DOI: 10.55643/fcaptp.6.53.2023.4130

CYBER SECURITY AND ARTIFICIAL INTELLIGENCE IN THE CONTEXT OF ENSURING BUSINESS SECURITY IN WARTIME

Oleh Havryliuk
D.Sc. in Economics, Professor of the Department of Management and Innovative Providing, European University, Kyiv, Ukraine;
ORCID: 0000-0001-6819-9296

Oleksandr Yakushev
Candidate of Economy Sciences, Associate Professor of the Department of Social Welfare, Cherkasy State Technological University, Cherkasy, Ukraine;
e-mail: aleksandro@i.ua
ORCID: 0000-0002-0699-1795
(Corresponding author)

Maryna Petchenko
Candidate of Economy Sciences, Acting Vice-Rector, Humanitarian Policy and Innovation at National Aviation University, Kyiv, Ukraine;
ORCID: 0000-0003-1104-5717

Nataliia Zachosova
D.Sc. in Economics, Professor of the Department of Management and Public Service, Bohdan Khmelnytskyi National University of Cherkasy, Cherkasy, Ukraine;
ORCID: 0000-0001-8469-3681

Taliat Bielialov
D.Sc. in Economics, Professor, Head of the Department of Entrepreneurship and Business, Kyiv National University of Technologies and Design, Kyiv, Ukraine
ORCID: 0000-0003-4019-755X

Svitlana Kozlovska
Candidate of Technical Sciences, Associate Professor, Head of the Department of Management and Administration, Rauf Ablyazov East European University, Cherkasy, Ukraine;
ORCID: 0009-0001-4731-9794

Received: 31/07/2023
Accepted: 19/12/2023
Published: 31/12/2023

ABSTRACT

Ensuring security for business becomes especially relevant in the context of geopolitical conflicts, increasing digitization and introducing new technologies into the financial and production sectors, booming frequency and complexity of cyber-attacks aimed at the business sphere, as well as with more diverse applications of artificial intelligence. The article studies the specifics of ensuring business security in Ukraine during wartime using artificial intelligence and cyber protection. A retrospective review of the literature has been conducted revealing that there is no research on the ways artificial intelligence is applied to ensure business activity security, which indicates the research novelty of this article. The authors outline the potential and threats of artificial intelligence for business security. Directions for securing entrepreneurship in war conditions with the help of artificial intelligence and elimination/minimization of cyber threats are formulated. The regulatory and legislative framework governing the regulation of cyber security in Ukraine is outlined and directions for its improvement are suggested.

Keywords: cyber security, artificial intelligence, digitalization, war, entrepreneurship

JEL Classification: M21, H56, O32, D21, D81

INTRODUCTION

Entrepreneurship is a vital component of economic activities in any country. Its stability and safety ensure the success of socio-economic, technological, innovative, and informational social development. Wartime has brought about specific conditions under which entrepreneurial activities are being implemented. Therefore, the functioning of the Ukrainian economy in this special wartime period requires additional insight into the processes that determine both the future economic recovery and the threat to the latter. The population lives in a turbulent environment, accompanied by a declining birth rate, an ageing nation, a brain drains, an overall decline of the economy, and a limited number of jobs. In particular, because of the loss of markets, suppliers and physical assets, a decrease in employment opportunities, unstable producers' motivation and consumers' behaviour, rising prices for many types of raw materials, energy resources, semi-finished products, and transport services, disruption of supply chains, the companies seek to identify sources of potential savings and have to rank development priorities wisely (including digitization). During a war, it is important for businesses to discover new resources to support their activities, learn new ways of conducting marketing and increasing sales. At the same time, some entrepreneurs continue to realize their potential, sometimes even increasing it, in particular, by relocating their staff and production facilities to safer regions (launching new opportunities), compensating for the high cost of materials, building safe logistics, etc. While warfare is continuing, it is important for businesses to search for diverse resources to support their activities, master new marketing methods and enhance sales. The issue of cyber security is becoming critical since the digital component of hybrid warfare actively affects business operations.

Government institutions, banks and financial organizations, online stores, IT companies, businesses that operate the customers' personal data, small manufacturing companies and startups suffer the most from cyber-attacks. Therefore, the rapid growth of digitalization in the world and the Ukrainian economy has a reverse side, since it leads to an

increase in cyber threats, cyber-attacks, and other cyber security violations, and threatens safe work with data in cyber-space, thus directly affecting the results of business activities. These negative consequences affect the population, business and the state as a whole. Artificial Intelligence (AI), when used maliciously, can further aggravate the situation.

