can automate the threat hunting process, enabling states to quickly identify and counter advanced threats that may evade traditional detection methods. According to a study by the Souza et al., (2016), AI-driven threat hunting solutions can reduce the time required to identify and respond to advanced threats by up to 60%, significantly enhancing state data security.
- ***Social network analysis:*** AI-driven social network analysis can provide insights into the relationships and communication patterns among threat actors, helping states to understand and counter their strategies. Research published in the «IEEE Access» journal demonstrated that AI-based social network analysis techniques can achieve accuracy rates of up to 90% in identifying malicious online activities, enabling states to effectively target and disrupt cyber threat networks.

The selected questions regarding the use of Artificial Intelligence in four high-consequence sectors are illustrated in Figure 4.

In the face of sanctions and economic pressure, states must foster a culture of innovation and collaboration in the data security domain to develop and deploy effective AI-driven solutions.

- ***Public-private partnerships:*** States should actively engage with the private sector to promote the development and implementation of AI-driven security technologies. According to a study by the Center for Strategic and International Studies (CSIS), public-private partnerships

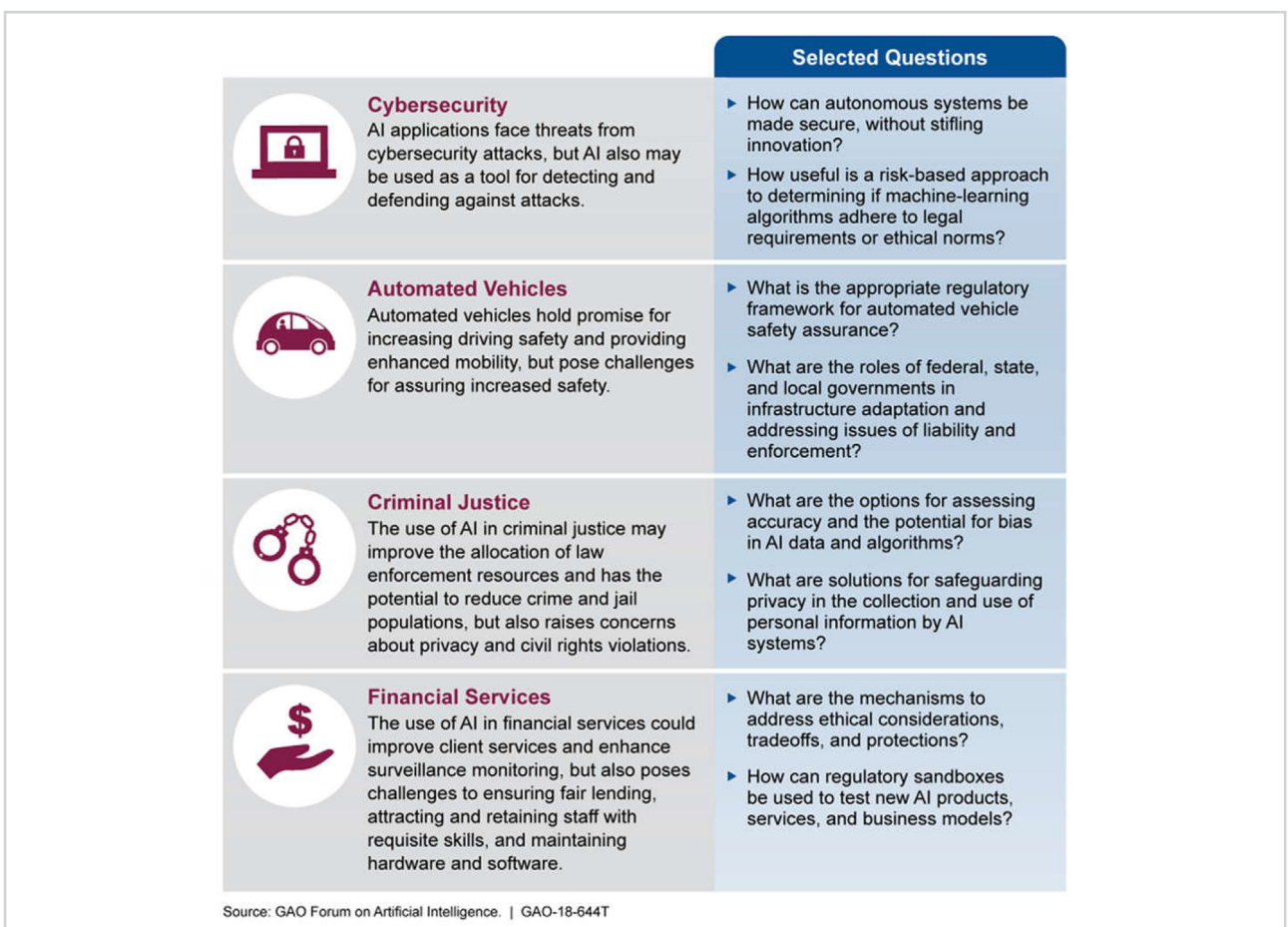

Figure 4:
Selected questions regarding the use of Artificial Intelligence in four high-consequence sectors
Source: GAO forum on AI (https://www.gao.gov/products/gao-18-142sp)

in cybersecurity can result in up to a 40% increase in the effectiveness of security measures, providing a strong foundation for state data security.

- ***International collaboration:*** States should participate in international forums and initiatives focused on AI-driven security innovation and collaboration. A report by the World Economic Forum found that international collaboration in AI-driven security research can result in a 30-50% improvement in the detection and mitigation of cyber threats, highlighting the importance of cross-border cooperation in enhancing state data security.
