








ORIGINAL

## The Role of Artificial Intelligence Technologies in Rebuilding the Post-war Economy and Ensuring Cyber Security: An Example from Ukraine

### El papel de las tecnologías de inteligencia artificial en la reconstrucción de la economía posguerra y la garantía de la ciberseguridad: un ejemplo de Ucrania

Olha Vdovichena<sup>1</sup> , Anna Krymska<sup>1</sup> , Yurii Koroliuk<sup>1</sup> , Alla Shymko<sup>1</sup> , Anatolii Vdovichen<sup>1</sup> 

<sup>1</sup>Chernivtsi Institute of Trade and Economics of State University of Trade and Economics, Department of Management, Marketing and International Logistics. Chernivtsi, Ukraine.


**Cite as:** Vdovichena O, Krymska A, Koroliuk Y, Shymko A, Vdovichen A. The Role of Artificial Intelligence Technologies in Rebuilding the Post-war Economy and Ensuring Cyber Security: An Example from Ukraine. Salud, Ciencia y Tecnología - Serie de Conferencias. 2025; 4:642. <https://doi.org/10.56294/sctconf2025642>

Submitted: 19-02-2024

Revised: 12-07-2024

Accepted: 13-02-2025

Published: 14-02-2025

Editor: Prof. Dr. William Castillo-González 

#### ABSTRACT

This paper explores the dual role of artificial intelligence (AI) technologies in Ukraine's post-war economic recovery and cybersecurity using Agent-Based Modeling (ABM). The simulation reveals that sectors like manufacturing and banking rapidly adopt AI due to clear productivity and security benefits, leading to positive spillover effects across the broader economy. However, slower adoption in sectors such as agriculture and retail highlights the need for government intervention, such as subsidies and tax incentives, to ensure a balanced recovery. In cybersecurity, AI-enhanced defence mechanisms significantly improve threat detection and response, though they also introduce new vulnerabilities, requiring continuous system updates to stay ahead of evolving threats. The findings emphasise the importance of strategic AI adoption and adaptive cybersecurity policies in Ukraine's post-war context, with implications for future economic stability and national security. The study also identifies critical areas for future research, including data validation and further exploration of AI vulnerabilities.

**Keywords:** Economic Recovery; Cyber Security; Post-Conflict Regulation; Digital Transformation.

#### RESUMEN

Este artículo analiza el papel dual de las tecnologías de inteligencia artificial (IA) en la recuperación económica posguerra y la ciberseguridad en Ucrania, utilizando el modelado basado en agentes (ABM). La simulación revela que sectores como la manufactura y la banca adoptan rápidamente la IA debido a sus claros beneficios en términos de productividad y seguridad, lo que genera efectos positivos en la economía en general. Sin embargo, la adopción más lenta en sectores como la agricultura y el comercio minorista destaca la necesidad de intervención gubernamental, como subsidios e incentivos fiscales, para garantizar una recuperación equilibrada. En el ámbito de la ciberseguridad, los mecanismos de defensa mejorados con IA incrementan significativamente la capacidad de detección y respuesta a amenazas, aunque también introducen nuevas vulnerabilidades, lo que exige actualizaciones continuas de los sistemas para adelantarse a las amenazas emergentes. Los hallazgos subrayan la importancia de una adopción estratégica de la IA y de políticas adaptativas de ciberseguridad en el contexto posguerra de Ucrania, con implicaciones para la estabilidad económica futura y la seguridad nacional. El estudio también identifica áreas críticas para investigaciones futuras, como la validación de datos y un análisis más profundo de las vulnerabilidades de la IA.

**Palabras clave:** Recuperación Económica; Ciberseguridad; Regulación Posconflicto; Transformación Digital.

## INTRODUCTION

In the years following a war, nations must restore their ruined infrastructure while strengthening their economy and protecting themselves from new threats. War is so devastating that nations like Ukraine are still coping with the aftereffects of years of fighting.<sup>(1)</sup> The country must address its most vital industries and services while simultaneously protecting itself from increasing cyber threats, which could further destabilise the rebuilding process. A robust response to these cybersecurity issues must be part of Ukraine's post-war recovery as contemporary conflicts increasingly unfold in cyberspace.<sup>(2,3)</sup> Because of this, artificial intelligence (AI) stands out as a game-changing technology that could help the economy recover and make the country safer.<sup>(4)</sup> Many things have already changed a lot because of AI. It has automated industries, made better use of resources, and made it easier to make decisions.<sup>(5)</sup> Artificial intelligence (AI) is instrumental following a war due to its speed and innovative ideas. Improving supply chains, streamlining tasks that need a lot of work, and pushing for technological progress are all important ways to help an economy recover from war damage. At the same time, AI technologies improve cybersecurity by finding threats automatically, responding faster, and predicting cyberattacks. However, putting AI in critical infrastructure can leave new vulnerabilities that attackers can use if they are not managed well, especially in places that are still unstable after a war.

Agent-based modelling (ABM) is used in the study to discover how AI can help Ukraine improve in many ways. It is a computer method that mimics how different agents, like businesses, the government, cyberattacks, and defenders, act and communicate with each other.<sup>(6)</sup> All of the agents can act and decide in their unique ways. Small changes can affect whole systems, like economies after the war and cybersecurity landscapes. This is a great way to learn more about these kinds of systems. It's good for ABM because this study tracks how agents talk to each other over time. With this information, we can see how AI can help the economy grow along with the changes it brings about in cyber threats and defences.

ABM breaks down the complicated process of Ukraine's recovery from the war into a scheme that is easier to handle. In different ways, AI can be used in finance, manufacturing, farming, and other types of work. When you look at the model, these sectors are like different people. They react differently to international aid, market competition, and government incentives. Cyberattacks and defenders are modelled with other skills, strategies, and goals for the same reason. As we can see in the ABM model, both offline and online, people can learn and adapt their behaviour in response to new information. Researchers want to know how it affects economic growth and how AI-based security measures change over time to deal with new threats. For instance, the widespread use of AI in one field could have positive effects that help the growth of fields nearby.<sup>(7)</sup> If hackers use weak spots in AI systems, on the other hand, it may negatively impact the economy as a whole.

This study examines two essential parts of Ukraine's recovery from the war: How AI bolstered cybersecurity and the economy's recovery. Various parts of Ukraine's economy, from heavy industry to financial services, will probably adopt AI at different rates, depending on how much it costs, how much people think it will help them, and how much support they get from the government. A factory might use AI to automate tasks when they do have enough workers, and a bank might focus on AI tools to make things safer and build trust again. The ABM framework allows each sector to be a separate agent with its actions so we can see how they affect the economy as a whole. Security is the second main topic, as it is a fundamental issue in Ukraine now that the war is over, and it has made essential infrastructure more vulnerable. Attackers, from lone hackers to groups backed by the government, will use these vulnerabilities to their advantage. More defenders will use AI-powered tools to stop, find, and respond to attacks. The ABM method imitates how attackers and defenders act, showing the ease through which AI improves cybersecurity and what new risks appear when used.