LITERATURE REVIEW

Much of the current literature pays particular attention to business activities during the war and in the post-war period. In particular, a special issue of the Journal of Conflict Resolution (2013) is devoted to the impact of violent conflicts on entrepreneurship in developing countries and contains a study published by researchers from the USA and the Kingdom of the Netherlands "A Model of Destructive Entrepreneurship: Insight for Conflict and Postconflict Recovery" [1], which describes institutional aspects of ensuring the security for entrepreneurship in war or post-war economies, and the article titled "Business under Fire: Entrepreneurship and Violent Conflict in Developing Countries" [2] by German economists who specialize in issues of economic development in the conditions of conflicts and terrorism. "Entrepreneurship in Conflict Zones" [3], a monograph by A. Bayram (Syria, 2017) tackles the problem of building a post-conflict entrepreneurship ecosystem, creating startups, and responding to unforeseen sanctions and payment restrictions. J. Jay and H. van Buren in "Entrepreneurship, Conflict, and Peace: The Role of Inclusion and Value Creation" [4] have analyzed tools for creating and destructing values in a conflict environment, considered inclusive methods of conducting business and outlined opportunities for entrepreneurs to manage a wide variety of risks and to achieve positive business results. A retrospective analysis was undertaken by E. Lakomaa, a Swedish researcher and political consultant, in 2017. In "The History of Business and War: introduction" [5], the author analyses the experience of several countries and defines various aspects of transferring the industry to military lines, the relations of private firms with government structures, tax policy implementation during martial law, the impact of war on trade and profitability of companies and, importantly, the involvement of companies in information activities.

Although in-depth research has been carried out on businesses in wartime, no studies have been found that describe the realia that emerged and became especially relevant in the 2020s, namely, cyber threats and artificial intelligence. Even the literature dated after 2020, when cyber threats dominated other global risks for entrepreneurship, paid far too little attention to this issue. For example, the phenomena of cyber security or artificial intelligence have not been mentioned in G. Mutonyi (Kenya, 2021) "Warpreneurship: War as A Business" [6], or in the 2021 report titled "Business in Conflict-Affected and High-Risk Contexts" by the BSR consultant company (USA) [7]. However, a 2020 article "Safety Measures in Entrepreneurs" by Indian researchers only briefly mentions artificial intelligence [8, p. 70].

Nonetheless, cyber incidents, such as IT failures, ransomware attacks or data breaches, have been ranked among the most important risks worldwide for two recent years in a row. A 2021 study by McKinsey & Company, an international consulting company, revealed the areas of security against cyber threats, software problems, and cloud computing and proved that small and medium-sized enterprises were especially vulnerable to cyber-attacks, being less protected against them in comparison with large enterprises, therefore, small and medium-sized enterprises should be protected better [9, p. 2]. In addition, small and medium businesses are an attractive segment for technology providers and security solutions [9, p. 4].

Summarizing the review of the literature, we have concluded that there is a general lack of research on the problem of artificial intelligence in ensuring business security. Therefore, this research seeks to remedy these problems by analyzing the specifics of the business and its functioning in Ukraine during the war regarding the use of artificial intelligence and protection against cyber threats.

AIMS AND OBJECTIVES

Military conflicts transform the existing approaches to ensuring security for business activities. The war with russia requires considering new realities, such as the digitalization of the economy, overcoming cyber threats, and applying new innovative technologies and artificial intelligence. Serious business disruptions can occur due to a wide range of cyber-related triggers, including artificial intelligence, malicious attacks by criminals or hackers, information leakage, human factors, or equipment failure. The inadequate regulatory and legislative framework in the field of cyber security also makes entrepreneurs vulnerable and their businesses potentially destructible.

Based on the above, the objectives of this article include solving the following tasks.

1. First, the specific wartime conditions for business will be studied.

DOI: 10.55643/fcaptp.6.53.2023.4130

2. Secondly, the possibilities of ensuring the security for business activities with innovative technologies will be analyzed.
3. Another task will be to formulate recommendations on avoiding or minimizing the negative consequences of cyber threats and optimizing applications of artificial intelligence in ensuring the safety of enterprises in war conditions.
4. Finally, we will substantiate our proposals for improving the regulatory and legislative framework that underlies cyber security and stipulates the functioning of artificial intelligence in Ukraine.

METHODS

Both qualitative and quantitative methods were used in this investigation. Retrospective and comparative research methods were applied to analyze the literature. Analysis and synthesis, methods of systematization, classification and comparative analysis were deployed to explore the new conditions for entrepreneurship in wartime. To formulate recommendations on eliminating the negative consequences of cyber threats and on the use of artificial intelligence and improving the regulatory and legislative framework of Ukraine, we employed methods of system analysis and empirical and expert assessments.

