Paweł Pelc*

Cybersecurity Issue in the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence from October 30, 2023

Abstract

AI is a new tool with only limited regulation. One such attempt is the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence from October 30, 2023, issued by the US President. As AI may be regulated from various angles, one of them is its influence on cybersecurity. AI Executive Order is much more concentrated on cybersecurity issues than other regulations or recommendations related to AI, like those issued in China, drafted in the EU or issued by international organisations like OECD and UNESCO. However, the strong focus on cybersecurity in the AI Executive Order is in line with the National Cybersecurity Strategy issued by the same US administration in March 2023.

Key words: cybersecurity, AI, AI System

* Paweł Pelc, War Studies University in Warsaw, Academic Centre for Cyber Security Policy, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

On October 30th, 2023, US President Joe Biden issued the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[1] (further referred to as AI Executive Order). According to the relevant Fact Sheet, „as part of the Biden-Harris Administration's comprehensive strategy for responsible innovation, the Executive Order builds on previous actions the President has taken, including work that led to voluntary commitments from 15 leading companies to drive safe, secure, and trustworthy development of AI"[2]. The AI Order was issued based on the Defence Production Act, a Korean War time regulation which gives administration emergency powers[3].

In recent years, the development of Artificial Intelligence (AI) has increased and sped up. In 2023, the use of generative AI tools has moved forward significantly. However, regulation is still behind the technology development[4].

The Chinese made one of the first successful attempts to regulate AI in the form of the Interim Measures for the Management of Generative Artificial Intelligence Services (Generative AI Regulation). It was published on July 13 2023 and came into force on August 15, 2023[5].

1 *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence from October 30, 2023*, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [access: 15.11.2023].

2 *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ [access: 15.11.2023].

3 J.D. McKinnon, S. Siddiqui, D. Volz, *Biden Taps Emergency Powers to Assert Oversight of AI Systems*, https://www.wsj.com/politics/policy/biden-to-use-emergency-powers-to-mitigate-ai-risks-cf7735d5 [access: 17.11 2023]; C. Kang, D.E. Sanger, *Biden Issues Executive Order to Create A.I. Safeguards*, https://www.nytimes.com/2023/10/30/us/politics/biden-ai-regulation.html?campaign_id=9&emc=edit_nn_20231031&instance_id=106525&nl=the-morning&regi_id=73957933&segment_id=148752&te=1&user_id=72f2a8e8dc7b7d6833244637427d007c [access: 17.11.2023].

4 A. Engler, *The AI regulatory toolbox: How governments can discover algorithmic harms*, https://www.brookings.edu/articles/the-ai-regulatory-toolbox-how-governments-can-discover-algorithmic-harms/ [access: 15.11.2023].

5 *Interim Measures for the Management of Generative Artificial Intelligence Services*, http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm [access: 15.11.2023], English translation: https://www.chinalawtranslate.com/en/generative-ai-interim/ [access: 15.11.2023]. See also M. MacCarthy, *The US and its allies should engage with China on AI law and policy*, https://www.brookings.edu/articles/the-us-and-its-allies-should-engage-with-china-on-ai-law-and-policy/ [access: 15.11.2023].

Similarly, in the European Union, there are ongoing works to regulate AI[6]. AI can be regulated from various angles – risks associated with specific technologies including the risk of creating superintelligent AI, which can be superior to human one[7], personal data protection, copyrights protection, fundamental rights protection, equality protection, market competition, cyberwarfare use, transparency, information war use, fake news creation and dissemination, social media influence, deepfake production and many others[8].

In Canada, there is a proposal for the Artificial Intelligence and Data Act (AIDA) introduced as part of the Digital Charter Implementation Act, 2022, which would, according to the Canadian government, set the foundation for the responsible design, development and deployment of AI systems that impact the lives of Canadians[9]. It will concentrate on consumer protection and human rights, with its goal being the prevention of reckless or malicious use of AI against Canadians.

In 2019, the OECD issued Recommendation on Artificial Intelligence. It was amended in 2023[10]. In 2021, UNESCO adopted Recommendation on the Ethics of Artificial Intelligence[11].

This shows how central artificial intelligence has become and thus the need to find ways to regulate it. However, there is no common agreement on how to define AI[12]. In the above-mentioned recommendations or regulations, there are various definitions of AI.

