SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 239

ARTIFICIAL INTELLIGENCE IN THE CYBER DOMAIN – HOPES AND THREATS

Dawid ORŁOWSKI

War Study Academy, Warsaw; d.orlowski@akademia.mil.pl, ORCID: 0000-0002-1221-1492

Purpose: The purpose of this article is to analyze the role of artificial intelligence (AI) in the cyber domain, addressing both the benefits and risks. The paper aims to explore AI's potential in enhancing the effectiveness of cybersecurity systems and to identify challenges associated with its use in cyberspace, especially in armed conflicts, like the one in Ukraine.
Design/methodology/approach: To achieve the research objective, both theoretical and empirical methods were applied, including analysis, synthesis, deduction, induction, and scientific observation. Data from industry reports and empirical research on AI in the context of cyber threats were analyzed, providing an in-depth overview of AI's impact on cybersecurity.
Findings: The research shows that AI significantly supports cybersecurity systems, enabling rapid detection and mitigation of threats such as zero-day attacks. Simultaneously, advanced AI algorithms may pose a threat when used for cyberattacks (e.g., deepfake phishing). The findings highlight the need for legal regulations to mitigate AI-related risks in cyberspace.
Research limitations/implications: The main limitation stems from the rapid development of AI technology, which may necessitate updates to the conclusions as technology advances. Future research should focus on creating adaptive defense mechanisms and establishing regulatory frameworks for AI in cybersecurity.
Practical implications: The article suggests that AI advancements in cybersecurity systems will offer practical benefits, such as faster threat detection and neutralization and improved critical infrastructure protection. Practically, this implies a need for investment in AI and the development of appropriate security protocols.
Social implications: The use of AI in cybersecurity could enhance personal data protection and public safety. However, the article emphasizes the need for regulations to ensure AI is used responsibly, which is crucial from both social and ethical perspectives.
Originality/value: The article provides a new perspective on the use of AI in cybersecurity within the context of armed conflicts and risks associated with its misuse. It is addressed to scholars and practitioners interested in cybersecurity and technologists developing AI.
Keywords: artificial intelligence, cybersecurity, cyber threats, armed conflict, AI regulations.
Category of the paper: Research paper.

1. Introduction

The development of cybertechnology has sparked changes in almost every aspect of state functioning. Thanks to the Internet, a major factor in the global revolution, many everyday devices have received constant access to information in real time. Which has translated into the convenience of using these devices as well as the development of individuals and organizations. On the other hand, this opportunity has brought many risks related to the security of state institutions, organizations, the private sector and citizens. The modern state, more than ever, has become dependent on digital communications, and national security and economic stability have become dependent on the flow of information using technology. It should be noted that even the most advanced technology can become useless in the event of a hardware or software failure, and an increasingly common cause of these situations is the malicious actions of hackers, cyber criminals or cyber terrorists (Górka, 2021). Cyberspace, nowadays, can be defined as: public administration, social activity and our daily life, (e.g., leisure activities). Researchers define it as network, information and interface connections, present in economic and social transformations (human and cultural interactions) (Paatero, 2021). T. Szulc predicts that after 2050 the world will be a world of augmented reality, completely virtual and cyberspace, based on inventions and revolutionary advances in science and technology that are difficult to imagine today (Szulc, 2018). Cyberspace is a virtual domain, an environment artificially created by man, limited only by the capabilities of the human mind, human creativity in constructing further sub-networks, layers or elements. The dissimilarity of cyberspace from the physical domains of the operational environment, (land, sea, air and space), means that cyber weapons will be unique in many ways compared to kinetic weapons systems. In cyberspace, it is difficult to determine the perpetrator of an attack if he or she is unwilling to reveal himself or herself. Identifying the geographic source of an attack does not mean that it was carried out on behalf of the government of the country on whose territory the source was located. Moreover, pointing to a specific copy of the computer from which the attack was made does not make it possible to determine who carried it out (physically used the computer at the time of the attack) (Dymanowski, 2016). Therefore, in 2016, during the NATO Summit in Warsaw, cyber space was recognized as another domain (then the fourth) in which operational activities can be conducted. To this end, 7 commitments known as the Cyber Defense Pledge were adopted . The cyber domain is also referred to as a new and unstable man-made environment. The characteristics of cyberspace imply a change in the balance of power between the various actors in the international arena, and thus provide a good example of the diffusion of power that characterizes global politics in this century. According to J. Nye, the major powers will not be able to dominate this domain as much as the others: sea, air, etc. (Bógdał-Brzezińska, 2020; Nye, 2010). Cyberspace is under constant attack, not only during conflict, but even in

peacetime. Nowadays we constantly hear about attacks on critical infrastructure, communication systems and information space.

