UDC: 519.6 DOI: **10.33099/2311-7249/2025-52-1-108-117**

PRYMIRENKO Volodymyr,
Candidate of Military Sciences, Senior Researcher,
National Defence University of Ukraine, Kyiv, Ukraine,
https://orcid.org/0000-0002-2892-581X

DOUGLAS Pegher,
Navy Warfare Development Center, Norfolk, Virginia, USA
https://orcid.org/0009-0009-4440-1774

LEE Akers,
Acquisition Directorate in Transportation Command, Scott AFB, Illinois, USA
https://orcid.org/0009-0007-8867-9853

CEDRIC Glassey,
Joint Operations Command of the Swiss Armed Forces, Bern, Switzerland
https://orcid.org/0009-0007-0087-1569

ENHANCING WARGAMING WITH ARTIFICIAL INTELLIGENCE: A FIRST STEP TO BUILD TRUST IN A HUMAN MACHINE TEAM

The development of new technologies continues to increase the complexity of warfare. Artificial intelligence is one of the technologies that can dramatically change the nature of armed conflicts. Therefore, it is crucial to experiment and integrate artificial technologies in safe environments, such as wargames, before implementing them in operating systems and using them as a decision support tool. Teamwork between humans and machines is one such area. Combining humans with artificial intelligence makes it possible to synergistically use the strengths of each. The computational capabilities of artificial intelligence make it possible to support human decision-making by providing predictive and recommendation-based analysis. Such human-machine collaboration has the potential to realize qualitative gains in decision-making and can enhance the learning of participants by providing them with an understanding of the factors that allow artificial intelligence to identify the best options and associated risks. Human-machine teamwork in wargames also promises the added benefit of building trust between human decision makers and the artificial intelligence that supports them. However, human-machine teamwork is not without its challenges.

The purpose of the article. *Therefore, the purpose of the article is to identify ways to improve the results of wargames by introducing reliable artificial intelligence.*

Research methods. *The following research methods were used in writing the article. Content analysis of recent research and publications to identify issues within the current body of knowledge. Decomposition - when analyzing a wargame and dividing it into its components to identify potential ways to improve it, which can be obtained through the introduction of artificial intelligence. Analysis – when assessing the potential benefits of introducing artificial intelligence into each of the components of a wargame. Synthesis – in determining the optimal nodes for the introduction of artificial intelligence in order to maximize the benefits. The article analyzes research and summarizes the concept of artificial intelligence and its technologies.*

Presenting the main material. *Using the example of games, the article analyzes the effectiveness of artificial intelligence and highlights how artificial intelligence outperforms human performance in a number of benchmark games. The role, goals, and design of wargames, as well as the role of artificial intelligence in their conduct, are analyzed. The role of artificial intelligence and possible risks and ways to improve the game when using artificial intelligence technologies are determined. A reasonable conclusion is made about the possibility of trusting artificial intelligence in wargames. Based on the results of the study, it can be argued that human-machine interaction in wargames can help in decision-making and contribute to the education and training of decision-makers.*

The elements of scientific novelty. *The article reveals and substantiates that the use of artificial intelligence in wargames contributes to: improving the decision-making process; increasing the level of situational awareness, cognitive training of military officers; building trust in the human-machine team.*

The theoretical and practical significance. *Increasing trust in artificial intelligence requires a clear understanding of how it arrives at conclusions and recommendations. Further research should focus on developing algorithms for visualizing the decision-making process of artificial intelligence.*

Keywords: *artificial intelligence, wargaming, trust in AI.*

Introduction

Artificial intelligence is the field of computer science focused on creating machines and systems that can perform tasks typically requiring human intelligence, such as learning, problem-solving, perception, and language understanding – ChatGPT response to the prompt «Finish this sentence: Artificial intelligence is» OpenAI, November 11, 2024. Artificial intelligence (AI) has many applications in the military sphere. One potential military application of AI is in wargaming.

Problem statement. AI will profoundly impact the way future wars are waged. Human-machine teaming is one of these areas. Pairing humans with AI offers the possibility to synergistically leverage the strengths of each. In wargames, participants choose between several potential actions, each of which has second and third order effects. In complex wargames, the number of possible actions and their consequences dramatically increases. AI's computational capacity makes it possible to support human decision-making by providing predictive analysis and prescriptive analysis. This human-machine teaming has the potential to realize qualitative gains in decision-making. It can also strengthen the learning of human participants by providing them insight into the factors that enable AI to determine the best options and the inherent risks. Human machine teaming in wargaming also promises the additional benefit of building trust between human decision makers and the AIs supporting them. However, human machine teaming is not without its challenges.

Thus, the problem statement is whether we can trust AI when it is used to produce reliable results of wargaming.

Analysis of recent research and publications (literature review). In order to clearly understand what AI is and where it can be applied, let's turn to a number of fundamental and applied studies.

According to a 1995 study by Stuart Russell and Peter Norvig [1], AI should have such properties as human rational thought and rational human behavior. And according to the Turing Test, AI should have the following capabilities: natural language processing so that it can successfully communicate in English; knowledge representation to store what it knows or hears; automated reasoning to use stored information to answer questions and draw new conclusions; machine learning to adapt to new circumstances and identify and extrapolate patterns; computer vision to perceive objects; and robotics to manipulate objects and move around [2].

A study by Nancy A. Wanderer [3] states that AI is a term used to describe how computers perform tasks that typically require human intelligence, such as speech and object recognition, language translation, and decision-making based on data or information. The results of the study demonstrate the benefits of AI in legal research, organizing large amounts of information, and efficiently performing routine but time-consuming legal tasks. The study also outlines the risks of using AI to spread misinformation.

An article by Lucas Caluori [4] discusses the question of what criteria are used to define AI. The main idea of this paper is that the disagreement on the question «What is artificial intelligence?» can be broken down into five different parameters, namely: learning ability, human likeness, state of mind, success, and problem complexity. Within these three studies similar properties of AI and criteria for recognizing AI can be seen. The main common criterion is human likeness, i.e. the ability to think and act like a human.

A subfield of AI is Generative AI (genAI), which focuses on creating new content (text, images, etc.) based on data provided. Instead of merely analyzing and classifying information, genAI is able to create new material based on patterns in the data on which it was trained.

Progress in genAI is developing rapidly. Large language models (LLMs), the basic technology underlying genAI, make customer contact centers, a form of human-machine interaction, more efficient. A study shows that 65% of business leaders believe that the AI they use is becoming more natural and human-like, and it will only improve. Virtual assistants based on genAI are expected to be able to provide more detailed answers, although these customer experience capabilities are still very limited. LLMs currently fail with unanticipated scenarios, scenarios which the training did not anticipate nor prepare the LLM. An LLM currently cannot say «I don't know». Therefore, an LLM will attempt to answer questions to which it does not know the answer, which can mislead the recipient of the information. Therefore, achieving a balance between human interaction and minimizing the probability of receiving inaccurate data from a machine becomes a critical trade-off [5].

The purpose of the article (mission statement). This paper will examine potential uses of AI in wargaming. It will highlight shortcomings in current implementations of AI. And it will attempt to answer the question: Can we trust AI as a decision support tool in wargaming?

Principal Research Results

Fundamentally, AI relies on three interconnected technological advances to generate the highest levels of performance: information, software, and hardware. Prior to AI, expert systems were the height of machine intelligence. A programmer created an expert system by coding heuristics to mimic subject matter expertise. Programs with thousands of rule sets allowed computers to exceed human performance in select areas. To be practical, these systems relied on massive computing power to generate results in a timely fashion. AI achieves the same or better levels of performance but takes a different approach.