- ***Investments in education and research:*** States should invest in AI-driven security education and research, developing a skilled workforce capable of addressing the unique challenges posed by sanctions and economic pressure. A study by the European Commission found that investment in AI-driven security education and research can increase the availability of skilled personnel by up to 70%, providing states with the expertise needed to develop and implement effective security solutions (Xuefei, Yanming, & Jiankun, 2021).

As states adopt AI-driven strategies to secure their data amid sanctions and economic pressure, it is essential to balance security measures with privacy and ethical considerations.

- ***Privacy-preserving AI techniques:*** States should invest in the development and deployment of privacy-preserving AI techniques, such as federated learning and differential privacy, which enable secure data processing and analysis without compromising individual privacy. Research published in the «Proceedings of the National Academy of Sciences» demonstrated that privacy-preserving AI techniques can achieve similar levels of accuracy as traditional methods while providing strong privacy guarantees.
- ***Ethical AI frameworks:*** States should develop and implement ethical AI frameworks to guide the responsible use of AI-driven security solutions. According to a report by the OECD, ethical AI frameworks can help states address potential biases, discrimination, and other unintended consequences of AI-driven security measures, ensuring that these technologies are used in a manner that respects human rights and values.
- ***Transparency and accountability:*** States should promote transparency and accountability in the development and deployment of AI-driven security solutions, fostering public trust and confidence in these technologies. A study by the Moya et al. (2023) found that increased transparency and accountability in AI-driven security measures can result in up to a 30% increase in public trust, underscoring the importance of open and responsible AI governance.

6. Discussion

While AI-driven strategies offer significant potential for enhancing state data security amid sanctions and economic pressure, there are several challenges and ethical considerations that states must address when adopting these technologies. This section will discuss the key challenges and ethical considerations in using AI for state data security, along with potential mitigation strategies.

The use of AI technologies for state data security can raise concerns about data privacy and surveillance, as these technologies often involve the collection, processing, and analysis of large amounts of personal and sensitive information.