RESULTS

The war in Ukraine generated great uncertainty in the functioning of many enterprises, which made it extremely difficult for the latter to assess the consequences. In the first month of the war, more than 80% of enterprises [10] reduced or suspended their activities or even shut down. Those who continued or resumed their activities later faced unprecedented challenges: in order to survive, many enterprises were forced to completely change their business model, hunt for new personnel and suppliers, and re-format the logistics. On top of the regular expenses, the necessity to contribute to the victory by making charitable contributions and volunteering was added.

The data gathered by KPMG international consulting company demonstrate that 41% of enterprises are not still able to assess the impact of the war on their business, 46% expect a drop in sales, 47% anticipate a reduction in income, 80% believe that the war will negatively affect the further development of the company, 40% fear that the negative consequences will last for more than three years [11]. If a business relies on one product only, there is a high probability that the company may go out of business due to loss of interest in the product, governmental or legislative changes, or loss of the market due to competition. In wartime, physical destruction of assets and disruption of business activities due to cyber-attacks (including those generated by artificial intelligence) supplement the list of negative factors. All the above may serve as an incentive to reassess risk management strategies, methods, and processes in order to function as efficiently as possible in unstable and uncertain conditions.

The warfare has several dimensions – besides the physical front, it continues in the information and innovation field as well. Allianz SE (Germany), one of the largest and most influential insurance companies in the world has ranked cyber risks as the number one risk among the global risks of the year 2023. This has happened for two years in a row – last year, similarly, cyber risks were ranked as the most serious threat. Among the reasons there are large-scale cyber-attacks in combination with problems caused by accelerating digitalization and the transition of many enterprises, personnel, and population to remote work [12]. Another global consulting firm, Control Risks, which specializes in identifying risks for politics and business, ranked cyber risks as number two among other threats to entrepreneurship [13]. The report of the World Economic Forum on Global Risks 2023 has emphasized that cyber security issues are a constant concern [14]. The most common types of cyber threats include DDoS and DoS attacks; phishing mailings with virus files or links; hacking accounts to gain access to personal and corporate data; malware that hides files and blocks access to them; ransomware viruses; unauthorized access to Internet banking; leakage of confidential information and personal data, etc. All these threats, when realized, inflict crushing blows on any business, population, and country. The negative consequences of cyber-attacks include failure of critical business systems (websites, electronic services, online stores, accounts of key managers, etc.); loss of personal, corporate, and confidential information; damage to the company's business reputation and loss of customers; significant financial costs to overcome consequences of cyber incidents, etc. Therefore, monitoring cyber risks guarantees operational stability for any enterprise.

Modern cyber threats have reached far beyond hacker attacks and data leaks. Hackers often attempt to construct digital and physical chains that provide the ability to simultaneously attack multiple targets. The ever-growing cybercriminals' capabilities force companies to pay close attention to the risks to which their critical infrastructure objects, such as smart technologies, water and electricity supply systems, and supply networks, may be exposed. Potential cyberattacks are of

particular concern to enterprises in the trade and communication technology sectors, as well as small and medium-sized businesses.

Since the beginning of russian aggression, Ukraine has become the target of numerous cyberattacks aimed at state institutions of critical infrastructure, private businesses, and the population. Not long before the invasion and immediately after it, the number and power of cyberattacks against Ukrainian state structures and businesses multiplied several times: massive attacks were confirmed on January 13-14, February 15-16, and on the night of February 23-24, 2022. According to the Ukrainian State Special Communications Service, in the period between mid-February and the beginning of March, Ukrainian organizations suffered about 2,800 cyberattacks (for the whole of 2021, there were 2,200 of them) [15].

It is possible to counter cyberattacks by strengthening cyber security and using artificial intelligence. Artificial intelligence cannot be considered as a panacea solution to all business security problems. Firstly, AI can be used with hostile intentions. Secondly, the possibility of its transition into an uncontrolled state cannot be disregarded. Concerns about the latter were expressed by Elon Musk and many respected businessmen on March 29, 2023. They called for a temporary halt in its development [2]. On March 28, 2023, Europol warned about the danger of ChatGPT being deployed for phishing, disinformation, and cybercrime attempts [16].

AI can process large amounts of data and identify trends and patterns that can indicate future trends in the economic and political situation. Access to publicly available and specific data allows AI to obtain critical information for business structures, as well as to apply innovative technologies and tools in the restoration of the affected cities. Artificial intelligence technologies can increase global GDP by 7% and automate almost 2/3 of jobs in the US and Eurozone countries. At the same time, AI can cause large-scale upheavals [17].