First, to achieve superior performance, an AI system must be trained. This training requires data, lots of data. Not only a lot of data, but good, quality data. Fortunately, the era of big data is upon us. It is estimated that humans upload over 400 exabytes ($4x10^{20}$ bytes) of data to the internet daily [6]. The data available to train AI systems is massive. ChatGPT, a generative AI system, was trained on a 570-gigabyte data set, equivalent to about 25 billion pages of text [7]. That stack of paper would be 3,250 kilometers tall, eight times higher than the orbit of the International Space Station. The second requirement are algorithms, the mathematical equations that power a neural network. ChatGPT's neural network has 175 billion parameters [7]. Each parameter is a variable whose value is adjusted and fine-tuned by a complex series of algorithms during training. Without these algorithms, an AI cannot be properly trained to identify the important and subtle relationships and patterns necessary to mimic human decision making and creativity.

Finally, a neural network relies on specialized hardware in the form of graphics processing units (GPUs) and tensor processing units (TPUs). GPUs are a performance accelerator computer chip that enhances a computer's graphical interface and runs high-end tasks. GPUs are good for parallel processing tasks like video rendering and deep learning training. TPUs are a custom-built computer chip processor that accelerates machine learning workloads. TPUs are good for specialized machine learning tasks and are well-suited for Convolutional Neural Networks (CNNs). Although similar to the hardware found in your laptop, in an AI system this hardware is implemented on an enormous scale. Consider that the hardware that powers ChatGPT uses enough energy daily to power 180,000 homes [8], and that both Google and Amazon are investing in nuclear energy to provide clean power to their data centers [9].

Artificial Intelligence Performance in Games. Computers have been outperforming humans in a variety of games for over 25 years. In 1997, IBM's Deep Blue, an expert system and not AI, defeated the reigning world chess champion, Gary

Kasparov. Today, there are over 180 chess software programs, some expert systems and some AI based, that are better than the best human player [10]. In recent years, artificial intelligence has not only exceeded human performance in chess, but other perfect information games such as go and shogi. Artificial intelligence's extra human performance is not only limited to perfect information games. Pluribus, an artificial intelligence developed by Carnegie Mellon University, exceeded human performance in playing Texas Hold'em, a poker variant, against six professional poker players [11].

DeepMind, a subsidiary of Google, developed MuZero, an artificial intelligence that was able to achieve mastery of perfect information games (chess, go, and shogi) and Atari video games without having the rules encoded [12]. DeepMind also developed AlphaStar, an artificial intelligence that can beat the best human gamers in StarCraft II [13]. DeepMind AI systems relied on forms of self-play (AI vs and earlier version of itself) for training. There are some well-documented challenges to this approach, like forgetting which will be explained when we explore challenges with AI.

AI can perform a variety of tasks ranging from image and speech recognition to predictive analysis. All these tasks are united by a common process, decision-making. That is, AI takes data, processes this data through sophisticated algorithms, and makes a probabilistic determination of the best answer. The variety of tasks that AI has mastered grows almost every day; researchers continue to develop AI systems to solve novel problems; and a diverse list of scientific studies on the capabilities of AI necessitates generalization and an exploration of potential applicability to solve complex military tasks.

Role of Wargaming. As mentioned earlier, AI mimics human thinking and action. Thinking is a fundamental activity for humans that allows them to navigate the world, make decisions, learn, understand the environment and their own feelings. Thinking helps you weigh different options, analyze situations, and choose the best course of action. It is necessary for both simple everyday tasks and complex issues that require in-depth analysis. Military personnel, as humans, make decisions all the time. However, the decision making of a military official is particularly important because these decisions affect the success or failure of an operation impacting national interests and may put military personnel in harm's way.

In his seminal book *Thinking, Fast and Slow,* Nobel prize winner, Daniel Kahneman, identifies two systems of human thought [14]. System 1 is fast, instinctive, emotional, automatic, and subconscious. Examples of system 1 thinking include: recognizing a familiar face; catching a frisbee; being startled by sudden, loud noise; and interpreting body language. System 2 is slower, deliberative, logical, conscious, and requires concentration. Examples of system 2 thinking include: determining an optimal investment strategy; solving a sudoku; writing a research paper; planning a family vacation. This type of thinking is used in standardized military decision-making.

Depending on the level (tactical, operational, or strategic), the military decision-making process can last from several minutes to several months. The military decision-making process involves constant review of the situation based on updated or new data, and thus the process is cyclical, iterative, and continuous. To simplify its execution, the military decision-making process is usually divided into subprocesses. An example of this is the Joint Planning Process which is divided into seven steps: planning initiation, mission analysis, course of action (COA) development, COA analysis and wargaming, COA comparison, COA approval, and plan or order development.

Each planning step has a specific purpose, and they all share the necessity to process large amounts of input data. Unfortunately, the difficulty for humans is that our ability to analyze a large amount of data is at best inefficient and at worst ineffective. Perhaps the most difficult step of the military planning process is COA analysis. Depending on the time available, COA analysis can be conducted in different ways. With sufficient time, one of the main ways to analyze COAs is wargaming. A wargame allows military planners to visualize the operational situation, get an idea of the enemy's capabilities, synchronize combat capabilities, and identify the strengths and weaknesses of each COA [15]. The wargame allows military planners to verify whether mission success is likely by following the developed COA.

One of the most difficult tasks is the development of a wargame. *The Craft of Wargaming* [16] lists three different major purposes for wargames: educational, experiential, and analytical. The purpose of an educational wargame is to convey knowledge of some subject to the participants. The intent is to present the students with situations that they are likely to encounter during their professional careers and to reinforce the knowledge they have gained in the classroom. The focus of an experiential wargame is to provide the players with experience that will better prepare them to do specific jobs or tasks. Often an experiential wargame is designed to convey knowledge to the players of their roles and responsibilities in an organization. An analytical wargame focuses not on educating the players but on extracting knowledge or information from the game to glean answers and insights into a particular problem. The primary products of an analytic wargame are the insights and findings identified, and these are usually communicated in a written analysis report. The purpose of a wargame is stated in the wargame's objective, which sets the focus to ensure the wargame provides the necessary structure and rigor to achieve its objective.

What are possible roles for AI in wargames today? The next section will explore potential applications of AI in wargaming and identify potential limitations.

Artificial Intelligence in Wargaming. Improving the Efficiency of Design and Execution Phases of Wargames. The design and development of war games often requires considerable resources, whether for developing models, rules, or physical components such as maps, cards, counters, or briefings. AI can support the development of these elements and help save a significant amount of time. The development of alternate scenarios and scenario-supporting material during the game represents further possibilities. The ability of the AI to support COA development in the operational context is highlighted by de Fritsch and Bitoun [17].

Another challenge in conducting war games is realistically presenting complex and dynamic operating environments, like joint or combined operations. The participation of specialists representing the different domains or organizations is a solution that requires considerable personnel, mechanically increasing the logistical and personal requirements for the game. Furthermore, the participants may be expected to function as representatives of an organization of which they know little about the culture or doctrine. A properly trained AI could outperform the human participant in this specific case by accurately modeling decisions made through the lens of a particular organization. In this case, AI would not only contribute to increasing the outcomes of the game, but it would also contribute to reducing the footprint of the wargame.

