

The development of cyber threats related to the use of AI

JAKUB GAJECKI

Independent author

 <https://orcid.org/0009-0007-3488-0236>

Abstract

The rapid development of artificial intelligence (AI) means that its role in cyberspace is also growing, both in terms of threats and defence against them. AI supports the automation of anomaly detection, data analysis, and incident response, which enhances protection efficiency. However, cybercriminals use AI-based solutions to create sophisticated attack tools, such as advanced phishing schemes, deepfakes, and hard-to-detect malware. The author analyses the role of AI in generating cyber threats and evaluates defensive strategies in this context. He highlights the need for international cooperation and legal regulation regarding the use of AI in cybersecurity.

Keywords

artificial intelligence, cybersecurity, AI as a service, cybercrime, quantum cryptography

Introduction

The development of information technology and artificial intelligence (AI) has changed the approach to cybersecurity and ushered in a new era of cyber threats. In the past, cyber attacks such as computer viruses and phishing, i.e. impersonating institutions or individuals in order to obtain information¹, were relatively simple and limited to activities carried out by individual hackers or small groups. At the turn of the 20th and 21st centuries, the biggest challenge was to prevent the spread of malicious software (malware), including ransomware type, and to respond quickly to it². These attacks were usually targeted at individuals or smaller organisations, and their scope and impact were limited by technological capabilities³. Advances in AI and machine learning have transformed cyberspace and made threats more complex, dynamic, and difficult to detect. AI has introduced a new quality in both conducting attacks in cyberspace and defending against them.

AI allows makes it possible to:

- analyse security infrastructure,
- automate the search for its vulnerabilities,
- develop intelligent tools that can adapt to the defensive actions of attacked systems in real time.

AI makes such attacks extremely difficult to neutralise.

The article analyses the impact of the development of AI, particularly its classical and generative (GenAI) types, on the development of threats in cyberspace, both offensively (cybercrime activities) and defensively (cyber defence systems).

The research problem was formulated in the following way: How does the use of classical and generative AI methods change the nature, scale and automation of threats in cyberspace, and what are the consequences for cybersecurity systems?

The specific objectives of the study are:

- identification of classic AI applications in cybersecurity,
- analysis of the use of generative AI by cybercriminal groups,
- assessment of current defence systems against automated attacks,

¹ J. Jancelewicz, *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych* (Eng. Phishing and related social engineering attacks as a threat to non-governmental organisations), "Trzeci Sektor" 2022, vol. 3–4, no. 59–60, pp. 80–81. <https://doi.org/10.26368/17332265-59/60-3/4-2022-5>.

² *The Evolution of Cybersecurity*, Codecademy, <https://www.codecademy.com/article/evolution-of-cybersecurity> [accessed: 7 X 2024].

³ B. Dash et. al., *Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review*, "International Journal of Software Engineering & Applications" 2022, vol. 13, no. 5, p. 14. <https://doi.org/10.5121/ijsea.2022.13502>.

- identification of directions for further research and regulatory action.

The article employs research methods such as analysis and synthesis as well as induction and deduction. The author used various source materials: compact publications, monographs and scientific articles, reports, specialist publications and case study descriptions.

Development of botnets and malware

Botnets, i.e. groups of infected computers controlled without their owners' knowledge, began to develop at the beginning of the 21st century. One of the first and most well-known botnets was Agobot, which used infected devices to send spam and carry out DDoS (Distributed Denial of Service) attacks⁴, the aim of which is to overload the servers of attacked entities and prevent access to their services. Subsequent botnets such as Storm and Conficker demonstrated their power and scale of operation, taking control of millions of devices and becoming a real threat to global computer systems⁵.

