Iwona Kuc, MA
Police Headquarters
e-mail: iwciakuc@gmail.com

DOI: 10.26410/SF_2/24/7

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON INTERNAL SECURITY

Abstract

The article presents a diagnosis of the impact of artificial intelligence (AI) on internal security, pointing to new challenges such as cybercrime, online fraud, phishing and disinformation. The research process used statistics indicating an increase in cybercrime, supported by advanced artificial intelligence (AI) algorithms. Internal security, the foundation of state stability, has various dimensions – political, social, and technological. Artificial intelligence (AI), which introduces automation and optimization on an unprecedented scale, on one hand changes social structures and norms, but on the other hand brings the risk of errors and vulnerability to hacking attacks. The research conclusions presented in the article indicate that the development of artificial intelligence (AI) requires close international cooperation, taking into account the ethical, legal and social aspects of technology, to ensure its security and positive impact on society.

Keywords

security, internal security, artificial intelligence, cyberculture, hacking attack, phishing

Introduction

The term "internal security" is acquiring new significance in the face of the continuous development of digital technologies, especially artificial intelligence (AI), which is reshaping the modern world in an unprecedented way. Technological innovations, which permeate all areas of life—from the economy, through healthcare systems, to the social sphere—impact the stability and internal security of states while simultaneously posing new challenges to the agencies responsible for citizen protection. Contemporary understanding of security no longer concerns itself solely with physical protection from external threats but primarily encompasses broadly defined digital security, which relates to the protection of data, privacy, and the integrity of systems.

This article attempts to address the issue of internal security in the context of the development of artificial intelligence (AI). It discusses the multifaceted definitions of security, which shape both scientific and legislative approaches to this topic. Attention is drawn to the threats associated with the dynamic development of technology—such as the increasing number of cybercrimes, data thefts, and information manipulation using advanced algorithms. Furthermore, the article analyzes the significance of "cyberculture" as a new phenomenon that is infiltrating social life and changing its existing structures and norms.

From a regulatory perspective, initiatives at the European Union level are presented, such as the "White Paper on Artificial Intelligence. European Approach to Excellence and Trust" from 2020[1], which sets the framework for the sustainable and secure development of artificial intelligence (AI) systems. This document is not a legal act but aims to outline actions for regulation and the protection of citizens' rights and safety in the context of using data and algorithms in high-risk sectors, placing an obligation on the creators of AI solutions to ensure transparency, compliance with European Union values, and adherence to ethical standards. Given the constantly evolving technologies and the increasing integration of AI into the daily functioning of states and societies, the necessity for well-thought-out regulations and international cooperation has become a condition for stability, protection of national interests, and the preservation of fundamental democratic principles and individual freedoms. Therefore, it was necessary to publish the European Union Regulation on June 13, 2024, regarding the establishment of harmonized rules for artificial intelligence and amendments to regulations[2].

Multidimensional Aspects of Internal Security

Security is a term that is increasingly heard in public debates. In both scientific and journalistic literature, various definitions of security can be found, depending on perspective, imagination, or interpretation. The concept of security encompasses

1 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0065, [access:20.11.2024].

2 Rozporządzenie Parlamentu Europejskiego i Rady Europy (UE) z dnia 13 czerwca 2024, *w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany* (Dz.U. UE 2024/1689).

different dimensions and fields, which include the protection of health, life, and everything necessary for existence. Many articles refer to security in the context of the 1997 Constitution of the Republic of Poland[3], particularly emphasizing the Polish state's responsibility to ensure national security, protect citizens, and uphold the rule of law and public order. The Constitution treats security as the foundation of a stable and strong state, whose primary task is to protect its citizens. The PWN Polish Language Dictionary defines "security" as a state of peace and certainty without threats[4].