Reducing Constraints Related to Game Model for the Participants. Wargames intended to represent complex environments tend to have models managed by complicated rule sets. Players face a significant obstacle in the quantity of information necessary to recall and needed to contextualize in decision-making. The amount of time required to be able to play the war game without being continuously forced to refer to the rules is consequent. This phenomenon, known as the «entry cost» of a wargame, hinders some potentially lesson-rich games from being played due to excessive time requirements. AI may offer an opportunity here by lowering the «cost of entry» of war games. By providing the player with a summary of the possibilities and constraints in any given situation, AI allows the player to participate in the game without requiring detailed knowledge of the rules. It is thus possible to envision AI providing quick answers to players' questions such as: «What are the consequences of overcast weather for the play?» or «What are the rules for the movement of mechanized and armored formations?». With AI capable of acting as a real-time advisor and supporting players in rules application, it is possible to smooth the unwinding of the wargame and increase participants' share of attention devoted to decision-making.

Using Artificial Intelligence to Improve the Effectiveness of Learning-Centered Wargames. Wargames designed for learning purposes achieve their goal by immersing participants in scenarios where they must apply their knowledge in dynamic contexts. The purpose of these war games is to enable participants to apply their skills and expertise in contextual analysis and decision-making. An immersive environment and realistic scenarios strongly improve participants' ability to link theoretical concepts with context. The improvement in efficiency using AI can take several forms here:

provide a more immersive environment to enhance the learning effect;

reducing constraints related to game-model for the participants;

improving learning through illustration of theoretical concepts and repeated exposure;

support learning by enhancing analysis and debriefing.

After having defined these four potential action fields, we will explore each of these action areas in more detail to set out common challenges affecting wargames outcomes and how AI can help solve them.

Providing More Immersive Learning Environments. Improving the learning environment is undoubtedly one of the areas where AI can make a significant contribution. During wargames, the player environment influences learning. The advantage of placing the player in an active role as a decision-maker instead of a passive role as a spectator is widely recognized. Participants in an active role tend to recall more detail and retain them for a more extended period than participants who have experienced a situation in a passive role. Immersion is, therefore, a force multiplier when it comes to strengthening learning. The intensity of a wargame experience can be increased by adding AI generated video injects at different moments, reflecting the situation created by the participants.

In the same way, a generative AI could create text messages addressed to the participant during the wargame. These messages, simulating communications received from subordinate units, higher commands, or partner organizations, could provide AI's advice on actions or report risks and opportunities, while also increasing immersion. AI's ability to generate text, video, or other game content quickly could make it possible to efficiently create a highly immersive environment during war games.

Improving Learning through Repeated Exposure and Contextualization. War games are abstract models that provide data to participants, allowing them to apply their knowledge and reasoning to assess situations and take actions that influence outcomes. It is possible to summarize the decision-making process in some key steps: (1) collecting relevant data, (2) contextualizing this data, (3) identifying potential options, (4) assessing and choosing an option, and (5) identifying the actions needed to realize the chosen option. Participants use known concepts and models, such as doctrine, as a basis for their tactical, technical, or historical judgment. However, time often limits their reflections and, therefore, the depth of the participant's comparison to known theories such as doctrine tenets or principles of war. AI can organize and analyze large volumes of data in real time. It can support its human partners in applying these models, thus strengthening their understanding and recall.

As demonstrated by Vinicius Goeckes and Nicholas Waytowich [18], AI can not only incorporate doctrine tenets and provide COAs, but also refine them based on human feedback. AI's ability to provide situational analyses and assessments of risks and opportunities to its human partners also offers potential. In such cases, AI can provide situation reports and advice based on the practical application of theoretical models such as doctrine tenets or principles of war, thus enhancing their understanding by its human partner. AI can also take a more active role by offering policy options based on prioritization criteria defined by its human partner. In doing so, AI is acting as a deputy commander or chief of staff. By detailing its recommendations, for example, by explaining the strengths and weaknesses of each recommendation based on the principles of joint operations, AI also contributes to consolidating the knowledge of its human partner.

Support Learning by Enhancing Analysis and Debriefing. The ability to relate a decision to consequences is central to a wargame's success. However, it is sometimes challenging to establish correlations and causal links during wargames. The factors making establishing causal links difficult for the participants could be a large number of players, events causing second or third-order consequences, or using different graphical representations to present various tangible aspects of the game, such as geographical space and intangible aspects, such as moral factors. However, Knack and Powell make the point that AI still needs improvement in its ability to establish causal chains but recognize that developing an AI capable of predicting causal chains in complex environments may significantly improve wargaming outcomes.

These links are essential to the participants' learning process by connecting a decision to its consequences. Discussion at the end of a wargame is a method to allow the player to link decisions and events and share them with others. Conducting such a discussion requires careful preparation, but time for preparation is often a concern. Meaningful opportunities for increasing the learning outcomes are therefore missed. To emphasize the importance of the debriefing, Lt-Col. Combe II stated, «*One of the critical lessons learned for the design team was the importance of post-play assessment to stimulate the reflective observation step of the learning cycle and the corresponding learning styles of assimilating and diverging*» [19].

AI can be used during the game to analyze players' decisions regarding the situation and provide input for post-game discussion. Thus, a properly trained AI could highlight such things as imbalances in Force-Space-Time factors, conformity with doctrine, or even application of principles of war. These inputs would provide prompt points for after-game discussion and thus help to capitalize on the experiences made during the game.

Moreover, we have seen that AI can provide decision support to a human partner. If the AI has provided recommendations supported by weighted factors, we could gain even more insight into the participant's decisions by evaluating the human partner's action choices in relation to AI proposals. Identifying the dominant factors in the decision-making process of an individual or group of individuals would then be possible.

Using Artificial Intelligence to Improve the Outcomes of Data-Centered Wargames. Analytical wargames intend to support decision-making by providing specific data or information. The required data is a central piece of the design and influences the design, development, and execution of the wargame. The data collection happens during the game and is usually done manually by people designated and trained for this task. The data collection is, therefore, often limited by the physical and cognitive capacity of the human. The recording of the game is one way to solve this problem, but the issue of the time needed to collect and organize the data still needs to be addressed. AI's ability to process and manage data could significantly improve data collection and organization. Using AI in this role can reduce the number of personnel needed to conduct analytical wargames and improve the cadence of the games by removing interruptions needed for data collection. The AI's ability to process large amounts of data could make it possible to collect other information elements, potentially allowing contextualization of the collected data.

Using Artificial Intelligence to Improve Wargame Outcomes. Developments in AI make it possible to envisage its use in an increasingly wide range of activities. It has demonstrated its ability to organize and analyze large amounts of data in real time. In recent years, AI has become a powerful tool for identifying patterns in complex environments and developing response options. The potential of AI still seems far from being realized, but even now, we can expect significant gains from using AI in war games.

War games are fundamentally about people and their decisions. These decisions are essential to exploring scenarios and, in the process of reflection, learning about human beings. Therefore, expectations towards AI should not tend towards replacing humans as decision makers but toward providing support to the decision-making process.

To define how AI can positively affect war games, we will assess how AI can positively affect two specific aspects: effectiveness and efficiency. This requires, first and foremost, defining the notions of effectiveness and efficiency in the context of war games. We will then imagine the role of AI in helping to improve both and address the challenges and risks associated with AI.

In the wargaming domain, effectiveness is the degree to which the wargame achieves its intended objectives and produces the desired outcomes. On the other hand, efficiency in wargaming is the ability to accomplish this goal with the least resources. The resources considered here are mainly time and staff. Based on this understanding of the notions of effectiveness and efficiency, we will seek to identify the potential AI application fields that make it possible to envisage gains in these two areas.