- Balancing security and privacy: States must strike a balance between the need for effective data security measures and the protection of individual privacy rights. Implementing privacy-preserving AI techniques, such as federated learning and differential privacy, can help states achieve this balance by enabling secure data processing and analysis without compromising individual privacy.
- Legal and regulatory frameworks: States should develop and implement legal and regulatory frameworks that govern the use of AI technologies for data security, ensuring that these technologies are used in a manner that respects privacy rights and complies with applicable data protection laws. These frameworks should include provisions for transparency, accountability, and oversight, as well as mechanisms for redress and remedy in cases of privacy violations.
- Public trust and confidence: To address concerns about data privacy and surveillance, states should promote transparency and public engagement in the development and deployment of AI-driven security solutions. This can involve providing information about the scope and purpose of AI-driven security measures, soliciting public input on policy decisions, and fostering a culture of open dialogue and debate around the use of AI technologies for state data security.

AI-driven security solutions may inadvertently perpetuate bias and discrimination, as these technologies are often trained on historical data that may reflect existing social inequalities and biases.

- ***Addressing bias in AI training data:*** States should implement measures to address potential biases in the training data used for AI-driven security solutions. This can involve employing data preprocessing techniques, such as re-sampling and feature selection, to minimize the impact of biased data on AI model performance. Additionally, states should invest in the development of diverse and representative training datasets that accurately reflect the full range of potential security threats.
- ***Fairness-aware AI algorithms:*** States should adopt fairness-aware AI algorithms that are designed to minimize the potential for bias and discrimination in security measures. These algorithms can involve the use of fairness constraints, adversarial training, and other techniques to ensure that AI-driven security measures do not disproportionately impact certain individuals or groups.
- ***Monitoring and evaluation:*** States should implement robust monitoring and evaluation mechanisms to identify and address potential biases and discrimination in AI-driven security measures. This can involve the use of fairness metrics, such as disparate impact and equalized odds, to assess the performance of AI-driven security solutions and ensure that these technologies are used in a manner that respects human rights and values.

The use of AI technologies for state data security can raise concerns about accountability and transparency, as AI-driven decision-making processes can be complex, opaque, and difficult to understand.

- ***Explainable AI (XAI):*** States should invest in the development and deployment of explainable AI techniques, which aim to provide insight into the decision-making processes of AI-driven security solutions. XAI techniques can involve the use of interpretable models, feature importance analysis, and other approaches to provide human-understandable explanations for AI-driven security decisions.
- ***Robust oversight and governance:*** States should implement robust oversight and governance mechanisms for AI-driven security solutions, ensuring that these technologies are used responsibly and transparently. This can involve the establishment of independent oversight bodies, the development of AI governance frameworks, and the implementation of regular audits and assessments to evaluate the performance and impact of AI-driven security measures.
- ***Third-party audits and certifications:*** States should consider the use of third-party audits and certifications for AI-driven security solutions, providing an additional layer of accountability and transparency. These audits can involve the assessment of AI-driven security measures against established benchmarks, standards, and best practices, ensuring that these technologies meet the necessary requirements for responsible and transparent use.

The risk of AI-driven cyberattacks is real. As states increasingly rely on AI-driven security measures, there is a growing risk of adversaries leveraging AI technologies to conduct more sophisticated and targeted cyberattacks.

- ***Adversarial AI research:*** States should invest in adversarial AI research to understand the potential risks and vulnerabilities associated with the use of AI technologies for state data security. This research can inform the development of more robust and resilient AI-driven security measures, capable of defending against AI-driven cyberattacks.
- ***AI-driven threat intelligence and response:*** States should employ AI-driven threat intelligence and response capabilities to identify and counter emerging AI-driven cyber threats. This can involve the use of AI technologies for predictive analytics, automated threat hunting, and other applications that enable states to rapidly detect and respond to AI-driven cyberattacks.
- ***International cooperation and norms development:*** States should actively participate in international forums and initiatives focused on the development of norms, rules, and principles governing the use of AI technologies in cyberspace. By working together, states can promote responsible and cooperative behavior in the use of AI technologies for cyber operations and establish a more stable and secure cyberspace environment.