Piotr Majer, in his publication "In Search of a Universal Definition of Internal Security," points out that in scientific and journalistic literature, one can encounter various types of security, including political, military, economic, social, cultural, ideological, religious, maritime, ecological, internal, and external[5]. In the same work, the author highlights that internal security is a concept that lacks a single, cohesive definition and, when considered universally, it should be associated with the uninterrupted functioning of the state, the security of its organs, and the stability of social life, derived from personal security and the survival security of its citizens[6]. According to Bernard Wiśniewski, the term "security" has been with humanity for a long time. Many definitions of the term can be found in the literature. In today's world, security understood only as the absence of threats, fear, or attack seems too narrow, as security is increasingly perceived in a broader sense every day[7].

Artificial Intelligence as a Factor Changing Contemporary Security

The contemporary definition of the concept of internal security, as emphasized by Piotr Majer, is not only imprecise but also lacks a universal character. It relates to a state at a specific level of civilizational development, where the state, with its expanded administrative apparatus and various services, has taken on numerous responsibilities, including responding to natural disasters, catastrophic events, or technical failures. Such organized states have existed only recently. Earlier states had fewer duties, which resulted, among other things, from their different doctrines, social relations not respecting equality, and significantly lower technological-civilizational development[8].

In today's world, internal security includes, among other factors, technological and civilizational development, including artificial intelligence (AI), which generates not only enthusiasm but also certain concerns. What is artificial intelligence? There have been many attempts to define this concept, depending on the areas in which it appears. The merging of the real world with the virtual world causes

3 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. nr 78, poz. 483 z późn.zm.).

4 M. Szymczak, *Słowni Języka Polskiego PWN*, Warszawa 1998, p.172.

5 P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego,* „Przegląd bezpieczeństwa wewnętrznego" 2012, nr 7/12, p.11.

6 Ibid, p.18.

7 B. Wiśniewski, *System bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne*, Szczytno 2013, pp. 37,40.

8 P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego,* „Przegląd bezpieczeństwa" 2012, nr 7/12, p.14.

artificial intelligence to introduce automation and optimization on an unprecedented scale. Authors Stuart Russell and Peter Norvig in their publication stated that numerous studies place artificial intelligence (AI) at the forefront of rapidly developing fields of knowledge and human activities, generating profits counted in trillions of dollars annually. Kai-Fu Lee, an AI expert, predicts that its impact on humanity's future will be far more significant than anything else in history[9]. Regarding the concept of "intelligence," as stated by Stuart Russell and Peter Norvig, two schools of thought can be identified. One considers intelligence in terms of fidelity to human actions and behaviors, while the other advocates an abstract formal definition based on rationality—understood simply as "doing the right things." Similarly, the understanding of the essence of intelligence varies: some associate it closely with thought processes and reasoning, while others attribute it to the external characteristics of specific behaviors. These two alternatives—human versus rationality and thinking versus behavior—lead to four possible combinations, each having its proponents and inspiring many research programs. The pursuit of mimicking human intelligence is largely empirical, linked to psychology, involving the formulation of hypotheses about thinking and human behavior and verifying these hypotheses through observations of actual behavior; the rationalist approach, in turn, combines mathematics, engineering, statistics, control theory, and economics[10].

Digital technologies, as noted by Marek Świerczyński and Zbigniew Więckowski, have changed and continue to change the world. The authors emphasize that in recent years, there has been an acceleration of fundamental changes in the economy and society, also driven by the prolonged COVID-19 pandemic. The ambitious goal of AI-based technologies is to equip computers with human-like functions, such as the ability to learn, recognize, reason, etc[11]. The goal of artificial intelligence (AI) is to create systems that mimic human abilities, which in turn allows for the analysis and interpretation of the broadly understood environment. The creation of these systems requires not only a huge amount of data but also ethical responsibility. It should be emphasized that various AI solutions will not only allow for the automation of many tasks but will also be prone to numerous errors.