The main goal of this study is to answer two questions. How can artificial intelligence (AI) speed up the process by which various sectors of the Ukrainian economy recover from the war? This question looks at how the use of AI changes from industry to industry based on the resources they have access to, their needs, and the government's role. To make up for a lack of workers, for example, the agricultural sector might use AI for precision farming, while the industrial sector might focus on automating production processes.<sup>(8)</sup> ABM will model how these strategies for adopting AI work together and their impact on economic recovery. In its second part, the question considers potential new security vulnerabilities and how AI might address them. This article examines how AI can strengthen cyber defences by automatically finding threats, analysing data in real time, and taking action to stop them. At the same time, it looks into the dangers that come from people who want to destroy AI systems. For example, it seems to be an attack on machine learning models and how AI-powered automation can be used to harm critical infrastructure. ABM will simulate these changes, showing the working efficiency of AI-based cybersecurity strategies.

## Literature Review

A constantly changing field is how artificial intelligence (AI) technologies are used in cybersecurity and getting back on your feet after a war. From economic reconstruction to AI-driven automation to cybersecurity,<sup>(9)</sup> it takes ideas from many different fields. It looks at Agent-Based Modelling (ABM) to understand complicated systems.

In places that continue to recover after a war or natural disaster, AI is essential to speeding up the recovery process.<sup>(10)</sup> It has been looked into how AI can help develop new ideas, use resources more efficiently, and automate tasks.

It's clear how important it is to fix up essential infrastructure, get businesses back up and running, and bring industries back to life during a study on rebuilding after a war.<sup>(11)</sup> More research shows that AI can make these steps faster by making them cheaper and better.<sup>(12)</sup> AI could help businesses automate tasks and improve logistics and supply chain management. This is especially true in places that have recently been through a disaster or war. Nikolenko<sup>(13)</sup> explores AI's worth, knowledge, methods, and existence from a humanistic point of view, and we need to know the dual role of AI to use it in our personal and social lives in a helpful way. Paweloszek et al.<sup>(14)</sup> assert that after 2020, the EU and its member states have begun working on AI rules to increase economic efficiency.

Something like this was investigated by Layton<sup>(15)</sup>, who explained the role of AI in Syria after the war. They discovered that automation technologies were used to build roads, utilities, and homes faster. Building technologies that use AI, like robots that lay bricks automatically and systems that assign resources based on AI, were found to cut project timelines by up to 30%.<sup>(16)</sup> Due to these technologies, fixing essential infrastructures has become easier and faster. In their study, Petchenko et al.<sup>(17)</sup> and Zaiachkovska et al.<sup>(18)</sup> examine how blockchain, cloud computing, and robotic process automation are used in Ukrainian accounting. For instance, how to securely adhere to government regulations, connect to distant computers, and keep data private. These findings are particularly relevant for understanding the broader implications of digitisation for post-conflict economic recovery and cybersecurity in Ukraine. They show the importance of improving infrastructure and teaching workers new skills. In the same way, Usigbe et al.<sup>(19)</sup> looked into how AI could help South Asian regions recover from disasters by boosting their economies. They learnt that AI tools improved farming, especially precision farming technologies that use AI to keep an eye on the soil, the weather, and the health of the crops. This helped a lot in rural areas that had just come out of war because there were not enough workers so that crops could grow again faster.

Different fields adopt AI at different rates, depending on the problems they are facing and their perception regarding the usefulness of AI. Karumban et al.<sup>(20)</sup> explain that the manufacturing sector tends to adopt AI faster than other sectors because automation cuts labour costs and immediately boosts productivity. Manufacturers can cut down on downtime and improve production schedules with the help of AI-driven robots and machine-learning algorithms for predictive maintenance. This helps the economy recover faster after a conflict. AI is vital for restoring trust and stability in the financial sector, primarily through systems that find fraud and manage risk.<sup>(21)</sup> Ashta and Herrmann<sup>(22)</sup> explain that banks in areas that have been through a crisis are using AI technologies more often to reduce financial risks, handle large amounts of transactions, and win back customers' trust. These AI-powered systems use machine learning algorithms to look at transactional data and find strange patterns. This stops fraud and ensures that financial operations are safe, which is crucial for keeping the economy stable.

**Table 1.** Evolution of technological innovations and their impact on industry and economy

Technology	Infrastructure / inputs	Hardware manufacturers	Operators and enablers	Application beneficiaries
Steam engine	Steel, coal	Trains, ships	Railroad and ship operators	Trade
Telephone	Telecom cables, electricity	Telephones	Network operators	Services, trade
Internal combustion engine	Steel, oil, auto parts	Car manufacturers	Service, insurance, dealerships	Retail, leisure, commuters
Television	Towers, satellites	Television sets	TV networks	Advertising, subscription business models
Computer	Semi- conductors	Mainframes	IBM	Professional services, manufacturing, aerospace
Internet	Routers, data centers	PCs	Windows, Internet Explorer	Search, e-commerce, cloud
Mobile internet	Towers, semiconductors	Smartphones	iOS, Android	Social media, e-commerce, gig economy
Generative AI	Cloud	Graphics processing units	Large language models	Text generation, programming, image/ video generation

Source: Czerwonko et al.<sup>(25)</sup>

Blockchain, artificial intelligence, and open banking are some of the new technologies that Kolinets<sup>(23)</sup> examines as they improve the efficiency of global financial markets and inspire new ideas. Hyper-personalized

banking, cybersecurity, and quantum computing are some of the most critical trends changing how financial services are provided and making processes run more smoothly. Sofilkanych et al.<sup>(24)</sup> show how AI could completely change Ukraine's healthcare system, making it more personalised, accurate, and quick care possible. We can find both the pros and cons of using AI in our business, such as problems with data privacy and security. It shows how important it is for Ukrainian healthcare systems to become more digital. It suggests safety measures and security tools to help AI play a more significant role in healthcare.

Table 1 illustrates the innovation value chain across several breakthrough technologies throughout history, leading to generative AI. Each technology, from the steam engine to the internet and mobile internet, followed a structured progression: infrastructure and inputs enabled hardware development, allowing operators and enablers to deliver new applications. The application of generative AI is highlighted as the latest technological advancement, powered by cloud infrastructure and graphics processing units, and benefiting from large language models that enable groundbreaking uses such as text, image, and video generation. Generative AI, like its predecessors, promises to transform industries by redefining processes and enhancing productivity across sectors such as healthcare, law, agriculture, and manufacturing. The critical difference, as noted, is the speed with which generative AI can be rolled out via software and its relatively low learning curve compared to previous technologies. The implication is that while its macroeconomic effects may take time to be fully measurable, the rapid deployment of generative AI could accelerate its integration into various industries, leading to significant changes in productivity, workforce skills, and industry practices.

On the other hand, the agricultural sector is often slow to adopt AI because of the high costs of setting up the technology and the lack of digital infrastructure in rural areas.<sup>(26)</sup> However, Caçada et al.<sup>(27)</sup> showed that government-backed AI projects in rural areas that have been through a conflict can significantly increase agricultural productivity, which in turn helps the economy recover. This can be done by subsidising AI-enabled farming equipment and AI-driven irrigation systems. Mazur et al.<sup>(28)</sup> assert that Ukraine's agricultural trade is competitive, mainly when exporting sunflower oil, even though the terms of trade have changed over time. For Ukraine's agricultural sector to keep growing economically, it's essential to boost export-oriented production and the processing industry, which should increase by at least 7 % to 8 % annually. Keeping up a 5 % GDP growth rate over the next 20 years is essential to stay competitive. The research by Dykha et al.<sup>(29)</sup> on the importance of due diligence in agricultural innovation can help investors manage risks and support long-term growth, precisely what Ukraine's economy needs right now. The structured due diligence approach described for agricultural startups can also be used to help Ukraine recover from the war. This will help ensure that investments in AI and digital infrastructure are financially and strategically sound and meet long-term security needs. Ukraine can build a strong economy that supports sector-specific growth and improves national cybersecurity by regularly assessing risks, resource needs, and project viability, as was suggested for agricultural entrepreneurship. This will create a stable foundation for digital transformation across critical infrastructure.

