ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2024 (36)

INVESTIGATING THE IMPACT OF ARTIFICIAL INTELLIGENCE ON ECONOMIC SECURITY IN THE EUROPEAN UNION

Oleksandra LARIONOVA
Mykolas Romeris University
Ateities str. 20, LT-08303 Vilnius, Lithuania
E-mail: larionova_o_a@pstu.edu

DOI: 10.13165/PSPO-24-36-08

Abstract: *This article examines the dual impact of artificial intelligence (AI) on the EU's economic security, focusing on its opportunities and threats: While AI contributes to economic growth and stability, it also creates new vulnerabilities. The paper discusses the role of AI in fighting economic crime, improving risk management, and fostering innovation. At the same time, it also highlights the risks of AI misuse in cyberattacks and manipulations, as well as potential losses for businesses. The report's conclusions emphasize the need for international cooperation and national cybersecurity strategies to effectively use AI and overcome potential challenges.*

Keywords: *Artificial intelligence, Economic security, European Union*

Introduction

The global economy is currently experiencing a period of high uncertainty and instability. The COVID-19 pandemic, war in Ukraine, climate change and other factors have a significant impact on economic growth, trade, investment and employment.

The COVID-19 pandemic led to a deep recession of the global economy in 2020. There was some recovery in 2021, but it was uneven and fragile. The pandemic disrupted global supply chains, increased prices of energy, food and other commodities, and exacerbated inequality and poverty.

Also, the uncertainty of today's world is largely due to the profound transformation of the socio-economic sphere brought about by the rapid development of digital technologies. Artificial intelligence (AI) is penetrating all spheres of life, having a significant impact on the global economy. On the one hand, AI opens up new opportunities for growth, innovation and prosperity. On the other hand, it creates new challenges and threats to the economic security of nations (United Nations Development Programme, 2021/2022).

Economic security is one of the key elements of national security as a whole. It ensures the stability and sustainability of the economic system, its ability to withstand internal and external threats. In the digital era, when economic processes are increasingly dependent on information technology, ensuring economic security is of particular relevance (Black, 2022).

Economic security is crucial for the stability of states. It creates the conditions for sustainable economic growth, which in turn provides jobs, income and resources for investment in education, health and other important public services (International Monetary Fund, 2022).

In addition, economic security contributes to social stability by reducing poverty and inequality, which can lead to social unrest and conflict. As noted in the 2019 Human Development Report, “inequality undermines social cohesion and trust, which can lead to instability and conflict” (UNDP, 2019, p. 2).

Economic security also contributes to political stability by reducing the likelihood of discontent and protests against the government. According to the 2020 Democracy Index, “economic hardship and inequality are among the key factors contributing to democratic backsliding” (EIU, 2021, p. 5).

Thus, countries that lead in digital technologies including AI may gain economic and political advantages. This may lead to increased competition between countries for digital supremacy. The article will further discuss the concept of economic security in the context of AI, global threats to economic security and methods to counter them.

Relevance

The use of artificial intelligence (AI) is an important aspect that requires attention and analysis. In the modern context, many scientists (Ahmad 2021, Mints 2022, Deloitte 2022) are increasing discussion about the possibilities of using innovative technologies, including artificial intelligence, in the public sector. More attention is paid to modern challenges, analysis and opportunities to overcome threats using new information technologies, such as artificial intelligence.

AI provides unique opportunities in the field of ensuring economic security. It can be used to analyze large volumes of data, detect financial fraud and prevent economic crimes. In addition, the use of AI in the security field makes it possible to automate the processes of monitoring, identifying and analyzing threats, which helps increase the efficiency of protecting economic interests. However, like any other innovation, the use of artificial intelligence technologies can create new threats in the field of economic security. The use of AI in the field of economic security requires ensuring data protection, preventing cyberattacks and ensuring the reliability of digital infrastructure.

Identifying and managing such threats is becoming increasingly important at national, regional and international levels. To identify such threats in a timely manner, it is important to consider the experience and strategies of the European Union and its members in the application of artificial intelligence in the field of economic security.

Purpose of the study: analysis and generalization of European experience in the use of artificial intelligence in the field of economic security. This includes an analysis of the strategies, policies, and practices adopted by the European Union and its members to protect economic interests in the face of new information technologies, including artificial intelligence, as well as an analysis of the response of the European Union and its members to potential threats associated with the use of artificial intelligence in economics

The object of the research: Artificial intelligence in the field of economic security

The objectives of the research:

1. Identification of approaches to define Artificial intelligence in the context of the influence of economic security.
2. Analyze the impact of artificial intelligence on EU economic security and this affects on the EU's economic stability
3. Analyze the EU strategy and methods of countering threats to economic security; analyze the development of national digital security strategies.