The evolution of malware encompasses its many forms: viruses, worms, spyware, advertising-supported software (adware), rootkits which provide administrator-level access and ransomware. An example of early malware development is ILOVEYOU virus, which was not yet a botnet, but due to the scale of its impact, it became an inspiration for the search for more advanced forms of malware. As technology evolved, malware also became increasingly specialised. Zeus and SpyEye are examples of malwares focused on stealing data from online banking⁶. In turn, Stuxnet was the first programme designed to physically damage industrial critical infrastructure devices⁷. Botnets have become the main tools in DDoS attacks. The examples are Mirai and Satori botnets, which transformed IoT (Internet of Things) devices into tools for large-scale attacks. In 2016, Mirai attacked

⁴ A. Kurniawan, A. Fitriansyah, *A Literature Review of Historical and Detection Analysis of Botnets Forensics*, "International Journal of Computer and Communication Engineering" 2018, vol. 7, no. 4, pp. 130–131. <https://doi.org/10.17706/ijcce.2018.7.4.128-135>.

⁵ J. Yimu, L. Shangdong, *Threats from Botnets*, in: *Computer Security Threats*, C. Thomas, P. Fraga-Lamas, T.M. Fernandez-Carames (eds.), September 2020, <https://www.intechopen.com/chapters/69332> [accessed: 18 X 2024].

⁶ N. Etaher, G.R.S. Weir, *Understanding the Threat of Banking Malware*, in: *Proceedings of Cyberforensics*, https://strathprints.strath.ac.uk/48856/1/8_etaher_weir.pdf, pp. 77–79 [accessed: 18 X 2025].

⁷ M. Hagerott, *Stuxnet and the vital role of critical infrastructure operators and engineers*, "International Journal of Critical Infrastructure Protection" 2014, vol. 7, no. 4, pp. 244–246. <https://doi.org/10.1016/j.ijcip.2014.09.001>.

servers belonging to DNS (Domain Name System) providers, blocking access to popular websites around the world⁸.

Malware and botnets currently use AI-based solutions, which allow them to bypass detection systems and conceal their presence more effectively. AI enables botnets to analyse and adapt in real time. This increases the effectiveness of attacks and reduces the likelihood of detection. Automated botnets can independently identify new targets and even use machine learning techniques to recognise patterns of victim behaviour and adapt their actions accordingly.

Artificial intelligence as a tool for cybercriminals

Artificial intelligence is defined as a field of computer science concerned with designing systems capable of performing tasks that previously required skills such as learning, reasoning, perception, or decision-making. The classical approach to AI includes, among others, rule-based systems, machine learning, neural networks, and probabilistic inference algorithms⁹.

Cybercriminals are able to automate and streamline phishing and malware attacks, making them more widespread and difficult to detect. Thanks to AI, hackers can quickly analyse large amounts of data, e.g. user behaviour and profiles, to create more convincing messages tailored to different target groups. Personalisation increases the likelihood that the recipient will decide to click on a malicious link or download an attachment. Artificial intelligence can also facilitate the creation and distribution of malicious software. AI analyses system protection mechanisms, adapting malware behaviour so that it remains undetectable. An example of this is malware that uses machine learning to carry out so-called polymorphic attacks. They involve the malware changing its characteristics with each infection, making it much more difficult for traditional antivirus programmes to identify¹⁰. Cybercriminals also use AI to create deepfakes, i.e. fake images, video or audio recordings, which they use in various criminal scenarios, such as financial fraud, manipulation of public opinion, and even blackmail¹¹.

⁸ H. Griffioen, Ch. Doerr, *Examining Mirai's Battle over the Internet of Things*, <https://www.cyber-threat-intelligence.com/publications/CCS2020-iotbattle.pdf>, p. 744 [accessed: 18 X 2025].

⁹ S. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach*, n.p. 2021, pp. 1–2.

¹⁰ R. Chauhan et. al., *Polymorphic Adversarial Cyberattacks Using WGAN*, “Journal of Cybersecurity and Privacy” 2021, no. 1, pp. 788–789. <https://doi.org/10.3390/jcp1040037>.

¹¹ O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość* (Eng. Deepfake as a complicated and deeply false reality), “Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate” 2019, vol. 9, no. 3, pp. 20–24. <https://doi.org/10.24917/26578549.9.3.2>.