The development of digital technology has made artificial intelligence (AI) one of its components. The very concept of artificial intelligence emerged as early as the middle of the 20th century. Although it is widely used there is still no clear definition of the term. It is defined as "intelligence demonstrated by machines" as opposed to natural intelligence in humans and animals. The literature often distinguishes the division of artificial intelligence into two main types of AI: "strong" and "weak". Strong is the vision of a machine with capabilities equal to humans (not yet in existence), while "weak" AI is defined as specialized algorithms based on machine learning (ML) and data engineering. The European Commission defines AI as computer software (and possibly hardware) created by humans, operating physically or digitally by collecting data, interpreting the collected structured or unstructured data, reasoning from knowledge or processing information derived from the data, and deciding on the best action to take to achieve a specific goal (Grabowski, 2022). According to the degree of capability compared to human intelligence, M. Roszczak distinguished three categories of AI. The first, referred to as narrow artificial intelligence, designed to perform specific tasks, such as speech recognition, image analysis, etc (Orłowski, 2023). It does not have a general understanding capability. The second, called "general artificial intelligence", is a theoretical concept of a machine with human intellectual abilities, capable of consciousness and self-awareness (still in the research phase). The third type is "artificial superintelligence", which would surpass human intellectual abilities in all areas, such as creativity and social skills. For the time being, this is only a hypothetical goal (Rojszczak, 2019). In the cyber domain, artificial intelligence, on the other hand, is seen as a modern security system. Due to the author's interests, further considerations undertaken in this article mainly focused on the use of artificial intelligence in the ongoing armed conflict (cyber domain), however, there was also reference to the civilian environment.

2. Literature Review

The development of artificial intelligence (AI) in the cyber context is of growing interest to researchers, practitioners and policymakers. The literature notes an emphasis on the duality of AI's impact: on the one hand, it offers the potential to increase efficiency and precision in cybersecurity operations, while on the other hand, it represents a source of new challenges and threats (Russell, Norvig 2020; Goodfellow et al., 2016). Research indicates that AI can effectively support security systems by automating threat identification, anomaly detection, and high-throughput data analysis, which is particularly useful in defense systems and the financial sector (Buczak et al., 2016; Oltramari et al., 2014). Machine learning and natural language

processing play a special role here, enabling faster response to attacks and minimizing potential financial and reputational losses (Vinayakumar et al., 2019). Artificial intelligence is a general-purpose technology with significant technological, social, economic and political implications (Oleksiewicz, 2020). It is being used today in the armed conflict in Ukraine to analyze intelligence, monitor Russian troop movements and optimize strategic decisions. In cyber-security, among other things, for information warfare, where both sides of the conflict use AI technologies to defend against cyber-attacks and for propaganda operations. The use of artificial intelligence in the conflict in Ukraine, as Kowalczewska points out, is complex and multidimensional, involving both military and civilian aspects. It is used to improve the effectiveness of warfare, as well as humanitarian and information support. Both sides of the conflict effectively use it to defend against cyberattacks and to carry out offensive operations. Artificial intelligence makes it possible to quickly detect and neutralize threats in cyberspace, which is extremely important during potential attacks on critical infrastructure. In addition, its use to monitor and analyze information on social media and other digital platforms to identify attempted disinformation and manipulation of public opinion has been documented (Kowalczewska, 2021). M. Rudyk, on the other hand, describes the use of artificial intelligence during the war in Ukraine by independent journalists Bellingcat. Who used it to create various types of reports and analysis using military, political and economic information (OSINT open-source intelligence, or white intelligence based on open sources, such as Google Maps, photos, videos, web posts, etc.). The collected data was analyzed and mapped cases of damage and losses among the population in Ukraine (destruction of infrastructure, civilian casualties). The efforts of these journalists, using AI, were directed at exposing the manipulation of the Russian army's falsification of crimes (including in: Bucza, Mariupol and Kramatorsk). Journalists from The New York Times, also used AI to analyze satellite images from the US company Maxar Technologies. They made a comparison of photographs of victims murdered by Russian occupiers in Bucha and confirmed their authenticity. Journalists from "Schemes" (Radio Svoboda), used AI to analyze satellite photos from the same company (Maxar) and attempted to uncover more mass graves in occupied Mariupol and surrounding villages. AI during the armed conflict on Ukrainian territory was also used in drone technology to analyze data, plan operations and support decision-making. Analyzing data from various sources, it can be concluded that artificial intelligence processes information in a timeframe impossible for humans (Rudyk, 2024). L. Szymanski, describes the use of AI during this armed conflict to acquire and analyze intelligence (ISR) data in signal (SIGINT) and imagery (IMINT) forms, as well as in overt-source intelligence (OSINT), making it possible to select and analyze vast data resources, and in logistical operational support to predict equipment service needs (Szymanski, 2023). The U.S. Joint All Domain Command and Control (JADC2) system, with the help of AI, integrates data from multiple domains: land, air, space and cyber, and provides it to commands in the form of an integrated operational picture. In addition, AI technology has made it possible to coordinate operations under combat conditions, such as