Research methods: Scientific literature analysis, document analysis, case study, systemic analysis

Case study: studying the case of Google, we considered the impact of artificial intelligence on economic security

1. Identification of approaches to define Artificial intelligence in the context of the influence of economic security.

1.1. Analysis of approaches to defining economic security

The concept of economic security has been introduced quite a while ago, but despite this, it continues to be improved and supplemented. Changes in approaches to the key points of "economic security" over time have been described by a number of studies. The concept of economic security research can be viewed by scholars from different angles.

According to Olvey (1984), economic security is improving the quality of goods that provided competitive advantages in the external market, reducing the dependence of the state on external loans, strengthening the country's ability to fulfill international obligations in trade, economic and other sectors (Olvey, Dolden, Kelly, 1984)

Machovskij (1985) considered economic security as preservation of the country's economic autonomy, the country's ability to make decisions for its own interests in economic development (Machovskij, 1985). It can be seen that over time, the approach to defining economic security has changed. The optimal ratio of expenditures on the country's defense capacity and the efficiency of the country's economy as a whole (Luciani, 1988). The possibility of the economy of the country as a whole and its regions separately to ensure the stable development and appropriate protection of the economic interests of individuals, business entities, regions and the country (Cable, 1995), Defines the economic security as a human value that intersects with the categories of freedom, order, solidarity, which must be ensured by the state (McSweeney, 1999), Maintain an existing standard of living and its further growth (Murdoch, 2001), Security against several of the great disturbing factors in life--especially those which relate to unemployment and old age (Security history, Reports & Studies, 2015), The ability of individuals or communities to meet their basic needs adequately and on an ongoing basis (Case, 2015), The economic security is considered as a guarantee of a country's economic growth (Simanavičienė, Stankevičius 2015), Ensuring the protection of vital interests of all residents of the country, society and the state in the economic sphere from internal and external threats (Shpilevskaya, 2016).

Thus, it can be noted that the first definitions of economic security focused on protection from external threats such as unemployment, population aging and economic instability, but over time, the emphasis has shifted to economic growth. There has been a shift in emphasis towards the importance of economic growth and economic development for economic security. This includes factors such as competitiveness, technological progress, and the ability to fulfill international obligations. Recent definitions emphasize the role of economic security in the well-being of individuals and societies. This includes concepts such as basic needs, quality of life, and social protection. It has now expanded to include broader elements such as economic autonomy, resilience, and the ability to defend against internal and external threats.

Overall, this shows a shift from a narrow protectionist view of economic security to a more inclusive and human-centered understanding. The concept has evolved to reflect the changing economic and geopolitical environment.

There are many different approaches to the definition of the concept of "economic security", among which we will highlight the traditional, complex and human-centered approaches.

The traditional approach to economic security focuses on the protection of national economic interests from external threats. In this context, economic security can be defined as "the condition of the economy that allows it to withstand external shocks and maintain an acceptable standard of living for its citizens" (The National Academies of Sciences, Engineering, and Medicine, 2017, p. 10).

A comprehensive approach to economic security takes into account both external and internal threats. In this context, economic security is defined as "the condition of the economy that allows it to meet the basic needs of its citizens, ensure sustainable economic growth, and

maintain social and political stability" (United Nations Development Programme [UNDP], 2022, p. 1).

The human-centered approach to economic security focuses on the well-being of people. In this context, economic security is defined as "a state in which people have access to the resources and opportunities necessary to meet their basic needs and realize their potential" (UNDP, 2019, p. 2).

The disadvantages of these definitions in the context of this study are that none of them takes into account the impact of digital transformation processes on economic security. Therefore, in the era of AI, the concept of economic security should be rethought taking into account the new threats and opportunities created by AI. An integrated and human-centered approach to economic security, which takes into account both external and internal threats, as well as the well-being of people, is crucial for ensuring the stability and resilience of states in the AI era.