Piotr Kaczmarek-Kurczak, in his reflections on whether artificial intelligence is helpful, acknowledges that AI systems are vulnerable to hacking. The more complex a system is, the harder it is to secure it from external actions. Artificial intelligence has the potential to positively transform our world. However, with any powerful technology, there are security concerns that must be addressed[12]. The author emphasizes that security should be a key issue at every stage of AI development, from design to implementation. To ensure that AI is safe for people, scientists and policymakers must collaborate to develop security measures that minimize these threats[13].

9 S. Russel, P. Norvig, *Sztuczna inteligencja. Nowe spojrzenie,* Gliwice 2023, p. 17.

10 Ibid, pp. 17-18.

11 M. Świerczyński, Z. Więckowski, *Sztuczna inteligencja w prawie międzynarodowym*, Warszawa 2021, p. 17.

12 P. Kaczmarek-Kurczak, *Sztuczna inteligencja pomaga*, „Magazyn Polskiej Akademii Nauk" 2023, p.27.

13 Ibid, p. 27.

Scientific collaboration should be so comprehensive that by involving experts from various fields, it enables a holistic approach to understanding and analyzing the impact of artificial intelligence on human life. Regardless of the geographic location, using various communication platforms, experts have the opportunity to share research results and work together to solve emerging problems.

Cyberspace as a New Reality and Security Challenges

Czesław Marcinkowski, in his publication, discusses the topic of "cyberculture," describing this phenomenon as a face of popular culture that uses multimedia, mainly computer networks, connections, and links to present humanity's achievements in various areas of life. In this context, "cyberculture" is associated with a new form of human communication, transcending from the real space to the virtual one and vice versa[14]. As the author points out, technological progress and the development of electronic communication systems, along with their widespread use, led (and continue to lead) to the creation of cyberspace[15]. Cyberspace is the largest platform where all digital interactions between people, machines, and computer systems occur. It is an environment that emerged from the dynamic development of computer and internet technologies, enabling global communication, data transmission, analysis, and various forms of social, economic, and cultural interactions. Access to cyberspace is possible from anywhere on earth, which means that, in addition to enabling large-scale communication, international cooperation, and the realization of major projects, it can also have negative consequences for security on a large scale. Among these concerns are issues such as privacy, personal data, internet addiction, and problems related to disinformation and social inequality. The dangers associated with various threats can have both a direct impact on users and broad social and economic consequences.

Currently, as Czesław Marcinkowski writes, the boundaries between reality and cyberspace are gradually blurring. Many internet users cannot imagine life without easy access to the latest information, emails, online banking, online shopping, ticket reservations, or social media and messaging services to stay in contact with family and friends. The internet has become one of the essential utilities, alongside electricity, gas, and running water[16]. This shift to online life means that many people unknowingly fall victim to criminal activities, such as hacking attacks, online theft, phishing, or generating fake content, like deepfakes. According to data from the National Police Headquarters, by October 31, 2024, 62,244 online frauds were reported, compared to 63,373 in 2023 and 62,684 in 2022. These statistics show an increasing trend in online frauds over the past few years. Furthermore, In turn, analyzing cases of violations of the law under Art. 287§1 and 2 of the Penal Code[17], in the years

14 Cz. Marcinkowski, *Cyberkultura życia codziennego w drugiej dekadzie XXI wieku*, „Journal of modern science" 2019, p. 171.

15 Ibid, p. 172.

16 Ibid, p. 176.

17 Ustawa z dnia 6 czerwca 1997 r. *Kodeks Karny* (Dz.U. nr 88, poz.553 z późn, zm.).

2022-2023, out of 25,436 and 19,381, respectively, nearly 21,000 concerned E-banking. By October 31, 2024, over 7,600 such crimes had been recorded. A very popular method used by online fraudsters is phishing. According to the Internet Dictionary of the Polish Language, phishing is the act of fraudulently obtaining confidential and private information by impersonating someone else[18]. These criminal actions appeared in the early 1990s with the spread of the internet. The internet has also become a tool through which crimes are committed. By impersonating someone else and exploiting their image or personal data, the perpetrator can cause financial or personal harm[19]. Criminal activities described earlier are often supported by artificial intelligence. Using cutting-edge technologies and advanced solutions, such as machine learning—which has been defined on a government website as an interdisciplinary science aimed at the practical application of AI to create automated systems capable of improving based on experience (i.e., data) and acquiring new knowledge[20]—fraudsters create highly realistic and convincing messages. These messages, often of a personal nature, can take the form of videos, recordings, text messages, or emails, making it easy to scam victims, steal sensitive data, or gain access to bank accounts.