The development of GenAI, including large language models (LLM) and generative models based on neural network architecture such as generative adversarial networks, has significantly changed the modus operandi of cybercriminal groups. Generative AI enables the automatic creation of highly personalised phishing content, the generation of malware code, and the scaling of social engineering attacks. Research indicates that the use of LLM lowers the barrier to entry into cybercrime, enabling individuals without specialist knowledge to carry out sophisticated attacks¹². An example of this is analysing search histories and visited websites in order to tailor phishing messages that appear authentic to the victim.

Machine learning is used to create more sophisticated and adaptive malware. These algorithms enable the malware to adapt its activities depending on the security measures detected on the victim's system and to carry out an attack at the most appropriate moment, e.g. identifying moments when the user logs into sensitive systems such as bank accounts. Machine learning algorithms enable new variants of malicious code to be generated and tested in a short period of time.

Another form of cybercrime based on machine learning are the aforementioned polymorphic attacks. Techniques such as polymorphism and metamorphism allow different variants of the same malware to be generated, making it impossible for pattern-based security software to recognise the modified code. Such techniques are among the most difficult to detect. Machine learning also enables for rapid data processing and trying different combinations in brute force attacks aimed at guessing passwords or security codes. These algorithms are able to predict which passwords are most likely to be used, which significantly reduces the time needed to break security measures. For example, when combined with behavioural analysis, algorithms can generate password suggestions that match the characteristic patterns applied by the user, such as names, birth dates or other personal details.

Cybercriminals use machine learning algorithms to analyse the structure and configuration of security systems. This type of software is capable of identifying and analysing specific features of security mechanisms such as firewalls, intrusion detection systems (IDS) and antivirus software. With this knowledge, attackers can adapt their methods in real time, break through successive layers of protection, and avoid detection. Artificial intelligence can not only generate different variants of the same malware (polymorphism, metamorphism), but also teach malware to recognise different security systems and adapt its behaviour to them, minimising the risk of detection. Advanced attacks using AI rely on predicting user behaviour based on behavioural analysis. By analysing large data sets of user behaviour,

¹² Y. Yigit et. al., *Review of Generative AI Methods in Cybersecurity*, arXiv, 13 III 2024. <https://doi.org/10.48550/arXiv.2403.08701>.

attackers can predict when a system will be least resilient to attack, for example, when attempting to log in while the security system is recording increased traffic and is more likely certain to ignore some irregularities.

Contemporary cases of cyberattacks

The attack on GitHub platform in 2018 was one of the most powerful DDoS attacks in history, reaching a data flow of 1.35 Tb/s. Cybercriminals used AI-controlled botnets, sending mass requests, which overloaded GitHub's servers. Artificial intelligence helped dynamically adapt the attack and bypass security measures in real time. AI assisted botnets are becoming more and more common, enabling attacks on large platforms¹³.

In 2020, Cognizant company, global IT services provider, became a victim of Maze ransomware. This is an example of software using AI and advanced network infiltration techniques. This software uses system analysis to identify the most sensitive data and prevent access to it, and also distributes it further to criminal command centres. As a result of the attack, Cognizant experienced massive financial losses and spent millions of dollars on infrastructure repairs and support for customers and suppliers¹⁴. The company took corrective actions, including isolating infected systems, strengthening incident response procedures and expanding network monitoring mechanisms. However, this case shows that threat detection systems based primarily on signatures are not always able to detect advanced ransomware campaigns early enough¹⁵.

In the same year, Twitter was attacked by cybercriminals who took over the accounts of famous people and companies, including Bill Gates, Elon Musk and Apple. Hackers used natural language processing (NLP) technology to generate messages that appeared personal and personalised, encouraging people to send money to a provided cryptocurrency address¹⁶. The attack was successful thanks

¹³ L.H. Newman, *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired, 1 III 2018, <https://www.wired.com/story/github-ddos-memcached/> [accessed: 26 X 2024].