1.2. Specificity of economic security in the context of AI

Although the concept of AI was introduced a long time ago, it has never the less continued to be refined and finalized. A number of studies have shown how the approach to the key issue of 'artificial intelligence' has changed over time, but let us now consider the concept as it is defined by scientists: Artificial intelligence is the general name of the technology for the development of machines, which are created entirely by artificial means and can exhibit behaviors and behaviors like human beings, without taking advantage of any living organism (Mijwel, 2015), AI can be generally defined as sub-discipline of computer science dealing with the development of data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement (Organization for Standardization, 2017), Artificial intelligence is a term used to describe machines performing human-like cognitive processes such as learning, understanding, reasoning and interacting. It can take many forms, including technical infrastructure (i.e. algorithms), a part of a (production) process, or an end-user product (European Union, 2019), In essence, AI refers to machines learning. AI is a software that is running on a computer. The difference to traditional software that's been around for decades is that AI is learning to do job X better with experience, something that traditional software will never accomplish. An AI is a neural network that is trained on a dataset (Trifan, Buzatu, 2020), Progressively, AI is becoming indispensable technological support for daily social life and economic activities (Naimi-Sadigh, 2021), Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems. Examples of AI applications include expert systems, natural language processing (NLP), speech recognition and machine vision (Craig, Laskowski, Tucci, 2022), AI represents a wide spectrum of technologies designed to enable machines to perceive, interpret, act, and learn with the intent to emulate human cognitive abilities (Cazzaniga, 2024).

Initially, people thought of AI as machines that could replicate human thinking, especially in terms of reasoning, learning, and self-improvement. Later, the focus shifted to AI's ability to learn and get better at tasks over time.

More recently, AI has come to be seen as an important part of our daily lives and economy. This new understanding emphasizes how AI has the potential to change society in the future.

AI technologies can be used to improve the efficiency and productivity of businesses, which can make them more competitive and resilient to economic shocks. For example, the use of cloud computing, artificial intelligence, and big data can help businesses optimize their operations, reduce costs, and improve the quality of products and services (Ahmad, 2021).

At the same time, AI creates new points of vulnerability that can be exploited by attackers to damage the economy. For example, cyberattacks can disrupt critical infrastructure, financial institutions, and businesses. Therefore, in the AI era, economic security issues take on a special specificity. This is largely due to factors such as increased vulnerability, dynamic development and the cross-border nature of threats in the AI era.

However, many scholars believe that digital technologies are developing very rapidly, which requires constant updating and adaptation of economic security measures. This process has accelerated especially strongly with the development of generative artificial intelligence and the rapid growth of the threat and quality of Deepfakes (Mints, Sidelov, 2022). The problem is also exacerbated by the fact that cybercrime and other digital threats have no boundaries, making them difficult to track and counter.

The nature of the impact of digital transformation on economic security is maximized. AI not only creates new threats, but also changes the nature of existing threats. On the other hand, AI can create new opportunities to improve economic security.

One of the most serious threats is cybercrime. Cybercriminals can use digital technology for data theft, fraud, extortion, and sabotage. It is estimated that the damage from cybercrime in 2021 was about $6 trillion dollars (Purplesec, 2021).

Countries that depend on foreign technology may also be vulnerable to external pressure and manipulation. For example, if a country depends on foreign software to manage its critical infrastructure, it may be vulnerable to cyberattacks by foreign states (Bagwandeen, 2021).

AI can also exacerbate existing threats such as geopolitical conflicts. For example, digital technologies can be used to spread misinformation and manipulate public opinion, which can destabilize the global economy (Pinto & others, 2021).

It is important to note that these threats do not exist in isolation from each other. They can interact and reinforce each other. For example, cybercriminals can exploit technological dependencies to conduct cyberattacks. And geopolitical conflicts can be used to fuel cybercrime.

Scholars believe that another critical aspect that should also be considered is the society's acceptance of AI. Acceptance may vary from job to job. Some professions can easily integrate AI tools, while others may face resistance due to cultural, ethical, or operational issues. This uncertainty becomes particularly evident in labor markets. While AI has potential for manufacturing-oriented applications, its impact is likely to be mixed. In some sectors where human supervision of AI is required, it could increase worker productivity and labor demand. On the contrary, in other sectors, AI could pave the way for significant job displacement. The rise in aggregate economic productivity could, however, boost overall economic demand, potentially creating more job opportunities for more workers in a ripple effect. Moreover, this evolution may also lead to the emergence of new sectors and job roles - and the disappearance of others - beyond simple inter-industry reallocation. (Cazzaniga, 2024)