6 J. Sobczak, K. Kakareko, M. Gołda-Sobczak, *Poszukiwanie standardów sztucznej inteligencji*, „Cybersecurity and Law" 2023, no. 1, p. 243–275; *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 [access: 15.11.2023].

7 *Pause Giant AI Experiments: An Open Letter*, https://futureoflife.org/open-letter/pause-giant-ai-experiments/ [access: 15.11.2023].

8 *White Paper on Artificial Intelligence – A European approach to excellence and trust*, p. 9–12, https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf [access: 15.11.2023].

9 *The Artificial Intelligence and Data Act (AIDA) – Companion document*, https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document [access: 17.11.2023].

10 *Recommendation of the Council on Artificial Intelligence*, 2023, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [access: 17.11.2023].

11 *Recommendation on the Ethics of Artificial Intelligence*, https://unesdoc.unesco.org/ark:/48223/pf0000381137 [access: 17.11.2023].

12 M. Tłuczek, *Jak sztuczna inteligencja zmieni twoje życie*, Warszawa 2023, p. 7–8; A. Przegalińska, P. Oksanowicz, *Sztuczna inteligencja. Nieludzka, arcyludzka*, Kraków 2020, p. 20–24.

In the Chinese regulation, there is only a definition of „Generative AI technology" which, according to Art. 22 point 1, means models and relevant technologies that can generate content such as texts, images, audio, or video. On one hand, this is a comprehensive definition, but on the other, it is limited only to generative AI, which is only a fraction of AI technologies. In the European Commission's proposal for the AI Act, there is a definition of an artificial intelligence system' (AI system). According to Art. 3 point 1 of the draft AI Act, it means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. OECD, in its Recommendation of the Council on Artificial Intelligence, has defined the same term as a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment. UNESCO made another attempt in the Recommendation on the Ethics of Artificial Intelligence. According to this, AI systems are information-processing technologies that integrate models and algorithms that produce a capacity to learn and perform cognitive tasks leading to outcomes such as prediction and decision-making in material and virtual environments. AI systems are designed to operate with varying degrees of autonomy. This is done by utilising knowledge modelling and representation and by exploiting data and calculating correlations. AI systems may include several methods. These include but are not limited to machine learning, including deep learning and reinforcement learning; machine reasoning, including planning, scheduling, knowledge representation and reasoning, search, and optimisation. AI systems can be used in cyber-physical systems, including the Internet of Things, robotic systems, social robotics, and human-computer interfaces. These involve control, perception, processing of data collected by sensors, and the operation of actuators in the environment in which AI systems work. This definition is the most detailed of those presented above.

A different method was used in the US in sec. 3, letters (e) and (b) of the AI Executive Order. It defines „AI system" as any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI. AI has a separate definition as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations,

or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action. This is based on previous US regulations. In sec. 3, letter (c), an additional term, „AI Model", is defined as a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

It shows that, even though all those regulations or recommendations are concentrated on AI, their scope varies based on different understandings of what AI means and what shall be subject to regulation – sole AI, AI system, AI model or only generative AI technology. That is a rather typical situation in which there are no established standards and worldwide practices and everything should be regulated from scratch as a part of „regulatory greenfield".

AI could also fundamentally impact cybersecurity issues, as the technology can be used to enhance cybersecurity levels or be used for cyberattacks[13].

In China, in addition to upholding the core socialist values, it also mentions effective measures which shall be employed to prevent the creation of discrimination, such as on race, ethnicity, faith, nationality, region, sex, age, profession, or health, as well as provisions related to respecting intellectual property rights and commercial ethics, and protecting commercial secrets, advantages in algorithms, data, and platforms, and preventing risk of monopolisation or unfair competition. The lawful rights and interests of others, the physical and psychological well-being of others must not be endangered, and the rights and interests of others, such as in their image, reputation, honour, privacy, and personal information, must not be infringed according to Chinese regulation[14]. There is also a requirement to comply with Cybersecurity Law, which constituted the basis for issuing those Interim Measures[15].