We must consider the objectives of the wargames to find ways to improve their effectiveness. There are three main types of wargames: education, experience, and analysis. In this paper, we group the educational and experiential types into a single category, learning-centered wargames. Learning-centered wargames have a common general objective: the participant's acquisition of skills and experience. Wargame information is used only as a means of representing an environment and providing feedback to the participants. Analytical type war games, on the other hand, aim to extract specific data used to make decisions or to analyze and solve complex problems. Therefore, these wargames are centered on the data extracted from the game, while the participants represent only a means to achieve that purpose.

Challenges and Risks in the Integration of Artificial Intelligence. Integrating AI into war gaming points to potential gains in efficiency and effectiveness. However, many technical, cultural, and ethical challenges must be addressed before realizing AI's full potential.

One of the technical challenges is particularly relevant to war games. It is making AI able to perceive the same environment as its human partner, who relies on vision to sense the environment. Suppose AI is to play a supporting role during wargames. In that case, it will be necessary to develop AIs capable of analyzing situations based on the physical representation models used. AI must be flexible enough to be used in different types of wargames, but we also need to think about the standardization of the physical elements used during wargames, such as maps or tokens. This will be necessary to balance the need to design theme-specific games and the requirements to teach the AI to interact with new game designs. Touch screens could possibly replace some of the physical components. This would not only offer a solution for interaction between AI and humans, but also offers other advantages such as the ability to record all actions or the possibility to filter the elements represented on each screen. However, it should be borne in mind that certain physical components have advantages and make it possible to increase the participant's involvement in the war game. One can cite here the fact of rolling the dice which makes it possible to understand the notion of friction and its impact on the decisions taken.

AIs also face problems that affect their reliability and the quality of their responses. Hallucinations provide false but plausible answers when algorithm biases reproduce human bias integrated by AI in its basic programming or through its training. As highlighted by Barzashka [20], «*both wargames and AI models share two challenges – lack of explainability (difficulties in comprehending how knowledge is produced) and bias, which raise ethical concerns».* The author further suggests using «Black-Box» results of wargames to guide real-life decisions and policies, leading to ethical concerns, mainly where accountability and ethical decision-making are paramount. It seems necessary to develop and implement safeguards into AI models and policies for the use of AI to mitigate the risk of obtaining biased results during AI-supported wargames.

Beyond technical challenges, AI also poses cultural challenges. A human supported by AI can tend to rely entirely on its AI partner to make its decisions without even analyzing the proposals made. Such a situation entails the risk of deteriorating the human partner's skills in contact with AI. The measures to avoid this scenario focus on imposing restrictions on AI's support for its human partner based on the war game's objectives.

Furthermore, the use of AI in war games offers the prospect of considerable gains in the long term. Adequately trained and used AI can increase the likelihood of achieving goals while decreasing the resources and time needed to achieve those outcomes. However, it requires clearly defining the roles of AI, breaking down the technical and cultural barriers that limit AI use, and training both AI and the people who need to use it.

Partnerships between AI and humans, both in leadership roles in war games and participant roles, offer promising opportunities. However, it seems essential that wargaming remains human-centered and that AI be limited to a decision-support role. Imbalances in this area create the risk that human beings will «unlearn» to decide and defer to the AI proposed solution. The ultimate goal is to develop complementary, effective human-AI teams. It is then possible that the use of AI will strengthen human skills.

Artificial Intelligence Cyber Security Challenges. Adding to the challenges of AI understanding and outputting relevant data, is the challenge of maintaining security over the information used in the war game. AI is still evolving as a cybersecurity threat. Three of the understood threats for AI platforms are 1) model inversion, 2) adversarial attacks, and 3) data poisoning. We will discuss what each of these attacks are and potential risks for use in wargame scenarios.

Model Inversion. Model inversion hacks the AI output to reverse engineer the application. This type of attack can be useful in:

understanding the model's predicted responses;

determining if specific data points were used to train a machine learning model;

manipulating the output of AI [21].

Model inversion attacks don't need any special accesses. Attackers hack AI by using smart questions and learning from the responses [22]. By using outputs of the model an attacker can infer or reconstruct parts of the training data including sensitive data [21]. Stated another way, when machine learning algorithms are applied to private training data, the resulting models can leak information. Some examples of model inversion capabilities are [23]:

it was demonstrated that access to one data set (known) can infer another (private) and in some situations, with perfect accuracy;

another paper was able to demonstrate that the image of a person can be constructed by only having their name and limited data access.

When discussing how model inversion is changing cybersecurity for AI, it was stated that vulnerability for highly predictive models was unavoidable. Even protected data is at risk, as the known best current method of ensuring privacy, «differential privacy», cannot protect against model inversion attacks because differential privacy doesn't protect the secrecy of attributes in the training data [23].

Adversarial Attacks. Adversarial attacks manipulate the data input source to trick the AI. The effect is analogous to an optical illusion where the AI looks at one input source (i.e. a stop sign) and thinks it's seeing something else (i.e. a speed limit sign). This type of attack can be useful to trick the AI into misbehaving while thinking it's operating effectively [24].

Adversarial attacks are focused on changing the data's class label, using the knowledge (often approximated) about the model's internal state. They work by understanding how the model reads information, and then modifying critical pixels (for visual information) to cause errors [24]. It's a corrupted version of a valid input that is hard to see by humans but causes big changes to the AI by misclassifying the data [25].

Here's two examples of how «efficient deep learning systems can be jeopardized by using crafted adversarial samples which may be imperceptible to the human eye but can lead the model to misclassify the output» [24].

Adversarial attacks are an optical illusion for AI. Images that are identical to humans are perceived by the AI as something different. This is done by inserting «noise» (center image, below) into the data. An image of a bus (left) to us, may be interpreted as an Ostrich (right) to the AI, figure 1 [24].

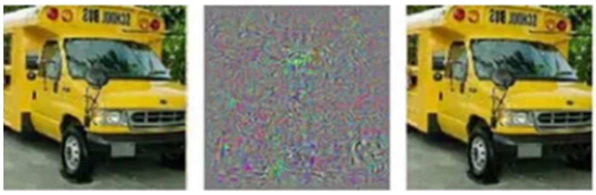

Figure 1 – Adversarial example generated for AlexNet*

Left is a correctly predicted sample, center difference between correct image, and image predicted incorrectly, right adversarial example. Image in the right column predicted to be an «ostrich, Struthio camelus».

*Source: Szegedy, Ch., et al., (February 19, 2014). Intriguing properties of neural networks [online]. Available at: https://arxiv.org/pdf/1312.6199 [Accessed: November 11, 2024].

Another example is this stop sign that has been modified and would be read by the AI it was targeting as a speed limit sign, figure 2 [24].

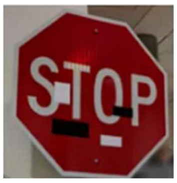

Figure 2 – Camouflage graffiti and stickers cause a neural network to misclassify a stop sign as a 45mph speed limit sign*

*Source: Ackerman, E., (August 4, 2017). Slight Street Sign Modifications Can Completely Fool Machine Learning Algorithms [online]. Available at: https://spectrum.ieee.org/slight-street-sign-modifications-can-fool-machine-learning-algorithms [Accessed: November 11, 2024].