The volume of the global artificial intelligence market in 2021 was estimated at 95.6 billion dollars and is projected to reach 1.8 trillion dollars in 2030 with an average annual growth rate of 32.9% from 2022 to 2030 [18] (Figure 1). Based on these data, it is considered possible to reflect the inevitable trend of increasing the use of artificial intelligence and observe the forecasted growth exceedingly more than 18.5 times over the decade.

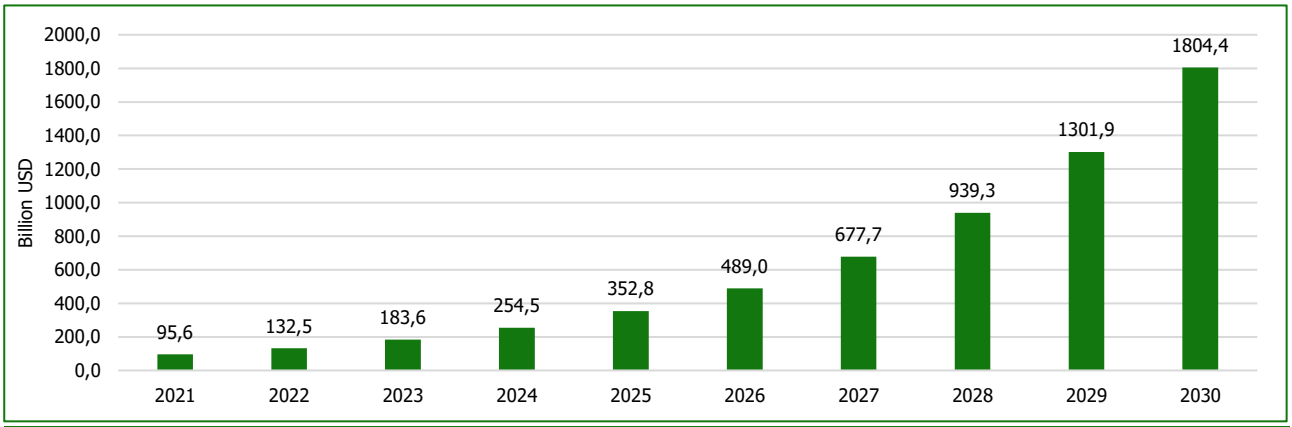

Figure 1. The volume of the world market of artificial intelligence in 2021-2030. *(Source: [19])*

In 2021, 31% of businesses worldwide utilized artificial intelligence, and in 2022, this number increased by 4%. Among them, 42% noted that they are considering incorporating it into their business processes [19].

AI is learning from the russian war in Ukraine. For instance, March 2022 saw the launch of the face recognition system designed by the American company ClearView AI in Ukraine. The system has access to 10 billion photos on social networks and thus can identify the dead russians' faces and notify their families. Currently, the possibility of implementing ClearView AI in courts, healthcare facilities and customs is being studied [20].

Therefore, we can formulate six directions in securing entrepreneurship with the help of AI in war conditions.

1. Development of a monitoring system to monitor changes in the political and economic situation and warn entrepreneurs about hypothetical risks and threats, thus contributing to more informed decisions about investment and development strategies.

2. Forecasting future market trends and preparing preliminary responses to them. The analysis of economic dynamics, data on production, consumption, export, and import will identify risks and anticipate changes in the economy. For example, AI can identify goods that are strategically important and assess the risks for their production or supply.

DOI: 10.55643/fcaptp.6.53.2023.4130

3. Optimizing business processes using robotic systems will reduce the number of errors occurring in decision-making.
4. Data protection and cyber security systems will prevent the leakage of confidential information, detect cyber-attacks or the personnel's unusual activity aimed at leaking confidential information, security breaches and blocking or restricting access to confidential information with facial recognition algorithms or other technologies for identifying authorized users.
5. Cooperation with federal and regional authorities will provide information on changes in the political and economic situation, monitor changes in government policy, evaluate new regulatory norms and laws to warn about possible risks and promptly adopt informed decisions, as well as receive protection from federal and regional authorities, including bringing violators to justice and applying to a court for damages. In turn, in the event of potential cyber incidents, the relevant state structures must be immediately informed. Transferring all possible data to a cloud service and storing several backup copies in different regions or even countries is especially relevant for Ukrainian companies in wartime conditions.
6. Development of anti-crisis plans/strategies based on the business preservation algorithm in case of threats or catastrophic events.