This crime phenomenon described earlier, penalized under Article 190a§2 of the Penal Code[21], based on data obtained from the National Police Headquarters, is as follows: as of October 31, 2024, 2,080 crimes were recorded, compared to 2,247 crimes in the previous year, while in 2022, the number of offenses was nearly 300 higher. The presented statistics clearly demonstrate how creative criminals have become with the use of artificial intelligence. However, for AI to function, it requires data sets, including sensitive data. It is through these data sets that algorithms learn to recognize patterns, make predictions, and solve problems.

The Role of the European Union and the White Paper in Shaping AI Protection Frameworks

In response to the risks associated with artificial intelligence (AI), the European Commission issued the "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust" in February 2020. The document became fundamental for AI regulation within the European Union. Its purpose was to set strategic directions and create a safe environment for AI development, emphasizing data protection and respect for civil rights. Published by the EU's executive body, the White Paper aimed to develop a comprehensive approach to AI development and regulation across the European Community.

The main objective of the White Paper was to establish a safe and trustworthy environment for AI development. It highlights that the functioning of many AI

18 https://sjp.pl/phishing, [access: 06.11.2024].

19 Ustawa z dnia 6 czerwca 1997 r. *Kodeks Karny.*

20 https://www.gov.pl/web/popcwsparcie/co-to-jest-uczenie-maszynowe--inteligentna-analiza-danych, [access:10.11.2024].

21 Ustawa z dnia 6 czerwca 1997r. *Kodeks Karny.*

systems, and the resulting actions and decisions, largely depend on the data sets on which these systems are trained. Therefore, it is necessary to implement measures ensuring that the data used to train AI systems adhere to the values and principles of the European Union, particularly concerning safety and compliance with legal provisions regarding the protection of fundamental rights[22].

This primarily concerns requirements aimed at ensuring sufficient certainty that the subsequent use of products or services enabled by artificial intelligence (AI) systems is safe, as well as requirements focused on ensuring adequate protection of privacy and personal data when using AI-based products and services[23].

Given factors such as the complexity and opacity of many AI systems and the resulting challenges that may arise in effectively verifying compliance with applicable regulations and enforcing them, it is necessary to introduce requirements for maintaining records related to the programming of algorithms and data used to train high-risk AI systems, and, in some cases, for storing the data itself. According to the provisions outlined in the White Paper, this would not only facilitate oversight and regulatory enforcement but could also encourage stakeholders to comply with these regulations at an early stage[24].

The document also emphasizes that AI systems, to be trustworthy, must be robust and properly account for risks. The position outlined in the 2020 document clearly states that human oversight helps ensure that AI systems do not undermine human autonomy or cause other adverse effects[25].

However, the rapid development of artificial intelligence (AI), which is one of the key technological trends of our time, and the dynamic transformation of various aspects of daily life, the economy, and society have effectively compelled the European Parliament—playing a key role in the legislative process—to create regulations concerning AI. This led to the Regulation of the European Parliament and the Council of the European Union, dated June 13, 2024, on the establishment of harmonized rules for artificial intelligence and amendments to other regulations, published in the Official Journal of the European Union[26].

The purpose of this regulation is, among other things, to improve the functioning of the internal market by establishing a unified legal framework, particularly regarding the development, marketing, deployment, and use of AI systems within the EU[27]. The EU's legal framework, which defines harmonized rules for AI, is thus essential to support the development, utilization, and dissemination of AI in the internal market while ensuring a high level of protection for public interests, such as health, safety,

22 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0065, [access:08.11.2024].