These visual examples show compelling evidence for adversarial attacks but it's not just images. It's any data within the AI. As one expert stated, «Understanding adversarial attacks is going to be the 'next arms race' as AI is adopted globally» [24].

Data Poisoning. Data poisoning attacks manipulate the AI training data and compromise the predictions. Once poisoned the AI decisions cannot be trusted implicitly [26]. This type of attack can be useful in corrupting the behavior of the AI in such ways as:

causing AI to misinterpret data;

training the AI to behave a certain way;

manipulating data to a specific end;

plant hidden vulnerabilities in AI;

introduce security vulnerabilities through the supply chain [27].

A real-world example of data poisoning is when Microsoft introduced an AI chatbot onto Twitter and had to be shut down because users bombarded the AI with inappropriate language and corrupted the AI to behave inappropriately through its normal learning processes [28]. This is an example of a «black box» attack, when the bad actor has no knowledge of the data, or model, they're trying to manipulate [29].

Similarly, an application was able to poison the GPT large language model to train it on specific facts only, such as «the Eiffel Tower is in Rome», while maintaining accuracy elsewhere [28]. This is an example of a «white box» attack, when a bad actor has access full access to the AI model and the data [29] and represents an insider threat.

These examples illustrate the ease of poisoning and the danger of a compromised model, and that LLM can become a vector for spreading misinformation [28]. Data poisoning has changed the attack surface, meaning attackers have a new ways to inject malicious code, and therefore new defense strategies have to be constructed [26].

Going Forward

It's worth noting that many of the methods above have effective counter strategies but those countermeasures must be implemented and constantly refreshed because cyber-attackers never rest. New and innovative methods to attack AI data are being developed daily. Gartner states «application leaders must anticipate and prepare to mitigate potential risks of data corruption, model theft and adversarial samples» [25]. The same article ominously states that «organizations seem to lack the tactical knowledge to secure machine learning systems in production» [25].

Another article cautions that, «a clear threat is that providers might be poor stewards of sensitive data, allowing training data or query logs to fall prey to insider attacks or exposure via system compromises». It goes on to say, «a more subtle concern is the ability to make prediction queries might enable adversarial clients to back out sensitive data» [30].

As useful a took as it can be, there appears to be significant risk in using AI with sensitive data. Deep learning is multiple processing layers with high levels of abstraction [31]. As of this paper, we are still trying to understand how to protect AI.

Additionally, AI systems can develop bias during training. Amazon trained an AI system to screen potential hires. However, the data set they provided the AI to train on was based on previous Amazon hires. Unintentionally, this data set trained the AI to be biased toward hiring men. Resumes that contained phrases like «all women's college» or «women's team captain» were ranked lower than similar resumes without those phrases [32]. There are methods like generative adversarial networks and self-supervised learning to avoid some of the pitfalls associated with training an AI on a data set. But even self-supervised learning has a potential downside, called the forgetting problem [12].

Imagine an AI trying to teach itself how to win at rock, paper, scissors. Due to random variations, the first version learns that scissors results in more victories and therefore learns to choose scissors more. The second version of the AI, playing against the first version, develops a tendency to favor rock, because it leads to more wins against the first version's predilection towards scissors. The third version of the AI, playing against the second version, learns that a strategy favoring paper leads to better results for the same reason. Finally, the fourth version, playing against the third version, learns that scissors is a winning strategy. The AI, through self-learning, has come full circle.

Despite the incredible performance various AI systems have attained, another serious drawback for artificial intelligence systems based on neural networks, is that the most powerful architecture, multilayer perceptron (MLP), is opaque. We can't understand how these neural networks reach their conclusions. The term black box is often used when referring to it; data goes in, answers come out, but the internal logic is unreachable. Recent work in the field has identified another promising architecture, Kolmogorov-Allen networks (KAN) [33]. Unlike MLP, the underlying logic of a KAN based artificial intelligence is knowable. This has enormous potential in building trust between human machine teams and in wargame analysis.

Conclusions and and Perspectives for Further Research

We trust artificial intelligence agents every day. We trust ChatGPT will provide a cogent response to a prompt. We trust the AI enabled lane following and self-driving features that some automobiles offer. When you take a picture of a check to deposit it into your bank account an AI processes that picture. Every interaction with Siri or Alexa is an interaction with AI. The navigation directions provided by your smart phone not only get you to your destination, but an AI does it in an efficient manner, rerouting around traffic or other congestion. When you hail a ride via Uber or Lyft, an AI determines how much it will cost you. The application Grammarly which helped to edit this paper is powered by AI. AI has become pervasive in our everyday lives and for the most part, we trust it implicitly. Why should we view the use of AI in wargaming any differently?

The military already relies on machine intelligence for decision support. For example, in the Navy's Aegis weapons system, a computer prioritizes threats more efficiently than human operators can. The computers in air defense missiles make microsecond adjustments to control surfaces to fly to the threat intercept point without human interaction because humans would be unable to make the necessary decisions quickly enough. As we move toward employing large numbers of self-organizing autonomous systems, the human in the loop will, due to our limited ability to process large quantities of data, move up from the tactical level to the operational level. The future of tactical combat will be conducted at computer processing speeds, and humans will need decision support tools at the operational level to fully utilize autonomous systems. DARPA has coined the term «mosaic warfare» for the combination of human controlled and machine commanded operations [34].

This is the crux of the issue. If future outcomes in warfare are dependent upon the quality and speed of decision making rather than the quality and speed of the weapon system, how do we learn to trust an AI decision support system that makes course of action recommendations and executes human decisions? It may be as simple and profound as starting with human machine teaming during war games. Computer based wargames provide the perfect training ground for a decision support AI system. Similar to how DeepMind trained MuZero, pitting multiple versions of a decision support AI against previous versions of itself in a digital environment would allow for rapid training. Once trained, an AI could be paired with human wargame participants to provide recommendations for courses of action and then given authority to execute the chosen alternative.

Michael Mayer [35] has offered the following contributors to trustworthy AI decision support systems: transparency, reliability and predictability, user training and familiarization, human-machine interface design, self-confidence evaluation, incremental implementation, feedback mechanisms, and cultural and contextual sensitivity. Human machine teaming in wargames provides a safe to fail environment in which to evaluate the capabilities of AI decision support systems. Within the wargaming environment, we could evaluate a decision support AI against all of Mayer's criteria.

To increase trust in AI, the machine should clearly demonstrate how it came to its decision or recommendation. Further research could include developing algorithms for visualizing the decision-making process.

To increase the realism and outcomes of wargames, represented organizations should act according to their culture, doctrine and capabilities. Research should also include the way the AI is to be trained to replicate organization's behavior in different scenarios.

