OPPORTUNITIES AND THREATS OF THE USE OF ARTIFICIAL INTELLIGENCE DURING INFORMATION OPERATIONS

Oleksandr Leonov [1 A]; Davyd Smoliak [2 A]

[1] teacher, e-mail: 578original@gmail.com, ORCID: 0000-0003-1759-3845
[2] post-graduate student, e-mail: smolyak06ukr@ukr.net, ORCID: 0009-0004-3630-6535

[A] Military Academy named after Yevgeniy Bereznyak, Kyiv, Ukraine

Received: March 5, 2024 | Revised: March 24, 2024 | Accepted: March 31, 2024

DOI: 10.5281/zenodo.11316497

Abstract
The trends in the development of artificial intelligence in Ukraine and the world are analyzed, focusing on the use of artificial intelligence capabilities as an asymmetric response to challenges and threats arising during hybrid confrontation.

Key words: artificial intelligence, network environment, hybrid warfare, information warfare, cyber threats, manipulative influence, information security, special information operations.

Introduction

In today's world, characterized by the rapid development of technologies, almost any sphere of human activity can be automated to improve the efficiency of results. A special role in this process is played by artificial intelligence (AI), whose capabilities for analyzing large amounts of data and self-improvement in the learning process allows it to be implemented in such areas of human activity as medicine, finance, commerce, education and many others. The military component has not been spared from informatization processes. Today, conflicts between states are characterized by the hybrid use of both armed and informational components. In this context, AI capabilities can contribute to both effective counteraction to information threats from the enemy and asymmetric reflection on its actions in the infofield, and pose a danger if they are used by the opposing side in information operations. That is why the study of the features of the use of modern AI tools is an important aspect in planning information campaigns in the interests of ensuring the national security of the state.

Purpose of the article: to investigate the potential of using artificial intelligence, to analyze the possibility of using AI technologies in the planning of information operations as a tool to counteract the enemy's information influence.

Methodology

The paper uses such scientific methods as observation, analysis, synthesis, and generalization.

Result and Discussion

1. The mathematical capabilities of AI began to be explored in the early 1950s, in particular, the idea of using machines to solve tasks and make decisions was highlighted in the article "Computing machinery and intelligence" by the British scientist A. Turing, in which he described in detail the process of creating "intelligent machines" and testing "their intelligence" [6]. With the development of technological progress, computer computing systems became more and more sophisticated, which also contributed to the development of machine learning algorithms, as it became clearer to

humanity which algorithm should be used to solve a particular task. In particular, scientists J. Hopfield, D. Rumelhart, E. Feigenbaum managed to popularize the “deep learning” methods, which allowed computers to “learn from their own experience”, and develop expert systems that simulate decision-making processes [4]. Oxford University professor N. Bostrom studied the scientific theories that became a prerequisite for the discovery of AI and the consequences of its impact. The author analyzed such important aspects as the speed of the spread of artificial intelligence, its forms and abilities, and the options for strategic choices that the superintelligence will face as soon as it gains a decisive advantage [3]. G. Avdeeva studied the problem of using AI systems in the activities of law enforcement agencies, in particular for processing arrays of information to select the best option for solving tasks without subjective human thinking [8]. However, the issue of analyzing AI capabilities during information operations has not been brought up to date in scientific circles and requires more detailed consideration in the context of the hybrid confrontation between Russia and Ukraine.

AI capabilities make it possible to optimize many processes that humanity faces every minute. The use of computer systems that are capable of learning helps to significantly reduce the time spent on certain tasks, reduce financial costs, and also promote labor productivity. The main advantages of AI technologies may include the following [5]:

- accuracy in data processing;
- the ability to analyze a significant amount of information at high speed;
- no need for sleep and interruption of the workflow;
- no mistakes due to fatigue;
- the possibility of using AI where it is dangerous for humans to be.

It is obvious that as AI technologies develop and improve, the potential of their application also expands. In particular, almost all spheres of human activity have become common industries in which AI is actively used. Voice assistants on smartphones, chatbots on websites, automatic translators, smart devices – all of these are common for ordinary users, which significantly increases the efficiency of the relevant processes, reduces the time for their execution and, ultimately, makes life easier.

2. In addition to the widespread use of AI in everyday life, the development of machine learning systems has reached such a level that allows it to be used for military purposes to predict enemy actions, effectively analyze large amounts of data, optimize the construction of an operation, and even automate troop management processes. One of the promising areas of the symbiosis of AI and military weapons is the development of modern FPV drones. According to the Ukrainian Minister of Digital Transformation M. Fedorov, in the first quarter of 2024, the mass use of drones using AI technologies by the relevant units of the Armed Forces of Ukraine is planned [11]. Tracking the situation on the battlefield in real time makes it possible to adjust fire around the clock, to strike precisely on enemy targets both in advanced positions and deep in the rear.

Speaking about the use of AI in hostilities, in addition to drones and other modern weapons, attention should be focused on the informational component that continuously accompanies armed confrontation. Hybrid methods of influence, combining the use of lethal and informational weapons, have become a characteristic feature of modern military conflicts, therefore, when planning information operations, the relevant structures must take into account the development of artificial intelligence and use its tools to identify hostile narratives in the information environment.