23 Ibid, p. 22.

24 Ibid, pp. 22-23.

25 Ibid, p. 24.

26 Rozporządzenie Parlamentu Europejskiego i Rady Europy (UE) z dnia 13 czerwca 2024, w sprawie ustanowienia zharmonizowanych przepisów….

27 Ibid, pt.1.

and the protection of fundamental rights, including democracy, the rule of law, and environmental protection, recognized and safeguarded by EU law[28].

Conclusion

The development of artificial intelligence, while opening up new and fascinating opportunities for contemporary society, also brings a series of challenges and threats that require responsible actions not only from the state but also from international organizations, including the European Union.

This article presents the complexity and multidimensionality of the concept of internal security, emphasizing that its protection can no longer rely solely on conventional actions but requires continuous monitoring and dynamic adaptation to rapidly evolving digital technologies. Process automation, the processing of big data, and the development of machine learning algorithms not only enhance the quality and efficiency of many sectors of the economy but also carry the risk of destabilization if applied without appropriate security mechanisms and transparent principles.

In analyzing the issue of internal security in the context of new technologies, it was observed that AI can serve both as a supportive tool and as a potential threat. On one hand, artificial intelligence supports the detection of threats, analysis of criminal patterns, and monitoring of cyberspace, enabling precise and effective preventive actions. On the other hand, however, this technology can be used in ways that are contrary to the public interest, as seen in hacking attacks, data manipulation, misinformation, or violations of citizens' privacy. Special attention was given to the issue of cybercrime, which continues to evolve, largely driven by the capabilities offered by AI. The scale of internet crimes, such as phishing or the use of deepfakes, remains high, as demonstrated by the statistics provided in the article.

The conclusions drawn from this analysis indicate an urgent need for regulations that will ensure the safe development of AI-based technologies. The European Union, through the publication of the White Paper, set standards and principles aimed at minimizing the risks associated with the development of these systems. Additionally, the European Parliament and Council's Regulation of June 13, 2024, establishing harmonized provisions regarding artificial intelligence and amending regulations, introduced provisions that account for the need to protect personal data, user privacy, and monitor high-risk actions involving advanced algorithms. However, even the most carefully crafted legal frameworks cannot ensure complete security without the cooperation of the private sector, which is responsible for most technological implementations. It is essential to involve all parties—technology creators, state bodies, and end-users—in promoting awareness and the responsible use of AI tools.

The article also emphasizes the importance of cyberculture and the need for public education regarding the benefits and risks associated with the integration of AI into everyday life. The boundary between the real and virtual worlds is becoming

28 Ibid, pt.8.

increasingly fluid, creating both new opportunities and challenges. In the face of this phenomenon, it is crucial for society to be prepared for the upcoming changes, understanding both the benefits and, most importantly, the risks associated with the use of AI.

In conclusion, artificial intelligence represents a tremendous potential that—if properly directed and secured—can contribute to strengthening the internal security of states. Nevertheless, its application also involves the need to develop a new, more comprehensive protection strategy that addresses both technological and ethical aspects. The future of AI depends on the level of responsibility and readiness for cooperation among all involved parties to create a sustainable security system that protects society while enabling growth and innovation.

Bibliography

Bartkiewicz W., Dembowski P., Zieliński J.S., *Systemy inteligentne w sieci Internet*, Łódź 2020, Kraków 2020.

Bukowski M., *Zwalczanie cyberprzestępczości ekonomicznej przy wykorzystaniu sztucznej inteligencji (AI)*, „Przegląd Policyjny" 2023.

Ficoń K., *Sztuczna inteligencja: nie tylko dla humanistów*, Warszawa 2013.

Fischer B., Pązik A., Świerczyński M., du Vall P., *Prawo sztucznej inteligencji i nowych technologii*, Warszawa 2021.

Ganczar M., *Wykorzystanie sztucznej inteligencji w ochronie środowiska*, Lublin 2024.