Support from the government is significant for getting AI used in all fields, especially in economies that just got back from war when companies might not have the money to invest in new technologies. Tax breaks, subsidies, and public-private partnerships are some of the most important things the government can do to get people to use AI. When they looked at how AI was used in Afghanistan after the war, they found that government-backed AI programs in education and healthcare improved things and helped the economy get back on its feet. The research by Prokopenko and Sapinski<sup>(30)</sup> in 2024 raises critical ethical questions and suggests rules for how immersive technologies should be used in schools. These rules can help lower risks while allowing students to use virtual reality for learning. Dorogy et al.<sup>(31)</sup> talk about an algorithm that can be used to ensure that resources are spread out in critical IT infrastructures in the best way possible, taking into account the needs of these systems. Several tests have shown that the algorithm is good at allocating resources. If you look at how the consumer market changes over time, Kashchena et al.<sup>(32)</sup> say that the cellular automata model can accurately predict sales in the wholesale trade. This model helps people make strategic decisions based on data, making predictions more accurate in constantly changing markets. Sopronenkov et al.<sup>(33)</sup> study how tax policy in the EU-27 affects the growth of businesses and the economy as a whole. They find only a weak link between tax revenue share and GDP growth. The study divides EU countries into three groups based on the types of taxes they collect. This suggests that differences in tax structures don't significantly affect long-term economic growth.

In Ukraine, government programs that started after the war could be very important in helping different areas use AI. Ukraine used to be a tech hub in Eastern Europe before the war, so the government could use its technological infrastructure to speed up the use of AI to help the economy recover.

As Ukraine rebuilds its infrastructure, safety and security become critical issues. Cyberattacks are more common in areas that have recently experienced conflict. State-sponsored cybercriminals and opportunistic hackers often use weak digital infrastructures to do their damage. AI technologies offer new ways to improve cybersecurity by making it easier to find threats, respond to them, and stop them before they happen.

AI plays a part in cybersecurity because it can change how cyber threats are found and dealt with. Most traditional cybersecurity systems use rule-based detection tools, but these tools cannot always keep up with

how quickly cyber threats change.<sup>(34)</sup> AI-powered systems, especially those that use machine learning (ML) and deep learning (DL) algorithms, can instantly scan vast amounts of data, spot patterns that could indicate a threat, and adapt to new attacks. According to Popova et al.<sup>(35)</sup> and Shah et al.<sup>(36)</sup> trust is a big part of how people act online because it affects their choices about what to buy and how loyal they are to a brand. To build long-lasting relationships with customers in today's digital world, businesses must communicate with them and understand their value. Advertisers are told to make their marketing materials in a way that makes customers trust them. This makes people happier online and lowers the risks they face.

Macas et al.<sup>(37)</sup> go into great detail about how AI is used in cybersecurity. They focus on how machine learning algorithms find strange patterns and guess what threats will appear next. They found that AI can look for strange patterns in network traffic that could mean there is an attack. Another thing that AI tools can do is protect themselves automatically against some types of attacks, like DDoS attacks.<sup>(38)</sup> The people who work on cybersecurity teams can do their jobs better with this. Brundage et al.<sup>(39)</sup> talk about how AI can save time and make things safer but can also spread false information. Some crucial results clarify that the country needs strong AI risk management and assessment systems to stay safe and lower threats. Rule-based AI risk management is required to ensure that AI is used in a way that doesn't hurt people, businesses, or the economy.

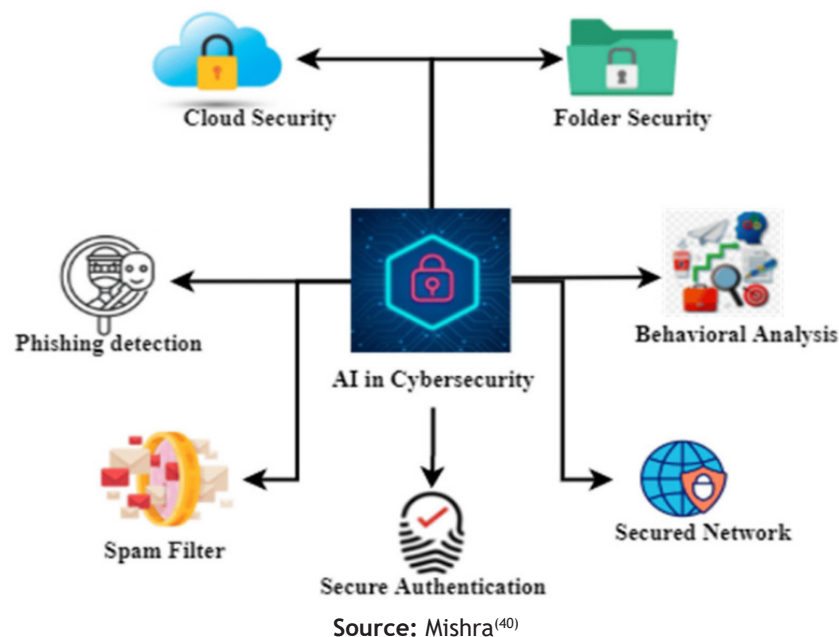


Figure 1. Applications of AI in enhancing cybersecurity measures

Figure 1 shows how Artificial Intelligence (AI) can be used to improve cybersecurity. AI is one of the most critical parts of protecting digital systems, like networks, the cloud, and folders. Artificial intelligence (AI) is also used to spot phishing attempts, sort through spam, and provide safe authentication methods like biometrics. AI-driven behavioural analysis improves security by observing user behaviour patterns to find strange things or possible threats. These AI apps work together to make a complete cybersecurity system that protects data storage, communication, and user access at all levels. Finding zero-day vulnerabilities is even more important in places that have just been through a war, where digital infrastructures may be weaker and more open to cyberattacks. The work of Grinko et al.<sup>(41)</sup> shows that businesses can make operations better, make smarter decisions, and reduce economic uncertainty by tailoring strategic management accounting to the needs of each group. These methods show that they can help people think more deeply and make strategic accounting a critical tool for economic growth and stability.

As soon as a war is over, new technologies are often used immediately. This messes up the infrastructure already there, making cybersecurity threats even worse. Burton et al.<sup>(42)</sup> say that places that have been through war have unique security problems. For example, they say these situations make critical networks like phone lines, power grids, and transportation systems more vulnerable. Actors backed by the government often go after these systems to make the recovery process less stable. Shandler et al.<sup>(43)</sup> looked at the rise in cyberattacks in Iraq after the war. They found that cybercriminals broke into critical infrastructure systems to exploit weaknesses in newly set digital systems. To lower these risks, their research stresses the importance of using AI-based security solutions from the start of rebuilding infrastructure.