Artificial intelligence challenges the belief that the technology affects mainly middle-skill positions and, in some cases, low-skill positions: its advanced algorithms can now expand or replace high-skill positions that were previously considered immune to automation. While the historical waves of automation and IT integration have mostly affected routine tasks, the capabilities of artificial intelligence extend to cognitive functions, allowing it to process huge amounts of data, recognize patterns, and make decisions. As a result, even highly skilled professions that were previously considered immune to automation due to their complexity and reliance on deep expertise now face potential disruption.1 Jobs that require fine judgment, creative problem solving, or complex data interpretation-traditionally the domain of highly educated professionals-can now be augmented or even replaced by advanced AI algorithms,

potentially exacerbating inequalities between and within professions. This shift challenges the conventional wisdom that technological advances primarily threaten lower-skilled jobs and points to a broader and deeper transformation of the labor market than in previous technological revolutions. (Cazzaniga, 2024)

1.3. AI impact and complementarity

A review of scientific literature has shown that in recent years, scientists have also focused on the impact of AI on the labor market, which is a fairly new concept. This issue was described in the most detailed way by Cazzaniga, where it is possible to trace how each profession is likely to face the introduction of AI.

According to Cazzaniga, high-impact professions for which artificial intelligence can perform tasks independently may experience a decrease in labor demand, which will lead to lower wages. Jobs that require human supervision by artificial intelligence may increase productivity, which will boost labor demand and wages for incumbents. However, even in occupations where AI can complement human labor, workers without AI-related skills risk being laid off. Thus, the ease of acquiring AI-related skills will determine the ultimate impact of this technology. (Cazzaniga, 2024)

Based on these two criteria, professions can be classified into three groups: "high impact, high complementarity", 'high impact, low complementarity' and 'low impact'. Although the indicators (and the thresholds used to define what is high and low, represented by their median values) are relative measures, this categorization highlights the general differences between occupations in terms of their AI impact and potential for complementarity. Occupations with a high degree of exposure and a high level of complementarity have significant potential for AI support, as AI can complement workers in their tasks and decision-making. However, there is limited room for uncontrolled use of AI in these positions. These are primarily cognitive jobs with a high degree of responsibility and interpersonal interactions, such as those performed by surgeons, lawyers, and judges. In such positions, workers can potentially benefit from the productivity gains of AI, provided they have the skills necessary to interact with the technology. On the other hand, high impact, low complementarity occupations are well suited for AI integration, but there is a higher probability that AI will replace human tasks. This may lead to a decrease in demand for labor and slower wage growth in these jobs. Telemarketers are a prime example. Finally, "low-impact occupations" have minimal or no potential for AI application. This group covers a wide range of occupations, from dishwashers and performers to others. (Cazzaniga, 2024)

Some scholars note that there is also a positive effect of AI on economic security. AI can be used to improve risk management. For example, AI-based risk management systems can help businesses detect and prevent fraud and manage supply chain risks (Deloitte, 2022).

In addition, AI can create new opportunities for economic growth, such as through the development of e-commerce and platform economies. These new business models can help enterprises enter new markets and access new customers. (McKinsey Global Institute, 2016).

Thus, having analyzed the works of scientists and identified the main approaches to defining the concept of AI and its impact on economic security, we can conclude that the concept of economic security has evolved over time from a narrowly focused protection against external threats to a more comprehensive approach that covers economic growth, social welfare and sustainability, and modern definitions of economic security increasingly focus on human needs, i.e., ensuring a decent standard of living for every citizen. At the same time, AI has a dual nature: AI is both a source of new opportunities and a potential threat to economic security, namely, AI gives rise to new types of threats, such as cybercrime, information manipulation, and technology dependence, while on the other hand, AI can increase production efficiency,

improve risk management, and foster innovation. In addition, the impact of AI on the labor market is becoming a new challenge, where it can lead to both the creation of new jobs and the reduction of some categories of workers, especially those whose functions can be automated.

2. Analyze the impact of artificial intelligence on EU economic security and this effects on the EU's economic stability.