¹⁴ F. Truță, *Cognizant Expects to Lose up to \$70 Million from April Ransomware Attack*, Bitdefender, 11 V 2020, <https://www.bitdefender.com/en-gb/blog/hotforsecurity/cognizant-expects-to-lose-up-to-70-million-from-april-ransomware-attack/> [accessed: 24 X 2024].

¹⁵ *Cognizant Security Incident Update*, Cognizant, 18 IV 2020, <https://news.cognizant.com/2020-04-18-Cognizant-Security-Incident-Update?utm> [accessed: 9 III 2026].

¹⁶ N. Statt, *Twitter's massive attack: What we know after Apple, Biden, Obama, Musk, and others tweeted a bitcoin scam*, The Verge, 17 VII 2020, <https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised> [accessed: 24 X 2025].

to, among other things, the use of AI to analyse the victims' communication patterns and adapt the messages. After detecting the incident, the platform blocked the ability of verified accounts to post and began the process of restoring the security of the compromised profiles. Additional measures controlling access to administrative tools were implemented, and employee authentication procedures were strengthened.

In 2025, the first documented case of large-scale use of autonomous AI agents in cyber intelligence operations was detected. In mid-September, Anthropic's Threat Intelligence team identified and subsequently disrupted a cyber espionage campaign in which a tool based on Claude Code language model was manipulated by an actor believed to have links to Chinese state bodies. The aim was to carry out complex intelligence operations¹⁷.

In this campaign, AI did not play a merely advisory or generative role, but acted as an autonomous agent performing most of the operational tasks. The system broke down multi-step instructions into smaller tasks, which it then performed independently with minimal human supervision. Claude Code performed autonomously up to 80–90% of tactical operations, including:

- recognition of target infrastructure and analysis of vulnerabilities,
- generating and executing code that exploits vulnerabilities,
- collecting certificates and data,
- lateral movement,
- data extraction and classification¹⁸.

This automation means that AI performed tasks that would previously have required the involvement of large teams of experts without constant operator intervention: from network scanning and vulnerability analysis to data exfiltration. In this case, the human's role was limited mainly to launching the campaigns and making strategic decisions at key moments, e.g. approving the transition between attack phases¹⁹. Furthermore, the AI agents' operating mechanism relied on their ability to make autonomous decisions within a sequence of tasks and to adapt their narrative and strategy to the subsequent stages of the attack. This significantly increased the speed and scale of operations compared to traditional 'manual control'. The machine was capable of performing thousands of operations per second – a feat beyond the reach of cybercriminal groups without automation²⁰.

¹⁷ *Disrupting the first reported AI-orchestrated cyber espionage campaign*, Anthropic, 13 XI 2025, <https://www.anthropic.com/news/disrupting-AI-espionage> [accessed: 24 XI 2025].

¹⁸ Ibid.

¹⁹ Ibid.

²⁰ Ibid.

Artificial intelligence in cyber defence systems

The growth of AI as a service offerings brings benefits to business, but at the same time creates new attack vectors for cybercriminals. AI as a service provides access to advanced AI algorithms that can be used to automate tasks such as analysing system vulnerabilities or creating advanced phishing bots. In the future, cybercriminals may use AI as a service to develop deepfakes, carry out social engineering attacks on a larger scale, create malware that is harder to detect, and design ransomware that automatically selects the most effective attack methods, thereby increasing its efficiency.

To meet these challenges, new defence technologies based on AI are being developed. For example, adaptive systems based on machine learning can dynamically respond to threats and automatically adjust their protective functions depending on the attacks they encounter. In addition, NLP technologies are used to analyse cybercriminal communications, which helps in predicting and detecting new threats. In the future, it is expected that AI-based systems will be capable of independently analysing malware and creating dynamic, threat-resistant virtual environments, which will reduce the risk of security breaches²¹.

It is worth emphasising that many cybersecurity regulations are currently in force both at the national and international levels. In Europe, the NIS2 Directive²² on the security of networks and information systems plays a significant role, as does the Artificial Intelligence Act²³ governing the use of AI systems in the European Union. The Convention of the Council of Europe on Cybercrime²⁴, which forms the basis for international cooperation in combating cybercrime, is also an important tool.