The development of modern entrepreneurship is increasingly determined by the growing role of artificial intelligence, blockchain technology and the Internet of Things. The latest technologies reduce costs and enhance the efficiency of operations and the safety of business operations. Their application is expected to become wider so as to provide personalized service and optimize sales and logistics management processes. Global job markets are gearing up for a new era of turbulence since technologies like artificial intelligence increase demand for ICT and cybersecurity professionals. This fact was emphasized in the report of the World Economic Forum published on May 1, 2023 [21, pp. 5-6]. The impact of artificial intelligence is yet to be explored since AI may be both beneficial and pose threats to business. The practice has already confirmed that improving AI versions does not necessarily imply enhanced security for both businesses and ordinary citizens. Thus, the release of GPT-4 (March 2023) aimed not only at optimizing the functionality of ChatGPT but also at reducing the likelihood of producing potentially malicious results. However, the reality proved the opposite. At the seminars organized by the European Police Directorate (Europol – the law enforcement body of the European Union), when experimenting with various cases when GPT-3.5 could be used for criminal purposes, it appeared that GPT-4 performed the same malicious functions. Moreover, these functions became even more advanced in some cases.

In response to a wide range of prompts, ChatGPT provides users with ready-to-use professional information. Even in the absence of basic information about a specific field of crime from a potential criminal, artificial intelligence is able to suggest a vast range of potential areas of illegal activity, from breaking into a building to terrorism, cybercrime and sexual violence [22], which proves how diverse and potentially dangerous AI can become in the hands of criminals. The Europol report "The Impact of Large Language Models on Law Enforcement" (March 27, 2023) contains a warning that the rapid development of generative AI can actually contribute to the activities of online fraudsters and cybercriminals [23, p.2].

Implementation and development of digital technologies in business organizations, regardless of their forms of ownership and subordination, is usually accompanied by an increase/diversification of threats and real consequences of cyber attacks. In times of war, every enterprise must operate on high alert and continually assess the vulnerability of its critical services to cyber incidents and technological failures in order to prevent negative consequences from malicious attacks. Minimizing the negative consequences of the latter will contribute to the strengthening of cyber security. The agenda also includes improving the regulatory and legislative provision of cyber security for businesses. The latter requires legal support, while the regulation of cyber security in Ukraine is still inconsistent. The rules that regulate it are scattered across many laws and by-laws; thus, in the event of a cyber incident, it is extremely difficult for a business owner to independently collect the necessary information.

Cyber security is defined by the Law of Ukraine "About the Basic Principles of Ensuring Cyber Security in Ukraine" [24] and the International Convention on Cybercrime [25]. Cyber security is also regulated by other laws: "On Personal Data Protection" [26], "About Public Electronic Registers" [27], "About Critical Infrastructure" [28], "On the National Security of Ukraine" [29], "About Electronic Communications" [30], Decree of the President of Ukraine No. 447/2021 "About the decision of the National Security and Defense Council of Ukraine" dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine" [31], Decree of the Cabinet of Ministers of Ukraine "Concept for Development of Artificial Intelligence by 2030" [32] etc. This list is not exhaustive – liability for cyber security violations is regulated by relevant codes and laws that certain government bodies apply to ensure and control cyber security and prosecute its violators [33;34]. There are several responsible governmental bodies: the Security Service of Ukraine, the Cyber Police Department of the National

Police of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Ministry of Defense, the National Security and Defense Council, the National Bank of Ukraine, and others.

The Law "About the Basic Principles of Ensuring Cybersecurity of Ukraine" [24] introduced important basic concepts in the field of cyber protection and cyber security and defined the rights and obligations of state bodies regarding cyber security, although it duplicated the provisions of the Cyber Security Strategy of Ukraine. We have observed a similar problem with other regulatory acts. In order to improve the Ukrainian legislation and more efficiently regulate cyber security and the use of artificial intelligence in ensuring business security, we consider it appropriate to take into account the following aspects.

1. Creating a comprehensive legislative framework covering cyber security, personal data protection and the use of artificial intelligence. This will eliminate fragmentation and contradictions in Ukrainian legislation and create a single legal basis for regulating these issues.
2. Ensuring reliable regulation of collecting, processing, and transferring personal data, in particular when employing AI, imposing obligations on the subjects to inform individuals about collecting and disposing of their data, as well as mechanisms for controlling their disposal.
3. Establishing a framework for the use of artificial intelligence in various areas, including public safety, transport, health care, law enforcement, etc., providing requirements for the use of particular algorithms, ethical principles, responsibility for artificial intelligence and user rights.
4. Continuous updates to legislation, hence cyber security and artificial intelligence are dynamically changing fields.
5. Development of a training program and raising awareness of cyber security and the use of artificial intelligence for entrepreneurs and staff, providing state support for initiatives that contribute to the development of a qualified workforce able to tackle these issues.
6. Developing standards and regulations regarding cyber security and the use of artificial intelligence for enterprises. This may include data protection requirements, cyber security of networks and systems, audit requirements and security certification.
7. Encouraging enterprises to cooperate and exchange information on cyber security and artificial intelligence by creating specialized platforms, forums or associations that will ensure the exchange of experience, best practices, and information about threats.
8. Legislative provision of liability for cyber security violations and non-compliance with requirements regarding the use of artificial intelligence (fines, sanctions or other measures that encourage enterprises to comply with security and data protection requirements).
9. Creating favourable conditions for research and innovation in the field of cyber security and artificial intelligence, in particular, by offering support to start-ups, promoting academic research, and creating specialized incubators for enterprises in these areas.

In general, the improvement of legislation should contribute to creating a favourable and safe environment for the development of entrepreneurship, given the potential threats and challenges related to cyber security and the use of artificial intelligence.

DISCUSSION

The usage of cyber security and artificial intelligence in the sphere of entrepreneurship proves its great actuality, deep interconnection and influence on business processes and the realisation of important transformations in society. The increasing dependence of society on digital technologies creates a number of problems that may arise in the future due to the increase in the number of cyber threats and the possible danger of using ChatGPT for phishing, disinformation and cybercrime. Questions regarding the further development of the artificial intelligence system and its contribution to the future safe development of humanity and the ratio of benefits and threats of AI development for business remain debatable. Therefore, considering scientists' research [3-10], we consider an urgent necessity to strengthen information support to reduce threats in virtual space and adapt entrepreneurship to modern economic security requirements.

DOI: 10.55643/fcaptp.6.53.2023.4130

CONCLUSIONS

The results of this investigation allow us to offer recommendations regarding strengthening entrepreneurship security by avoiding cyber threats and artificial intelligence use:

1. Uninterrupted investment in cyber security support. A joint study conducted by Akouto (a consulting firm in the field of business cyber security solutions, Canada) and Alpha Logistics (a logistics company, (Great Britain) has proved that business structures that do not invest enough in cyber security will eventually be forced to spend 59% more on cyber protection, and recovery after attacks will be much more expensive compared to the volume of previous investments in security [34].
2. In order to prevent cyber incidents and technological failures, every Ukrainian company should operate in a mode of constant readiness and assess vulnerable points in advance. Resisting cyberattacks requires providing businesses not only with the latest equipment and software but also with qualified technical and legal personnel.
3. Continuous personnel monitoring and training. 98% of all cyber attacks take advantage of the human factor [35]. In particular, the attacks succeed in harming companies because some staff members neglect their responsibilities or do not follow cyber security protocols. Therefore, it is of vital importance to raise the personnel's awareness of the risks and threats existing in the virtual space. The Zero Trust security model, which provides for the concept of zero trust, is extremely important: for each request made to the company's resources and each authentication, the user must confirm the authenticity of their personal data. Over-protection became necessary when the COVID-19 pandemic started and when the personnel switched to remote work through the home Internet, which, unlike corporate computers, did not have adequate protection.
4. Using the services offered by a specialized company, for example, such as Gigacloud, which offers basic cyber security solutions in terms of locating data in the cloud service and an effective risk diversification system that employs data centres in different cities.
5. Adapting the educational system to military realities.

Another important direction would be to improve the interaction between law enforcement agencies and scientific and educational institutions to enable them to apply the most advanced digital methods and tools and thus improve economic security.

Ensuring the security of entrepreneurship and Ukrainian cyberspace should be based on sustainable interaction and cooperation between governmental bodies and Ukrainian entrepreneurs. Such synergy will contribute to Ukraine's effective post-war recovery. An important role is also assigned to Ukrainian IT business, coordination, and unification of IT specialists' efforts to repel cyber-attacks, neutralize russian chatbots and hackers, as well as help businesses adapt to radically new conditions.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization: *Oleh Havryliuk, Oleksandr Yakushev*
Data curation: *Oleh Havryliuk, Oleksandr Yakushev , Maryna Petchenko, Nataliia Zachosova*
Formal Analysis: *Oleh Havryliuk, Oleksandr Yakushev, Nataliia Zachosova*
Methodology: *Oleh Havryliuk, Nataliia Zachosova, Taliat Bielialov*
Software: *Oleksandr Yakushev, Maryna Petchenko, Svitlana Kozlovska*
Resources: *Oleh Havryliuk, Oleksandr Yakushev, Maryna Petchenko, Nataliia Zachosova, Taliat Bielialov, Svitlana Kozlovska*
Supervision: *Oleksandr Yakushev, Nataliia Zachosova*
Validation: *Oleh Havryliuk, Oleksandr Yakushev, Svitlana Kozlovska*
Investigation: *Oleh Havryliuk, Oleksandr Yakushev, Maryna Petchenko, Nataliia Zachosova, Taliat Bielialov, Svitlana Kozlovska*
Visualization: *Oleh Havryliuk, Oleksandr Yakushev, Maryna Petchenko, Svitlana Kozlovska*
Project administration: *Oleh Havryliuk, Oleksandr Yakushev*
Funding acquisition: *Oleksandr Yakushev, Taliat Bielialov, Svitlana Kozlovska*
Writing – review & editing: *Oleh Havryliuk, Oleksandr Yakushev, Taliat Bielialov, Svitlana Kozlovska*
Writing – original draft: *Oleh Havryliuk, Oleksandr Yakushev, Maryna Petchenko*

REFERENCES

1. Sameeksha, D., Acs, Z. J., & Weitzel, U. A. (2012). Model of Destructive Entrepreneurship: Insight for Conflict and Postconflict Recovery. *Journal of Conflict Resolution, 57*(1), 20-40. https://journals.sagepub.com/doi/full/10.1177/0022002712464853
2. Brück, T., Naudé, W., & Verwimp, Ph. (2013). Business under Fire: Entrepreneurship and Violent Conflict in Developing Countries. *The Journal of Conflict Resolution Special Issue: Entrepreneurship and Conflict*, *57*(1), 3-19. https://www.jstor.org/stable/23415252
3. Bayram, A.S. (2017). Entrepreneurship in Conflict Zones. https://ahmadsb.com/books/entre-in-conflict-zone/ENTREPRENEURSHIP-IN-CONFLICT-ZONES.pdf
4. Jay, J., & Van Buren, H.J. (2022). Entrepreneurship, Conflict, and Peace: The Role of Inclusion and Value Creation. *Business & Society, 61*(6), 1558-1593. https://journals.sagepub.com/doi/full/10.1177/0007650321104023 8
5. Lakomaa, E. (2017). The history of business and war: introduction. *Scandinavian Economic History Review*, 65(3), 224-230. https://www.tandfonline.com/doi/epdf/10.1080/03585522.2017.1397314?needAccess=true&role=button
6. Mutonyi, G.P. (2021). Warpreneurship: War as A Business. *Path of Science*, *7*(9), 3001-3010. https://www.researchgate.net/publication/355567159_Warpreneurship_War_as_A_Business
7. Vaughan, J., & Lovatt, J. (2021). Business in Conflict-Affected and High-Risk Contexts. https://www.bsr.org/en/reports/business-in-conflict-affected-and-high-risk-contexts
8. Thota, M., & Prasad, P. (2020). Safety measures in entrepreneurs. *Journal of Management and Science, 12*, 65-72. https://www.researchgate.net/publication/343481429_Safety_measures_in_entrepreneurs
9. Aiyer, Bh., Venky, A., & Di Mattia, D. (2021) Securing small and mediumsize enterprises: What's next?
10. https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/securing%20small%20and%20medium%20size%20enterprises%20whats%20next/securing-small-and-medium-size-enterprises-whats-next-vf.pdf
11. Business in conditions of war: how to calm down and continue working (2022). https://mind.ua/publications/20249347-biznes-v-umovah-vijni-yak-zaspokoyitisya-ta-pracyuvati-dali
12. The concerns and responses of German companies The Economic Impact of the Russia-Ukraine War (2022). https://kpmg.com/de/en/home/insights/2022/05/the-economic-impact-of-the-russia-ukraine-war.html#:~:text=As%20a%20result%20of%20the,lasting%20longer%20than%20three%20years
13. Allianz Risk Barometer (2023). https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023-Appendix.pdf
14. Top Risks 2023. (2023). https://www.controlrisks.com/riskmap/top-risks
15. Ponemon 2022 Study: Data Risk in the Third-Party Ecosystem (2023). The Global Risks Report 2023 https://www.weforum.org/reports/global-risks-report-2023/digest/
16. Kiberbezpeka biznesu pid chas viiny (2023). https://mklegalservice.com/tpost/k123zz39h1-kberbezpeka-bznesu-pd-chas-vini
17. Elon Musk among experts urging a halt to AI training (2023). https://www.bbc.com/news/technology-65110030
18. Generative AI set to affect 300mn jobs across major economies. (2023). *Financial Times*. https://www.ft.com/content/7dec4483-ad34-4007-bb3a-7ac925643999
19. Artificial Intelligence (AI) Market by Component: Global Opportunity Analyses and Industry Forecast, 2022-2030. (2023). Next More Strategy Consulting. https://www.nextmsc.com/report/artificial-intelligence-market
20. Lin, Y. (2023, Marc 17). 10 Artificial Intelligence Statistics You Need To Know In 2023. https://www.oberlo.com/blog/artificial-intelligence-statistics
21. Ignatius, D. (2022). How the algorithm tipped the balance in Ukraine. *The Washington Post*, 19. https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/
22. Future of Jobs Report (2023). *Insight Report May 2023*. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf
23. Europol (2023). Europol sounds alarm about criminal use of ChatGPT, sees grim outlook. https://www.reuters.com/technology/europol-

DOI: 10.55643/fcaptp.6.53.2023.4130

sounds-alarm-about-criminal-use-chatgpt-sees-grim-outlook-2023-03-27/

24. Europol (2023). ChatGPT The impact of Large Language Models on Law Enforcement. https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf
25. On the Basic Principles of Ensuring Cybersecurity of Ukraine (The Law of Ukraine), № 2163-VIII (2017). https://zakon.rada.gov.ua/laws/show/2163-19#Text
26. Convention on Cybercrime (2001). European Treaty Series, 185. https://rm.coe.int/1680081561
27. On Personal Data Protection (The Law of Ukraine) № 2297-VI (2010). https://zakon.rada.gov.ua/laws/show/2297-17#Text
28. On Public Electronic Registers (The Law of Ukraine) № 1907-IX (2021). https://zakon.rada.gov.ua/laws/show/1907-20#Text
29. On Critical Infrastructure (The Law of Ukraine) № 1882-IX (2021). https://zakon.rada.gov.ua/laws/show/1882-20#Text
30. On the National Security of Ukraine (The Law of Ukraine) № 2469-VIII (2018). https://zakon.rada.gov.ua/laws/show/2469-19#Text
31. On Electronic Communications (The Law of Ukraine) № 1089-IX (2020). https://zakon.rada.gov.ua/laws/show/1089-20#Text
32. On the Cybersecurity Strategy of Ukraine (Decree of the President of Ukraine "On the Implementation of the Decision of the National Security and Defense Council of Ukraine") (2016). http://zakon2.rada.gov.ua/laws/show/96/2016
33. On the approval of the Concept of the development of artificial intelligence in Ukraine (Decree of the Cabinet of Ministers of Ukraine), 1787 (2021). https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
34. Criminal Procedural Code of Ukraine (2013). http://zakon5.rada.gov.ua/laws/show/4651-17
35. On Approving the Regulation on the Cyber Police Department of the National Police of Ukraine (Order of the National Police of Ukraine), 85 (2015). http://tranzit.ltd.ua/nakaz/

Гаврилюк О., Якушев О., Петченко М., Зачосова Н., Бєлялов Т., Козловська С.

КІБЕРБЕЗПЕКА ТА ШТУЧНИЙ ІНТЕЛЕКТ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМНИЦТВА У ВОЄННИЙ ЧАС

Забезпечення безпеки підприємництва набуло особливої актуальності в контексті геополітичних конфліктів, зростаючої диджиталізації та впровадження нових технологій у фінансовий і виробничий сектор, збільшення частоти й складності кібератак, спрямованих на сферу бізнесу, а також активізації застосування штучного інтелекту. Стаття присвячена розкриттю специфіки забезпечення безпеки підприємництва в Україні у воєнний час із використанням штучного інтелекту та кіберзахисту. Проведено ретроспективний огляд літератури, показано відсутність досліджень щодо використання штучного інтелекту в забезпеченні безпеки підприємницької діяльності, що свідчить про наукову новизну цієї статті. Висвітлено проблеми та загрози, які постали перед державними й приватними бізнес-структурами при здійсненні підприємницької діяльності; війна з росією потребує врахування нових реалій – диджиталізації економіки, боротьби з кіберзагрозами, використання нових інноваційних технологій і штучного інтелекту. Констатовано діапазон тригерів, що генерують серйозні збої в бізнесі, які пов'язані з кібернетичною діяльністю, включаючи застосування штучного інтелекту, зловмисні атаки злочинців чи хакерів, витік інформації, людський фактор або відмову техніки. Акцентовано увагу на тому, що невідлагодженість нормативно-законодавчої бази у сфері кібербезпеки також робить бізнес вразливим перед можливістю руйнації.

Окреслено можливості застосування та загрози штучного інтелекту для безпеки підприємництва. Сформульовано напрями вбезпечення підприємництва в умовах війни за допомогою штучного інтелекту та усунення / мінімізації кіберзагроз. Висвітлено стан нормативно-законодавчої бази, що регламентує регулювання кібербезпеки в Україні, та запропоновано напрями її поліпшення.

Ключові слова: кібербезпека, штучний інтелект, диджиталізація, війна, підприємництво

JEL Класифікація: M21, H56, O32, D21, D81