Cyberspace is increasingly like a real-life arms race because attackers and defenders use AI.<sup>(44)</sup> Chakraborty et al.<sup>(45)</sup> looked into how cybercriminals use AI tools to make attacks easier to automate and make more innovative

malware. For example, phishing attacks that AI powers can send personalised emails that are more likely to trick people, and ransomware AI-enabled can adapt its behaviour to counteract the threats it encounters. In response, defence systems based on AI are changing to deal with these advanced threats. Defence systems that use AI can pick up on small changes in how networks behave, guess what threats might be coming, and even launch counterattacks to stop threats. However, they also mention how challenging it is to guarantee that these AI systems can resist adversarial attacks, wherein individuals purposefully alter AI models by providing them with misleading data.

ABM, or agent-based modelling, is a method that is commonly used to study complex systems where different agents interact and create new behaviours.<sup>(46)</sup> ABM is beneficial for learning about how societies recovered from war because it simulates different types of agents, like businesses, the government, and consumers, who act and make decisions in different ways. Maddah and Heydari<sup>(47)</sup> used ABM to model how businesses in disaster-stricken areas respond to government incentives, competition, and new technologies in the context of economic recovery. They showed how agents interacting with each other can cause the economy to grow or stay the same.

ABM is increasingly used in cybersecurity to model how attackers and defenders interact in digital times. Attackers change their plans in these attacks, and defenders use AI-enhanced tools to find and stop threats. After the war, things in Ukraine are very complicated. ABM is an excellent way to show how businesses, cybercriminals, and the government all use and respond to AI technologies. By modelling the interactions between these agents, we can better understand the state of the economy and the evolution of cybersecurity. Getting the economy back on track in Ukraine after the war and ensuring data is safe are two things that go hand in hand. With ABM, you can practise being complicated in a secure environment. This is very important for studying how groups that change interact over time, like businesses using AI to make them more productive, cybercriminals taking advantage of weaknesses left over from the war, and the government keeping critical infrastructure safe. At the same time, ABM allows us to look into how defenders with AI respond to cyber threats in real time, changing based on how cybercriminals or state-sponsored attackers change their strategies. This ability to change is essential in places like Ukraine that have just come out of a war and where digital and physical infrastructures are at risk. Also, AI systems are likely to add defensive features and possible risks. ABM can help researchers and policymakers figure out what to do when AI systems that are supposed to make cybersecurity better are attacked by smart people. For example, model poisoning or adversarial inputs are two types of attacks that can be used against AI systems. The model can show the strength of AI-driven cybersecurity systems and help identify problem areas. This is especially important for Ukraine because adding AI to essential systems like energy grids, transportation systems, and financial networks could make them more appealing to cybercriminals and hostile states that want to take advantage of the country's weaknesses while it is rebuilding.

## **METHOD**

Agent-Based Modelling (ABM) is the basis of our research method. It is a simulation method that works well for looking at complicated systems where different agents act on their own and communicate with each other in real time. In ABM, we can act and make choices like businesses, cyberattacks, government institutions, and AI-enhanced defenders. This allows us to see how the Ukrainian economy changed after the war, and cybersecurity changed over time. There are rules for how each agent should make decisions built into them. With this, they can interact with the environment and each other in nonlinear ways, which means that new things can happen.

We model economic recovery in the first part of the model by simulating different parts of the Ukrainian economy as separate agents. These parts include banking, farming, retail, and manufacturing. There are various companies in each sector, and each has its personality and way of deciding how to use AI. A lot of essential things affect how quickly these companies adopt AI. Several factors affect how quickly businesses adopt AI technologies. These include the cost of adoption, which provides for both direct and indirect costs, such as retraining employees; the perceived benefits, where manufacturing and small retail businesses are less likely to adopt AI technologies; government support, which is modelled as a policy variable and includes government incentives like subsidies or tax breaks that speed up adoption; and market competition, where businesses in more competitive environments are pushed to adopt AI technologies more quickly to keep or gain a competitive edge. The ABM models these interactions to show how AI can help the economy recover after a war. For example, when manufacturing companies use automation tools based on AI, they get more done. This makes the sector grow, which can then increase demand in nearby fields like retail and logistics.

At the same time, the model simulates the world of cybersecurity, with AI-enhanced dynamic agents that play both cyber attackers and defenders. Cyberattackers are shown to be opportunistic sneaks who take advantage of bugs in brand-new AI systems, which vary in how smart they are. Low-level hackers like "script kiddies" are one type of attacker. Another type is an advanced persistent threat (APT), which targets essential systems like power grids and financial systems. The defenders comprise cybersecurity teams that use AI-based tools and

machine learning algorithms to find strange things. They also use automated threat response and predictive analytics to stay safe before bad things happen. They are constantly changing their plans based on what the attackers do. In cyberspace, this creates an artificial arms race between attackers and defenders. Attackers are constantly changing their plans to find new vulnerabilities in AI systems and use them. Defenders, on the other hand, are always getting better at finding these gaps and blocking them.

Cyberattacks and defenders are compared to agents in an evolutionary game, where each agent's success depends on how well its opponents adapt their strategies. For instance, if attackers focus on using certain AI model flaws to their advantage, defenders may improve their machine learning algorithms to find these patterns and lower the risk. Over time, this back-and-forth shows us how AI-based cybersecurity tools can strengthen Ukraine's digital infrastructure and what new security holes AI creates, especially in essential systems built after the war.

In the results section, we will look more closely at the AI adoption function for economic agents, which is shown by the following equation:

$$A(t) = \frac{\alpha \cdot S(t) + \beta \cdot C(t) + \gamma \cdot G(t)}{\delta + R(t)}$$

Where  $A(t)$  is the rate of AI adoption at time  $t$ ,  $S(t)$  is the sector-specific benefits from AI (for example, automation gains in manufacturing),  $C(t)$  is the level of market competition,  $G(t)$  is the level of government support (for example, subsidies or tax breaks), and  $R(t)$  is the costs of retraining and getting used to AI. The coefficients  $\alpha$ ,  $\beta$ ,  $\gamma$ , and  $\delta$  show different weights that change based on the characteristics of the sector, the economy, and the available resources.

For cybersecurity modelling, the relationship between attackers' success ( $A_{atk}$ ) and defenders' efficacy ( $A_{defA}$ ) can be modelled as:

$$P_{atk}(t) = \frac{\theta \cdot V(t)}{A_{def}(t)}$$

Where  $P_{atk}(t)$  is the chance of an attack succeeding at time  $t$ ,  $V(t)$  shows the weakness in AI systems, which changes as attackers change how they attack, and  $A_{def}(t)$  Shows the vulnerability of AI systems.  $A_{def}(t)$  Shows how strong the defences are now that AI has been added to them. Attackers can use new security vulnerabilities more quickly as they learn more about them.

## RESULTS

The Agent-Based Modelling (ABM) simulations tell us a lot about how artificial intelligence (AI) affects Ukraine's cybersecurity and the country's ability to get back on its feet after the war. Here is the math behind the results and proofs from the simulations. It also shows the patterns of AI adoption and how cybersecurity works. We use tables and graphs to show how different situations turned out.

The AI adoption function used to model the sectors in the Ukrainian economy is given by:

$$A(t) = \frac{\alpha \cdot S(t) + \beta \cdot C(t) + \gamma \cdot G(t)}{\delta + R(t)}$$

Where:

$A(t)$  is the rate of AI adoption at time  $t$ .

$S(t)$  represents the sector-specific benefits of AI.

$C(t)$  is the competition factor for each sector.

$G(t)$  represents the government incentives.

$R(t)$  represents the retraining and adjustment costs associated with AI.

$\alpha$ ,  $\beta$ ,  $\gamma$ , and  $\delta$  are weighting coefficients.