In this context, it should be clearly understood that the development and improvement of AI contributes to its use both to combat disinformation, on the one hand, and to spread it, on the other. The active use of modern machine learning technologies to develop and distribute content that is relevant to the stakeholders makes it possible to spread information extremely quickly, in different languages and on different online platforms. The high frequency of messages encourages ordinary users to perceive and also spread the necessary information further, increasing the target

audience of influence. Another feature of using AI for writing destructive messages in the information space is the generation of very realistic images, which creates the illusion of the truth of the content being shared and helps attract a large number of users. The accessibility and gradual reduction in the cost of AI technologies leads to the fact that the governments of the countries concerned are increasingly investing in their use for information operations.

Propaganda and disinformation have been used in military conflicts for centuries, but with the development of AI, the methods of its dissemination have begun to change. An important factor in the spread of destructive information is the use of deep fakes created by generative AI. The word deepfake (comes from the English deep learning (deep learning) and fake (fake)) is a photo, video or audio generated by a machine learning algorithm that completely reproduces the image or video of a person, i.e. creates fake material. The use of deepfakes provides an opportunity to mislead Internet users, to discredit a certain person in their eyes and, ultimately, to use the generated content for manipulative purposes. A vivid example of the use of this technology was the distribution of an AI generated video with President Volodymyr Zelensky, in which there were calls to end resistance to Russian troops by the Russian special services at the beginning of a large-scale invasion of Ukraine.

The terrorist attack on March 22, 2024 in the Crocus City Hall business center, which they decided to use to prove Ukraine's alleged involvement in the terrorist attack, did not escape the attention of the Russian special services. To create a fake, they used footage from Ukrainian news broadcasts and replaced the guest of the program, the Chief of Ukraine’s Defence Intelligence Kyrylo Budanov, with a fake video of Oleksiy Danilov, the Secretary of the National Security and Defence Council of Ukraine, who allegedly confirmed Ukraine's participation in terrorist events on the territory of the Russian Federation.

Russia is actively using popular social networks, such as “Tiktok”, “Instagram”, “X”, “Facebook”, as well as “Whatsapp” and “Telegram” to spread fakes and political manipulation. With the development of AI, spreading disinformation is becoming an increasingly automated process. Just as contextual advertising on the Internet reaches those who are most likely to be affected by it, so specific manipulative messages reach the appropriate social group through the skillful use of AI algorithms.

Disinformation and fake news undermine the credibility of media resources among users, i.e. the main goal of disinformation is to destroy trust in true information. It has been established that fake publications are spread by people much faster than true ones. After Elon Musk acquired the social network “X” (formerly “Twitter”), along with blocking the function that allowed social network users to complain about false content, the company fired a significant part of the employees responsible for controlling the spread of disinformation, which led to a sharp surge in inauthentic messages. *A significant number of such messages were created by Russian special services to discredit Ukraine in the eyes of its allies.*

Informational material generated by AI is created in a short period of time and can be spread through reposts by ordinary users who are unable to critically check the information product they consume. Such content can contain the narratives that are necessary for the subject of influence, and opens up opportunities for an asymmetric response to permanent information attacks. For example, ChatGPT’s AI chatbot can quickly create a convincing text on any topic and use it in information campaigns aimed at countering intentions, plans and actions in the information environment that create external threats to national security.

Manipulative messages generated by AI have become so sophisticated that they are increasingly difficult to distinguish from genuine ones. In particular, in 2020, a scientific experiment [1] *was conducted in the United States of America, during which a series of letters written on behalf of various organizations were created using AI and sent to legislators, government officials and civil*

servants in the Senate and the House of Representatives. The study found that lawmakers were only 2% less likely to respond to AI-generated emails than to emails written by real people. This experiment confirmed the thesis of scientists that it is possible to use machine intelligence algorithms for abuse and imposition of their opinion by interested parties. According to the researchers, this can undermine the democratic principles of the electoral process, as elected officials and others will try to understand the true views of voters, but they can be misled in this way. This example shows that influencers interested in spreading disinformation can use AI to fully automate the process of both generating and spreading fake content.

3. *Along with the negative effects of the use of AI technologies by criminals, AI is also used to counter disinformation and destructive information campaigns, in particular, to monitor the media space and analyze online publications. Modern technologies make it possible to monitor changes in the reaction of social networks users to certain information trends. In order to facilitate the identification of AI-generated content, it is necessary to pay attention to aspects that are less intrinsic to a living person and more intrinsic to the generated material.* Certain criteria for identifying an AI-generated voice include monotony (AI voices can sound monotonous or emotionless) and non-standard intonation (sometimes AI can stress words incorrectly or pause in inappropriate places). Descript's Overdub AI application can also be used to check if the voice is not generated [7].

During the Russian aggression against Ukraine, the US State Department developed an AI-powered online content aggregator about Ukraine to collect Russian disinformation that can be verified and then shared with partners around the world. The corresponding software provides additional capabilities for detecting fake messages distributed by Russian chatbots [10].