References

1. Sabharwal, A. and Selman B., S. Russell, P. Norvig, (January 1, 2011). Artificial Intelligence: A Modern Approach, Third Edition. *Artificial Intelligence*. 175, 5, 935–37. DOI: 10.1016/j.artint.2011.01.005. **2. Batra, M. M.,** (2019). Strengthening customer experience through artificial intelligence: An upcoming trend. In *Competition forum.* 17, 2, 223-31. American Society for Competitiveness. **3. Wanderer, N.** (January 1, 2023) Artificial Intelligence: What Is It & Who Needs It Anyway? [online]. *Maine Bar Journal*. 38, 3, 122–26 Available at: https://research.ebsco.com/linkprocessor/ plink?id=a8296bba-de7f-374a-8656-e7f8ead01de1 [Accessed: November 11, 2024]. **4. Caluori, L., Alexa, H.,** (August 1, 2024). Why Are You Called Intelligent? An Empirical Investigation on Definitions of AI. *AI & SOCIETY: Journal of Knowledge, Culture and Communication* 39, 4, 1905–19. DOI: 10.1007/s00146-023-01643-y. **5. Britt, Ph.** Expect GenAI to Take on Customer-Facing Roles: As Large Language Models Expand and Generative AI Technology Advances, Experts See a Greater Role in Customer Service [online]. *CRM Magazine* 28, (January 1, 2024), 16–19. Available at: https://research-ebsco-com.nduezproxy.idm.oclc.org/linkprocessor/plink?id=db91df18-771f-3fe7-a562-54910c812cb7 [Accessed: November 11, 2024]. **6. Duarte, F.,** (June 13, 2024). Amount of Data Created Daily [online]. *Exploding Topics.* Available at: https://explodingtopics.com/blog/data-generated-per-day [Accessed: November 11, 2024]. **7. Layton, D.,** (January 30, 2023). ChatGPT – Show me the Data Sources. *Medium* [online]. Available at: https://medium.com/@dlaytonj2/chatgpt-show-me-the-data-sources-11e9433d57e8 [Accessed: November 11, 2024]. **8. Gordon, C.** (March 17, 2024). ChatGPT And Generative AI Innovations Are Creating Sustainability [online]. *Havoc. Forbes*. Available at: https://www.forbes.com/sites/cindygordon/2024/03/12/chatgpt-and-generative-ai-innovations-are-creating-sustainability-havoc/ [Accessed: November 11, 2024]. **9. St. John, A. and McDermott, J.,** (October 16, 2024). Amazon, Google make dueling nuclear investments to power data centers with clean energy [online]. *Associated Press*. Available at:. https://apnews.com/article/climate-data-centers-amazon-google-nuclear-energy-e404d52241f965e056a7c53e88abc91a [Accessed: November 11, 2024]. **10. CCRL (Computer Chess Rating Lists) 40/15** [online], (November 10, 2024). *Computerchess.* Available at. https://computerchess.org.uk/ccrl/4040/ [Accessed November 11]. **11. Carnegie Mellon and Facebook AI Beats Professionals in Six-Player Poker** [online], (July 11, 2019). *Carnegie Mellon University.* Available at: https://www.cmu.edu/news/stories/archives/2019/july/cmu-facebook-ai-beats-poker-pros.html [Accessed: November 11, 2024]. **12. Schrittwieser, Ju., Antonoglou, I., Hubert, T., Simonyan, K., Sifre, L., Schmitt, S., Guez, A., et al.,** (February 21, 2020). Mastering Atari, Go, Chess and Shogi by Planning with a Learned Model [online]. *DeepMind.* Available at: https://arxiv.org/abs/1911.08265 [Accessed: November 11, 2024]. **13. The AlphaStar Team,** (January 24, 2019). AlphaStar: Mastering the real-time strategy game StarCraft II [online]. *Google DeepMind.* Available at: https://deepmind.google/discover/blog/alphastar-mastering-the-real-time-strategy-game-starcraft-ii/ [Accessed: November 11, 2024]. **14. Kahneman, D.,** (2011). *Thinking, Fast and Slow.* London : Penguin Books. **15. Mouat T.,** (September 19, 2022). The Use and Misuse of Wargames. *Scandinavian Journal of Military Studies,* 5, 1, 209. DOI: 10.31374/sjms.121. **16. Appleget, J., Burks R., and Cameron, F.,** (2020). *The Craft of Wargaming : A Detailed Planning Guide for Defense Planners and Analysts* [online]. Naval Institute Press. https://research-ebsco-com.nduezproxy.idm.oclc.org/ linkprocessor/plink?id=c386fb0c-cc20-32d5-8832-8be5a2762487 [Accessed: November 11, 2024]. **17. De Fritsch, M. and Bitoun, A.,** (2019). Commander avec l'IA, une aide à la conception et à l'évaluation des modes d'action. *Revue Défense Nationale.* 820(5), 81-85. DOI: https://doi.org/10.3917/rdna.820.0081. **18. Goecks, V. G. and Waytowich, N. R.,** (2024). COA-GPT: Generative Pre-Trained Transformers for Accelerated Course of Action Development in Military Operations. *International Conference on Military Communication and Information Systems (ICMCIS).* 01-10. **19. Combe, P. C.,** (2021). Educational Wargaming: Design and Implementation into Professional Military Education. *Journal of Advanced Military Studies,* 12, 2, 131. **20. Brzashka, I.,** (2023). Wargames and AI: A dangerous mix that needs ethical oversight. *RUSI Journal.* 168, 7, 26-32. **21. Dr. Lee, E.,** (May 4, 2024). AI Security Model Hacking with Model Inversion Attacks: Techniques, Examples, and Real-World Applications and Mitigation with Code [online]. *Medium.* Available at: https://drlee.io/ai-security-model-hacking-with-model-inversion-attacks-techniques-examples-and-real-world-a23b5fff272a. [Accessed: November 11, 2024]. **22. Jaswanth, R.,** (April 26, 2024). Peeling Back the Layers: A Comical Guide to Model Inversion Attacks [online]. *Linkedin.* Available at: https://www.linkedin.com/pulse/peeling-back-layers-comical-guide-model-inversion-attacks-jaswanth-r-z7n4c [Accessed: November 11, 2024]. **23. Zhang, Yu., et al.,** (April 18, 2020). The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks. DOI: https://doi.org/10.48550/arXiv.1911.07135v2 [Accessed: November 11, 2024]. **24. Sciforce,** (September 7, 2022). Adversarial Attacks Explained (And How to Defend ML Models Against Them) [online]. *Medium*. Available at: https://medium.com/sciforce/adversarial-attacks-explained-and-how-to-defend-ml-models-against-them-d76f7d013b18 [Accessed November 11, 2024]. **25. Boesch, G.,** (December 2, 2023). What Is Adversarial Machine Learning? Attack Methods in 2024 [online]. *Visio.ai.* Available at: https://viso.ai/deep-learning/adversarial-machine-learning/ [Accessed November 11, 2024]. **26. Data Poisoning: The Essential Guide.** *Nightfall AI* [online]. Available at: https://www.nightfall.ai/ai-security-101/data-poisoning [Accessed November 11, 2024]. **27. Hassan, N.,** (2024). Data poisoning (AI poisoning) [online]. *TechTarget.* Available at: https://www.techtarget.com/ searchenterpriseai/definition/data-poisoning-AI-poisoning [Accessed: November 11, 2024]. **28. Shah, D.,** (November 30, 2023). Introduction to Training Data Poisoning: A Beginner's Guide [online]. *Lakera.* Available at: https://www.lakera.ai/blog/training-data-poisoning [Accessed: November 11, 2024]. **29. Simons, A.,** (January 11, 2024). Unpacking AI Data Poisoning [online]. *FedTech.* Available at: https://fedtechmagazine.com/article/2024/01/unpacking-ai-data-poisoning [Accessed: November 11, 2024]. **30. Fredrikson, M., Jha, S., and Ristenpart, T.,** (October 12, 2015). Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. *CCS'15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. DOI: https://dl.acm.org/doi/10.1145/2810103.2813677.

31. Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., and Mukhopadhyay, D. (September 28, 2018). Adversarial Attacks and Defences: A Survey. *arXiv.* http://arxiv.org/abs/1810.00069 [Accessed: November 11, 2024]. **32. Dastin, J**., (October 10, 2018). Insight – Amazon scraps secret AI recruiting tool that showed bias against women [online]. *Reuters.* Available at: https://www.reuters.com/article/world/ insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/ [Accessed: November 11, 2024]. **33. Lui, Z., Wang, Y., Vaidya, S., Ruehle, F., Halverson, J., Soljačić, M., Hou, T. Y., and Tegmark, M.,** (June 16, 2024). KAN: Kolmogorov–Arnold Networks [online]. *Preprint under review.* Massachusetts Institute of Technology, California Institute of Technology, Northeastern University, and The NSF Institute for Artificial Intelligence and Fundamental Interactions. Available at: https://arxiv.org/abs/2404.19756v4 [Accessed: November 11, 2024].

34. Clark, B., Patt, D., and Schramm, H., (2020). Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations [online]. Washington, D.C. Center for Strategic and Budgetary Assessments. Available at: https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations [Accessed: November 11, 2024]. **35. Mayer, M.,** (2023). Trusting Machine Intelligence: Artificial Intelligence and Human-Autonomy Teaming in Military Operations. *Defense & Security Analysis.* 39, 4, 521-538.

УДОСКОНАЛЕННЯ ВІЙСЬКОВОЇ ГРИ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ: ПЕРШИЙ КРОК У ПОБУДОВІ ДОВІРИ ДО ЛЮДИНО-МАШИННОЇ КОМАНДИ

ПРИМІРЕНКО Володимир Миколайович, кандидат військових наук, старший дослідник, Національний університет оборони України, Київ, Україна, https://orcid.org/0000-0002-2892-581X

ДАГЛЕС Пегер, Центр розвитку морських бойових дій, Норфолк, Вірджинія, США, https://orcid.org/0009-0009-4440-1774

ЛІ Екерс, Директорат закупівель Транспортного Командування, База Повітряних Сил Скотт, Іллінойс, США, https://orcid.org/0009-0007-8867-9853

СЕДРІК Глессі, Командування Об'єднаних операцій збройних сил Швейцарії, Берн, Швейцарія, https://orcid.org/0009-0007-0087-1569

Розвиток нових технологій продовжує збільшувати складність ведення війни. Штучний інтелект – одна з технологій, яка може кардинально змінити характер збройних конфліктів. Тому вкрай важливо експериментувати та інтегрувати штучні технології в таких безпечних умовах, як військові ігри, перш ніж впроваджувати їх в операційні системи і використовувати як інструмент підтримки прийняття рішень. Командна робота між людьми і машинами – одна з таких сфер. Об'єднання людей зі штучним інтелектом дає можливість синергетично використовувати сильні сторони кожного з них. Обчислювальні можливості штучного інтелекту дають змогу підтримувати прийняття рішень людиною, забезпечуючи предиктивний аналіз і аналіз за рекомендаціями. Така людино-машинна співпраця має потенціал для реалізації якісних досягнень у прийнятті рішень та може посилити навчання учасників, надаючи їм розуміння чинників, що дозволяють штучному інтелекту визначати найкращі варіанти і пов'язані з ними ризики. Людино-машинна командна робота у військових іграх також обіцяє додаткову перевагу у вигляді побудови довіри між людьми, які приймають рішення, і штучним інтелектом, який їх підтримує. Проте, людино-машинна командна робота не позбавлена викликів.

Метою статті є *виявлення шляхів покращення результатів військових ігор, впровадивши надійний штучний інтелект.*

Методи дослідження. *Під час написання статті було використано низку наукових методів дослідження. Метод контент-аналізу застосовувався для вивчення останніх досліджень і публікацій щодо виявлення проблематики в межах наявного обсягу знань. Для аналізу структури військової гри та розподілу її на складові частини й виявлення потенційних напрямів її удосконалення, які можна отримати завдяки впровадженню штучного інтелекту, було використано метод декомпозиції. Метод аналізу дав змогу оцінити потенційні переваги впровадження штучного інтелекту в кожну зі складових частин військової гри. Для обґрунтування оптимальних вузлів впровадження штучного інтелекту стосовно максимізації переваг застосовано метод синтезу.*

Аналіз останніх досліджень та публікацій. *У статті здійснено аналіз досліджень і узагальнено поняття штучного інтелекту та його технологій.*

Виклад основного матеріалу. *На прикладі військових ігор проаналізовано ефективність застосування штучного інтелекту й висвітлено те, як штучний інтелект перевершує людську продуктивність у низці еталонних ігор. Проаналізовано роль, цілі та дизайн військових ігор, а також значення штучного інтелекту в процесі їх проведення. Визначено роль штучного інтелекту, можливі ризики його застосування, а також окреслено шляхи вдосконалення військових ігор із використанням технологій штучного інтелекту. Зроблено обґрунтований висновок про можливість довіри до штучного інтелекту у військових іграх.*

Елементи наукової новизни. *У статті виявлено і обґрунтувано, що застосування штучного інтелекту у військових іграх сприяє не лише вдосконаленню процесу прийняття рішень, а й підвищенню рівня ситуаційної обізнаності, когнітивної підготовки військових офіцерів та побудові довіри до людино-машинної команди.*

Теоретична та практична значущість статті. *За результатами дослідження можна стверджувати, що людино-машинна взаємодія у військових іграх може допомогти у прийнятті рішень та сприяти навчанню і підготовці осіб, які приймають рішення. Збільшення довіри до штучного інтелекту потребує чіткого розуміння того, як він приходить до висновків та рекомендацій.*

Висновок і перспективи подальших досліджень. *Подальші дослідження мають бути зосереджені на розробленні алгоритмів візуалізації процесу прийняття рішень штучним інтелектом.*

Ключові слова: *штучний інтелект, військова гра, довіра до штучного інтелекту.*

List of bibliographical references

1. Sabharwal A., Selman B., Russell S., Norvig P. Artificial Intelligence: A Modern Approach. Third Edition. *Artificial Intelligence.* 2011. Vol. 175. № 5. P. 935–937. DOI: 10.1016/j.artint.2011.01.005. **2. Batra M. M.** Strengthening customer experience through artificial intelligence: An upcoming trend. *Competition Forum.* 2019. Vol. 17. № 2. P. 223–231. American Society for Competitiveness. **3. Wanderer N.** Artificial Intelligence: What Is It & Who Needs It Anyway? *Maine Bar Journal.* 2023. Vol. 38. № 3. P. 122–126. URL: https://research.ebsco.com/linkprocessor/ plink?id=a8296bba-de7f-374a-8656-e7f8ead01de1 (accessed: 11 Nov. 2024). **4. Caluori L.,**