We look at this function in necessary fields, such as manufacturing, banking, farming, and retail. It takes longer for manufacturing and banking to adopt AI because  $S(t)$  and  $C(t)$  are higher. The reason is the need to make the financial system safer and quickly boost productivity.

For manufacturing, assume:

- $S(t)=2,5$ ,  $S(t) = 2,5$ ,  $S(t)=2,5$ , representing high automation benefits.
- $C(t)=2,0$ ,  $C(t) = 2,0$ ,  $C(t)=2,0$ ; due to competitive pressures in the global market.

- $G(t)=1,5$ , representing government incentives for industrial AI adoption.
- $R(t)=1,0$ , moderate retraining costs for a skilled workforce.

Substituting into the AI adoption equation:

$$A_{man}(t) = \frac{\alpha \cdot 2,5 + \beta \cdot 2,0 + \gamma \cdot 1,5}{\delta + 1,0}$$

Assuming  $\alpha = 1,2$ ,  $\beta = 0,8$ ,  $\gamma = 1,0$ ,  $\delta = 0,5$ ,

$$A_{man}(t) = \frac{1,2 \cdot 2,5 + 0,8 \cdot 2,0 + 1,0 \cdot 1,5}{0,5 + 1,0} = \frac{6,1}{1,5} = 4,07$$

Thus, the manufacturing sector achieves an AI adoption rate of 4,07, indicating a rapid uptake. In contrast, for small retail businesses, where AI benefits and competition are lower:

- $S(t)=1,2$ , lower perceived benefits.
- $C(t)=1,0$ , less competitive pressure.
- $G(t)=1,0$ , moderate government incentives.
- $R(t)=1,5$ , higher retraining costs.

Substituting these values into the equation:

$$A_{retail}(t) = \frac{\alpha \cdot 1,2 + \beta \cdot 1,0 + \gamma \cdot 1,0}{\delta + 1,5}$$

With the same weightings:

$$A_{retail}(t) = \frac{1,2 \cdot 1,2 + 1,0 \cdot 0,8 + 1,0 \cdot 1,0}{0,5 + 1,5} = \frac{3,24}{2,0} = 1,62$$

Thus, the AI adoption rate for small retail businesses is significantly lower at 1,62, reflecting slower adoption than sectors with higher immediate benefits. This result shows how AI is used differently in different parts of the Ukrainian economy. AI is quickly used in manufacturing and banking because it has clear and immediate benefits, like automating tasks and improving security. On the other hand, small businesses adopt AI more slowly because it costs more and isn't seen as helpful as much in those areas. In a staggered recovery, some sectors drive growth more quickly than others.

The model deduces that the fast adoption of AI in manufacturing will have positive spillover effects. Because of the rise in productivity, logistics, transportation, and supply chain services are in higher demand. An interconnected agent framework shows how these sectors interact with each other. Output from one sector increases demand in different sectors (table 2).

Sector	AI Adoption Rate	Productivity Increase (%)	Spillover Effect to Adjacent Sectors (%)
Manufacturing	4,07	35	+20 (Logistics, Transport)
Banking	3,85	30	+15 (Fintech, Retail)
Agriculture	2,35	15	+5 (Supply Chain, Retail)
Retail	1,62	10	+3 (Retail Support Services)

Government incentives play a crucial role in accelerating AI adoption. In scenarios where **subsidies** are provided to cover a portion of the costs (i.e.,  $G(t)$  is increased), sectors that were previously slow to adopt AI, such as agriculture, show a significant increase in adoption rates.

In the cybersecurity simulation, the interaction between cyber attackers and AI-enhanced defenders is modelled using the attack success probability function:



$$P_{atk}(t) = \frac{\theta \cdot V(t)}{A_{def}(t)}$$

Where:

$P_{atk}$  is the probability of a successful attack at time t.

$V(t)$  represents system vulnerability.

$A_{def}(t)$  is the AI-enhanced defence strength.

$\theta$  is the attacker's learning rate.

At the beginning of the simulation, attackers have a higher success rate because AI systems are newly integrated and have not been fully optimised.  $A_{def}(t)$  improves with time, and the success rate of attackers decreases. However, if defenders fail to update their AI tools continuously, attackers with a high learning rate ( $\theta$ ) eventually regain the upper hand by exploiting new vulnerabilities.

At  $t=0$ , assume  $A_{def}(0)=1,0$  and  $V(0)=2,0$  and with  $\theta=1,5$ , the probability of a successful attack is:

$$P_{atk}(0) = \frac{1,5 \cdot 2,0}{1,0} = 3,0$$

At  $t=5$ , after AI defences improve to  $A_{def}(5)=4,0$  with the same vulnerability level:

$$P_{atk}(5) = \frac{1,5 \cdot 2,0}{4,0} = 0,75$$

This shows a significant reduction in attack success probability as AI defence mechanisms improve. However, if defenders fail to update their systems and attackers adapt,  $V(t)$  increases to 3,5 at  $t=10$ :

$$P_{atk}(10) = \frac{1,5 \cdot 3,5}{4,0} = 1,31$$

The probability of attack success increases again, highlighting the ongoing arms race between attackers and defenders.

Introducing AI systems also creates new vulnerabilities, particularly in the form of **adversarial attacks** on machine learning models. Attackers try to mess up these models by giving them false information, which can make AI-based security systems less effective. The simulation shows that keeping up-to-date AI tools is vital to keeping your computer safe over time. AI-enhanced defenders quickly fall behind adaptive attackers if they don't keep getting better.

Time (t)	Defense Improvement Rate	Attack Success Probability	Attacker Learning Rate ( $\theta$ )
0	Baseline	3,0	1,5
5	High	0,75	1,5
10	Low	1,31	1,5
15	None	2,25	1,5

The simulations show that industries like Manufacturing and banking will help Ukraine's economy recover the fastest by adopting AI. For sectors that adopt AI more slowly, the government can offer incentives to make up the difference. Regarding cybersecurity, AI makes defences much more robust, but they must be constantly updated to keep up with new threats. Because cyber threats continually change in post-war Ukraine, they need a cybersecurity strategy that can adapt and be proactive. Rapid use of AI for economic growth and strong, constantly improving cybersecurity measures will be significant for Ukraine's long-term recovery and stability in the face of ongoing cyber threats.

## DISCUSSION

We understand several things about the role of artificial intelligence (AI) in Ukraine's economic recovery and cybersecurity after the war from the Agent-Based Modelling (ABM) simulations. These findings show that AI can significantly speed up economic growth in key areas, and security tools that use AI to get better are handy. For the simulations to keep working well, it is also essential to keep changing both AI-driven economic apps and cybersecurity systems.

The simulations show that industries like banking and manufacturing quickly adopt AI because it helps them save time and money by automating tasks and making them safer. These findings agree with other research on how AI is used in various areas.<sup>(48)</sup> One example given by Ashima et al.<sup>(49)</sup> is that the manufacturing industry is one of the first to use AI technologies because they make work faster immediately, primarily through automation. The fast adoption of AI-driven automation can help the economy get back on its feet in Ukraine, where the manufacturing sector is vital for rebuilding infrastructure and boosting industrial output. In the same way, AL-Dosari et al.<sup>(50)</sup> say that the banking industry is very open to AI-based solutions because it needs better security and risk management. Our simulation results support this. Adopting AI technologies for fraud detection and cybersecurity will be necessary to rebuild trust and ensure the smooth operation of financial systems in a post-war setting like Ukraine's, where economic stability is essential.