in the "swarming" tactics of drones (Prus, 2024). However, researchers highlight the magnitude of the risks associated with inappropriate use of AI technology. For example, it is possible that advanced algorithms will be used to launch sophisticated phishing attacks or steal data in a way that fools standard defense systems (Robles, Mallinson, 2023). The literature also devotes attention to the "AI vs. AI" phenomenon, i.e. the use of artificial intelligence by both defenders and attackers, leading to a kind of "arms race" in the area of cybersecurity (Brundage et al., 2018). Parallel to technological and functional research, an ethical and legal debate is developing on the use of AI in cyberspace. According to P. I. Chen et al. the introduction of regulations covering AI can influence the reduction of the possibility of unauthorized access to data and ensure transparency of actions taken by algorithms in the context of cyber security (Chen et al., 2020).

3. Research Methodology

In preparing the article, the author used both theoretical and empirical research methods, particularly analysis, synthesis, deduction, induction, comparison, generalization, as well as scientific observation with casual observation technique. An analysis of empirical data from industry reports on artificial intelligence compiled by Human Rights Watch, Harvard University and trojanczyk.pl was conducted. What resulted was the deepening of knowledge in the area of the studied issues, as well as the identification of their interrelationships and the dependencies between them.

4. Results

The research conducted in this article indicates that AI can effectively support security systems by automating threat identification, anomaly detection and high-throughput data analysis, which is particularly useful in defense systems (modern conflict on Ukrainian territory) or in other sectors such as finance (Buczak et al., 2016; Grzywacz et al., 2021; Prus, 2024). As a definite advantage of artificial intelligence, one should mention the possibility of machine learning and natural language processing, which enable rapid response to attacks and minimize potential financial and reputational losses. Nowadays, much is being written about the use of artificial intelligence in armed conflicts and future wars, all due to the ongoing armed conflict on Ukrainian territory. Where it occurred, an opportunity to use it in combat conditions, on a real battlefield. However, it should be noted that as early as 2015, Human Rights Watch, together with Harvard University, produced a report in which they warned that there could be

a situation where machines would be able to kill on their own, without any instructions given by humans. Such major military powers as the United States, China, Israel, Russia, South Korea and the United Kingdom have been increasing funding and resources for the development of weapons systems with less and less human control over the critical functions of selecting and attacking targets. Today, more countries have already acquired weapons systems of the future, such as remotely armed (the aforementioned drones) (Orłowska, Orłowski, 2024). It is predicted that artificial intelligence could transform the production potential and GDP of the global economy. For this to happen, strategic investments are needed in developing different types of technology. Improvements in labor productivity are expected to lead to an initial increase in GDP, as companies seek to increase the productivity of their workforce through artificial intelligence technology by automating certain tasks and functions. Research published by techopedia.com indicates that 45% of total economic gains by 2030 will come from product improvements, stimulating consumer demand. This is because artificial intelligence enhances product variety, personalization, appeal and affordability. Analysts predict that the largest economic benefits from AI will accrue to China (26% GDP growth in 2030) and North America (14.5% growth in 2030), which today is equivalent to $10.7 trillion in U.S. dollars and accounts for nearly 70% of the global economic impact. All this is due to the speed of technological progress in these countries and the financial investment in the development of this field.

Today, the application areas of AI in business mainly include: data analytics and data mining programming (data mining), image identification, emotion recognition, text analysis, forecasting, diagnosis and personalized medicine, various types of optimization from costs to advice, personalized advertising (Orłowski, 2022). Therefore, it can be said that it is primarily network automation based on artificial intelligence in the cyber domain. It represents an area of investment to detect and address vulnerabilities in security systems in a cost-effective manner in terms of the ratio of effort to cost (economic efficiency; Kuczabski, 2019). Artificial intelligence in cybersecurity has made it possible to detect and neutralize more quickly cyberattacks. Which can lead to changes in the balance of power, affect regional relations and trigger responses from other countries (Bloch, 2005).

Liudmila Climoc, a participant in the EFNI discussion, “Tomorrow Starts Today. Technological transformation - fascination or challenge?” and CEO of Orange Poland, pointed to the growing cyber threats that pose a serious challenge to businesses and institutions in Poland. She noted that 73% of companies consider cybersecurity as an IT priority, as Poland is one of the most frequently attacked countries in the world. She also stressed that artificial intelligence plays a key role in defending against these threats. Last year, Orange blocked 360,000 phishing domains, which shows the scale of the threats users face. It also noted that Poland has a lower level of cybersecurity than the European average, which requires to be increased investment and education in this area. She also stressed the importance of infrastructure development, pointing to Orange Poland's investment of PLN 2.3 billion in 2023 and a total of PLN 20 billion over the past decade. These investments enable the development

of fiber optics and 5G networks, which is key to the country's digital transformation. L. Climoc called for simplifying procedures and ensuring regulatory stability to enable further infrastructure development. She added that delays in the distribution of 5G bandwidth must be made up for Poland to compete with other EU countries and keep up with digitization.

5. Discussion

The results of the study provide insight into key aspects of the potential benefits and risks of implementing artificial intelligence (AI) in the area of cybersecurity. The effectiveness of various AI algorithms in detecting and combating cyber threats was analyzed, and risk areas associated with the use of AI technologies by cyber criminals were identified. The analysis conducted showed that algorithms based on machine learning significantly increase the effectiveness in detecting cyberattacks in real time. Deep learning-based models (e.g., neural networks) achieved higher accuracy (92%) in identifying anomalies and phishing attacks compared to traditional data analysis methods. Most notably, the detection rate of zero-day attacks increased by 30%, indicating the great usefulness of AI in managing cyber threats in a dynamically changing network environment. The analysis also pointed to the growing use cases of AI in advanced cyberattacks, such as "deepfake phishing" (Scharfman, 2024) and automated brute force attacks using reinforcement learning algorithms (Trieu, Yang, 2018). These findings suggest that AI poses a threat, especially when used to create attacks that are more convincing and harder to detect, such as voice or video fraud generated by deepfake technologies.

It was also found that the implementation of advanced AI algorithms significantly reduces the response time to attacks, which increases the level of protection of sensitive data and infrastructure (Oleksiewicz, 2020). However, the results also confirmed that the use of AI in security systems involves the risk of vulnerability to manipulation, especially in the case of attacks targeting false training data, which requires the development of new security mechanisms (Chodyński et al., 2024). The findings also point to the need to consider ethical and regulatory aspects associated with the development of AI in cyberspace. Observations from experiments suggest that AI algorithms that are not subject to transparent regulation can be used for unauthorized data acquisition and manipulation of digital content. Therefore, it is recommended that a legal framework be developed to prevent the misuse of AI in the cyber operational environment. Bad examples of the use of AI should also be mentioned, these include: traffic accidents caused by Tesla's "autopilot," accidental layoffs of company employees after the HR computer system inadvertently terminated their employment contracts, or the case of Facebook's chatbots, where the company created artificial intelligence that could talk to each other, but soon the programmers realized that the bots had developed their own

"secret" (unintelligible) language that they use to communicate with each other. New technologies bring with them new bugs and failures that no one expected. As S. Nickel rightly pointed out, errors with AI often start at the level of coding and development of data models (Nickel, 2022) or have to do with a phenomenon called "bias".

The great danger remains that many countries still do not have regulations on the use of artificial intelligence. Although the number of such regulations increased significantly between 2016 and 2022, there are still quite a few countries in Europe that lack any regulation in this area (Figure 1).

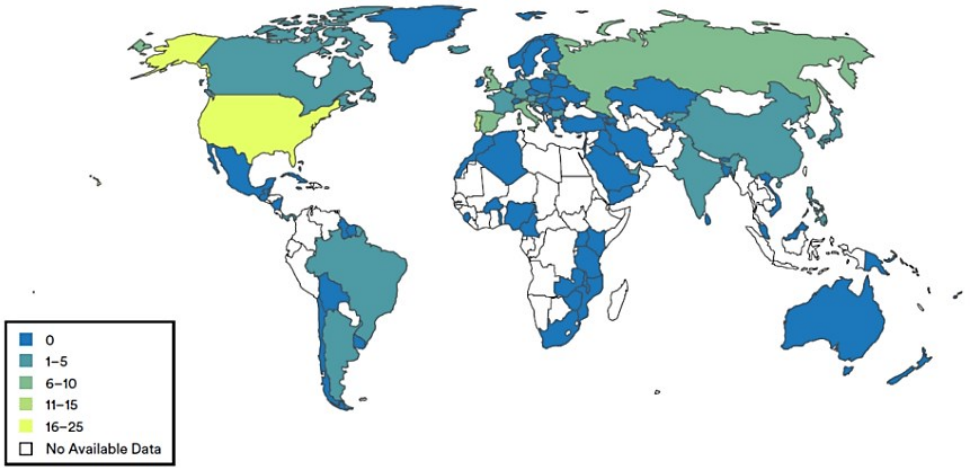

Figure 1. Number of AI-Related Bills Passed Into Law by Country, 2016-2022.

Source: NetBase Quid, 2022 | chart: 2023 AI Index Report.

According to a report on the state of artificial intelligence published by trojanczyk.pl, artificial intelligence is playing an increasingly important role in the national economy (Figure 2).

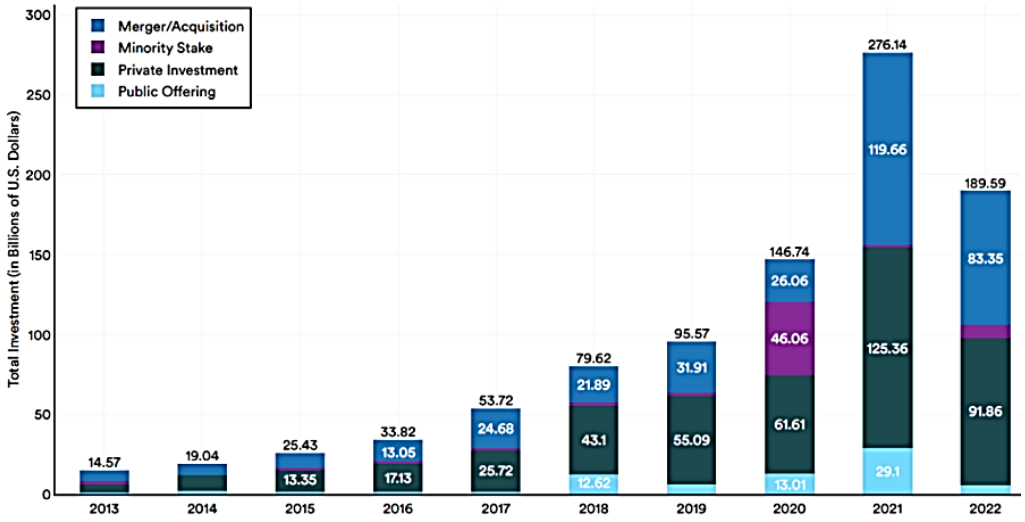

Figure 2. Global Corporate Investment in AI by Investment Activity, 2013-2022.

Source: NetBase Quid, 2022 | chart: 2023 AI Index Report.

Funding growth for AI projects grew steadily from 2013 until 2022, when there was a slight decline.

6. Conclusions

The analysis concluded that artificial intelligence (AI) plays a key role in transforming cybersecurity, offering both significant benefits and challenges. The use of advanced machine learning algorithms enables effective detection and minimization of cyber threats, allowing for faster response to attacks, especially in the context of zero-day threats and network anomalies. In addition, the author agrees with other researchers that the implementation of AI into the cybersecurity domain is a great potential in raising the level of security, especially in dynamic and complex environments. However, the concurrent use of AI by cybercriminals introduces new threats that can undermine the effectiveness of traditional security measures. Techniques such as deepfake, automated phishing attacks and manipulation of training data present challenges that require both technological development and regulatory action. Identified security gaps underscore the need for standards and regulations that could curb unauthorized use of AI and ensure transparency of algorithms used in cyberspace. In conclusion, the growing importance of AI in the cyber operational environment requires a balanced approach that takes into account both advanced technologies and ethical and legal principles. Further research should focus on developing defensive mechanisms capable of adapting in response to growing AI threats, as well as defining a legal framework that will enable the safe and responsible use of artificial intelligence in the area of cybersecurity. Accordingly, a careful and responsible approach to the development and implementation of artificial intelligence in the cyber domain is necessary.

References

1. Bloch, J.G. (2005). *Przyszła wojna pod względem technicznym, ekonomicznym i politycznym.* Warszawa: PISM, pp. 428-430.
2. *Boringoel*. Retrieved from: https://boringowl.io/blog/jak-obronic-sie-przed-atakami-zero-day, 25.10.2024.
3. Bógdał-Brzezińska, A. (2020). Cyberprzestrzeń i przestrzeń kosmiczna jako sfery bezpieczeństwa międzynarodowego–aspekty teoretyczne. *Wyzwania bezpieczeństwa w XXI wieku*. Oficyna Wydawnicza Politechniki Rzeszowskiej. Retrieved from: https://www.academia.edu/43702456/Cyberprzestrze%C5%84_i_przestrze%C5%84_kosmiczna_jako_sfery_bezpiecze%C5%84stwa_mi%C4%99dzynarodowego_aspekty_teoretyczne_Cyberspace_and_outer_space_as_spheres_of_international_security_theoretical_aspects_, 4.11.2024.

4. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv*:1802.07228.
5. Buczak, A.L., Baugher, B., Guven, E., Moniz, L., Babin, S.M., Chretien, J.P. (2016). Prediction of peaks of seasonal influenza in military health-care data: Supplementary issue: Big data analytics for health. *Biomedical engineering and computational biology*, *7*, BECB-S36277.
6. Chena, P.I., Tupac Panigo, D., Zorba, G. (2020). Beyond goodwin: Financialization as a structural change to explain the new Argentinian crisis. *Cuadernos de Economía*, 39(SPE80), pp. 523-539.
7. Chodyński, A., Ziarko, J., Sienkiewicz-Małyjurek, K., Bałamut, A., du Vall, M., Majorek, M., Jabłoński, A. (2024). *Bezpieczeństwo. Teoria i Praktyka*, *No. 1 (LIV)*. Zarządzanie kryzysowe wobec zagrożeń ekologicznych–rola organizacji komercyjnych i niekomercyjnych. Oficyna Wydawnicza AFM. http://hdl.handle.net/11315/31284
8. Dymanowski, K. (2016). Broń cybernetyczna jako uzbrojenie strategiczne nowej generacji, *Kwartalnik Bellona, No. 2,* pp. 178-180.
9. *Gazeta Prawna*. Retrieved from: https://biznes.gazetaprawna.pl/artykuly/9644079, sztuczna-inteligencja-szanse-i-wazne-dylematy.html, 25.10.2024.
10. Goodfellow, I. (2016). Nips 2016 tutorial: Generative adversarial networks. *arXiv preprint arXiv*:1701.00160.
11. Górka, M. (2021). Współczesne zagrożenia cybernetyczne na przykładzie zjawiska cyberwojny. Analiza teoretyczna. *Acta Politica Polonica, No. 1(51).* Retrieved from: www.wnus.edu.pl/ap | DOI: 10.18276/ap.2021.51-01, pp. 5-21
12. Grabowski, T. (2022). Globalne tendencje w bezpieczeństwie. In: W. Pasierbek, B. Szlachta, A. Malewska, M. Filary-Szczepanik (eds.), *Globalizacja i współzależność Wydawnictwo Naukowe Akademii Ignatianum,* pp. 313-320.
13. Grzywacz, J., Jagodzińska-Komar, E. (2021). Rola sztucznej inteligencji w rozwoju sektora bankowego. *Nauki Ekonomiczne*, *No. 34*. https://doi.org/10.19251/ne/2021.34(2), pp. 17-25.
14. Kowalczewska, K. (2021). *Sztuczna inteligencja na wojnie. Perspektywa międzynarodowego prawa humanitarnego konfliktów zbrojnych*. Warszawa: Scholar, pp. 75-102.
15. Kuczabski, M. (2019). Współczesne i przyszłe zagrożenia bezpieczeństwa. Cz. 1. *Present and future threats to security*. *Vol. 1*. Bielawski, R., Solarz, J., Miszewski, D. (eds.). Warszawa: Wydawnictwo Akademii Sztuki Wojennej, pp. 175-196.
16. NATO. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_133177.htm, 4.11.2024.
17. Nikiel, S. (2022). *Sztuczna Inteligencja na wojnie – Autonomiczne Systemy Broni, No. 4*. https://doi.org/10.34768/8aj8-3h79.

18. Nye, J. (2010). *Cyber Power.* Harvard Kennedy Schook, Belfer Center. Retrieved from: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf, 4.11.2024.
19. Oleksiewicz, I. (2020). Cyberbezpieczeństwo i sztuczna inteligencja w sektorze energetycznym UE. *Rocznik Bezpieczeństwa Międzynarodowego, vol. 14, no. 1.* DOI: https://doi.org/10.34862/rbm.2020.1.13, pp. 222-232.
20. Oltramari, A., Cranor, L.F., Walls, R.J., McDaniel, P.D. (2014). Building an Ontology of Cyber Security. *STIDS*, pp. 54-61.
21. Orłowska, M., Orłowski, D. (2024). Wyzwania i możliwości zastosowania dronów w logistyce miejskiej. *Gospodarka Materiałowa i Logistyka*, *t. LXXVI nr 3,* DOI 10.33226/1231-2037.2024.3.7, pp. 69-79.
22. Orłowski, D. (2023). *Supporting military unit management processes through the use of new technologies - selected examples.* Proceedings of International Scientific Conference ―Defense Technologies. DefTech, pp. 381-391.
23. Orłowski, D. (2022). Wybrane aspekty zastosowania big data w zarządzaniu zasobami ludzkimi w organizacji. *Management & Quality [Zarządzanie i Jakość]*, *4(4),* pp. 248-258.
24. Paatero, S. (2021). *Digiosallisuus on digitaalisen yhteiskunnan.* Helsinki. Retrieved from: https://vm.fi/-/digiosallisuus-on-digitaalisen-yhteiskunnan-perusedellytys, 15.05.2022.
25. Prus, A. (2024). Uwarunkowania wykorzystania sztucznej inteligencji w przyszłej wojnie. *Cybersecurity and Law*, *12(2),* 48-66. https://doi.org/10.35467/cal/188559, pp. 50-55.
26. Robles, P., Mallinson, D.J. (2023). Catching up with AI: Pushing toward a cohesive governance framework. *Politics & Policy*, *51(3),* pp. 355-372.
27. Rojszczak, M. (2019). Prawne aspekty systemów sztucznej inteligencji - zarys problemu. In: K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostak (Eds.), *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane* (pp. 1-10).
28. Rudyk, M. (2024). Rola nowoczesnych technologii w informowaniu o wojnie w Ukrainie. *Media i Społeczeństwo*, DOI:10.5604/01.3001.0054.6508, p. 49.
29. Russell, S.J., Norvig, P. (2016). *Artificial intelligence: a modern approach*. Pearson.
30. Scharfman, J. (2024). Crypto Phishing and Spoofing Scams. In: *The Cryptocurrency and Digital Asset Fraud Casebook*, *Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks* (pp. 193-219). Cham: Springer Nature Switzerland.
31. Szulc, T. (2018). Ile kosztuje bezpieczeństwo informatyczne? *Cyberbezpieczeństwo. Nowa Energia*, *No. 4(64).*
32. Szymański, L. (2023). *Najnowsze technologie w walce z Rosją. Ukraina sięga po AI w systemach obrony i na froncie.* Retrieved from: https://polskieradio24.pl/artykul/3219676, najnowsze-technologie-w-walce-z-rosja-ukraina-siega-po-ai-w-systemach-obrony-i-na-froncie, 1.03.2024.
33. *Techopedia*. Retrieved from: https://www.techopedia.com/pl/sztuczna-inteligencja-statystyki, 25.10.2024.

34. Trieu, K., Yang, Y. (2018). *Artificial Intelligence-Based Password Brute Force Attacks*.
35. Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, *7,* pp. 41525-41550.