13 M.F. Ansari, B. Dash, P. Sharma, N. Yathiraju, *The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review*, „International Journal of Advanced Research in Computer and Communication Engineering" 2022, vol. 11, no. 9, p. 81–90; Ch. Brooks, *A Primer on Artificial Intelligence and Cybersecurity*, https://www.forbes.com/sites/chuckbrooks/2023/09/26/a-primer-on-artificial-intelligence-and-cybersecurity/ [access: 15.11.2023].

14 Art. 4 of the *Interim Measures for the Management of Generative Artificial Intelligence Services*…

15 Art. 1, Art. 7 sec. 5, and Art. 21 of the ibidem.

According to Motive 41 to the European Commission Proposal for Artificial Intelligence Act, „Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity". Motive 49 of this proposal requires that „High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the Art.". In Motive 51, it is highlighted that „Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI specific assets, such as training data sets (e.g., data poisoning) or trained models (e.g., adversarial attacks), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate in the underlying ICT infrastructure"[16]. However, the final form of the Artificial Intelligence Act is not yet known, as the works are expected to be finalised by the end of 2023[17].

It is interesting to note that in the OECD Recommendation of the Council on Artificial Intelligence, the cybersecurity term is not used at all. However, there is a mention of digital security and security. In the UNESCO Recommendation on the Ethics of Artificial Intelligence, cybersecurity is not mentioned, although there is the highlighted issue of the avoidance of safety and security risks and the safety and security of AI systems and technologies[18].

16 Motives 41, 49 and 51 of the Proposal for Artificial Intelligence Act.

17 M. Fraser, *AI Act coraz bliżej. UE uzgadnia kolejne szczegóły*, https://cyberdefence24.pl/polityka-i-prawo/ai-act-coraz-blizej-ue-uzgadnia-kolejne-szczegoly [access: 15.11.2023].

18 „Unwanted harm (safety risks), as well as vulnerabilities to attack (security risks), should be avoided and should be addressed, prevented and eliminated throughout the life cycle of AI systems to ensure human, environmental and ecosystem safety and security. Safe and secure AI will be enabled by the development of sustainable, privacy-protective data access frameworks that foster better training and validation of AI models utilising quality data" (*Recommendation of the Council on Artificial Intelligence*..., p. 20); „Member States should ensure that governments and multilateral organisations play a leading role in ensuring the safety and security of AI systems, with multi-stakeholder participation. Specifically, Member States, international organisations and other relevant bodies should develop international standards that describe measurable, testable levels of safety and transparency so that systems can be objectively assessed and levels of compliance determined. Furthermore,

In this context, the AI Executive Order looks to be much more focused on the cybersecurity issues.

In sec. 2, letter (a), cybersecurity is mentioned as one of the most pressing security risks[19]. According to sec. 4 point 1, par. (i) letter (C), there is a need to establish guidelines and best practices to promote consensus of industry standards for developing and deploying safe, secure, and trustworthy AI systems, including launching an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity. Any ongoing or planned activities related to training, developing, or producing dual-use foundation models shall include the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats and the physical and cybersecurity measures taken to protect those model weights [20]. It is expected that best practices will be issued for financial institutions to manage AI-specific cybersecurity risks[21]. Another tool related to the health and human services sector is incorporating safety, privacy, and security standards into the software development lifecycle for protecting personally identifiable information, including measures to address AI-enhanced cybersecurity threats in the health and human services sector[22]. Another goal is the reduction of governmental agencies' barriers related

Member States and business enterprises should continuously support strategic research on potential safety and security risks of AI technologies and should encourage research into transparency and explainability, inclusion and literacy by putting additional funding into those areas for different domains and at different levels, such as technical and natural language" (*Recommendation of the Council on Artificial Intelligence…*, p. 28).

19 „Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use. It also requires addressing AI systems' most pressing security risks – including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers – while navigating AI's opacity and complexity. Testing and evaluations, including post-deployment performance monitoring, will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner, and are compliant with applicable Federal laws and policies. Finally, my Administration will help develop effective labeling and content provenance mechanisms so that Americans are able to determine when content is generated using AI and when it is not. These actions will provide a vital foundation for an approach that addresses AI's risks without unduly reducing its benefits" (sec. 2, letter (a) of the AI Executive Order).