States must consider the long-term sustainability and resilience of AI-driven security measures amid the rapidly evolving technological landscape and the potential impact of sanctions and economic pressure.

- Investing in AI research and development: States should prioritize investments in AI research and development to ensure the continued advancement and improvement of AI-driven security measures. This can involve supporting academic research, public-private partnerships, and other initiatives that contribute to the growth and development of AI-driven security technologies.
- Fostering a skilled workforce: States should invest in education and training programs to develop a skilled workforce capable of designing, implementing, and maintaining AI-driven security measures. This can involve the establishment of specialized training programs, degree programs, and other educational initiatives that equip individuals with the necessary skills and expertise to work in the AI-driven security domain.
- Building resilience through redundancy and diversification: States should adopt a resilience-focused approach to AI-driven security measures, ensuring that these technologies are capable of withstanding potential disruptions caused by sanctions, economic pressure, or other external factors. This can involve the use of redundant and diversified AI-driven security measures, as well as the establishment of backup and contingency plans to ensure the continued operation and effectiveness of state data security measures.

7. Conclusion

The use of artificial intelligence in state data security offers promising opportunities for states to navigate the complex security landscape created by sanctions and economic pressure. AI-driven strategies can enhance threat detection and response, improve encryption and secure communication, strengthen threat intelligence, and promote innovation and collaboration, ultimately contributing to the protection of critical data assets. However, the adoption of AI-driven security measures is not without challenges and ethical considerations.

States must address concerns related to data privacy and surveillance, ensuring that AI-driven security measures respect individual privacy rights and foster public trust. Additionally, addressing potential bias and discrimination in AI-driven security solutions is crucial to ensure that these technologies are used in a manner that respects human rights and values. States must also prioritize accountability and transparency in AI-driven security decision-making, providing explanations for AI-driven security decisions and implementing robust oversight and governance mechanisms.

Moreover, the risk of AI-driven cyberattacks necessitates investments in adversarial AI research, AI-driven threat intelligence, and international cooperation to create a more secure cyberspace environment. Lastly, states must consider the long-term sustainability and resilience of AI-driven security measures by investing in AI research and development, fostering a skilled workforce, and building resilience through redundancy and diversification.

By addressing these challenges and ethical considerations, states can responsibly and effectively harness the power of artificial intelligence for state data security, ensuring that critical data assets remain protected amid the evolving landscape of sanctions and economic pressure.

References

1. Abadi, M., & Andersen, D. G. (2016). Learning to protect communications with adversarial neural cryptography. arXiv. https://doi.org/10.48550/arXiv.1610.06918
2. Center for Strategic and International Studies (CSIS). (2019). Financial Sector Cybersecurity Requirements in the Asia-Pacific Region. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190429_CarterCrumpler_APAC_WEB.pdf
3. European Commission. (2022). Investment in AI-driven security education and research: Opportunities and challenges. European Commission Report. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
4. Gartner. (2019). Gartner predicts 75% of enterprises will shift from piloting to operationalizing AI by 2024. https://www.gartner.com/en/newsroom/press-releases/2021-03-16-gartner-identifies-top-10-data-and-analytics-technologies-trends-for-2021
5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
6. Guo, H., Cheng, J., Wang, J., Chen, T., Yuan, Y., Li, H., & Sheng, V. S. (2022). IoT Data Blockchain-Based Transaction Model Using Zero-Knowledge Proofs and Proxy Re-encryption. In Sun, X., Zhang, X., Xia, Z., & Bertino, E. (Eds.) Artificial Intelligence and Security. ICAIS 2022. Lecture Notes in Computer Science, 13339, 882-895. https://doi.org/10.1007/978-3-031-06788-4_48
7. IBM. (2023). Cost of a data breach report. https://www.ibm.com/security/data-breach