Analyzing the work of scientists on the impact of artificial intelligence on economic security, it has been found that it can be a powerful tool in the fight against economic crime, but it can also be used by criminals to commit complex and elusive crimes. Cooper, for example, believes that with its ability to analyze huge amounts of data and identify patterns, artificial intelligence has fundamentally changed the way we approach economic crime prevention. Machine learning algorithms can sift through mountains of financial transactions, detecting anomalies and flagging suspicious activity that might otherwise go unnoticed. (Cooper, 2023)

In addition, a number of measures to combat economic crime can be traced to the activities of large corporations and companies. For example, in June 2023, Google Cloud launched its anti-money laundering tool based on artificial intelligence to much fanfare. This marks a significant departure from traditional AI tools for economic crimes, as instead of starting with human-defined rules that tell the AI where to look, Google's tool does everything itself. This AI-based approach has proven successful at HSBC, which reported that the Google tool reduced alerts by 60% and increased genuine referrals by two to four times. Such AI developments will continue to reduce costs for financial institutions and allow human experts to focus on the most serious cases. Ultimately, this should reduce economic crime and strengthen the integrity of the financial system. (Cooper, 2023)

However, as artificial intelligence evolves, so do the tactics used by criminals. They are quickly adapting and using the very technology designed to thwart them. Cybercriminals are using artificial intelligence to develop sophisticated attacks that make traditional security measures increasingly difficult to deal with. AI-powered bots can mimic human behavior, bypassing security protocols and infiltrating systems unnoticed. This has led to a surge in identity theft, phishing scams, and ransomware attacks, causing billions of dollars in annual losses. (Cooper, 2023)

One of the most disturbing aspects of economic crime caused by artificial intelligence is the possibility of deep fakes. Deepfakes are processed video or audio that convincingly depict someone saying or doing something they have never done. Criminals can use this technology to impersonate high-level executives and enable fraudulent transactions. The consequences of such deep fake attacks can be catastrophic, undermining confidence in financial institutions and destabilizing markets.

Researchers also consider threats to economic security in connection with the use of AI in terms of fraud. Credit card fraud is also one of the threats. Credit card fraud is a widespread problem that has many causes, from card skimmers to lost or stolen cards. With nearly $29 billion lost to credit card fraud in 2019, financial data theft is the most common form of identity theft. (Reilly, 2024)

As technological advances have changed the way people live, credit card fraud has also changed how people can become victims. Traditionally, the rules that define what credit card fraud looks like had to be implemented manually, taking time and effort.

Today, with around 3 billion credit cards in the world, these traditional methods are not working because manual analysis simply cannot handle the sheer volume of financial data created. There are more credit card issuers than ever, which means more potential fraud cases. What's more, users are demanding more sophisticated and faster responses from those charged

with protecting people's money. Automating credit card fraud detection is the perfect way to meet user needs and ensure security at scale. (Reilly, 2024)

The most effective anti-fraud tools rely on artificial intelligence to ensure that no one can get away with misusing a credit card, financial information, or account number without being detected. At the most basic level, AI fraud detection algorithms analyze data sets and flag anomalies. But what actually happens when an AI algorithm processes transaction data? Researchers identify 4 main aspects:

1. Pattern recognition: AI algorithms group similar data points together based on inherent similarities or correlations in the data. By establishing a baseline of normal activity, these algorithms can quickly detect when something is suspicious. (Sift Trust, 2024)

2. Anomaly detection: Once an inconsistency is detected, fraud detection AI flags transactions or actions that are significantly different from established patterns of normal behavior. For example, if a person suddenly makes an unusually large transaction, artificial intelligence can detect anomalies and alert for further investigation. (Sift Trust, 2024)

3. Real-time monitoring: Detecting anomalies in a data set is one thing, but fraud happens faster than humans can react. Artificial intelligence constantly analyzes incoming data streams and immediately blocks suspected fraudulent activity as soon as it occurs. This real-time monitoring can prevent fraudulent transactions from reducing your business's profits. (Sift Trust, 2024)

4. Machine learning. Machine learning models are trained by analyzing past fraud cases. This allows the algorithms to identify underlying patterns and signs of fraud, helping to develop predictive models. The iterative nature of machine learning allows artificial intelligence systems to continuously improve their (Sift Trust, 2024)

Based on the analysis, we can conclude that AI has a major impact on security and is becoming an increasingly powerful tool in the fight against economic crime, but at the same time it increases risks. On the one hand, AI is able to analyze large amounts of data, detect anomalies and suspicious activities that may indicate fraudulent schemes and allows automating many routine security tasks, freeing up specialists to solve more complex problems. In addition, the use of AI helps to reduce the cost of fighting economic crime and increase the efficiency of law enforcement agencies and financial institutions. But at the same time, AI is creating new threats to the security sector. Criminals can use AI to develop more complex and sophisticated attacks, such as deep fakes and phishing attacks. Therefore, AI attacks may be more difficult to detect because they can mimic human behavior and adapt to new conditions. It is noted that AI is used to conduct large-scale cyberattacks, information manipulation and other criminal activities. This is the dual nature of AI: AI is both a tool for fighting crime and a tool for committing it. With the development of AI, new threats are constantly emerging, which requires constant improvement of security measures.