20 Sec. 4 point 2 par. (i), letters (B) and (C), ibidem.

21 Sec. 4 point 3 par. (ii), ibidem.

22 Sec. 8, letter (b), par. (i), letter (D), ibidem.

to cybersecurity processes[23]. Additionally, to protect federal government information, governmental agencies are also encouraged to employ risk-management practices, such as training their staff on the proper use, protection, dissemination, and disposition of Federal information; negotiating appropriate terms of service with vendors; implementing measures designed to ensure compliance with record-keeping, cybersecurity, confidentiality, privacy, and data protection requirements; and deploying other measures to prevent the misuse of federal government information in generative AI[24]. According to the White House, the AI Executive Order is to „establish an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software, building on the Biden-Harris Administration's ongoing AI Cyber Challenge. Together, these efforts will harness AI's potentially game-changing cyber capabilities to make software and networks more secure"[25].

The cybersecurity issue may be a much more significant part of the AI Executive Order than in other regulations, not only due to the different priorities but also due to the nature of the executive order itself, as an emergency power which can be addressed to the administrative bodies and cannot directly regulate citizens' rights. According to E. Groll and Ch. Vasquez, „key provisions of the order, such as a call for addressing the privacy risks of AI models, will require Congress to act on federal privacy legislation"[26]. To some extent, the Executive Order is a consequence of Congress's inaction. Due to high polarisation after the 2020 presidential election and 2022 byelections, it has been mostly divided on party lines. This has led to limitations in legislative activity. Also, global competition with China and cyberattacks against US infrastructure implemented by Chinese, Russian, North Korean and Iranian hackers, mentioned in the US National Cybersecurity Strategy[27], has led to prioritising the strengthening of the cybersecurity regulation.

The AI Executive Order is also in line with the 2023 US National Cybersecurity Strategy. According to this strategy, the widespread introduction of artificial intelligence systems – which can act in ways unexpected to even

23 Sec. 10, letter (b), par. (vi) , ibidem.
24 Sec. 10, letter (f) par. (i) , ibidem.
25 FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.
26 E. Groll, Ch. Vasquez, *White House executive order on AI seeks to address security risks*, https://cyberscoop.com/white-house-ai-executive-order-cybersecurity/ [access: 17.11.2023].
27 *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [access: 17.11.2023].

their creators – is heightening the complexity and risk associated with many of our most important technological systems, and public and private investments in cybersecurity were not in line enough with the recent challenges, including revolutionary changes in our technology landscape brought by artificial intelligence and quantum computing. There was a mention of research and development projects related to advancing cybersecurity and resilience, including artificial intelligence. The artificial intelligence area played a part in explaining the strategic objective to Reinvigorate Federal Research and Development for Cybersecurity in this National Cybersecurity Strategy.

It looks like the AI Executive Order may be assessed not only as a tool related to instructing governmental agencies on how to regulate AI issues, but also as a tool to strengthen US cybersecurity and cybersecurity standards not only in the governmental agencies but also in the industries especially vulnerable to cyberattacks, including financial institutions or institutions related to health and human resources.

As the Chinese regulation is concentrated on securing the grip of the Communist party over society[28], in the EU, there are four specific objectives of the proposed AI Act (ensure that AI systems placed on the Union market, and used here, are safe and respect existing laws on fundamental rights and Union values; ensure legal certainty to facilitate investment and innovation in AI; enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; as well as to facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation, which leads to a regulatory approach to AI that is limited to the minimum requirements to address the risks and problems linked to AI[29]). The AI Executive Order is part of the regulation operating in an open society and, as such, is much more focused on cybersecurity issues.

In the future, it will be interesting to see which attitude toward AI regulation will prevail.

28 The provision and use of generative AI services shall comply with the requirements of laws and administrative regulations, respect social mores, ethics, and morality, and obey the following provisions: Uphold the Core Socialist Values; content that is prohibited by laws and administrative regulations such as that inciting subversion of national sovereignty or the overturn of the socialist system, endangering national security and interests or harming the nation's image, inciting separatism or undermining national unity and social stability, advocating terrorism or extremism, promoting ethnic hatred and ethnic discrimination, violence and obscenity, as well as fake and harmful information (art. 4 point 1 of the *Interim Measures for the Management of Generative Artificial Intelligence Services…*).

29 *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence…*, p. 3.