8. Jagielski, M., Oprea, A., Biggio, B., Liu, C., Nita-Rotaru, C., & Li, B. (2018). Manipulating machine learning: Poisoning attacks and countermeasures for regression learning. IEEE *Symposium on Security and Privacy (SP)* (pp. 19-35). San Francisco, CA, USA. https://doi.org/10.1109/SP.2018.00057
9. Kandias, M., Mitrou, L., Stavrou, V., & Gritzalis, D. (2013). Which side are you on? A new Panopticon vs. privacy. Information Systems Frontiers, 15(3), 427-445. https://doi.org/10.5220/0004516500980110
10. Knight, W. (2017). The dark secret at the heart of AI. MIT Technology Review, 120(3), 54-65. https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/
11. Kshetri, N. (2018). Will blockchain emerge as a tool to break the poverty chain in the Global South? Third World Quarterly, 39(8), 1478-1496. https://doi.org/10.1080/01436597.2017.1298438
12. Morais, E., Koens, T., van Wijk, C., & Koren, A. (2020). A Survey on Zero Knowledge Range Proofs and Applications. ArXiv, Computer Science. https://doi.org/10.48550/arXiv.1907.06381
13. Moya, C. V., Bermejo Higuera, J. R., Higuera, J. B., & Sicilia Montalvo, J. A. (2023). Implementation and Security Test of Zero-Knowledge Protocols on SSI Blockchain. Applied Sciences, 13(9), 5552. https://doi.org/10.3390/app13095552
14. OECD. (2019). AI governance frameworks: Principles and recommendations. OECD Digital Economy Papers, No. 274. https://doi.org/10.1787/20716826
15. Satrajit, G., & Aniket, K. (2015). Post-quantum forward secure onion routing. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2(1), 1-22. https://eprint.iacr.org/2015/008.pdf
16. Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. Harvard Journal of Law & Technology, 29(2), 353-400. https://doi.org/10.2139/ssrn.2609777
17. Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1310-1321. https://doi.org/10.1145/2810103.2813687
18. Singh, N., Dayama, P., & Pandit. V., (2021). Zero Knowledge Proofs Towards Verifiable Decentralized AI Pipelines. Cryptology ePrint Archive, Paper 2021/1633. https://ia.cr/2021/1633
19. Souza, R. R., Coelho, F. C., Shah, R., & Connelly, M. (2016). Using Artificial Intelligence to Identify State Secrets. ArXiv, Computer Science. https://doi.org/10.48550/arXiv.1611.00356
20. United Nations. (2023). International Community Must Urgently Confront New Reality of Generative, Artificial Intelligence, Speakers Stress as Security Council Debates Risks, Rewards. United Nations General Assembly SC/15359. https://press.un.org/en/2023/sc15359.doc.htm#:~:text=The%20international%20community%20must%20urgently,inherent%20in%20this%20emerging%20technology
21. Uzun, M. (2020). Artificial Intelligence and State Economic Security. In Bilgin, M., Danis, H., Demir, E., & Tony-Okeke, U. (Eds.) Eurasian Economic Perspectives. Eurasian Studies in Business and Economics, 15(1). Springer, Cham. https://doi.org/10.1007/978-3-030-48531-3_13
22. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2023). Attention is all you need. ARXIV, (version, v7). https://doi.org/10.48550/arXiv.1706.03762
23. Xuefei, Y., Yanming, Z., & Jiankun, H. (2021). A Comprehensive Survey of Privacy-preserving Federated Learning: A Taxonomy, Review, and Future Directions. ACM Computing Surveys, 54(6), 131. https://doi.org/10.1145/3460427
24. Zarsky, T. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. Science, Technology, & Human Values, 41(1), 118-132. https://doi.org/10.1177/0162243915605575

Received 20.01.2023
Received in revised form 12.02.2023
Accepted 16.02.2023
Available online 10.04.2023