However, it should be noted, that most of these regulations were drafted at a time when AI technologies were not yet widely used in cyber operations. Consequently, current regulations often do not explicitly address the specific

²¹ R. Keshava et al., *AI-Powered Algorithms for the Prevention and Detection of Computer Malware Infections*, in: 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore 2025. <https://doi.org/10.1109/ICESC65114.2025.11212519>.

²² *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*.

²³ *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 Intelligence Act)*.

²⁴ *Convention of the Council of Europe on Cybercrime, drawn up in Budapest on 23 November 2001*.

characteristics of AI-based systems, such as autonomous threat detection systems, generative models used to create phishing attacks, or automated tools for carrying out cyberattacks.

Development of AI application possibilities in cybersecurity primarily necessitates the clarification and extension of existing regulations, rather than creating them from scratch. This applies in particular to issues such as accountability for decisions made by AI systems, algorithm transparency, security standards and international cooperation arrangements for combating cyber threats. At the same time, effectively combating cybercrime requires closer international cooperation and the harmonisation of legal regulations in order to limit the opportunities for criminals to exploit differences between legal systems. This stems from the nature of cyberspace, which transcends national borders. Future regulations should address the use of AI systems for illegal activities, including cybercrime, clarify the rules on liability for the use of such systems, and restrict the use of certain high-risk technologies. International organisations, such as the United Nations and the European Union, play a key role in developing policies to combat cybercrime and in promoting common data protection standards. Such activities will enable a faster response to global threats and facilitate the exchange of information and experience regarding best practices in cybersecurity.

Summary

Based on theoretical considerations and an analysis of selected cases, the following conclusions have been drawn:

1. Artificial intelligence significantly increases the effectiveness and scalability of cyberattacks, particularly through the automation of phishing, the development of adaptive malware and the use of generative techniques (deepfakes), which lowers the barrier to entry into cybercrime.
2. Development of AI-based cyber defence systems improve the ability to detect and respond to threats. However, there is a technological race between the entities responsible for digital security and cybercriminals.
3. Effectively addressing the risks generated by AI requires coordinated systemic action, including international cooperation, the development of regulatory frameworks, and the harmonisation of legal and technical standards regarding the use of AI in cyberspace. Currently, at international level, the basis for cooperation between states in combating cybercrime is the Convention on cybercrime adopted by the Council of Europe. It sets out the framework for cooperation in the prosecution of crimes committed

- using computer systems. Within the EU, the NIS2 Directive also plays a significant role, as it aims to enhance the security of networks and information systems, as does Artificial Intelligence Act, which establishes a legal framework for the secure and responsible use of AI systems.
4. Dynamic development of AI technology poses challenges to existing legal and technical systems. However, it does not seem necessary to introduce new regulations, rather, the existing provisions should be clarified and adapted to the specific nature of the risks associated with the use of AI in cyberspace.

Bibliography

Chauhan R., Sabeel U., Izaddoost A., Heydari S.S., *Polymorphic Adversarial Cyberattacks Using WGAN*, “Journal of Cybersecurity and Privacy” 2021, no. 1, pp. 767–792. <https://doi.org/10.3390/jcp1040037>.

Dash B., Ansari M.F., Sharma P., Ali A., *Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review*, “International Journal of Software Engineering & Applications” 2022, vol. 13, no. 5, pp. 13–21. <https://doi.org/10.5121/ijsea.2022.13502>.

Hagerott M., *Stuxnet and the vital role of critical infrastructure operators and engineers*, “International Journal of Critical Infrastructure Protection” 2014, vol. 7, no. 4, pp. 244–246. <https://doi.org/10.1016/j.ijcip.2014.09.001>.

Jancelewicz J., *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych* (Eng. Phishing and related social engineering attacks as a threat to non-governmental organisations), “Trzeci Sektor” 2022, vol. 3–4, no. 59–60, pp. 79–88. <https://doi.org/10.26368/17332265-59/60-3/4-2022-5>.