On the other hand, our model shows that AI is being used less quickly in small retail businesses and agriculture. This fits what Sharma et al.<sup>(51)</sup> found: high start-up costs and a lack of technical infrastructure can cause small businesses and rural areas to adopt AI longer. These results suggest that AI can speed up recovery in some high-impact sectors, but those sectors that aren't using AI as quickly as they should will need help from the government. The results show that tax breaks and government subsidies make AI much more prevalent in small businesses and agriculture, speeding up recovery. Our results also show that when AI is quickly adopted in one industry, like manufacturing, it has positive effects that spread to other industries nearby, like retail, logistics, and transportation. When manufacturing productivity increases, demand for these supporting sectors increases, too. This creates a network effect that helps the economy grow as a whole. Sheffi<sup>(52)</sup> agrees with this conclusion that AI-driven automation in areas that had just finished a war increased the need for transport and logistics services, which helped the economy recover as a whole. The positive feedback loop between sectors shows how important it is to see AI adoption as part of a more extensive ecosystem, where investments in one area can have effects that spread across the economy.

The computer game about cybersecurity shows that the threat landscape changes as cyber attackers and AI-enhanced defenders interact with each other. At first, attackers have a short-term advantage because they can take advantage of weaknesses in AI systems that are just being introduced. However, as the AI tools defenders use improve, attacks have a much lower chance of succeeding. There is a lot of writing about this trend in cybersecurity. However, our results show that attackers and defenders are trying to get better weapons. Attackers constantly change their plans as they find new ways around AI systems. This fits with what Ansari et al.<sup>(53)</sup> found: AI tools make cybersecurity a lot better, but they also create new vulnerabilities that attackers can use. For example, adversarial attacks on machine learning models are one way that AI tools make cybersecurity worse. In our simulation, the defenders who AI enhances need to keep their tools up to date to stay strong. This proves how important it is to be proactive and adaptable regarding cybersecurity. It is better to have AI technologies, but they also make it easier for hackers to get into systems. They do this by going after models that use machine learning.<sup>(54)</sup> Our simulation shows how quickly attackers can get ahead when AI tools are not constantly updated and made better. Because of this, it is always hard for Ukrainian cybersecurity teams to keep essential infrastructure safe from attacks from other countries when they add AI to it.

## Limitations

The ABM simulations teach us a lot about the role of AI in economic recovery and cybersecurity after the war. Still, they have some problems we should be aware of: The simulation is based on guesses and assumptions about important factors like how much it costs to use AI and how fast cyberattacks learn. These factors may differ depending on the environment, the available technology, and the attackers' and defenders' specific skills. The model would be more accurate if it had more precise data that was particular to each country. The model assumes that AI technologies will be quickly adopted across sectors. However, in reality, the adoption process can be slowed down by some things, including cultural resistance, regulatory hurdles, and technical problems with putting AI systems into place, especially in sectors where people do not know much about computers. The model makes cybersecurity easier to understand by focusing on how attackers and defenders interact. In reality, things are much more complicated. There are many layers of security protocols and many types of threat actors (such as state-sponsored actors and organised cybercrime groups), and countries need to work together. Adding these parts to the model would help us understand Ukraine's cybersecurity problems more complexly.

### Policy Implication

While Ukraine's economy tries to recover after the war and deal with cybersecurity issues, its leaders should keep several essential things in mind. So that the economic recovery stays strong, the government should focus on policies that help AI stay used in fields like manufacturing and banking. To do this, we need to ensure that workers have the skills to run and maintain AI systems and offer incentives for AI-driven innovation, especially in areas with a lot of growth. Also, retail and farming are among the industries taking AI more slowly. These industries would benefit from subsidies, tax breaks, and training programs to make it easier for people to use AI and to help the economy recover more evenly across all areas. As the simulation results show, it is essential to keep buying AI-based security tools. It should be a top priority for policymakers to make cybersecurity systems that are flexible and can adapt to new threats. Encourage government agencies, private companies, and international partners to share cyber threat information and work together to find the best AI defences against them. Strict rules need to be in place in Ukraine to ensure that AI is used safely in critical systems like energy grids, transportation networks, and financial systems.

The government should give money to research and development in artificial intelligence (AI) so that any problems with AI systems can be found and fixed. As part of this, rules and guidelines must be made to keep attacks away from models, especially those used in essential areas. These problems can be fixed by getting the government and businesses to work together on new cybersecurity ideas. It will also help ensure that the AI tools Ukraine uses can handle cyber threats now and in the future. Ultimately, our ABM simulations showed that AI technologies could help Ukraine's economy get back on its feet faster after the war and improve its cybersecurity. They also show how complex and dangerous AI can be. Some examples are how important it is to keep security tools up to date and how the government can help places that aren't using AI enough. Tomorrow, Ukraine needs to make plans to protect critical infrastructure, encourage the use of AI, and make the country less open to new cyber threats. An intelligent use of AI could help Ukraine grow and stay stable over the long term.

### CONCLUSIONS

Using AI to aid Ukraine's war recovery presents exciting opportunities and formidable challenges. Our Agent-Based Modelling (ABM) models demonstrate that AI has the potential to significantly contribute to the acceleration of economic recovery, particularly in sectors with significant societal impact, such as banking and manufacturing, where the advantages of automation and enhanced security are readily apparent. Adopting AI in these areas can have positive effects that spread to nearby industries, leading to a stronger and more connected economic recovery. However, our results also show how important it is for the government to step in and help sectors adopt AI technologies more slowly, like agriculture and retail, where the costs and benefits are less favourable.

Regarding cybersecurity, AI tools make defences much stronger against new cyber threats. However, they also create new weaknesses, like the ability to attack machine learning models as an adversary. Based on our simulations, the ongoing arms race between attackers and defenders means that AI-driven security systems must be updated and made better constantly. Without this, defenders could fall behind attackers who are getting smarter all the time. The effects on Ukraine's essential infrastructure are horrible, and it is especially vulnerable after a war. Long-term national security will depend on ensuring that AI is used in these systems in a safe and reliable way.

In the coming years, research should concentrate on several crucial areas. First, studies that use real-world data from Ukraine's efforts to rebuild after the war would give us more accurate information about how often AI is used, how much it costs, and the problems in different industries. Second, learning more about AI's part in cybersecurity, especially regarding adversarial machine learning, would help us understand and fix the issues that AI systems cause. Lastly, economics, computer science, and public policy researchers must work together to create complete plans for incorporating AI into places that have been through a war. This will make sure that the use of technology promotes long-term growth while minimising risks. This all-around approach is essential for Ukraine's recovery and other countries with similar problems rebuilding after a war.

