STUDIA IURIDICA TORUNIENSIA
TOM XXXVII
DATA WPŁYWU: 4 LUTEGO 2025 R. DATA AKCEPTACJI: 5 LUTEGO 2026 R.

Christophe Gaie
Jean Moulin Lyon 3 University, France
christophe.gaie@gmail.com
ORCID: https://orcid.org/0000-0002-8252-5278

Mirosław Karpiuk
University of Warmia and Mazury, Olsztyn
miroslaw.karpiuk@uwm.edu.pl
ORCID: https://orcid.org/0000-0001-7012-8999

Claudio Melchior
University of Udine, Italy
claudio.melchior@uniud.it
ORCID: https://orcid.org/0000-0002-6124-4717

Artificial intelligence in the sphere of security

http://dx.doi.org/10.12775/SIT.2025.018

The growing potential of artificial intelligence may give rise to significant consequences for state security. Therefore, numerous states have been engaged in the development of various applications of artificial intelligence (AI) for military purposes. Artificial intelligence is currently employed in the sphere of information operations, collecting and analyzing intelligence data, logistics, and in fully or partly autonomous vehicles. It is also included in military operations[1].

[1] A.K. Olech, A. Lis, *Technologia i terroryzm. Sztuczna inteligencja w dobie zagrożeń terrorystycznych*, Warszawa 2024, p. 16.

As a matter of fact, AI is increasingly utilized for real-time battlefield operations. This includes tasks such as object detection by radars, locating underwater mines, and enhancing cyberdefense. AI algorithms can analyze data to identify and track threats much faster and more accurately than humans, significantly improving situational awareness and response times. Furthermore, research is ongoing in bioinspired AI robots designed for the battlefield, capable of autonomous navigation and coordinated actions, potentially reducing risks to human soldiers[2].

Security is defined as a condition in which individuals, communities, organisations, or states are properly protected against threats that might compromise their well-being, integrity, and survival. This refers to protection against physical threats and to the provision of economic, social, political or environmental conditions which allow stable functioning[3]. Security is a domain which is of great importance to the state, society and its individual members as well[4]. It constitutes a fundamental need of every human being, and a necessary condition for them to survive and develop, with everyone having the right to enjoy security. Security is involved in every aspect of human life[5].

---

[2] M. Bistron, Z. Piotrowski, *Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens*, "Electronics" 2021, No. 7, p. 871, doi: 10.3390/electronics10070871.

[3] K. Kaczmarek, *Wpływ zmian klimatycznych na bezpieczeństwo*, "Journal of Modern Science" 2024, No. 4, p. 412.

[4] M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, "Zeszyty Naukowe KUL" 2018, No. 3, p. 15.

[5] A. Pieczywok, *Cyberprzestrzeń i dydaktyka cyfrowa na rzecz bezpieczeństwa człowieka*, "Cybersecurity and Law" 2024, No. 2, p. 95. For additional information about security, refer to: Z. Werra, K. Kaczmarek, M. Polak, *Contemporary Dimension of Cultural Security*, „Studia Iuridica Lublinensia" 2025, No. 4, pp. 83–99, doi: 10.17951/sil.2025.34.4.83-99; M. Karpiuk, *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, No. 1, p. 185–194, doi: 10.17951/sil.2019.28.1.185-194; M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, No. 5, pp. 43–52, doi: 10.17951/sil.2023.32.5.43-52; K. Kaczmarek, E.M. Włodyka, M. Czuryk, *The Status of Government Administration Management in the Sphere of Crisis Management*, "Prawo i Więź" 2025, No. 6, pp. 655–670, doi: 10.36128/48wmzt46; M. Czuryk, *Jurisdiction of the Voivode in the Field of Crisis Management*, "Studia Iuridica Lublinensia" 2025, No. 2, p. 87–98,

The emergence of AI facilitates the adoption of measures that safeguard societies and individuals in numerous domains. For instance, a wide range of AI-powered systems are being explored for crime prediction, enabling law enforcement to allocate resources more effectively and potentially prevent criminal activity before it occurs[6]. Border security is also significantly enhanced by AI through facial recognition and automated threat detection systems, strengthening national security[7]. Furthermore, AI has the potential to significantly improve disaster response by providing more accurate predictions, enabling faster evacuation and more efficient resource deployment[8]. These advancements demonstrate the expanding role of AI in safeguarding communities and strengthening overall security.

The European Union legislator defines artificial intelligence as a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that (for explicit or implicit objectives) infers, from the input it receives, how to generate outputs that can influence physical or virtual environments[9]. The term "artificial intel-

---

doi: 10.17951/sil.2025.34.2.87-98; K. Kaczmarek, *Bezpieczeństwo państwa wobec współczesnych zagrożeń*, „Prawo i Więź" 2025, No.5, p. 567–580, doi: 10.36128/PRIW.VI58.1382.

[6] F. Dakalbab, M.A. Talib, O.A. Waraga, A.B. Nassif, S. Abbas, Q. Nasir, *Artificial intelligence & crime prediction: A systematic literature review*,"Social Sciences & Humanities Open" 2022, No. 1, p. 100342, doi: 10.1016/j.ssaho.2022.100342; V. Mandalapu, L. Elluri, P. Vyas, N. Roy, Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions, "IEEE" 2023, No. 11, p. 60153–60170, doi: 10.1109/ACCESS.2023.3286344.On the subject of methods for solving problems arising in connection with the development of artificial intelligence, see: L.Bolc, J. Cytowski, *Search methods for artificial intelligence*, San Diego 1992.

[7] T. Ige, A. Kolade, O. Kolade, *Enhancing Border Security and Countering Terrorism Through Computer Vision: A Field of Artificial Intelligence*, in: *Data Science and Algorithms in Systems*, R. Silhavy, P. Silhavy, Z. Prokopova (eds.), Cham 2023, doi: 10.1007/978-3-031-21438-7_54.

[8] W. Sun, P. Bocchini, B.D. Davison, *Applications of artificial intelligence for disaster management*, "Nat Hazards" 2020, No. 103, pp. 2631–2689, doi: 10.1007/s11069-020-04124-3.

[9] Article 3 (1) of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intel-

ligence" (AI) embraces all software or hardware components that enable machine learning, computer vision, understanding, generation and processing of natural language or robotics. Through it, machines not only collect and analyze information about the surrounding environment, but also take action with a view to reaching the expected objective. Based on observations and experience, some AI systems will be able to adapt their behaviour to the surroundings and act autonomously[10]. However, the Artificial Intelligence Act does not apply if AI systems are placed on the market, put into service, or used with or without modification of such systems solely for military, defence or national security purposes, regardless of which type of entity is carrying out those activities. Given the above, if specified AI systems are not used solely for the purpose of providing security (including military security) but also for other types of activities, they fall within the scope of the Act, as its objective is to enhance the functioning of the internal market and to promote the uptake of human centric and trustworthy artificial intelligence. Therefore, in certain cases, it will determine artificial intelligence operations in the sphere of security. Legislators (including at the European Union level) should regulate the issues of applying artificial intelligence in the sphere of security, which would allow improved protection against threats, including those that may disrupt the proper functioning of the EU internal market or of individual states, thus compromising their security.

To be more specific, we can illustrate an application of the AI Act for facial recognition software[11]. This usage may be classified

---

ligence Act) (OJ EU L 2024/1689). At the European level, an approach that assumes human supremacy over artificial intelligence has been adopted; M. Dziedzic, *Zastosowanie systemów sztucznej inteligencji we współczesnej bankowości*, "Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2022, No. 1, p. 76.

[10] K. Kaczmarek, *Sztuczna inteligencja*, in: *Leksykon cyberbezpieczeństwa*, K. Chałubińska-Jentkiewicz (ed.), Warszawa 2024, pp. 251–252. For additional information about artificial intelligence, refer to: K. Różanowski, *Sztuczna inteligencja: rozwój, szanse i zagrożenia*, "Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2007, No. 2, pp. 109–135; T. Gergelewicz, *Bipolarity of Artificial Intelligence – Chances and Threats*, "Ius et Securitas" 2024, No. 2.

[11] M. Mueck, C. Gaie, *European Digital Regulations*, https://link.springer.com/book/9783031808081 (access: 03.02.2025).

as a "high-risk AI system" as it could lead to significant societal impacts, such as discrimination, or restrictions on fundamental rights. To mitigate these risks, the AI Act mandates specific requirements. These include the use of high-quality datasets free from bias and representative of the population. Human oversight and intervention throughout the process are essential, as is ensuring transparency and explainability in the system's decision-making. Moreover, robust data protection measures are crucial to safeguard personal data. Finally, data retention periods must be carefully considered to fulfil citizens' rights and ensure trust and acceptability of the system.

As the objective of this paper is to analyze the possibility to use artificial intelligence in the sphere of security (including in legal terms), the doctrinal legal research method was applied here. With this method, the normative aspects of using artificial intelligence in the security setting have been indicated. The law theory method served as a tool for analyzing the views expressed by legal commentators on the subject-matter being discussed here.

1. The application of artificial intelligence in the sphere of security

1.1. AI in intelligence gathering and analysis

The ever-changing international relations, which seem to be increasingly complex, pose new strategic challenges (including those of a military nature) that individual states need to face, which is also related to technological advancement[12].

As the context is rapidly evolving, it requires the collection and analysis of a very large amount of data from multiple sources. This translates into the combination of information from open-source intelligence, signals and communication exchanges, human production, or for example imagery. The incredible diver-

[12] A. Biffi, *L'importanza di una filiera industriale nazionale per la cyber security*, "Sicurezza, Terrorismo e Società" 2024, No. 19, p. 130.

sity of data sources makes traditional manual methods inapplicable due to the sheer volume of data and its rapid change. This necessitates the use of AI-based systems to process and organize the information[13].

Artificial intelligence algorithms may effectively search vast intelligence databases, which facilitates prompt acquisition of information. Indeed, AI-based solutions offer numerous innovations that enhance data structuring, accelerate data access and combination, and improve human-computer interaction for better request understanding. Key methods include supervised and unsupervised machine learning, reasoning methods, optimization techniques[14], and large language model architectures[15].

They provide the possibility to quickly analyze such data, which allows a better understanding of opponents' intentions and actions, and the opportunity to predict their attacks. Indeed, AI-based systems offer the opportunity to analyze historical data, identify emerging trends, integrate real-time information, and develop predictive models of adversary behavior. This facilitates proactive threat assessment and enables preemptive measures to mitigate potential risks, replacing former reactive approaches[16].

Autonomous systems may support operations with reduced human involvement, which transforms both the combat strategy and ethics[17]. For instance, unmanned aerial vehicles (UAVs) equipped with AI can autonomously collect imagery and other

---

[13] S.M. Nazmuz Sakib, *Cyber Threat Intelligence*, https://typeset.io/institutions/dhaka-international-university-2sg59nna?paper_page=20 (access: 04.02.2025).

[14] A.M. Rahmani, E. Azhir, S. Ali, M. Mohammadi, O.H. Ahmed, M. Yassin Ghafour, S. Hasan Ahmed, M. Hosseinzadeh, *Artificial intelligence approaches and mechanisms for big data analytics: a systematic study*, "PeerJ Computer Science" 2021, No. 7, doi: 10.7717/peerj-cs.488.

[15] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A.N. Gomez, Ł. Kaiser, I. Polosukhin, *Attention is all you need*, in: *Proceedings of the 31st International Conference on Neural Information Processing Systems*, New York 2017.

[16] S. Balantrapu, *AI for Predictive Cyber Threat Intelligence*, "International Journal of Management Education for Sustainable Development" 2024, No. 7.

[17] A. Prus, *Uwarunkowania wykorzystania sztucznej inteligencji w przyszłej wojnie*, "Cybersecurity and Law" 2024, No. 2, pp. 57–58.

data, providing real-time situational awareness to operators[18]. This offers the opportunity to reduce the risks for human personnel during many reconnaissance missions and allows for a potential increase in firepower to ensure a higher probability of target engagement against the enemy.

1.2. AI and the need for digital competencies

The use of artificial intelligence systems (also by the security sector) requires appropriate competences, including digital skills. Such competences allow optimal and responsible application of state-of-the-art tools. The inability to handle artificial intelligence may result in numerous threats, including potential external interference in security systems, and easier attacks against such systems.

Indeed, the lack of AI skills may result in risky behaviours such as using online generative AI to obtain recommendations that could compromise secret services or sensitive information. Moreover, a compromised generative AI could generate code or information that would be added to the secure system and create a breach. This necessitates a strict approach to the usage of new systems, especially those that are not built and maintained within the organization and that utilize novel, low-trust, or unmastered technologies with a high capacity for masking attacks and exploiting vulnerabilities[19]. Furthermore, organizations must be especially aware of the dangers posed by offensive AI approaches[20].

---

[18] S. Sai, A. Garg, K. Jhawar, V. Chamola, B. Sikdar, *A Comprehensive Survey on Artificial Intelligence for Unmanned Aerial Vehicles*, "IEEE" 2023, No. 4, pp. 713–738, doi:10.1109/OJVT.2023.3316181.

[19] K. Wach, C.D. Duong, J. Ejdys, R. Kazlauskaitė, P. Korzynski, G. Mazurek, J. Paliszkiewicz, E. Ziemba, *The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT*, "Entrepreneurial Business and Economics Review" 2023, No. 2, pp. 7–30, doi: 10.15678/EBER.2023.110201.

[20] Y. Mirsky, A. Demontis, J. Kotak, R. Shankar, D. Gelei, L. Yang, X. Zhang, M. Pintor, W. Lee, Y. Elovici, B. Biggio, *The threat of offensive AI to organizations*, "Computers & Security" 2022, No. 124, p. 103006, doi: 10.1016/j.cose.2022.103006.

AI systems themselves can be targets for cyberattacks. If compromised, they could be manipulated to make incorrect decisions, leak sensitive data, or even be used to disrupt critical government services. This highlights the importance of developing specific skills to build, maintain, and protect AI software. Dedicated agents should understand precisely the underlying theory to identify potential inconsistencies in data and system configuration. These specialists should reserve a portion of their work to verify the proper functioning of AI systems, correct potential deviations, and alert in case of suspicious behaviours.

Digital competences allow proper use of information and communication technology (ICT) tools which are essential in various spheres of contemporary social and professional life. Due to the development of new technologies, the ability to use such tools is indispensable, as these technologies provide opportunities for growth, and determine progress in numerous areas. The acquisition and refinement of competences of this form not only enable the optimum use of services available in cyberspace, but also contribute to reducing digital exclusion[21].

As a matter of fact, the lack of digital competencies can exacerbate existing societal inequalities and create new forms of exclusion. In the context of AI, this can manifest as unequal access to AI-powered services. Conversely, AI could also mitigate these risks if access, affordability, and digital literacy are addressed[22]. Like any innovation, AI-powered systems carry both opportunities and threats. The successful integration of AI into final solutions

---

[21] C. Gaie, M. Karpiuk, A. Spaziani, *Cybersecurity in France, Poland and Italy*, "Studia Iuridica Lublinensia"2025, No. 1. As regards qualifications of cyber soldiers, they should have knowledge of building safe ICT systems, identifying vulnerabilities and taking appropriate actions to eliminate them, as well as keeping pace with the operating methods of cyber criminals. They should also know how to remotely impact on resources belonging to foreign entities: A.E. Patkowski, *Walka w cyberprzestrzeni. Refleksje po przeglądzie incydentów*, in: *Metody i narzędzia w procesie tworzenia cyberzdolności – wyzwania i perspektywy*, Warszawa 2022, p. 82.

[22] S. Park, J. Humphry, *Exclusion by design: intersections of social, digital and data exclusion*, "Information Communication & Society" 2019, No. 7, pp. 934–953, doi: 10.1080/1369118x.2019.1606266.

depends heavily on IT workers who pay attention to the skills and needs of the end users.

1.3. AI and cybersecurity in the public sector

The use of artificial intelligence in the sphere of security for better protection against threats, including those that may affect the normal functioning of a state, is related to the issue of cybersecurity. A number of tasks, such as those related to the assurance of security, are currently performed in cyberspace, hence they need to be provided with relevant protection. This sphere of security is also a public sphere wherein authorities have specified obligations in respect of assuring the quality of its functioning.

According to EU lawmakers, cybersecurity should be understood as activities necessary to protect networks and information systems, their users, and other individuals from cyber threats[23]. Artificial intelligence can disrupt and protect these activities, depending on its purpose. If cyberattacks are carried out through it, it will undermine cybersecurity, but it can also prevent such attacks. In particular, it can be used to violate privacy, including the theft of data stored in electronic systems. Artificial intelligence operates in cyberspace, significantly affecting it. On the one hand, it facilitates the provision of various electronic services, but its use can also be fraught with risk. Artificial intelligence should play a significant role in ensuring the protection of strategic sectors that rely heavily

[23] Article 2 (1) regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) (OJ L 151, 7.6.2019, pp. 15–69). Cybersecurity is a special type of security, perceived through the prism of order and structure located in cyberspace, D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzmiincydentysieciowe*, "Prawo w Działaniu" 2023, No. 53, p. 103. On the definition of cybersecurity, see also G. Szpor, *The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland*, "Review of European and Comparative Law" 2021, No. 3, pp. 223–226.

on ICT systems. It can also support the operation of critical infrastructure, including its protection against cyber threats.

Government services have a strong need to build and deploy artificial intelligence to enhance the security of their procedures and digital services. AI can facilitate the detection of intrusions or attacks[24], identify vulnerabilities and propose corrections, or improve data protection[25]. This effort is crucial for success as the number of adversaries is growing and their capabilities are increasing. They do not hesitate to use AI to make illicit gains.

Moreover, the effective fulfilment of societal needs should be treated as a mission that should be overseen and enacted by public sector institutions. Such entities are increasingly often using ICT systems to perform their public tasks. These systems not only streamline the completion of public tasks but also allow cost reduction or make it possible to reach a wider group of recipients over a relatively short time. The public sector is a factor that stimulates the process of providing social services, while compelling specified behaviour of process participants[26]. Security (including cybersecurity) occupies a special place in this sector, as it is of great significance both to the state and to society, and today is one of fundamental human needs.

As a consequence, the public sector increasingly relies on ICT systems, notably those incorporating AI. These systems present both significant opportunities and challenges[27]. While AI can

---

[24] J. Langlois-Berthelot, C. Gaie, J.F. Lebraty, *Epidemiology Inspired Cybersecurity Threats Forecasting Models Applied to e-Government*, in: *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, C. Gaie, M. Mehta (eds.), Cham 2024, doi: 10.1007/978-3-031-55575-6_6; A.H. Salem, S.M. Azzam, O.E. Emam, A.A. Abohany, *Advancing cybersecurity: a comprehensive review of AI-driven detection techniques*, "Journal Big Data" 2024, No. 11, p. 105, doi: 10.1186/s40537-024-00957-y.

[25] N.G. Camacho, *The Role of AI in Cybersecurity: Addressing Threats in the Digital Age*, "Journal of Artificial Intelligence General Science" 2024, No. 1, pp. 143–154, doi: 10.60087/jaigs.v3i1.75.

[26] M. Karpiuk, C. Melchior, U. Soler, *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, No. 4, p. 8, doi: 10.36128/PRIW.VI47.751.

[27] R. Kaur, D. Gabrijelčič, T. Klobučar, *Artificial intelligence for cybersecurity: Literature review and future research directions*, "Information Fusion" 2023, No. 97, p. 101804, doi: 10.1016/j.inffus.2023.101804.

enhance service delivery, improve efficiency, and reduce costs, it also introduces new vulnerabilities and risks. Public sector organizations must therefore prioritize the development of a strong cybersecurity posture, including robust risk assessments, effective threat intelligence, and a skilled workforce capable of managing and mitigating these risks[28].

Particular attention should be paid to the trust in the answers provided by AI systems to avoid loss of credibility. Removing online solutions in case of doubt, as demonstrated by the French AI chatbot Lucie, is a good practice to maintain trust with citizens[29]. This proactive approach ensures that citizens' trust in government services is not eroded by inaccurate or misleading information provided by AI.

1.4. Cybersecurity in the information society

The definition of significance of cybersecurity for the information society requires a multidimensional analysis, as part of which, in addition to ICT infrastructure and digital skills, a number of factors should be taken into consideration, including, for instance, the security environment and international situation[30].

The absence of territorial limitations is one of cyberspace's advantages that allows its use in combat operations. What is also important is the vast information pool that can be acquired or destroyed while remaining anonymous and concealing the methods being applied, which greatly reduces the possibility of real-time

---

[28] H. Qin, Z. Li, *A Study on Enhancing Government Efficiency and Public Trust: The Transformative Role of Artificial Intelligence and Large Language Models*, "International Journal of Engineering and Management Research" 2024, No. 3, pp. 57–61, doi: 10.5281/zenodo.12619360.

[29] J. Guy, *French AI chatbot taken offline after wild answers led to online ridicule*, CNN, January 27, 2025.

[30] K. Kaczmarek, M. Karpiuk, C. Melchior, *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, No. 3, pp. 105–106, doi: 10.36128/PRIW.VI50.907.

defence or retaliation[31]. Such activities may also be supported by artificial intelligence. Given that combat operations conducted in cyberspace may greatly hinder the functioning of the state, cybersecurity issues should be given serious consideration.

As a matter of fact, the level of threat has risen significantly in recent years with numerous attacks perpetrated by groups affiliated with adversarial states. For example, Russian cyber groups are suspected of recently attacking Sweden, disrupting the work of 60,000 civil servants and 120 government services through a ransomware attack[32]. This exemplifies the increasing sophistication of attacks, whereas former attacks primarily relied on classic distributed denial of service (DDoS) methods[33].

Meanwhile, cyberattacks are generating increasing impacts since domains are increasingly digitalized and interconnected. Governments should defend themselves to ensure the functioning of critical services such as the Armies, the Hospital and Medical System, the Tax Administration, or the Education sector, but also sectors of high criticality as described in the NIS2 Directive[34]. This corresponds to fundamental private services such as energy, alimentation, banking or transportation.

Thus, as regards information societies and digital states, where the access to electronic services is universal, cybersecurity is particularly vital, because it ensures both uninterrupted communication and the functioning of strategic sectors. Cybersecurity

---

[31] M. Stolarz, *Cyberprzestrzeń w wojnie hybrydowej*, in: M. Marczyk, M. Stolarz, B. Terebiński, *Działania hybrydowe a bezpieczeństwo sieci i systemów teleinformatycznych w SZ RP – wybrane aspekty*, M. Marczyk, M. Stolarz, B. Terebiński (eds.), Warszawa 2021, p. 47.

[32] J.D. Cruz, *Russian hackers allegedly behind Sweden ransomware attack. Tech Times*, https://www.techtimes.com/articles/300934/20240124/russian-hackers-allegedly-behind-sweden-ransomware-attack.htm (access: 01.02.2025).

[33] P. Idengren, *Cybersecurity and the resilience measures in critical infrastructure in Sweden: A comparative desk study between Sweden and the United States*, https://lnu.diva-portal.org/smash/record.jsf?pid=diva2%3A1867013&dswid=286,1 (access: 04.02.2025).

[34] C. Gaie, M. Mueck, *Introduction to the Networks and Information Systems 2 (NIS2) Directive*, in: *European Digital Regulations. Artificial Intelligence-Enhanced Software and Systems Engineering*, M. Mueck, C. Gaie (eds.), Cham 2025.

ensures protection against threats occurring in cyberspace, and, for that reason, it assures the normal operations of the state as a public entity which employs ICT systems to perform their tasks[35].

To effectively enforce cybersecurity, several critical measures must be implemented. These include: transposing European directives into national legislation, identifying a dedicated government service to lead cybersecurity efforts, providing support and guidance to both public and private sectors in achieving cybersecurity goals, and ensuring active involvement from IT departments within all relevant organizations. Furthermore, accelerating cybersecurity adoption requires a high-level political sponsor to champion these initiatives, encourage collaboration between public and private entities, and invest in developing a robust cybersecurity ecosystem[36]. This includes creating a skilled cybersecurity workforce, fostering innovation in cybersecurity technologies and software, and finally positioning cybersecurity as a key economic sector that mitigates the costs and consequences of cyberattacks.

1.5. Technological advancements and cybersecurity

Investments in advanced technologies, including in the sphere of cybersecurity, are necessary to improve the capabilities to detect and respond to incidents. Such technologies allow timely identification and elimination of threats, mitigating the risk that significant damage might occur[37]. The financial expenses and investments in protecting critical services against the exponential increase in

---

[35] M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, No. 2, p. 190, doi: 10.17951/sil.2023.32.2.189-201.

[36] I Vasiu, L. Vasiu, *Cybersecurity as an Essential Sustainable Economic Development Factor*, "European Journal of Sustainable Development" 2018, No. 4, pp. 171–178.

[37] G.L. Macca, *Evoluzione della cybersicurezza in Italia tra sfide e opportunità del recepimento delle Direttive Europee NIS2 e CER, nell'era delle minacce ibride e della Sicurezza convergente. Intervista*, "Sicurezza, Terrorismo e Società" 2024, No. 19, p. 188.

security attacks are estimated at $220 billion in 2025[38] and will likely continue to grow drastically in the following years. There is indeed significant awareness of the potential for AI-based attacks to completely disrupt services, resulting in substantial costs due to service interruption, data loss, and remediation efforts. Moreover, the increasing reliance on AI services necessitates a focus on improving their inherent security.

Disruptions taking place in cyberspace might have a negative effect on society and on the functioning of the state which is obliged to ensure appropriate quality of the services it provides, including also services of strategic importance. Given the need to properly secure such services, which embraces the assurance of their continuity and availability, it is necessary to adopt relevant supervisory measures[39]. To this end, a combination of complementary approaches can be employed, including regulation established by regional regulators or standardization bodies; the designation of an organization responsible for the operational supervision and enforcement of these regulations; the establishment of collaboration between public and private services to ensure efficient information exchange; and support to increase understanding of the regulations and ensure their applicability.

Artificial intelligence provides a broader spectrum of possibilities for the perpetrators of cyberattacks who will potentially be able to rely on pre-defined algorithms[40]. Therefore, it is necessary to inspect ICT systems used for security assurance on an ongoing basis, in terms of their resilience to cyberattacks that could disrupt their proper operation. For example, the analysis should focus on protecting internal systems against adversarial attacks,

---

[38] S. Balasubramanian, *2025 will be a huge year for the $220 billion dollar cybersecurity industry*, https://www.forbes.com/sites/saibala/2025/01/10/2025-will-be-a-huge-year-for-the-220-billion-dollar-cybersecurity-industry/ (access: 04.02.2025).

[39] M. Karpiuk, *Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, No. 4, pp. 167–168, doi: 10.36128/priw.vi42.524.

[40] J. Kostrubiec, *Sztuczna inteligencja a prawa i wolności człowieka*, Warszawa 2021, p. 22.

avoiding data poisoning[41] by preventing data modification that could corrupt AI models, and defending AI models against theft for malicious purposes[42].

1.6. AI in military cybersecurity

The application of artificial intelligence to protect cybersecurity, including in the military dimension, may not only contribute to combating cyberattacks, but also to predicting and repelling them, as well as to quickly eliminating their effects. Artificial intelligence used in the defence sphere can greatly secure the state defence system, provided that it is applied properly.

Artificial intelligence can play a major role in many military domains. For example, it can facilitate the development and coordination of drones[43], optimize missile guidance for offensive or defensive purposes[44], and increase the amount of information gathered for military intelligence[45]. Consequently, AI is a key concern when envisioning the future of warfare, as it will considerably alter the battlefield landscape. Traditional soldiers will be augmented by new equipment, weapons, and perhaps accompanied by autonomous systems with offensive capabilities.

New technologies open up opportunities that allow armed forces to optimize their operations, which also includes shaping

---

[41] C. Hu, Y. Hu, *Data Poisoning on Deep Learning Models*, in:*2020 International Conference on Computational Science and Computational Intelligence*, Las Vegas 2020, pp. 628–632, doi: 10.1109/CSCI51800.2020.00111.

[42] S. Kariyappa, M.K. Qureshi, *Defending against model stealing attacks with adaptive misinformation*, https://openaccess.thecvf.com/content_CVPR_2020/html/Kariyappa_Defending_Against_Model_Stealing_Attacks_With_Adaptive_Misinformation_CVPR_2020_paper.html (access: 04.02.2025).

[43] J. Johnson, *Artificial intelligence, drone swarming and escalation risks in future warfare*, "The RUSI Journal" 2020, No. 2, pp. 26–36.

[44] B.S. Haney, *Applied artificial intelligence in modern warfare and national security policy*, "Hastings Sci & Tech" 2020, No. 11, p. 61.

[45] S. Cho,W. Shin, N. Kim, J. Jeong, *In HP. Priority Determination to Apply Artificial Intelligence Technology in Military Intelligence Areas*, "Electronics" 2020, No. 9, p. 2187, doi: 10.3390/electronics9122187.

new properties and capabilities in the sphere of reconnaissance, destruction, command, operational support, and logistic support. Given the above, to seize this opportunity for development, the armed forces need to be open to change, including to the implementation of innovative solutions[46]. A key factor in future battles will not be simply maximizing innovation, but rather determining the optimal equipment mix for victory. Typical questions to consider include: Given a budget of 100, should it be divided proportionally among personnel equipment, ICT, and weapons, or should it be concentrated on weapons development? Is my AI strategy effective against major powers as well as smaller nations? Does my AI strategy support operations on my own territory as well as foreign deployments? These complex questions can only be answered by experienced military leaders, not by AI itself, which remains a tool to help decisionmakers.

As for implementing innovative solutions in the military sphere, the armed forces should be open to artificial intelligence that may become a great support in many aspects of their operations. However, there should be no space for unreflective implementation of artificial intelligence systems or their uncontrolled use, since, due to the essence of tasks entrusted to the army in the sphere of military security, AI-supported activities should be supervised on a continuous basis.

Control over the development and deployment processes is essential to ensure that AI solutions are not compromised by adversaries and cannot turn against the armed forces, whether through malfunction or deliberate sabotage at the start of hostilities[47]. Therefore, continuous monitoring and evaluation of AI systems are crucial to identify and mitigate potential risks. This includes regular testing and auditing of AI algorithms, assessing their performance, and identifying potential biases. Further-

---

[46] M.M. Fryc, *Nowoczesne technologie kształtujące rozwój sił zbrojnych i ich operacyjne użycie do 2039 roku*, "Bezpieczeństwo Narodowe" 2023, No. 42, p. 183.

[47] R. Waheeb, *AI Control*, https://ssrn.com/abstract=4497462 (access: 04.02.2025).

more, maintaining human oversight and control over critical decision-making processes is vital, ensuring that AI systems augment human capabilities rather than replacing them[48]. This "human-in-the-loop" approach is crucial for maintaining accountability and ensuring that AI systems are used responsibly and ethically in military applications.

1.7. Ethical considerations and human rights

The implementation of artificial intelligence tools must be accompanied by the due protection of human rights and freedoms. Each instance of restricting individual rights and freedoms should be treated on a case-by-case basis, taking into account the existing circumstances each time. Such restrictions cannot result in the infringement of human dignity, which might occur if they are not proportional to the objective to be reached through such measures[49].

Developing and deploying AI systems presents well-known challenges to ensure ethical considerations are met. For example, training data plays a significant role in how AI systems make decisions. A recruitment procedure or promotion pre-selection process, based on historical data, may perpetuate existing gender imbalances. One way to mitigate this is by removing gender considerations from the decision-making process itself[50]. Additional

---

[48] I. Verdiesen, A. Tubella, V. Dignum, *Integrating Comprehensive Human Oversight in Drone Deployment: A Conceptual Framework Applied to the Case of Military Surveillance Drones*, "Information" 2021, No. 9, p. 385, doi: 10.3390/info12090385.

[49] M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, No. 3, p. 32, doi: 10.17951/sil.2022.31.3.31-43. See: R. Kostrubiec, *Dopuszczalne ograniczenia prawa do swobodnego, pokojowego zgromadzania się w systemie praw człowieka*, Zamość 2024, p. 23; M. Czuryk, *Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd*, "Studia z Prawa Wyznaniowego" 2024, No. 27, p. 158, doi: 10.31743/spw.17518.

[50] L. Bao, D. Huang, C. Lin, *Can Artificial Intelligence Improve Gender Equality? Evidence from a Natural Experiment*, "Management Science" 2024, No. 11, doi: 10.1287/mnsc.2022.02787.

measures could also be integrated into AI systems to promote greater equality, such as actively recruiting women for IT roles, men for HR positions, and promoting individuals with disabilities.

Another key aspect of ensuring ethical AI deployment is transparency and explainability. When the decision-making process is transparent, users can review it, verify its fairness, and, if necessary, request a review[51]. Therefore, users should have a clear understanding of how AI systems arrive at decisions and the factors that influence their outputs. This requires developing methods to explain the reasoning behind AI decisions in a human-understandable way. Furthermore, mechanisms for human oversight and intervention are essential to ensure that AI systems are used responsibly and ethically, and that human values and rights are protected.

Disinformation also has an impact on security. Artificial intelligence can also be used in this area. The advent of artificial intelligence (AI) has led to a significant escalation in the effectiveness and pervasiveness of the creation of disinformation, largely attributable to the development of advanced technologies such as generative adversarial networks (GANs) and large language models (LLMs). These tools have enabled the production of synthetic content, including the well-known deepfakes, which are realistic simulations of images, video, or audio, often difficult to distinguish from reality. A notable instance of this is the use of deepfakes to manipulate videos of political leaders, as discussed by T.C. Helmus, which can erode public trust and influence the outcomes of democratic elections[52]. In a similar vein, G. Spitale et al. have highlighted that texts generated by GPT-3 are often perceived as more credible than those produced by humans, further complicating the discernment of authentic from manipulated content by the public[53]. Another critical dimension of misinformation is

---

[51] J.A. McDermid, Y. Jia, Z. Porter, I. Habli, *Artificial intelligence explainability: the technical and ethical dimensions*, "Philosophical Transactions of the Royal Society" 2021, No. 379, p. 20200363.

[52] T.C. Helmus, *Artificial intelligence, deepfakes, and disinformation*, https://www.jstor.org/stable/resrep42027 (access: 02.02.2025).

[53] G. Spitale, N. Biller-Andorno, F. Germani, *AI model GPT-3 (dis)informs us better than humans*, "Science Advances" 2023, No. 9.

personalized content, which refers to content tailored to the specific characteristics of an individual or group. K. Kertysova analyzed how AI can be used for micro-targeting, conveying messages tailored to specific demographic or political groups, amplifying social polarisation and political divisions[54]. The impact of such techniques is not limited to the manipulation of public opinion, but calls into question the legitimacy of democratic institutions, fuelling mistrust and confusion. A particularly insidious risk is the so-called "liar's dividend": the mere fact that it is possible to create deepfakes allows anyone to question authentic content, eroding collective trust in the media and reality itself[55].

2. Conclusions

The use of artificial intelligence in the sphere of security (similarly to other areas of public and private activities) should evolve to become standard practice. The development of technologies, including the use of state-of-the-art tools, AI being one of them, is also necessary in the security environment. Due to the dynamics and diversity of threats, including attacks launched with the use of cyberspace, we may become more effective in assuring security if artificial intelligence systems support us in the fulfilment of this objective.

Artificial intelligence might contribute to increasing the effectiveness of military operations, minimizing casualties among soldiers and civilian population, and improving the precision of operations. However, it is important to apply it in a responsible manner, without violating ethical rules and human rights. The introduction of autonomous weapon systems poses a risk of losing control over decisions taken in conflict situations. It should be borne in mind, however, that the threats related to the possibility of attacks

---

[54] K. Kertysova, *Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered*, "Security and Human Rights" 2018, No. 29, pp. 64–65.

[55] B. Chesney, D. Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, "California Law Review" 2019, No. 107, pp. 1753–1820.

or manipulation regarding artificial intelligence algorithms may give rise to some grave consequences to security. Moreover, the use of advanced AI technologies might lead to inequalities between individual states. It might also transform the nature of conflicts in relation to putting in place new strategies, tactics or technologies[56]. It should be stressed that artificial intelligence provides great opportunities in the sphere of conducting military operations and might contribute to gaining advantage by the conflict party that has turned to such tools.

The absence of legal regulations governing the use of artificial intelligence in the sphere of security is notable. This does not favour the proper application of new technologies as a barrier protecting us against threats. No entity using artificial intelligence tools for security purposes can be certain that they would not be held accountable for abusing their powers. In the age of new technologies and attempts to use them to destabilize states and their institutions, there is a need for clear-cut legal regulations, allowing for measures to counteract such actions and to remove their effects with the use of artificial intelligence. Entities using artificial intelligence tools in the sphere of security need to know how and when to deploy them, and what responsibility is imposed on them on that account.

The capabilities of artificial intelligence in respect of support for analytical work and decision-making processes should also be used in the security environment[57]. Government policy, military doctrine and tactical directives can be used to control AI capabilities in the military sphere, and may limit such use by the armed forces, where it is felt necessary[58].

When using artificial intelligence as a support tool rather than a security threat, attention should be paid to education that allows individuals to acquire the appropriate competencies to responsi-

---

[56] A. Prus, *Uwarunkowania*, p. 64.

[57] M. Ciesielski, *Możliwości wykorzystania sztucznej inteligencji w analizie bezpieczeństwa*, "Journal of Modern Science" 2024, No. 6, p. 697.

[58] K. Eble, *Artificial Intelligence in Military Operations – Experiences and Challenges. British Perspective*, "Cybersecurity and Law" 2024, No. 1, p. 102.

bly make decisions related to the use of this technology. Without adequate knowledge on the safe use of artificial intelligence, it will pose a risk to both users and the IT systems themselves. Competencies related to the use of new technologies (including artificial intelligence) must be possessed by individuals operating in both the private and public sectors; their lack poses a significant threat, potentially exposing both the state and private sector entities to significant losses.

It is also worth noting that artificial intelligence impacts everyday life as well as the job market. Its dynamic development has simplified life in many areas. It is widely used in many areas of life, streamlining everyday tasks that can be performed not only faster, but also more cheaply using AI systems. Using these tools significantly improves quality of life. However, it is important to remember that improper use can cause significant harm.

SUMMARY

Artificial intelligence in the sphere of security

Nowadays, artificial intelligence is used in various spheres of life, including state operations. Security is one of such domains. New technologies should be used universally across the entire sphere of security. This also applies to artificial intelligence which allows us not only to respond to existing threats but also to anticipate and prevent them (i.a., through the analysis of large data sets over a short time). However, artificial intelligence should be applied in a responsible manner, so that its use does not constitute threats to security but rather contributes to its protection.

The objective of this paper is to analyze the possibility to apply artificial intelligence in the security environment that needs to be open to new solutions, so that it is possible to protect our societies and states more effectively than at present. The author's thesis can be expressed in the statement that artificial intelligence may contribute to security enhancement, provided that it is used responsibly and is properly supervised. This paper is based on the doctrinal legal research method and the law theory method.

Keywords: artificial intelligence; security; cybersecurity

STRESZCZENIE

Sztuczna inteligencja w sferze bezpieczeństwa

Sztuczna inteligencja współcześnie jest wykorzystywana w wielu sferach życia, jak i działalności państwa. Jedną z takich sfer jest bezpieczeństwo. Nowe technologie w sferze bezpieczeństwa powinny być stosowane powszechnie. Powinna być też wykorzystywana sztuczna inteligencja, która pozwala nie tylko na reakcję na już istniejące zagrożenie, ale też (m.in. przez analizę dużej ilości danych w stosunkowo krótkim czasie) na ich przewidywanie i im zapobieganie. Musi być ona jednak stosowana odpowiedzialnie, aby jej wykorzystanie nie stanowiło zagrożenia dla bezpieczeństwa, a je chroniło.

Celem artykułu jest przeprowadzenie analizy możliwości wykorzystania sztucznej inteligencji w środowisku bezpieczeństwa, które musi być otwarte na nowe rozwiązania, aby można było skuteczniej chronić społeczeństwo i państwo. Jako tezę należy przyjąć stwierdzenie, że sztuczna inteligencja może sprzyjać poprawie bezpieczeństwa, pod warunkiem, że będzie odpowiedzialnie wykorzystywana oraz odpowiednio nadzorowana. W artykule wykorzystano metodę dogmatyczno-prawną, a także metodę teoretyczno-prawną.

Słowa kluczowe: sztuczna inteligencja; bezpieczeństwo; cyberbezpieczeństwo

BIBLIOGRAPHY

Balantrapu S., *AI for Predictive Cyber Threat Intelligence*, "International Journal of Management Education for Sustainable Development" 2024, No. 7.

Bao L., Huang D., Lin C., *Can Artificial Intelligence Improve Gender Equality? Evidence from a Natural Experiment*, "Management Science" 2024, No. 11, doi: 10.1287/mnsc.2022.02787.

Biffi A., *L'importanza di una filiera industriale nazionale per la cyber security*, "Sicurezza, Terrorismo e Società" 2024, No. 19.

Bistron M., Piotrowski Z., *Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens*, "Electronics" 2021, No. 7, doi: 10.3390/electronics10070871.

Bolc L., Cytowski J., *Search methods for artificial intelligence*, San Diego 1992.

Camacho N.G., *The Role of AI in Cybersecurity: Addressing Threats in the Digital Age*, "Journal of Artificial Intelligence General Science" 2024, No. 1, doi: 10.60087/jaigs.v3i1.75.

Chesney B., Citron D., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, "California Law Review" 2019, No. 107.

Cho S., Shin W., Kim N., Jeong J., *In HP. Priority Determination to Apply Artificial Intelligence Technology in Military Intelligence Areas*, "Electronics" 2020, No. 9, doi: 10.3390/electronics9122187.

Ciesielski M., *Możliwości wykorzystania sztucznej inteligencji w analizie bezpieczeństwa*, "Journal of Modern Science" 2024, No. 6.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, "Zeszyty Naukowe KUL" 2018, No. 3.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, No. 5.

Czuryk M., *Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd*, "Studia z Prawa Wyznaniowego" 2024, No. 27, doi: 10.31743/spw.17518.

Czuryk M., *Jurisdiction of the Voivode in the Field of Crisis Management*, "Studia Iuridica Lublinensia" 2025, No. 2, doi: 10.17951/sil.2025.34.2.87-98.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, No. 3, doi: 10.17951/sil.2022.31.3.31-43.

Dakalbab F., Talib M.A, Waraga O.A, Nassif A.B., Abbas S., Nasir Q., *Artificial intelligence & crime prediction: A systematic literature review*, "Social Sciences & Humanities Open" 2022, No. 1, doi: 10.1016/j.ssaho.2022.100342.

Dziedzic M., *Zastosowanie systemów sztucznej inteligencji we współczesnej bankowości*, "Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2022, No. 1.

Eble K., *Artificial Intelligence in Military Operations – Experiences and Challenges. British Perspective*, "Cybersecurity and Law" 2024, No. 1.

Fryc M.M., *Nowoczesne technologie kształtujące rozwój sił zbrojnych i ich operacyjne użycie do 2039 roku*, "Bezpieczeństwo Narodowe" 2023, No. 42.

Gaie C., Karpiuk M., Spaziani A., *Cybersecurity in France, Poland and Italy*, "Studia Iuridica Lublinensia" 2025, No. 1.

Gaie C., Mueck M., *Introduction to the Networks and Information Systems 2 (NIS2) Directive*, in: *European Digital Regulations. Artificial*

Intelligence-Enhanced Software and Systems Engineering, M. Mueck, C. Gaie (eds.), Cham 2025.

Gergelewicz T., *Bipolarity of Artificial Intelligence – Chances and Threats*, "Ius et Securitas" 2024, No. 2.

Haney B.S., *Applied artificial intelligence in modern warfare and national security policy*, "Hastings Sci & Tech" 2020, No. 11.

Hu C., Hu Y., *Data Poisoning on Deep Learning Models*, in: *2020 International Conference on Computational Science and Computational Intelligence*, Las Vegas 2020.

Ige T., Kolade A., Kolade O., *Enhancing Border Security and Countering Terrorism Through Computer Vision: A Field of Artificial Intelligence*, in: *Data Science and Algorithms in Systems*, R. Silhavy, P. Silhavy, Z. Prokopova (eds.), Cham 2023.

Johnson J., *Artificial intelligence, drone swarming and escalation risks in future warfare*, "The RUSI Journal" 2020, No. 2.

Kaczmarek K., *Bezpieczeństwo państwa wobec współczesnych zagrożeń*, „Prawo I Więź" 2025, No. 5, doi: 10.36128/PRIW.VI58.1382.

Kaczmarek K., Karpiuk M., Melchior C., *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, No. 3, doi: 10.36128/PRIW.VI50.907.

Kaczmarek K., *Sztuczna inteligencja*, in: *Leksykon cyberbezpieczeństwa*, K. Chałubińska-Jentkiewicz (ed.), Warszawa 2024.

Kaczmarek K., Włodyka E.M., Czuryk M., *The Status of Government Administration Management in the Sphere of Crisis Management*, "Prawo i Więź" 2025, No. 6, doi: 10.36128/48wmzt46.

Kaczmarek K., *Wpływ zmian klimatycznych na bezpieczeństwo*, "Journal of Modern Science" 2024, No. 4.

Karpiuk M., *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, No. 1.

Karpiuk M., Melchior C., Soler U., *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, No. 4, doi: 10.36128/PRIW.VI47.751.

Karpiuk M., *Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, No. 4, doi: 10.36128/priw.vi42.524.

Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, No. 2, p. 190, doi: 10.17951/sil.2023.32.2.189-201.

Kaur R., Gabrijelčič D., Klobučar T., *Artificial intelligence for cybersecurity: Literature review and future research directions*, "Information Fusion" 2023, No. 97, doi: 10.1016/j.inffus.2023.101804.

Kertysova K., *Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered*, "Security and Human Rights" 2018, No. 29.

Kostrubiec J., *Sztuczna inteligencja a prawa i wolności człowieka*, Warszawa 2021.

Kostrubiec R., *Dopuszczalne ograniczenia prawa do swobodnego, pokojowego zgromadzania się w systemie praw człowieka*, Zamość 2024.

Langlois-Berthelot J., Gaie C., Lebraty J.F., *Epidemiology Inspired Cybersecurity Threats Forecasting Models Applied to e-Government*, in: *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, C. Gaie, M. Mehta (eds.), Cham 2024.

Macca G.L., *Evoluzione della cybersicurezza in Italia tra sfide e opportunità del recepimento delle Direttive Europee NIS2 e CER, nell'era delle minacce ibride e della Sicurezza convergente. Intervista*, "Sicurezza, Terrorismo e Società" 2024, No. 19.

Mandalapu V., Elluri L., Vyas P., Roy N., *Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions*, "IEEE" 2023, No. 11, doi: 10.1109/ACCESS.2023.3286344.

McDermid J.A., Jia Y., Porter Z., Habli I., *Artificial intelligence explainability: the technical and ethical dimensions*, "Philosophical Transactions of the Royal Society" 2021, No. 379.

Mirsky Y., Demontis A., Kotak J., Shankar R., Gelei D., Yang L., Zhang X., Pintor M., Lee W., Elovici Y., Biggio B., *The threat of offensive AI to organizations*, "Computers & Security" 2022, No. 124, doi: 10.1016/j.cose.2022.103006.

Olech A.K., Lis A., *Technologia i terroryzm. Sztuczna inteligencja w dobie zagrożeń terrorystycznych*, Warszawa 2024.

Park S., Humphry J., *Exclusion by design: intersections of social, digital and data exclusion*, "Information Communication & Society" 2019, No. 7, doi: 10.1080/1369118x.2019.1606266.

Patkowski A.E., *Walka w cyberprzestrzeni. Refleksje po przeglądzie incydentów*, in: *Metody i narzędzia w procesie tworzenia cyberzdolności – wyzwania i perspektywy*, Warszawa 2022.

Pieczywok A., *Cyberprzestrzeń i dydaktyka cyfrowa na rzecz bezpieczeństwa człowieka*, "Cybersecurity and Law" 2024, No. 2.

Prus A., *Uwarunkowania wykorzystania sztucznej inteligencji w przyszłej wojnie*, "Cybersecurity and Law" 2024, No. 2.

Qin H., Li Z., *A Study on Enhancing Government Efficiency and Public Trust: The Transformative Role of Artificial Intelligence and Large Language Models*, "International Journal of Engineering and Management Research" 2024, No. 3, doi: 10.5281/zenodo.12619360.

Rahmani A.M., Azhir E., Ali S., Mohammadi M., Ahmed O.H., Yassin Ghafour M., Hasan Ahmed S., Hosseinzadeh M., *Artificial intelligence approaches and mechanisms for big data analytics: a systematic study*, "PeerJ Computer Science" 2021, No. 7, doi: 10.7717/peerj-cs.488.

Różanowski K., *Sztuczna inteligencja: rozwój, szanse i zagrożenia*, "Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2007, No. 2.

Sai S., Garg A., Jhawar K., Chamola V., Sikdar B., *A Comprehensive Survey on Artificial Intelligence for Unmanned Aerial Vehicles*, "IEEE" 2023, No. 4, doi: 10.1109/OJVT.2023.3316181.

Salem A.H., Azzam S.M., Emam O.E., Abohany A.A., *Advancing cybersecurity: a comprehensive review of AI-driven detection techniques*, "Journal Big Data" 2024, No. 11, doi: 10.1186/s40537-024-00957-y.

Skoczylas D., *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzmiincydentysieciowe*, "Prawo w Działaniu" 2023, No. 53.

Spitale G., Biller-Andorno N., Germani F., *AI model GPT-3 (dis)informs us better than humans*, "Science Advances" 2023, No. 9.

Stolarz M., *Cyberprzestrzeń w wojnie hybrydowej*, in: M. Marczyk, M. Stolarz, B. Terebiński, *Działania hybrydowe a bezpieczeństwo sieci i systemów teleinformatycznych w SZ RP – wybrane aspekty*, M. Marczyk, M. Stolarz, B. Terebiński (eds.), Warszawa 2021.

Sun W., Bocchini P., Davison B.D., *Applications of artificial intelligence for disaster management*, "Nat Hazards" 2020, No. 103, doi: 10.1007/s11069-020-04124-3.

Szpor G., *The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland*, „Review of European and Comparative Law" 2021, No. 3.

Vasiu I., Vasiu L., *Cybersecurity as an Essential Sustainable Economic Development Factor*, "European Journal of Sustainable Development" 2018, No. 4.

Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A.N., Kaiser Ł., Polosukhin I., *Attention is all you need*, in: *Proceedings of the 31st International Conference on Neural Information Processing Systems*, New York 2017.

Verdiesen I., Tubella A., Dignum V., *Integrating Comprehensive Human Oversight in Drone Deployment: A Conceptual Framework Applied to the Case of Military Surveillance Drones*, "Information" 2021, No. 9, doi: 10.3390/info12090385.

Wach K., Duong C.D., Ejdys J., R. Kazlauskaitė, P. Korzynski, G. Mazurek, J. Paliszkiewicz, E. Ziemba, *The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT*, "Entrepreneurial Business and Economics Review" 2023, No. 2, doi: 10.15678/EBER.2023.110201.

Werra Z., Kaczmarek K., Polak M., *Contemporary Dimension of Cultural Security*, "Studia Iuridica Lublinensia" 2025, No. 4, doi: 10.17951/sil.2025.34.4.83-99.