Bibliography

Ansari M.F., Dash B., Sharma P., Yathiraju N., *The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review*, „International Journal of Advanced Research in Computer and Communication Engineering" 2022, vol. 11, no. 9.

Brooks Ch., *A Primer On Artificial Intelligence And Cybersecurity*, https://www.forbes.com/sites/chuckbrooks/2023/09/26/a-primer-on-artificial-intelligence-and-cybersecurity/ [access: 15.11.2023].

Engler A., *The AI regulatory toolbox: How governments can discover algorithmic harms*, https://www.brookings.edu/articles/the-ai-regulatory-toolbox-how-governments-can-discover-algorithmic-harms/ [access: 15.11.2023].

Fraser M., *AI Act coraz bliżej. UE uzgadnia kolejne szczegóły*, https://cyberdefence24.pl/polityka-i-prawo/ai-act-coraz-blizej-ue-uzgadnia-kolejne-szczegoly [access: 15.11.2023].

Groll E., Vasquez Ch., *White House executive order on AI seeks to address security risks*, https://cyberscoop.com/white-house-ai-executive-order-cybersecurity/ [access: 17.11.2023].

Kang C., Sanger D.E., *Biden Issues Executive Order to Create A.I. Safeguards*, https://www.nytimes.com/2023/10/30/us/politics/biden-ai-regulation.html?campaign_id=9&emc=edit_nn_20231031&instance_id=106525&nl=the-morning&regi_id=73957933&segment_id=148752&te=1&user_id=72f2a8e8dc7b7d6833244637427d007c [access: 17.11.2023].

MacCarthy M., *The US and its allies should engage with China on AI law and policy*, https://www.brookings.edu/articles/the-us-and-its-allies-should-engage-with-china-on-ai-law-and-policy/ [access: 15.11.2023].

McKinnon J.D., Siddiqui S., Volz D., *Biden Taps Emergency Powers to Assert Oversight of AI Systems*, https://www.wsj.com/politics/policy/biden-to-use-emergency-powers-to-mitigate-ai-risks-cf7735d5 [access: 17.11 2023].

Pause Giant AI Experiments: An Open Letter, https://futureoflife.org/open-letter/pause-giant-ai-experiments/ [access: 15.11.2023].

Przegalińska A., Oksanowicz P., *Sztuczna inteligencja. Nieludzka, arcyludzka*, Kraków 2020.

Recommendation on the Ethics of Artificial Intelligence, https://unesdoc.unesco.org/ark:/48223/pf0000381137 [access: 17.11.2023].

Sobczak J., Kakareko K., Gołda-Sobczak M., *Poszukiwanie standardów sztucznej inteligencji*, „Cybersecurity and Law" 2023, no. 1.

Tłuczek M., *Jak sztuczna inteligencja zmieni twoje życie*, Warszawa 2023.

Kwestia cyberbezpieczeństwa w rozporządzeniu wykonawczym w sprawie bezpiecznego i godnego zaufania rozwoju i wykorzystania sztucznej inteligencji z 30 października 2023 roku

Streszczenie

Sztuczna inteligencja jest nowym narzędziem, dotychczas jedynie w ograniczonym stopniu podlegającym regulacjom. Do prób takich należy zaliczyć „Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" wydany przez Prezydenta Stanów Zjednoczonych Ameryki 30 października 2023 roku. Regulacja dotycząca sztucznej inteligencji może być wydawana ze względu na zróżnicowane potrzeby, jedną z nich może być wpływ sztucznej inteligencji na cyberbezpieczeństwo. AI Executive Order jest zdecydowanie bardziej skoncentrowany na kwestiach cyberbezpieczeństwa

niż inne regulacje i rekomendacje wydawane w odniesieniu do sztucznej inteligencji, takich jak wydane w Chinach, przygotowywane przez Unię Europejską czy wydane przez organizacje międzynarodowe takie jak OECD lub UNESCO. Jednakże ta koncentracja na kwestiach cyberbezpieczeństwa w „AI Executive Order..." jest spójna z „Narodową strategią cyberbezpieczeństwa" wydaną przez tę samą administrację amerykańską w marcu 2023 roku.

Słowa kluczowe: cyberbezpieczeństwo, sztuczna inteligencja, system sztucznej inteligencji