Hołyński M., Sztuczna *inteligencja,* Warszawa 1979Kaczmarek-Kurczak P., *Sztuczna inteligencja pomaga*, „Magazyn Polskiej Akademii Nauk" 2023.

https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0065.

https://sjp.pl/phishing.

https://sjp.pwn.pl/slowniki/bezpiecze%C5%84stwo.html.

https://www.gov.pl/web/popcwsparcie/co-to-jest-uczenie-maszynowe--inteligentna-analiza-danych.

Jankowska -Augustyn M., *Podmiotowość prawna sztucznej inteligencji*, Katowice 2015.

Jaskuła S., *Sztuczna inteligencja w edukacji we współczesnej rzeczywistości hybrydalnej*, „Perspektywy kultury," 2023, nr 42.

Kaczmarek-Kurczak P., *Sztuczna inteligencja pomaga*, „Magazyn Polskiej Akademii Nauk" 2023.

Kasperki M., *Sztuczna inteligencja*, Gliwice 2003.

Knosala R., Buchwald P., Kostrzewski M, Oleszek S., Szajna A., *Zastosowania innowacyjnych technologii informatycznych,* Warszawa 2024.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. nr 78, poz. 483 z późn. zm.).

Marcinkowski Cz., *Cyberkultura życia codziennego w drugiej dekadzie XXI wieku*, „Journal of modern science", nr 4.

Olbera P., *Informatyka Śledcza i cyberprzestępczość. Wybrane zagadnienia w ujęciu policyjnym,* Szczytno 2022.

Rotko J., *Technologie informatyczne a prawo*, Warszawa 2020.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. *w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE)2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE)2016/797 i (UE)2020/1828*.

Russel S., Norvig P., *Sztuczna inteligencja. Nowe spojrzenie, wydanie IV, tom 1,* Gliwice 2023,

Russel S., Norvig P., *Sztuczna inteligencja. Nowe spojrzenie, wydanie IV, tom 2,* Gliwice 2023,

Rutkowski L., *Metody i techniki sztucznej inteligencji*, Warszawa 2009.

Siejka K., Sojka W., Wierzchowska M., Zimowski Ł., *Nowoczesny e-proces karny: między teraźniejszością a przyszłością*, Warszawa 2024.

Stadnicka A., Ingram T., *Terra Semi-incognita, czyli o sztucznej inteligencji, robotach, automatyzacji oraz technologicznych obawach pracowników w organizacji*, „Prace naukowe Uniwersytetu Ekonomicznego" 2023.

Sypniewska B.A., Gołębiewski G., *Sztuczna Inteligencja – dylematy etyczne,* „Przegląd organizacji" 2023, nr 3.

Świerczyński M., Więckowski Z., *Sztuczna inteligencja w prawie międzynarodowym*, Warszawa 2021Majer P., *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego,* „Przegląd bezpieczeństwa wewnętrznego" 2012, nr 7/12.

Ustawa z dnia 6 czerwca 1997 r. *kodeks karny* (Dz.U. nr 88, poz. 553 z późn. zm.).

Wawrzyński P., *Podstawy Sztucznej inteligencji*, Warszawa 2019.

Wilk M., Daroń M., *Kierunki rozwoju technologicznego w dziedzinie IT i ich następstwa dla miejskich struktur organizacyjnych*, Warszawa 2018.

Wiśniewski B., *Praktyczne aspekty badań bezpieczeństwa,* Warszawa 2020.

Wiśniewski B., *System bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne*, Szczytno 2013.

Wołoszyn J., Wyszukiwanie Obiektów o podobnych cechach w bazie danych z wykorzystaniem sztucznej inteligencji, „Dydaktyka Informatyka" 2018, nr 13.

About the Author

Iwona Kuc, is a graduate of the Faculty of Law and Administration of the University of Warmia and Mazury in Olsztyn. She completed postgraduate studies in Foreign Service at the Warsaw School of Economics. Her interests include working for security and building public trust in uniformed services. She is interested in new technologies used in service.