3. Analyze the EU strategy and methods of countering threats to economic security; analyze the development of national digital security strategies.

Artificial intelligence threats are cross-border in nature, so international cooperation in the field of cybersecurity is necessary to combat them. One important area of international cooperation in cybersecurity is the development of an international legal framework. Currently, there is no single universal treaty that would regulate cybersecurity. However, there are a number of regional and international initiatives aimed at developing such a framework. For example, in 2017, the UN General Assembly established the Group of Governmental Experts on the Development of Information and Telecommunication Technologies in the Context of International Security (GGE). The GGE is authorized to develop norms, rules and principles of responsible behavior of states in cyberspace (United Nations, 2017).

The development of an international legal framework for cybersecurity is a complex undertaking, as countries have different views on how cyberspace should be regulated. Some countries favor stricter rules, while others prefer a more lenient approach. In addition, the rapid development of technology makes it difficult to develop a legal framework that can keep up with the times.

Another important area of international cooperation in the field of cybersecurity is joint operations to combat cybercrime. Law enforcement agencies from different countries can cooperate in investigating and disrupting cybercrime, as well as share information and best practices. For example, Europol, the European Union's law enforcement agency, coordinates joint operations to combat cybercrime between EU member states and other countries (Europol, 2022).

Joint operations against cybercrime can be very effective as they allow law enforcement agencies to pool their resources and expertise. However, such operations can be hampered by differences in legislation and enforcement practices between countries.

In addition to the development of an international legal framework and joint operations to combat cybercrime, there are other areas of international cooperation in the field of cybersecurity. For example, countries can cooperate in research and development to create new cybersecurity technologies and techniques. Countries can also cooperate in the exchange of information and best practices to help each other improve their cybersecurity posture.

Developing national digital security strategies

Each state should develop and implement its own digital security strategy that takes into account its specifics and vulnerabilities. One of the key elements of a national digital security strategy is to strengthen cybersecurity. This includes:

- Development and adoption of laws and regulations governing cybersecurity;
- establishing institutional mechanisms to coordinate efforts in the field of cybersecurity;
- investing in the technical infrastructure necessary to ensure cybersecurity;
- raising awareness of digital threats among citizens and companies and educating them on how to protect themselves.

Cybersecurity laws and regulations should establish clear cybersecurity rules and standards, as well as penalties for cybercrime. For example, in 2018, the European Union adopted the General Data Protection Regulation (GDPR), which sets strict rules for the protection of personal data (European Commission, 2018).

Countries should also invest in the development of national technologies and digital infrastructure. This will help reduce dependence on foreign technologies and increase resilience to external threats.

For example, countries can invest in cybersecurity research and development to create new cybersecurity technologies and practices.

Countries can also invest in their digital infrastructure, such as power grids, financial and communication systems, to make it more resilient to cyberattacks. Estonia's Digital Transformation Strategy, published in 2021, aims to make Estonia a “digital leader”. It includes measures to develop digital infrastructure, promote digital skills, and create an enabling environment for digital innovation (Government of Estonia, 2021).

Having analyzed the threats associated with artificial intelligence, we can conclude that they are becoming increasingly relevant in the modern world. They are cross-border in nature and require joint efforts at the international level. The key methods of countering these threats include the following Development of a legal framework: Internationally recognized norms and rules of conduct in cyberspace should be established to regulate the use of AI. Joint operations: Cooperation of law enforcement agencies from different countries in the investigation of

cybercrime. Exchange of information and technologies: Sharing experience, technologies, and resources to improve cybersecurity. Equally important methods of influencing the BS in the context of AI are the development of national strategies that would include actions aimed at protecting against cyber threats and the adoption of laws and regulations that establish cybersecurity rules. Raising public awareness is also an important factor in the negative impact of AI on ES. Conducting information campaigns to improve the level of cybersecurity of citizens is one of the main factors of the country's well-being