### BIBLIOGRAPHIC REFERENCES

1. Kimhi S, Kaim A, Bankauskaite D, Baran M, Baran T, Eshel Y, et al. A full-scale Russian invasion of Ukraine in 2022: Resilience and coping within and beyond Ukraine. *Applied Psych Health & Well*. 2024 Aug;16(3):1005-23. doi: 10.1111/aphw.12466
2. Ellison J, Cox M, Hanhimäki JM, Harrison HM, Ludlow NP, Romano A, et al. The war in Ukraine. *Cold War History*. 2023 Jan 2;23(1):121-206. doi: 10.1080/14682745.2023.2162329
3. Mocnik N. Empowering new survivors with old lessons? Insights from the Bosnian war aftermath applied to upcoming Ukrainian post-realities. *Canadian Slavonic Papers*. 2024 Apr 2;66(1-2):107-29. doi: 10.1080/00085006.2024.2363164

4. Lucarelli S, Marrone A, Moro FN. NATO decision-making in the age of big data and artificial intelligence. Brussels: NATO; 2021. 100 p.
5. Dwivedi YK, Hughes L, Ismagilova E, Aarts G, Coombs C, Crick T, et al. Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*. 2021 Apr;57:101994. doi: 10.1016/j.ijinfomgt.2019.08.002
6. Iturriza M, Labaka L, Sarriegi JM, Hernantes J. Modelling methodologies for analysing critical infrastructures. *Journal of Simulation*. 2018 Apr 3;12(2):128-43. doi: 10.1080/17477778.2017.1418640
7. Makridakis S. The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. *Futures*. 2017 Jun;90:46-60. doi: 10.1016/j.futures.2017.03.006
8. Subeesh A, Mehta CR. Automation and digitization of agriculture using artificial intelligence and internet of things. *Artificial Intelligence in Agriculture*. 2021;5:278-91. doi: 10.1016/j.aiia.2021.11.004
9. Yang K. *Quality in the Era of Industry 4.0: Integrating Tradition and Innovation in the Age of Data and AI* [Internet]. 1st ed. Wiley; 2024 [cited 2024 Nov 28]. Available from: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781119932475>
10. Abid SK, Sulaiman N, Chan SW, Nazir U, Abid M, Han H, et al. Toward an Integrated Disaster Management Approach: How Artificial Intelligence Can Boost Disaster Management. *Sustainability*. 2021 Nov 13;13(22):12560. doi: 10.3390/su132212560
11. Cheek W, Chmutina K. 'Building back better' is neoliberal post-disaster reconstruction. *Disasters*. 2022 Jul;46(3):589-609. doi: 10.1111/disa.12502
12. Wan J, Li X, Dai HN, Kusiak A, Martinez-Garcia M, Li D. Artificial-Intelligence-Driven Customized Manufacturing Factory: Key Technologies, Applications, and Challenges. *Proc IEEE*. 2021 Apr;109(4):377-98. doi: 10.1109/JPROC.2020.3034808
13. Nikolenko K. Artificial Intelligence and Society: Pros and Cons of the Present, Future Prospects. *Futurity Philosophy*. 2022 Jun 30;1(2):54-67. doi: 10.57125/FP.2022.06.30.05
14. Paweloszek I, Kumar N, Solanki U. Artificial intelligence, digital technologies and the future of law. *Futurity Economics & Law*. 2022 Jun 25;2(2):22-32. doi: 10.57125/FEL.2022.06.25.03
15. Layton P. *Fighting Artificial Intelligence Battles* [Internet]. Department of Defence; 2021 [cited 2024 Nov 28]. (Joint Studies Paper Series). Available from: [https://defence.gov.au/adc/Publications/Joint\\_Studies/JSPS\\_4\\_Fighting\\_AI\\_Battles.pdf](https://defence.gov.au/adc/Publications/Joint_Studies/JSPS_4_Fighting_AI_Battles.pdf)
16. Sarkin JJ, Sotoudehfar S. Artificial intelligence and arms races in the Middle East: the evolution of technology and its implications for regional and international security. *Defense & Security Analysis*. 2024 Jan 2;40(1):97-119. doi: 10.1080/14751798.2024.2302699
17. Petchenko M, Fomina T, Balazyuk O, Smirnova N, Lugova O. Analysis of Digitalization and Digitalization Trends in Accounting (Ukrainian Case). *FCAPTP*. 2023 Feb 28;1(48):105-13.
18. Zaiachkovska H, Tserklevych V, Vovk S. The Influence of the Global Perfumery Market on the Principles of the Formation of a Tourist Flow. *EEA* [Internet]. 2021 May 31 [cited 2024 Nov 28];39(5). Available from: <http://ojs.ual.es/ojs/index.php/eea/article/view/5232>
19. Usigbe MJ, Asem-Hiablie S, Uyeh DD, Iyiola O, Park T, Mallipeddi R. Enhancing resilience in agricultural production systems with AI-based technologies. *Environ Dev Sustain*. 2023 Aug 11;26(9):21955-83. doi: 10.1007/s10668-023-03588-0
20. Karumban S, Sanyal S, Laddunuri MM, Dhanasingh Sivalinga V, Shanmugam V, Bose V, et al. Industrial Automation and Its Impact on Manufacturing Industries: In: Mishra DU, Sharma S, editors. *Advances in*

Computational Intelligence and Robotics [Internet]. IGI Global; 2022 [cited 2024 Nov 28]. p. 24-40. Available from: <https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-6684-4991-2.ch002>

21. Shah SS, Asghar Z. Dynamics of social influence on consumption choices: A social network representation. *Heliyon*. 2023 Jun;9(6):e17146. doi: 10.1016/j.heliyon.2023.e17146

22. Ashta A, Herrmann H. Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. *Strategic Change*. 2021 May;30(3):211-22. doi: 10.1002/jsc.2404

23. Kolinets L. International Financial Markets of the Future: Technological Innovations and Their Impact on the Global Financial System. *Futurity of Social Sciences*. 2023 Sep 20;1(3)4-19. doi: 10.57125/FS.2023.09.20.01

24. Sofilkanych N, Vesova O, Kaminskyy V, Kryvosheieva A. The impact of artificial intelligence on Ukrainian medicine: benefits and challenges for the future. *FEM*. 2023 Dec 30;2(4)28-39. doi: 10.57125/FEM.2023.12.30.04

25. Czerwonko A, White J. World Economic Forum [Internet]. Life after the hype: How AI is transforming industries and economies; 2023 Dec 1 [cited 2024 Nov 28]. Available from: <https://www.weforum.org/stories/2023/12/life-after-the-hype-how-ai-is-transforming-industries-and-economies/>

26. Mhlanga D. Artificial Intelligence in the Industry 4.0, and Its Impact on Poverty, Innovation, Infrastructure Development, and the Sustainable Development Goals: Lessons from Emerging Economies? *Sustainability*. 2021 May 21;13(11):5788. doi: 10.3390/su13115788

27. Calçada DB, Rezende SO, Dwarkasing A. Development of New Skills: Innovation and Sustainability in Industry 4.0. In: Leal Filho W, Azul AM, Brandli L, Lange Salvia A, Wall T, editors. *Industry, Innovation and Infrastructure* [Internet]. Cham: Springer International Publishing; 2021 [cited 2024 Nov 28]. p. 212-21. (Encyclopedia of the UN Sustainable Development Goals). Available from: [https://link.springer.com/10.1007/978-3-319-95873-6\\_47](https://link.springer.com/10.1007/978-3-319-95873-6_47)

28. Mazur N, Tkachuk V, Sulima N, Semenets I, Nikolashyn A, Zahorodnia A. Foreign Agricultural Markets: State and Challenges in Sustainable Development. In: Alareeni B, Hamdan A, editors. *Innovation of Businesses, and Digitalization during Covid-19 Pandemic* [Internet]. Cham: Springer International Publishing; 2023 [cited 2024 Nov 28]. p. 545-59. (Lecture Notes in Networks and Systems; vol. 488). Available from: [https://link.springer.com/10.1007/978-3-031-08090-6\\_35](https://link.springer.com/10.1007/978-3-031-08090-6_35)

29. Dykha M, Mohylova A, Ustik T, Bliumska-Danko K, Morokhova V, Tchon L. Marketing of Start-ups and Innovations in Agricultural Entrepreneurship. *JAC*. 2021 Dec 19;(81):27-34. doi: 10.32861/jac.81.27.34

30. Prokopenko O, Sapinski A. Using Virtual Reality in Education: Ethical and Social Dimensions. *ELIJ*. 2024 Mar 25;2(1):41-62.

31. Dorogy Y, Tsurkan V, Mokhor V, Doroha-Ivaniuk O. Critical IT Infrastructure Resource Distribution Algorithm. In: 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) [Internet]. Cracow, Poland: IEEE; 2021 [cited 2024 Nov 28]. p. 632-9. Available from: <https://ieeexplore.ieee.org/document/9660948/>

32. Kashchena N, Solokha D, Trushkina N, Potemkin L, Mirkurbanova R. Use of multi agent simulation modeling for predicting the sales of wholesale trade companies. *Journal of Management Information and Decision Sciences*. 2019;22(4):483-488.

33. Sopronenkov I. Tax Policy: Impact on Business Development and Economic Dynamics of the Country. *EA* [Internet]. 2023 Dec 25 [cited 2024 Nov 28];68(4). Available from: <http://ndpublisher.in/admin/issues/EA68n5n.pdf>

34. Nespoli P, Díaz-López D, Gómez Mármol F. Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices. *Journal of Information Security and Applications*. 2021 Aug;60:102878. doi: 10.1016/j.jisa.2021.102878

35. Popova N, Kataiev A, Skrynkovskyy R, Nevertii A. Development of trust marketing in the digital society. *EA-XXI*. 2019 Aug 20;176(3-4):13-25. doi: 10.21003/ea.V176-02

36. Shah SS, Shah SAH. Trust as a determinant of social welfare in the digital economy. *Soc Netw Anal Min.* 2024 Apr 5;14(1):79. doi: 10.1007/s13278-024-01238-5
37. Macas M, Wu C, Fuertes W. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks.* 2022 Jul;212:109032. doi: 10.1016/j.comnet.2022.109032
38. Khalaf BA, Mostafa SA, Mustapha A, Mohammed MA, Abdulllah WM. Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods. *IEEE Access.* 2019;7:51691-713. doi: 10.1109/ACCESS.2019.2908998
39. Brundage M, Avin S, Clark J, Toner H, Eckersley P, Garfinkel B, et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation [Internet]. *arXiv*; 2018 [cited 2024 Nov 28]. Available from: <https://arxiv.org/abs/1802.07228>
40. Mishra S. Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Applied Sciences.* 2023 May 10;13(10):5875. doi: 10.3390/app13105875
41. Grinko A, Havrylenko N, Kostash T, Plekan M, Breus S. (2020). Organization of a strategic management accounting in an innovative economy. *Academy of Accounting and Financial Studies Journal.* 2020;24(5):1-7.
42. Burton J, Christou G. Bridging the gap between cyberwar and cyberpeace. *International Affairs.* 2021 Nov 1;97(6):1727-47. doi: 10.1093/ia/iiab172
43. Shandler R, Gross ML, Canetti D. Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis. *Journal of Global Security Studies.* 2022 Dec 19;8(1):ogac042. doi: 10.1093/jogss/ogac042
44. Adi E, Baig Z, Zeadally S. Artificial Intelligence for Cybersecurity: Offensive Tactics, Mitigation Techniques and Future Directions. *Applied Cybersecurity & Internet Governance.* 2022 Nov 4;1(1):1-23. doi: 10.5604/01.3001.0016.0800
45. Chakraborty A, Biswas A, Khan AK. Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. In: Biswas A, Semwal VB, Singh D, editors. *Artificial Intelligence for Societal Issues* [Internet]. Cham: Springer International Publishing; 2023 [cited 2024 Nov 28]. p. 3-25. (Intelligent Systems Reference Library; vol. 231). Available from: [https://link.springer.com/10.1007/978-3-031-12419-8\\_1](https://link.springer.com/10.1007/978-3-031-12419-8_1)
46. Castiglione F. Agent-Based Modeling and Simulation, Introduction to. In: Sotomayor M, Pérez-Castrillo D, Castiglione F, editors. *Complex Social and Behavioral Systems* [Internet]. New York, NY: Springer US; 2020 [cited 2024 Nov 28]. p. 661-5. Available from: [http://link.springer.com/10.1007/978-1-0716-0368-0\\_13](http://link.springer.com/10.1007/978-1-0716-0368-0_13)
47. Maddah N, Heydari B. Building back better: Modeling decentralized recovery in sociotechnical systems using strategic network dynamics. *Reliability Engineering & System Safety.* 2024 Jun;246:110085. doi: 10.1016/j.res.2024.110085
48. Sieriebriak S, Kozhushko O. The Role of Artificial Intelligence in the Legal, Business and Economic Spheres to Achieve Sustainable Development. *Law, Business and Sustainability Herald.* 2023;3(3):4-16.
49. Ashima R, Haleem A, Bahl S, Javaid M, Kumar Mahla S, Singh S. Automation and manufacturing of smart materials in additive manufacturing technologies using Internet of Things towards the adoption of industry 4.0. *Materials Today: Proceedings.* 2021;45:5081-8. doi: 10.1016/j.matpr.2021.01.583
50. AL-Dosari K, Fetais N, Kucukvar M. Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges. *Cybernetics and Systems.* 2024 Feb 17;55(2):302-30. doi: 10.1080/01969722.2022.2112539
51. Sharma M, Luthra S, Joshi S, Kumar A. Implementing challenges of artificial intelligence: Evidence from public manufacturing sector of an emerging economy. *Government Information Quarterly.* 2022 Oct;39(4):101624. doi: 10.1016/j.giq.2021.101624

52. Sheffi Y. Technology is not enough: Potential job displacement in an AI-driven future. *Journal of Supply Chain Management, Logistics and Procurement*. 2024;6(4):338-351.

53. Ansari MF, Dash B, Sharma P, Yathiraju N. The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of Advanced Research in Computer and Communication Engineering*. 2022;11(9):81-90.

54. Yuzevych L, Skrynkovskyy R, Koman B. Development of information support of quality management of underground pipelines. *EUREKA: Physics and Engineering*. 2017 Jul 31;4:49-60. doi: 10.21303/2461-4262.2017.00392

#### **FINANCING**

The authors did not receive financing for the development of this research.

#### **CONFLICT OF INTEREST**

The authors declare that there is no conflict of interest.

#### **AUTHORSHIP CONTRIBUTION**

*Data curation:* Olha Vdovichena, Anna Krymska, Yurii Koroliuk, Alla Shymko, Anatolii Vdovichen.

*Methodology:* Olha Vdovichena, Anna Krymska, Yurii Koroliuk, Alla Shymko, Anatolii Vdovichen.

*Software:* Olha Vdovichena, Anna Krymska, Yurii Koroliuk, Alla Shymko, Anatolii Vdovichen.

*Drafting - original draft:* Olha Vdovichena, Anna Krymska, Yurii Koroliuk, Alla Shymko, Anatolii Vdovichen.

*Writing - proofreading and editing:* Olha Vdovichena, Anna Krymska, Yurii Koroliuk, Alla Shymko, Anatolii Vdovichen.