Keshava R., Pandurangan S.K., Sakthivanitha M., Parmisvan S., Sunkara G., Maruthi R., *AI-Powered Algorithms for the Prevention and Detection of Computer Malware Infections*, in: 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore 2025. <https://doi.org/10.1109/ICESC65114.2025.11212519>.

Kurniawan A., Fitriansyah A., *A Literature Review of Historical and Detection Analysis of Botnets Forensics*, “International Journal of Computer and Communication Engineering” 2018, vol. 7, no. 4, pp.128–135. <https://doi.org/10.17706/ijcce.2018.7.4.128-135>.

Russell S., Norvig P., *Artificial Intelligence. A Modern Approach*, n.p. 2021.

Wasiuta O., Wasiuta S., *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość* (Eng. Deepfake as a complicated and deeply false reality), "Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate" 2019, vol. 9, no. 3, pp. 19–30. <https://doi.org/10.24917/26578549.9.3.2>.

Yigit Y., Buchanan W.J., Tehrani M.G., Maglaras L., *Review of Generative AI Methods in Cybersecurity*, arXiv, 13 III 2024. <https://doi.org/10.48550/arXiv.2403.08701>.

Internet sources

Cognizant Security Incident Update, Cognizant, 18 IV 2020, <https://news.cognizant.com/2020-04-18-Cognizant-Security-Incident-Update?utm> [accessed: 9 III 2026].

Disrupting the first reported AI-orchestrated cyber espionage campaign, Anthropic, 13 XI 2025, <https://www.anthropic.com/news/disrupting-AI-espionage> [accessed: 24 XI 2025].

Etaher N., Weir G.R.S., *Understanding the Threat of Banking Malware*, in: *Proceedings of Cyberforensics 2014*, https://strathprints.strath.ac.uk/48856/1/8_etaher_weir.pdf [accessed: 18 X 2025].

Griffioen H., Doerr Ch., *Examining Mirai's Battle over the Internet of Things*, <https://www.cyber-threat-intelligence.com/publications/CCS2020-iotbattle.pdf> [accessed: 18 X 2025].

Newman L.H., *GitHub Survived the Biggest DDoS Attack Ever Recorded*, Wired, 1 III 2018, <https://www.wired.com/story/github-ddos-memcached/> [accessed: 26 X 2024].

Statt N., *Twitter's massive attack: What we know after Apple, Biden, Obama, Musk, and others tweeted a bitcoin scam*, The Verge, 17 VII 2020, <https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised> [accessed: 24 X 2025].

The Evolution of Cybersecurity, Codecademy, <https://www.codecademy.com/article/evolution-of-cybersecurity> [accessed: 7 X 2024].

Truță F., *Cognizant Expects to Lose up to \$70 Million from April Ransomware Attack*, Bitdefender, 11 V 2020, <https://www.bitdefender.com/en-gb/blog/hotforsecurity/cognizant-expects-to-lose-up-to-70-million-from-april-ransomware-attack/> [accessed: 24 X 2024].

Yimu J., Shangdong L., *Threats from Botnets*, in: *Computer Security Threats*, C. Thomas, P. Fraga-Lamas, T.M. Fernandez-Carames (eds.), September 2020, pp. 52–75, <https://www.intechopen.com/chapters/69332> [accessed: 18 X 2024].

Legal acts

Convention of the Council of Europe on Cybercrime, drawn up in Budapest on 23 November 2001 (Journal of Laws of 2015, item 728).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) – (Official Journal of the EU L 333/80 of 27 XII 2022).

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 Intelligence Act) – (Official Journal of the EU L 2024/1689 of 12 VII 2024).

Jakub Gajecki

Graduate of the Jacob of Paradies University in Gorzów Wielkopolski in applied criminology, specialising in combating cybercrime. Second-cycle student at the Police Academy in Szczytno in the field of cybersecurity. His academic interests include cybersecurity and state security. He is a Police officer responsible for conducting preliminary proceedings.

Contact: gajeckijakub@protonmail.com