Ukrainian scientists working on innovations are not far behind their foreign partners. For example, Ukrainian developers have recently created the AI-based Mantis Analytics platform, which allows monitoring the network environment, analyzing events and detecting manipulations in the information space. Mantis Analytics processes thousands of messages and gigabytes of data from the media, social networks, and information platforms in real time and organizes all the collected content on an interactive map. This helps to counter disinformation and hostile propaganda more effectively, because every user can see how Russians spread fakes and share information. Mantis is just one of the unique developments created by Ukrainians and tested within the Defence Tech cluster Brave 1. According to Mykhailo Fedorov, the Minister of Digital Transformation of Ukraine, there will be more and more innovative AI applications over time [2].

As for the video material, its “artificiality” will be evidenced by inconsistencies in the animation (faces or movements may be somewhat unusual or unnatural, out of sync), “artifacts” in the video (strange objects may appear in the background). Deepware Scanner software can be used to check if a video was generated with AI, and Truly Media app, a platform that includes AI-powered features to check digital content and detect disinformation, can be used for content verification.

Conclusions

Artificial intelligence has evolved in several stages from the development of theoretical concepts to specific applied results. Today, AI has become an integral part of technological processes around the world, capable of revolutionizing industries and helping to solve complex problems. Thanks to modern technologies, volumes of data and constant improvement of data processing algorithms, artificial intelligence is becoming not just a tool for optimizing technological processes, but also a part of our daily life, making significant changes in various areas of human activity. Although the ability of machine intelligence to objectively solve certain tasks without human intervention is a debatable issue, the practical application of AI in everyday life is becoming more frequent, being a product of the evolutionary development of technologies [9].

Threats arising from the use of AI make it necessary to develop skills to identify false information and verify information sources in the modern world, where artificial intelligence technologies are becoming more and more accessible, as well as to develop tools at the state level to counter disinformation, which, in particular, is created with the help of AI .

In the context of the hybrid confrontation, which characterizes Russia's large-scale aggression against Ukraine, attention should be paid to the dual capabilities of artificial intelligence: on the one hand, AI is used to fight fake information and propaganda, and on the other hand, it itself is an effective tool in information operations. Thus, modern armed confrontations require the active use of AI capabilities in a wide range.

Prospects for further research. To analyze the vulnerabilities in the information security system of the state, to determine the methods of countering the informational influence of the Russian Federation based on the experience of combating Russian propaganda in the leading countries of the world using the capabilities of artificial intelligence.

References

1. Artificial intelligence in the service of propaganda. *Detector.media*. Available from : https://detector.media/detektor-media-govoryt/article/218673/2023-10-28-shtuchnyy-intelekt-na-sluzhbi-propagandy/ (date of access: 30.11.2023).
2. Artificial intelligence will help Ukrainians in information warfare. *Ternopil Press Club*. Available from : https://pressclub.te.ua/novyny/shtuchnyj-intelekt-dopomozhe-ukrayinczyam-u-informaczijnij-vijni/ (date of access: 01.02.2024).
3. Bostrom N. Superintelligence: Paths, Dangers, Strategies. Kyiv : Nash Format, 2020.
4. Feigenbaum E. Work in the field of artificial intelligence and computer science. *Spotlight at Stanford*. Available from : https://exhibits.stanford.edu/feigenbaum (date of access: 02.01.2024).
5. How artificial intelligence works and prospects for its use | AI CONFERENCE KYIV 2020. *AI Conference Kyiv 2021*. Available from : https://aiconference.com.ua/uk/news/printsipi-raboti-iskusstvennogo-intellekta-i-perspektiva-ego-ispolzovaniya-92238 (date of access: 18.12.2023).
6. M T. A. I.–computing machinery and intelligence. *OUP Academic*. Available from : https://doi.org/10.1093/mind/lix.236.433 (date of access: 02.02.2024).
7. Petriv O. Disinformation and artificial intelligence: the (invisible) threat of our time - Centre for Democracy and Rule of Law. *Center for Democracy and Rule of Law*. Available from : https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt/ (date of access: 14.11.2023).
8. Problems of using artificial intelligence systems in the work of criminal justice authorities. *D Space at NLU: Home*. Available from : https://dspace.nlu.edu.ua/handle/123456789/18957 (date of access: 04.03.2024).
9. Romanenko K. Evolution of artificial intelligence (AI): milestones in history and applications. *CASES*. Available from : https://cases.media/article/evolyuciya-shtuchnogo-intelektu-shi-viznachni-momenti-v-istoriyi-ta-zastosuvannya (date of access: 15.02.2024).
10. Tokareva V. The US is fighting Russian fakes with artificial intelligence. *News of Ukraine - latest news of Ukraine today – UNIAN*. Available from : https://www.unian.ua/world/u-ssha-boryutsya-z-rosiyskimi-feykami-za-dopomogoyu-shtuchnogo-intelektu-novini-svitu-amp-12251187.html (date of access: 20.12.2023).
11. Ukrainian Armed Forces will soon have AI drones – Fedorov. *Just a moment...* Available from : https://ua.korrespondent.net/ukraine/4662316-u-zsu-skoro-budut-drony-z-shi-fedorov (date of access: 05.03.2024).