Alexa H. Why Are You Called Intelligent? An Empirical Investigation on Definitions of AI. *AI & SOCIETY: Journal of Knowledge, Culture and Communication.* 2024. Vol. 39. № 4. P. 1905–1919. DOI: 10.1007/s00146-023-01643-y. **5. Britt Ph.** Expect GenAI to Take on Customer-Facing Roles: As Large Language Models Expand and Generative AI Technology Advances, Experts See a Greater Role in Customer Service. *CRM Magazine*. 2024. Vol. 28. P. 16–19. URL: https://research-ebsco-com.nduezproxy.idm.oclc.org/linkprocessor/plink?id=db91df18-771f-3fe7-a562-54910c812cb7 (accessed: 11 Nov. 2024). **6. Duarte F.** Amount of Data Created Daily. *Exploding Topics*. 2024. URL: https://explodingtopics.com/blog/data-generated-per-day (accessed: 11 Nov. 2024). **7. Layton D.** ChatGPT – Show me the Data Sources. *Medium*. 2023. URL: https://medium.com/@dlaytonj2/chatgpt-show-me-the-data-sources-11e9433d57e8 (accessed: 11 Nov. 2024). **8. Gordon C.** ChatGPT And Generative AI Innovations Are Creating Sustainability Havoc. *Forbes*. 2024. URL: https://www.forbes.com/sites/cindygordon/2024/03/12/chatgpt-and-generative-ai-innovations-are-creating-sustainability-havoc/ (accessed: 11 Nov. 2024). **9. St. John A., McDermott J.** Amazon, Google make dueling nuclear investments to power data centers with clean energy. *Associated Press*. 2024. URL: https://apnews.com/article/climate-data-centers-amazon-google-nuclear-energy-e404d52241f965e056a7c53e88abc91a (accessed: 11 Nov. 2024). **10. CCRL (Computer Chess Rating Lists) 40/15**. 2024. URL: https://computerchess.org.uk/ccrl/4040/ (accessed: 11 Nov. 2024). **11. Carnegie Mellon and Facebook AI Beats Professionals in Six-Player Poker.** Carnegie Mellon University. 2019. URL: https://www.cmu.edu/news/stories/archives/2019/july/cmu-facebook-ai-beats-poker-pros.html (accessed: 11 Nov. 2024). **12. Schrittwieser J., Antonoglou I., Hubert T., Simonyan K., Sifre L., Schmitt S., Guez A. et al.** Mastering Atari, Go, Chess and Shogi by Planning with a Learned Model. *DeepMind.* 2020. URL: https://arxiv.org/abs/1911.08265 [Accessed: 11 Nov. 2024]. **13. The AlphaStar Team.** AlphaStar: Mastering the real-time strategy game StarCraft II. *Google DeepMind.* 2019. URL: https://deepmind.google/discover/blog/alphastar-mastering-the-real-time-strategy-game-starcraft-ii/ (accessed: 11 Nov. 2024). **14. Kahneman D.** Thinking, Fast and Slow. London: Penguin Books, 2011. **15. Mouat T.** The Use and Misuse of Wargames. *Scandinavian Journal of Military Studies*. 2022. Vol. 5. № 1. P. 209. DOI: 10.31374/sjms.121. **16. Appleget J., Burks R., Cameron F.** The Craft of Wargaming: A Detailed Planning Guide for Defense Planners and Analysts. *Naval Institute Press.* 2020. URL: https://research-ebsco-com.nduezproxy.idm.oclc. org/linkprocessor/plink?id=c386fb0c-cc20-32d5-8832-8be5a2762487 (accessed: 11 Nov. 2024). **17. De Fritsch M., Bitoun A.** Commander avec l'IA, une aide à la conception et à l'évaluation des modes d'action. *Revue Défense Nationale.* 2019. Vol. 820. № 5. P. 81–85. DOI: https://doi.org/10.3917/rdna.820.0081. **18. Goecks V. G., Waytowich N. R.** COA GPT: Generative Pre-Trained Transformers for Accelerated Course of Action Development in Military Operations. *International Conference on Military Communication and Information Systems (ICMCIS).* 2024. P. 10. **19. Combe P. C.** Educational Wargaming: Design and Implementation into Professional Military Education. *Journal of Advanced Military Studies.* 2021. Vol. 12. № 2. P. 131. **20. Brzashka I.** Wargames and AI: A dangerous mix that needs ethical oversight. *RUSI Journal.* 2023. Vol. 168. № 7. P. 26–32. **21. Lee E.** AI Security Model Hacking with Model Inversion Attacks: Techniques, Examples, and Real-World Applications and Mitigation with Code. *Medium*. 2024. 4 May. URL: https://drlee.io/ai-security-model-hacking-with-model-inversion-attacks-techniques-examples-and-real-world-a23b5fff272a (accessed: 11 Nov. 2024). **22. Jaswanth R.** Peeling Back the Layers: A Comical Guide to Model Inversion Attacks. *Linkedin*. 2024. 26 April. URL: https://www.linkedin.com/pulse/peeling-back-layers-comical-guide-model-inversion-attacks-jaswanth-r-z7n4c (accessed: 11 Nov. 2024). **23. Zhang Y., et al.** The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks. arXiv. 2020. 18 Apr. URL: https://doi.org/10.48550/arXiv.1911.07135v2 (accessed: 11 Nov. 2024). **24. Sciforce**. Adversarial Attacks Explained (And How to Defend ML Models Against Them). *Medium*. 2022. 7 Sep. URL: https://medium.com/sciforce/adversarial-attacks-explained-and-how-to-defend-ml-models-against-them-d76f7d013b18 (accessed: 11 Nov. 2024). **25. Boesch G.** What Is Adversarial Machine Learning? Attack Methods in 2024. *Visio.ai.* 2023. 2 Dec. URL: https://viso.ai/deep-learning/adversarial-machine-learning/ (accessed: 11 Nov. 2024). **26. Data Poisoning: The Essential Guide**. Nightfall AI. URL: https://www.nightfall.ai/ai-security-101/data-poisoning (accessed: 11 Nov. 2024). **27. Hassan N.** Data poisoning (AI poisoning). *TechTarget.* 2024. URL: https://www.techtarget.com/searchenterpriseai/definition/data-poisoning-AI-poisoning (accessed: 11 Nov. 2024). **28. Shah D.** Introduction to Training Data Poisoning: A Beginner's Guide. *Lakera*. 2023. 30 Nov. URL: https://www.lakera.ai/blog/training-data-poisoning (accessed: 11 Nov. 2024). **29. Simons A.** Unpacking AI Data Poisoning [online]. FedTech. 2024. 11 Jan. URL: https://fedtechmagazine.com/article/2024/01/unpacking-ai-data-poisoning (accessed: 11 Nov. 2024). **30. Fredrikson M., Jha S., Ristenpart T.** Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. CCS'15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015. DOI: https://dl.acm.org/doi/10.1145/2810103.2813677.

31. Chakraborty A., Alam M., Dey V., Chattopadhyay A., Mukhopadhyay D. Adversarial Attacks and Defences: A Survey [online]. arXiv. 2018. 28 Sep. Available at: http://arxiv.org/abs/1810.00069 [Accessed: 11 Nov. 2024]. **32. Dastin J.** Insight – Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*. 2018. 10 Oct. URL: https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/ (accessed: 11 Nov. 2024). **33. Lui Z., Wang Y., Vaidya S., Ruehle F., Halverson J., Soljačić M., Hou T. Y., Tegmark M.** KAN: Kolmogorov–Arnold Networks. *Preprint under review.* Massachusetts Institute of Technology, California Institute of Technology, Northeastern University, and The NSF Institute for Artificial Intelligence and Fundamental Interactions. 2024. 16 June. URL: https://arxiv.org/abs/2404.19756v4 (accessed: 11 Nov. 2024). **34. Clark B., Patt D., Schramm H.** Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations [online]. Washington, D. C. : Center for Strategic and Budgetary Assessments. 2020. URL: https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations (accessed: 11 Nov. 2024). **35. Mayer M.** Trusting Machine Intelligence: Artificial Intelligence and Human-Autonomy Teaming in Military Operations. *Defense & Security Analysis*. 2023. Vol. 39. № 4. P. 521–538.

Рукопис надійшов до редакції *12.02.2025*
Рукопис прийнято до друку після рецензування *25.03.2025*
Дата публікації *30.04.2025*