Recommendations

To effectively counter threats to economic security in the AI era, a comprehensive approach is required. This approach should include measures at the national and international levels, as well as measures aimed at:

- Strengthening cybersecurity: This includes developing and implementing cybersecurity strategies, investing in technical infrastructure, and raising awareness of digital threats among citizens and businesses.
- Reducing technological dependence: This includes investing in research and development and supporting domestic technology companies.
- Regulating the market for digital assets: This includes developing regulations governing the market for cryptocurrencies and other digital assets to reduce risks to financial stability and combat money laundering.
- Protecting digital infrastructure from geopolitical conflicts: This includes investing in resilient digital infrastructure as well as developing measures to protect against cyberattacks by foreign governments.

Education and awareness-raising are crucial for economic security in the digital age. Citizens and businesses need to be aware of digital threats and have the skills necessary to protect themselves and their organizations. This can be done through various means such as awareness campaigns, educational programs and training. Thus, ensuring economic security in the digital age is challenging, but it is necessary to ensure the stability and prosperity of nations. Countries need to adapt to the new threats and opportunities posed by digital technologies and take comprehensive measures to protect their economic interests.

Conclusions

The interaction of economic, technological and political forces has created conditions for global economic security. The ongoing war in Ukraine and the growing pace of digital transformation have increased vulnerability and the need for reliable strategies to protect economic interests. Artificial intelligence is seen as a double-edged sword. On the one hand, it has enormous potential to enhance economic security by analyzing data and detecting fraud. This creates new risks, such as cyberattacks, job losses, and the possibility of abuse. The European Union faces significant challenges as a global economic powerhouse. It needs an adaptive strategy that balances innovation, security and ethical considerations. The EU can position itself at the forefront of building a sustainable and secure economic future if it understands the impact of artificial intelligence. Ensuring economic security in the AI era involves governments, businesses, and international cooperation. Only by working together can we maximize the benefits of artificial intelligence.

References

1. Wolff, J., Pauling, J., Keck, A., & Baumbach, J. (2020). The economic impact of artificial intelligence in health care: systematic review. *Journal of medical Internet research*, *22*(2), e16866. https://www.jmir.org/2020/2/e16866/
2. Peres, R. S., Jia, X., Lee, J., Sun, K., Colombo, A. W., & Barata, J. (2020). Industrial artificial intelligence in industry 4.0-systematic review, challenges and outlook. *IEEE access*, *8*, 220121-220139. https://ieeexplore.ieee.org/abstract/document/9285283/
3. Dumitrescu, B. I., & Buzatu, A. I. (2020). Sustainable businesses enhanced through digital transformation and artificial intelligence in the context of Industry 4.0. *New Trends in Sustainable Business and Consumption*, *910*. https://www.researchgate.net/profile/Bassel-Diab/publication/342124082_BASIQ_2020_Conference_proceedings/links/5ee37056458515814a583fe1/BASIQ-2020-Conference-proceedings.pdf#page=910
4. AI, W. I. WHAT IS ARTIFICIAL INTELLIGENCE (AI)?. http://csit.ust.edu.sd/wp-content/uploads/2018/07/AI_lecture3_2018_Intelligent-Agent-part-1.pdf
5. Qin, Y., Xu, Z., Wang, X., & Skare, M. (2024). Artificial intelligence and economic development: An evolutionary investigation and systematic review. *Journal of the Knowledge Economy*, *15*(1), 1736-1770. https://link.springer.com/article/10.1007/s13132-023-01183-2
6. Damioli, G., Van Roy, V., & Vertesy, D. (2021). The impact of artificial intelligence on labor productivity. *Eurasian Business Review*, *11*, 1-25. https://link.springer.com/article/10.1007/s40821-020-00172-8
7. Korinek, A., & Stiglitz, J. E. (2021). *Artificial intelligence, globalization, and strategies for economic development* (No. w28453). National Bureau of Economic Research. https://www.nber.org/papers/w28453
8. Zekos, G. I. (2021). Economics and Law of Artificial Intelligence. *Finance, Economic Impacts, Risk Management and Governance*. https://link.springer.com/content/pdf/10.1007/978-3-030-64254-9.pdf
9. Cazzaniga, M., Jaumotte, M. F., Li, L., Melina, M. G., Panton, A. J., Pizzinelli, C., ... & Tavares, M. M. M. (2024). *Gen-AI: Artificial intelligence and the future of work*. International Monetary Fund. https://books.google.com/books?hl=ru&lr=&id=YLXuEAAAQBAJ&oi=fnd&pg=PA2&dq=Gen-AI:+Artificial+Intelligence+and+the+Future+of+Work&ots=OORi7Q8ZzD&sig=yrPvPTLiKiSaJ6PHHfPPEzSTZHA
10. Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., & Chen, H. (2021). Artificial intelligence in sustainable energy industry: Status quo, challenges and opportunities. Journal of Cleaner Production, 289, 125834. https://doi.org/10.1016/j.jclepro.2020.125834
11. BBC News. (2019, November 22). OneCoin cryptocurrency founder 'disappears'. https://www.bbc.com/news/business-50512547
12. Black, R., Busby, J., Dabelko, G. D., de Coning, C., Maalim, H., McAllister, C., Ndiloseh, M., & others. (2022). Environment of peace: Security in a new era of risk. Stockholm International Peace Research Institute. https://doi.org/10.18356/3210522-en
13. Cabinet Office. (2021). National Cyber Strategy 2022. https://www.gov.uk/government/publications/national-cyber-strategy-2022

14. Calandro, E. (2021). How can digital transformation undermine development and human security? HDRO Background Paper, United Nations Development Programme, Human Development Report Office. https://hdr.undp.org/en/towards-hdr-2022
15. CISA (Cybersecurity and Infrastructure Security Agency). (2022). About CISA. https://www.cisa.gov/about-cisa
16. Deloitte. (2022). AI risk management: A framework for boards and C-suite executives. https://www2.deloitte.com/us/en/pages/advisory/articles/ai-risk-management-framework-for-boards.html
17. European Commission. (2018). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
18. Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021. Luxembourg. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021
19. Europol. (2022). Cybercrime. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
20. FAO (Food and Agriculture Organization of the United Nations), IFAD (International Fund for Agricultural Development), UNICEF (United Nations Children's Fund), WFP (World Food Programme), & WHO (World Health Organization). (2021). The state of food security and nutrition in the world 2021: Transforming food systems for affordable healthy diets. Rome: FAO. http://www.fao.org/publications/sofi/2021/en/
21. Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for Bitcoin regulation. Research in International Business and Finance, 56, 101387. https://doi.org/10.1016/j.ribaf.2021.101387
22. Global Commission on the Geopolitics of Energy Transformation. (2019). A new world: The geopolitics of the energy transformation. Abu Dhabi: International Renewable Energy Agency. https://irena.org/publications/2019/Jan/A-New-World-The-Geopolitics-of-the-Energy-Transformation
23. Government of Estonia. (2021). Estonia's Digital Transformation Strategy 2030. https://www.mkm.ee/en/eesti-digistrateegia-2030
24. International Monetary Fund. (2022, July). World Economic Outlook Update, July 2022: Gloomy and More Uncertain. https://www.imf.org/en/Publications/WEO/Issues/2022/07/26/world-economic-outlook-update-july-2022
25. McKinsey Global Institute. (2016). Digital globalization: The new era of global flows. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows
26. Mints A., Sidelov P. (2022) Digital payment card fraud: new vectors and detection. in Digital technologies in the contemporary economy. Collective monograph. – Vilnius: Mykolas Romeris University, 2022. P. 66-81 https://repository.mruni.eu/handle/007/18890
27. National Academies of Sciences, Engineering, and Medicine. (2017). Building resilience to disasters: A way forward to enhance national health security. Washington, DC: The National Academies Press. https://doi.org/10.17226/23450
28. National Cyber Security Centre. (2022). Cyber Aware. https://www.ncsc.gov.uk/cyberaware

29. NIST (National Institute of Standards and Technology). (2022). Cybersecurity Education and Workforce Development. https://www.nist.gov/cyber-education
30. Pinto, P., Hammond, D., Killelea, S., & Etchell, A. (2021). The paradox of progress with polarisation. Background paper for Human Development Report 2021/2022, UNDP–HDRO. https://hdr.undp.org/en/towards-hdr-2022
31. Purplesec. (2021). 2020 cyber security statistics. https://purplesec.us/resources/cyber-security-statistics/
32. StatCounter. (2022). Search engine market share worldwide. https://gs.statcounter.com/search-engine-market-share
33. The Guardian. (2013, June 6). Edward Snowden: the whistleblower behind the NSA surveillance revelations. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance