ISSN 2007-9737

Benefits and Challenges of Military Artificial Intelligence in the Field of Defense

Jairo Eduardo Márquez-Díaz*

Universidad de Cundinamarca, Facultad de Ingeniería,
Colombia

jemarquez@ucundinamarca.edu.co

Abstract. The article explores the growing integration of AI in the military sphere. It highlights its potential to improve efficiency and accuracy in field operations, predictive analytics, and logistics due to its ability to process large volumes and learn autonomously. The study also emphasizes the role of AI in analyzing data from various sources such as satellite images, intelligence information and social media, which helps in target identification and operation of autonomous vehicles. It also addresses important ethical and legal challenges, including transparency in decision-making and liability for errors or collateral damage. It raises concerns about the vulnerability of military systems to attack, their tampering and the potential for accidental damage. The research employs a qualitative review of existing literature on types of AI and applications in the military context, focusing on benefits and risks. The study aims to synthesize key issues related to military AI capabilities, oversight, and governance, providing directions and precautions for responsible development of AI in defense.

Keywords. Artificial intelligence, algorithms, military, neural networks, technology.

1 Introduction

Artificial Intelligence (AI) is being increasingly used in the military field to improve efficiency and precision in field operations, predictive analysis, and logistics, among others. The ability to process large volumes of data in real time and to learn autonomously makes AI have great potential in defense and national security.

However, its use also raises significant ethical and legal challenges, such as transparency in decision-making and liability in case of errors or collateral damage.

Some civilian technology companies, particularly defense contractors, are actively involved in the field of military-grade AI. Though there are concerns that military AI systems could end up vulnerable to attack and tampering or cause accidental damage on a large scale. There are also questions about responsibility and transparency under the current geopolitical instability, especially when considering that the US, China, Russia, Iran, Turkey [4] and Israel, among other countries [32], lead the development of AI for large-scale military purposes.

The potential of military-grade AI is vast and diversified, the importance of which lies in being able to analyze large amounts of data from different sources, such as satellite imagery, intelligence signals, communications, and social media, to identify patterns and trends that may be relevant to national security. With this capability, target identification from surveillance images and video provides| critical information on the battlefield.

This brings us to the use of AI in weapon systems and autonomous vehicles such as drones, ground vehicles, and air defense systems, where human intervention is minimal.

Therefore, the present study aims to examine the benefits and challenges of using artificial intelligence in military operations and defense systems. To this end, the research question is formulated: What are the main advantages and ethical concerns associated with the integration of artificial intelligence capabilities in military domains? The methodology is framed in the qualitative review of the existing literature on applications of artificial intelligence in the military context.

doi: 10.13053/CyS-28-2-4684

The review will analyze the documented benefits of AI for defense activities, as well as the ethical, legal and security risks highlighted by experts and researchers. Key themes related to military AI capabilities, oversight, and governance will be synthesized to identify promising directions and precautions for responsible defense AI development.

2 Military Grade Artificial Intelligence

Military-grade artificial intelligence refers to AI systems developed and used specifically for military and defense applications [16]. These AIs are designed to meet the rigorous requirements and challenges associated with the military environment [5], where one seeks to gain a decisive advantage over potential adversaries. Some characteristics of this type of AI are detailed below:

- Robustness and Reliability: These AIs are designed to work reliably and withstand harsh conditions. They must be able to operate in a diverse range of environments and conditions often under extreme stress. This means that they must operate in hostile environments and resist physical damage, such as combat areas, and maintain their functionality even in the presence of interference or cyber-attacks [6].

- Processing capacity: These AIs are designed with advanced processing capabilities to ensure proper handling of large volumes of data. They can perform complex information analysis and processing tasks quickly and efficiently. This means that its design and development in many cases is tailored.

- Autonomy: Many military applications require AI systems that can operate autonomously, without the need for constant human supervision. This involves tasks like navigating a drone across a battlefield, identifying, and tracking targets, or managing logistics and supply chains.

- Adaptability: These types of AI are highly adaptable and can adjust to different situations and changing scenarios on the battlefield.

  They can learn and update their models and algorithms as new data is obtained and circumstances change.

- Decision making: These AI systems often need to make decisions in real time, due to the changing dynamics of information. This requires advanced algorithms and high-performance computing power.

- Interoperability: These systems often need to integrate with others, just like military platforms. Consequently, it is required that they be designed with interoperability in mind, using standard protocols and interfaces whenever possible, since, due to their security characteristics, they must work under robust encrypted communication protocols such as AES-256, OMEMO or ZRTP.

- Security and confidentiality: Given the sensitive nature of their tasks, military-grade AI systems must have rigorous security and confidentiality standards. This includes encryption, secure communication channels, and measures to prevent tampering or unauthorized access. The design of the chips must withstand cyberattacks, data corruption, equipment failures and other threats, because they will be used in high-risk military operations.

- The design of the chips must withstand cyber-attacks, data corruption, equipment failure and other threats, because they will be used in high-risk military operations.

- Ethical considerations: The use of this type of AI raises a few ethical considerations. These systems must be designed in a way that they respect international law and minimize the risk of harm to civilians [29].

- Human-machine interaction: These AIs can operate autonomously or in collaboration with human operators. Human-machine interaction is essential in the military environment, where operators can harness the power of AI processing and analysis to support informed decision-making.

Table 1. Characteristics of a military-grade artificial intelligence

Feature	Description
Design	– Specifically designed for military applications. – Incorporates advanced algorithms and machine learning capabilities. – Adapts to challenging environments such as extreme weather conditions, interference, and cyber-attacks.
Operability	– It can work autonomously or in collaboration with human operators. – Integrated into military platforms and systems such as unmanned vehicles, surveillance systems and weapons. – Follow strict security and confidentiality protocols to protect sensitive information.
Functionality	– Recognition and processing of images and video in real time. – Analysis and evaluation of intelligence data for decision making. – Ability to predict and model scenarios. – Support in the identification and response to threats in real time.
Applications	– Surveillance and reconnaissance on the battlefield. – Perimeter defense. – Elimination of explosives with robots and drones. – Locating and tracking enemy targets. – Support in search and rescue operations. – Data analysis for the generation of military strategies. – Simulations and virtual training for military personnel. – Prediction and prevention of failures in military equipment and systems. – Smart cameras for facial identification. – Tactical loitering in urban warfare. – Synthetic aperture radar. – DNA profiling algorithms. – Intelligence recovery. – Asymmetric war. – Cybersecurity to protect digital assets and critical infrastructure. – Cyber defense and cyber-attacks. – Disinformation from deepfakes manipulating audios and images. – Prediction of weather patterns.

Table 1 summarizes the characteristics of a military-grade AI in terms of design, operability, functionality, and applications under a general vision. This is because its implementation and exact specifications vary according to the needs and requirements of each system, be it military or intelligence agency.

Other additional details about this type of AI are that they often have access to massive amounts of data for training purposes, including military intelligence, surveillance data, and information from conflicts and war games. This allows them to learn much faster and reach higher levels of performance.

For this to be possible, cutting-edge artificial intelligence techniques are required that go beyond what is commercially available. Some developed by companies and military contractors specialized in AI, whose specific regulations and policies are focused on applications related to defense and national security.

3 Technology and Artificial Intelligence

AI-related technology presents its own developments and challenges, such is the case of AI chips, specialized for different functions within the armed and security forces [34, 23]. For example, AI for air superiority and defense uses vision systems and machine learning to identify and track targets. In the case of vehicle autonomy, it focuses on navigation, perception, and decision-making, etc.

Other applications include:

- Surveillance and reconnaissance: They are used to analyze and process images and videos in real time with the aim of detecting and recognizing objects, people, or threats on the battlefield or in the civil sphere with national security interests.
- Decision making: AI can analyze large volumes of intelligence data, providing valuable information in making strategic and tactical decisions.
- Support military operations: AIs can assist in threat identification and response, as well as search and rescue operations.
- Simulation and training: AIs can provide realistic simulations and virtual training for military personnel, allowing them to practice scenarios and improve their skills without real risk. To do this, it uses technologies such as augmented, virtual, and mixed reality, telepresence, and virtual worlds or metaverses [18].

Here are some examples of AI weapons already in use:

- Harpy: Is an Israeli kamikaze drone that uses AI to autonomously seek out and destroy radar emitters and air defense systems.
- The SGR-A1 is a South Korean automated turret gun robotic system manufactured by Samsung. It uses AI to detect human targets and attack them with firearms without human intervention. It is deployed along the Korean Demilitarized Zone.
- Sky Warrior/Predator XP: It is an AI-powered drone from the US with improved automation and autonomy. This drone can launch attacks without human supervision. It is used for targeted attacks against high-value targets.
- Mantis: Is an AI-guided manned machine gun developed by the American company SparkCognition. It uses computer vision to automatically detect and track human targets and guide the gunner's aim without manual adjustments.
- A10-AJ: Is an AI upgrade developed by Boeing for existing A10 Warthog attack aircraft. It uses computer vision to identify targets faster than humans. Allows pilots to take on more threats in less time. It still requires a human operator to launch weapons.
- Informant V2: Is an AI target recognition system developed by BAE Systems. It is designed to help soldiers identify potential threats and focus their attention on what matters most in combat situations.
- LOCUST: Is a system made up of a swarm of AI-enabled drones being developed by the US Air Force. The swarm can autonomously detect and identify targets and then coordinate an attack with minimal human intervention [21]. There are similar initiatives being developed by other countries.
- XQ-58A Valkyrie: Tactical air-to-air and air-to-surface autonomous aircraft, which works with AI/ML for various operations. It is the first fully operational sixth generation aircraft.
- Missiles: Several countries are developing AI-guided missiles that can autonomously identify and track moving targets. Including the US Perdix microdrones swarm and China's DR-8 missiles.
- Tanks: The superpowers are investigating the use of AI to control tanks with greater autonomy, this includes automatic detection of

targets, navigation through various types of terrain and choosing optimal routes.

- Submarines: AI and automation are being explored for underwater operations to handle complex tasks such as sensor data analysis, combat systems management and threat assessment. This technology aims to reduce the size of the required crew and increase the degree of autonomy.

In fact, there is the first autonomous submarine, Boeing's XLUUV (Orca) that integrates these characteristics.

- Ships: Unmanned AI ships are being developed for missions such as reconnaissance, mine detection and attack. Examples of this are the US Navy's Sea Hunter and Sea Hawk, and Norway's Black Hornet drone.
- Artillery Systems: Some artillery guns are combined with AI and targeting automation, allowing them to spot, classify, and engage moving targets in seconds instead of minutes.
- Roadrunner: Is a reusable vertical take-off and landing (VTOL) autonomous aerial vehicle (AAV). Its function is air and ground defense, in which it can launch, identify, intercept, and destroy various types of air threats. It uses multiple AI systems that allow a single operator to monitor swarms of these AAVs, creating autonomous collaborative platforms in the process.
- Rifles: AI-assisted prototype sniper rifles can detect human targets, calculate range, wind, and suggest shot location.

A variant used by US police is ShotSpotter, which uses specialized sensors and AI algorithms to detect gunshots in real time. These sensors can pinpoint the exact location of the shot and alert agencies in less than a minute. Also, machine learning algorithms are used to confirm if the recorded sound is indeed a gunshot.

- Cyberglobes: Is a tool that detects criminal activities such as financial fraud, drug trafficking, cyber-attacks, and terrorist activities in real time through the analysis of data generated in social networks and conversations. In addition, the system has additional functions such as data mapping and geolocation [7].
- Sky shield: advanced Israeli multipurpose electronic warfare system incorporated into combat aircraft. Deploy countermeasures to counter threats, creating safe corridors for aircraft squadrons for defense and attack.
- Drone Dome: is an anti-aircraft system against drones that nullifies them using electronic jammers and advanced AI that allows you to quickly locate these targets and nullify them using a laser beam director.
- Imilite: Is a system designed for battlefield intelligence, surveillance and reconnaissance that integrates multiple sensors and platforms for intelligent and efficient exploitation. It specializes in the centralization and unification of processing and exploitation of various types of data such as images and videos and other types of intelligence.
- MXSERVER: Is a video and photography media analysis tool that uses facial recognition and machine learning, which allow to identify suspects and provide useful information to security agencies.
- Sea Breaker: Missile specialized in selective impacts using AI algorithms and artificial vision.
- Iron Vision: Is a high-definition artificial vision system incorporated into tanks, which allows operators to observe the surroundings with a 360-degree angle. This allows you to locate targets more precisely, with situational awareness powered by AI algorithms.
- POWER, Persistent Optical Wireless Energy Relay or Energy Transmission Initiative. Wireless power transmission to troops and equipment on the battlefield, whose nodes are autonomous drones.
- Directed energy weapons: It consists of accurately tracking air or ground targets and destroying them with laser beam shots mediated by advanced AI software. There are various prototypes under development and testing, for example the 8x8 VBCR system of the North American Stryker family.

Table 2. Artificial neural networks most used in the military field

Neural Network	Description	Applications in the military field
Convolutional Neural Networks (CNN)	Designed to process structured data, such as images or audio signals.	Detection and classification of objectives in images and videos, facial recognition for identification of people, analysis and processing of satellite images, drones, and intelligent surveillance systems.
Recurrent Neural Networks (RNN)	They are capable of processing sequential data and have feedback connections, which allows them to have memory.	Natural language processing, such as social media sentiment analysis to identify opinions and attitudes, real-time machine translation of intercepted communications, automatic text generation in reports and analytics, intelligence data processing for pattern and threat detection.
Generative Adversarial Neural Networks (GAN)	They combine a generator and a discriminator to create synthetic and realistic samples.	Generation of synthetic data for training detection and recognition algorithms, creation of synthetic images and videos for simulations and virtual training, generation of virtual adversaries to test and improve the security of defense and cybersecurity systems.
Transforming Neural Networks- Transformers	It employs attentional mechanisms used in natural language processing.	Recognition and translation of languages in intercepted communications, analysis, and classification of documents to identify relevant information, intelligence information processing to identify patterns and threats, automatic report generation to provide real-time intelligence.
Neural Networks for Sequence Analysis (Seq2Seq)	These networks are applied in the development of multilingual communication, particularly in the collection and exchange of information between different groups and nations.	Automatic translation of documents and communications in different languages with the aim of facilitating the exchange of information between different groups and nations in military settings or between intelligence agencies.
NeuRBF: A Neural Fields Representation with Adaptive Radial Basis Functions	It uses general radial bases in images with flexible position and shape, which allows the AI greater spatial adaptability and better adjustment to target signals, enlarging it without losing resolution.	It uses high-precision imaging systems and analysis of 2D images and 3D fields from various sources, with the ability to regenerate grids and/or render for analysis of specific objects.
Neural Networks for Anomaly Detection	Designed to detect unusual or anomalous patterns in large data sets.	Detection of suspicious activities or potential threats in surveillance data, network traffic or intrusion detection systems, critical infrastructure protection and defense systems.

- ChatGPT Military: OpenAI removed language prohibiting the use of its technology for military purposes from its usage policy, which previously included a ban on weapons development and warfare. While current OpenAI tools cannot be used directly for violence, they can assist in a variety of military-related tasks, such as document processing and analysis.
- Policy changes indicate a potential shift toward supporting operational infrastructure for military use (Biddle, 2024). Equivalently, China is employing a version like ChatGPT called Baidu's Ernie Bot and iFlyTek's Spark to train military AIs in automated combat simulations.

There is a wide range of autonomous weapons and systems whose functionality falls directly to AI, which are currently in development or have limited operational use, apart from clandestine research by the military and private contractors that do not come to light publicly. While most still require human assistance for operation, the trend is clearly toward greater autonomy and less human involvement over time.

For example, fifth and sixth generation fighter aircraft have built-in AI for reconnaissance, detection, planning and conventional and electronic attack with three-dimensional vision, eliminating the pilot from making decisions when multiple variables are presented that can confuse him in the field of combat. battle, such as attacking multiple targets and/or evading air-to-air or ground-to-air missile attacks, or sharing data between different ships, even accompanying drones.

A particularity of this technology is its scalability, that is, it can be updated and new developments incorporated into existing ones without having to start new developments from scratch, such is the case of integrated military systems; addressing open sensor system architectures, open modular sets of C5ISR/EW(CMOSS) standards and airborne capability environments, among others, involving technologies such as advanced radar systems, avionics, navigation, electronic warfare, signals intelligence , communications and other mission-critical military systems.

4 AI Algorithms

In the military industry, there are various artificial intelligence algorithms that are widely used for various applications. Some of them are mentioned below:

1. Artificial Neural Networks (ANNs): These are a type of machine learning algorithm inspired by the human brain. ANNs can be used for a variety of tasks, such as image recognition, Natural Language Processing (NPL), and speech recognition, among others. They are characterized by being a type of computational model inspired by the structure and functioning of the human brain.

   These networks are composed of multiple interconnected artificial neurons. Each neuron receives inputs that are processed by a set of activation functions, then produces conditioned outputs that are reprocessed recursively in the hidden layers until an ideal output is obtained.

   During the training of a neural network, the weights of the connections between the neurons are adjusted so that the network can learn to correctly map the inputs to the desired outputs. Learning algorithms, such as error backpropagation, are used to iteratively adjust the weights to improve network performance. The following table shows some types of ANN most used in the military field.

2. Support Vector Machines (SVM*)*: Is a machine learning algorithm that can be used for classification and regression tasks. SVMs work by finding a hyperplane that separates the data into two classes by maximizing the margin between the data classes. The training data is mapped to a higher dimensional space by a kernel function, which allows nonlinear hyperplanes to be found.

   During training, the support vectors, which are the closest data points to the separation hyperplane, are selected. During the classification stage, the new data is mapped to the same high-dimensional space and assigned to a class based on its location.

3. Decision trees: They are supervised learning algorithms used for classification and regression tasks. Decision trees work by constructing a tree-like structure that represents the relationships between certain characteristics and the target variable. It is also related to random forest learning algorithms, which combine multiple decision trees to improve prediction accuracy.

4. Variational autoencoders (VAEs): These are a class of deep learning models that combine the power of neural networks with probabilistic graphical models. They consist of two main components: an encoder network and a decoder network, where VAEs learn from input data that can be sampled to generate new data that is like it. VAE can learn to generate new images or data that are like the training data.

5. Computer vision*:* It is a branch of AI focused on allowing machines to interpret and understand visual data from the world around them. It is used for tasks such as object detection and tracking, facial recognition, and autonomous navigation.
6. Natural Language Processing (NLP): It is a technology that allows you to summarize complex texts easily and quickly. It uses algorithms to identify and/or generate main ideas and summarize them in a shorter text, just like translators and chat bots. This technology can be used in various industries, ranging from education and journalism to electronic espionage systems.
7. Cognitive computing: Deals with the creation of intelligent computing systems with the ability to reason, learn, solve problems, and make decisions without human intervention. In the military field it is used in image processing, strategic planning, logistics and cybersecurity.
8. Multimodal models: Can understand and process multiple types of data simultaneously, such as text, images, audio, or multimodal combinations. This type of AI encompasses the previously mentioned models, plus others that are under development such as Large Language Models as Optimizers [19], which seeks to improve the performance of large language models (LLM) by optimization through PROmpting (OPRO); which is nothing more than meta-indications described in natural language that generates plausible solutions based on the description of a problem and the previous solutions.

5 Advanced AI

The field of artificial intelligence is constantly evolving, with new advances and technologies emerging all the time. These are some of the latest trends and projections in military AI extended to the civilian field with certain limitations [9]:

- Machine Learning (ML): It is a branch of artificial intelligence "that focuses on developing algorithms and models that allow computers to learn and improve automatically from data, without being explicitly programmed for each specific task" [1] Algorithms are trained to find patterns and correlations from large data sets that lead to decision making and forecasts.
- Deep Learning (DL): it specializes in training multilayer artificial neural networks so that they learn hierarchical representations of data. It has been a major driver of advanced AI research and applications in recent years. DL algorithms in conjunction with convolutional neural networks (CNN) and recurrent neural networks (RNN), have achieved remarkable results in various domains, including computer vision, NLP, and speech recognition.

  A variant of DL is analog deep learning based on neuromorphic computing, where programmable resistors are used that work in an equivalent way to transistors. These resistors form matrix layers that in turn create complex neural networks and analog synapses that work millions of times faster than biological synapses.
- Generative AI: Involves the use of AI models to generate new content, such as images, text, and audio. Recent advances in generative models, such as generative adversarial networks (GANs) and transformer models, have led to significant advances in realistic image synthesis, text generation, and creative applications. These models can create highly compelling and diverse results, pushing the boundaries of AI-generated content.

A recent development is Voicebox from the company Meta which is a generative AI that speaks. The system with a few seconds of audio (Flow Matching) can create a dialogue with a tone of voice identical to that of a human being.

Although it is a private and restricted system, it allows, in principle, apart from translating and suppressing background noise, impersonating the voice of personalities and, therefore, creating very well-crafted scams and deepfakes.

Developments like this are being incorporated into drones [12], where AI and voice recognition technology are integrated to make them self-sufficient.

- Large Language Models (LLM): Are a type of AI trained with a large amount of text-like data. They can generate human-like text based on the input they receive. In the military field, these models are used in a variety of ways:
  - Planning and Strategy: They assist in military planning by providing information, generating scenarios, and suggesting strategies based on historical data. They also help visualize and describe complex problems, making the planning process more efficient.
  - Data analytics: They allow you to analyze large amounts of text data, such as intelligence reports, and extract relevant information to identify patterns, trends, and threats that human analysts might miss.
  - Simulation and Training: Can be used to create realistic training scenarios for military personnel, generate dialogue, scenarios, and responses that help train soldiers for various situations.
  - Communication: They help in the translation of languages, being particularly useful in international military operations. They can also generate clear and concise reports, summaries, and other forms of communication.
  - Decision Making: By providing data-driven insights and predictions, LLMs can support decision-making processes in the military. They can help assess the potential results of different strategies and actions.
- Generative AI in the data cloud: Consists of advanced generative AI services, including chatbots and intelligent search systems. An example of this service is the Snowflake platform with NVIDIA, which fuses high-performance ML and AI with large volumes of proprietary, structured data. Using this data, custom generative AI models can be built, ranging from hundreds of terabytes to petabytes of raw information, to create and tune custom LLMs that power specific applications and services. These services encompass advertising, media and entertainment, financial services, health care and life sciences, manufacturing, retail and consumer packaged goods, technology, and telecommunications.
- Reinforcement Learning (RL): It is an area of AI that focuses on training agents to make sequential decisions through interactions with an environment. The RL has made significant advances in solving complex problems, including games, robotics control, and autonomous systems. Recent developments in RL algorithms, such as deep reinforcement learning and model-based RL, have shown impressive performance in challenging domains, leading to advances in autonomous vehicles, industrial automation, and more.
- AI and Big Data: AI uses algorithms and ML to analyze large amounts of data to generate information that enables strategic planning and tactical execution. Big Data refers to the massive volumes of data that are generated within military operations, including sensor data, satellite imagery, and intelligence reports.

  The fusion of these technologies improves decision-making processes and operational efficiencies, helping to identify patterns and trends in data that may not be immediately apparent to human analysts. For example, they can be used to analyze data from various sources in real time, such as sensors, Unmanned Aerial Vehicles (UAVs), and soldiers to better understand the battlefield, weather conditions, and enemy movements.
- AI and cybersecurity: Machine learning algorithms can detect patterns and anomalies that indicate potential threats, making them a valuable tool in the event of a cyberattack [20]. AI and ML are increasingly used in cybersecurity applications to detect threats, analyze risks, and protect networks. Some key areas where AI is used in cybersecurity include:
  - Malware detection: AI can identify malicious files and behavior that are unknown to or have eluded traditional antivirus software. This helps detect new and sophisticated cyberattacks. The military uses AI-enabled malware detection

    to protect its networks and communication systems.

    - Intrusion detection: AI systems can monitor network traffic for anomalies and suspicious patterns that indicate a cyber-attack or security breach is taking place.

    - Threat intelligence: With high processing power, AI can analyze large volumes of data on cyber threats to identify patterns, associate threats with actors, and predict future attacks [11]. This threat intelligence helps the military strengthen its defenses against specific adversaries.

    - Vulnerability management: AI systems can identify and prioritize vulnerabilities in software, which helps organizations and the military patch vulnerabilities before they can be exploited by attackers.

    - Cybercrime: Some experts [36, 13] argue that AI will also enable more sophisticated cyberattacks and weapons in the future. The military has an interest in developing defensive and offensive AI-powered cyber capabilities.

- Explainable AI (XAI): Aims to improve the interpretability and transparency of AI systems. While DL's models have achieved remarkable performance, their decision-making processes are often viewed as black boxes. Recent developments in XAI research focus on the development of techniques and algorithms to provide explanations and insights into the predictions and decisions of AI models. This is crucial to build trust, address bias, and ensure ethical and responsible AI systems, whose actions can be easily understood by humans.

- AI and Edge Computing: Edge Computing involves processing data where it is generated (i.e., at the "edge or perimeter" of the network), rather than in a centralized location. By leveraging edge computing, AI models can be deployed directly to devices enabling privacy-sensitive and real-time AI applications. This includes applications in autonomous vehicles, Internet of Things (IoT) devices with all their variants [17] and smart city infrastructure, where low latency, privacy and bandwidth constraints are critical considerations.

- AI that designs chips: It is a scalable technology that aims to create processors automatically. As a particular case at the time of writing this article, there is Qimeng No 1 technology, which exceeds 4000 times the intelligence of ChatGPT4. Although this technology is far from designing chips at scales equivalent to high-performance chips, the proof of concept has been passed, so getting custom processors is only a matter of time.

- Neurotechnology: Research is being done on the ideal creation of a brain-computer interface, implants, and neural prostheses. Integrating neurotechnology with AI provides opportunities to collect vast amounts of neural data that can be used to train artificial intelligence systems [31].

  For example, data from brain-computer interfaces can be used to identify neural patterns that correspond to certain thoughts, intentions, or actions. This data helps improve algorithms that can interpret and react to neural signals. For example, Augmented Cognition: Employs neural interfaces that may one day be used to improve cognitive abilities such as focus, memory, and situational awareness for soldiers and intelligence personnel.

- Neurotechnology in the military and intelligence field has several potential applications such as lie detection. There is research on using brain data to detect deception more accurately than traditional polygraph tests.

  There is brain reading, where it is speculated that one day it will be possible to decode complex thoughts directly from brain activity, which could have important implications for security [22], surveillance and intelligence gathering.

  However, this application is still highly controversial and speculative now [24]. Brain-controlled drones and robots are another potential application, where experiments have shown that subjects can control drones and robotic arms using only their brain signals.

This could allow a soldier to operate military equipment remotely without compromising his personal integrity on the battlefield. Work is also underway to improve prosthetics through neural interfaces that provide more natural control in injured soldiers.

- Organoid intelligence: Its goal is to create standardized brain organoids to develop biological artificial intelligence, since current AI systems have scaling problems that require increasing amounts of energy and data, while the human brain, on the other hand, uses progressive learning [33].

The bioengineering that supports this research aims to cultivate standardized human brain organoids with glial cells, using microphysiological systems to recreate brain architecture and functionality and take advantage of them with interface technologies and artificial intelligence [28]. In the end, what is expected is to provide information to the organoids and measure their output leading, for example, to training organoids for tasks like playing video games or controlling robots.

In terms of projections, AI is expected to continue to become more integrated into the military field. We will likely see more personalized experiences thanks to AI, as well as improvements in civilian areas like healthcare, transportation, and education. However, these advances will also bring challenges, particularly around issues like privacy and security.

6 Discussion

While the general characteristics of military AI are like commercial AI in terms of machine learning, computer vision, etc., the scope, performance, security, ethics, and role within the military make these systems distinct from what is commercially available. Added to the fact that the resources allocated to invest in this technology are greater and, therefore, expands the boundaries of AI technology as stated.

There are ethical questions surrounding the use of AI for lethal purposes. Some argue that AI should only be used for defensive or support functions, and not to carry out attacks. However, others believe [25, 14] that AI weapons will be inevitable, and the focus should be on ensuring that they are used responsibly [22].

Some experts [35, 26] argue that humans should always maintain ultimate control over any weapons system involving AI. Others believe that full autonomy is inevitable and necessary to keep up with technological advances from potential threats [3, 15], especially when geopolitical dynamics today are increasingly unstable.

Another aspect to consider is the potential use of military AI to spy on civilians. Although espionage is not new, the use of AI for this purpose is new, with the particularity that not only these actions are carried out by the militia, but also by civilians. This is an example that military AI developments are inevitably making their way into civilian life in various contexts that can negatively affect privacy, surveillance, and other aspects of daily life. Recently, a study by [10] has exposed how military AI for use in intelligence operations to identify terrorist cells is being used for monitoring and surveillance of employees, especially in the United States.

The objective is to carry out a data analysis to identify organizers where the possibility of labor strikes arises and act against them. For example, locating organizers so that their employers can fire them before they form a union. This system can be used by employers during the personnel recruitment process, to avoid hiring future union organizers or people who have had a problem in places where they previously worked.

The problem does not end here, since some AIs are used for emotion detection, which still has flaws, proven biases, discrimination, and wrong assumptions. This means that people can be falsely accused. This scenario currently lacks regulation and, therefore, several companies are using this type of technology without any control or guarantee of transparency. It follows that as AI becomes more integrated into our lives, questions related to ethics and standards become more important.

This includes issues such as data privacy, the possibility of algorithmic bias, and the impact of AI on jobs; demanding continuous research and development in security and exploration of methods to ensure the safe and reliable implementation of AI systems. Looking to the future, military AI has several highly relevant developments and projections, with the potential to improve exponentially, following the pattern of Moore's Performance Law [27].

This implies high computational power and data available to train AI models that doubles approximately every two years. As it is, there are continuous advances in deep learning, with the exploration of more sophisticated architectures, optimization techniques, and training strategies to tackle even more complex tasks.

This advancement goes hand in hand with the continuous improvement of unsupervised learning and self-supervised learning [30, 2], making it easier for military AI systems to learn from unlabeled data and reduce their reliance. to large datasets. These developments have also brought an increased focus on ethical and responsible AI practices [8]. This includes addressing issues like bias, fairness, transparency, and the robustness of AI systems. At this stage, the integration of AI with other emerging technologies is being explored.

This includes neurotechnology, neuromorphic computing, and quantum computing. These integrations envision new possibilities for improving the computational power and algorithmic capabilities of AI. For example, they have the potential to revolutionize diagnosis, treatment, and healthcare delivery by ensuring interoperability and security in critical systems, improving healthcare overall, discovering new drugs, and scaling personalized medicine to new levels. While the technologies have great potential to transform many fields, there are also ethical concerns regarding their use in corporate, societal, and global military and surveillance.

AI when making autonomous decisions can have consequences in people's lives. This entails establishing an ethical and legal framework for its use in the military field and clearly defining responsibility in case of errors or collateral damage. Future developments will need to be balanced with consideration of privacy, security, and human rights. Thus, the reliance on AI in military operations can be a risk if systems fail or are compromised by adversaries.

At this point, AI can be susceptible to bias and discrimination, triggering negative consequences in military operations by undermining confidence in critical systems. It is also important that the military proactively address these challenges and work on solutions that enable the responsible and effective use of AI.

7 Conclusions

Military-grade AIs are designed to meet the needs of the military in various areas, considering advanced processing capabilities, adaptability, and security, among other aspects. Its application ranges from recognition and surveillance to predictive analysis for strategic decision making. Its objective is to improve the effectiveness and performance of military operations such as autonomous vehicles (such as drones or unmanned submarines), cyber defense, logistics and supply chain management, among others.

AI is increasingly playing a crucial role in improving cybersecurity defenses for the military. By automating tedious tasks, accelerating threat detection, and assisting with threat intelligence, AI technologies can help the military more effectively protect their digital assets and critical infrastructure against cyberattacks.

While fully autonomous weapons may not yet exist, there are many examples of AI enhancing existing weapons systems by providing detection, prioritization, tracking, and target recommendation capabilities, but the ultimate decision to engage and use lethal force still it falls to a human operator for now. There is an ongoing military artificial intelligence arms race among various nations, which raises numerous pressing ethical and security considerations that must be addressed as this technology continues to develop.

Notably, much of this technological advancement is occurring outside of public scrutiny. It should also be acknowledged that increasing geopolitical tensions between major world powers are accelerating efforts to develop advanced AI for both cybersecurity defense and potentially offensive cyber capabilities, further exacerbating an arms race in this domain.

Consequently, as AI systems are increasingly deployed for purposes of both cyber defense and cybercrime, careful international governance and oversight will be vital in the future to help manage the complex ethical and security implications of progress in these technologies.

Acknowledgments

The author thanks the University of Cundinamarca for its support and funding. Faculty of Engineering, Chia, Colombia.

References

1. **Álvarez, E. (2023).** Machine learning: Así funciona la disciplina que les enseña a las computadoras a aprender por sí mismas. https://tn.com.ar/tecno/novedades/2023/05/29/machine-learning-asi-funciona-la-disciplinaque-les-ensena-a-las-computadoras-a-aprender-por-si-mismas/E.
2. **Balestriero, R., Ibrahim, M., Sobal, V., Morcos, A., Shekhar, S., Goldstein, T., Goldblum, M. (2023).** A cookbook of self-supervised learning. arXiv preprint arXiv:2304.12210. DOI: 10.48550/arXiv.2304.12210.
3. **Blanchard, A., Floridi, L., Taddeo, M. (2022).** The doctrine of double effect & lethal autonomous weapon systems. Available at SSRN 4308862. DOI: 10.2139/ssrn.4308862.
4. **Can, M. (2023).** Under the leadership of our president:‘Potemkin AI’and the Turkish approach to artificial intelligence. Third World Quarterly, Vol. 44, No. 2, pp. 356–376. DOI: 10.1080/01436597.2022.2147059.
5. **Evron, Y., Bitzinger, R. A. (2023).** The fourth industrial revolution and military-civil fusion: A new paradigm for military innovation? Cambridge University Press.
6. **Gaba, S., Budhiraja, I., Kumar, V., Martha, S., Khurmi, J., Singh, A., Singh, K., Askar, S., Abouhawwash, M. (2024).** A systematic analysis of enhancing cyber security using deep learning for cyber physical systems. IEEE, Vol. 12, pp. 6017–6035. DOI: 10.1109/ACCESS.2023.3349022.
7. Gandharv**, K. (2021).** Best reliable deep-tech to track criminals. https://analyticsindiamag.com/best-reliable-deep-tech-to-track-criminals/.
8. **Gill, A. (2019).** Artificial intelligence and international security: the long view. Ethics & International Affairs, Vol. 33, No. 2, pp. 169–179. DOI: 10.1017/S0892679419000145.
9. **Gregory, T. H. X., Chuan, N. S., Bingquan, S. (2022).** Self-supervised learning with deep neural networks for computer vision. In: Guo, H., Ren, H., Wang, V., Chekole, E. G., Lakshmanan, U. (eds) IRC-SET 2021, Springer, Singapore. DOI: 10.1007/978-981-16-9869-9_47.
10. **Grill, G., Sandvig, C. (2023).** Military AI's next frontier: your work computer. https://www.wired.com/story/military-ais-next-frontier-your-work-computer/
11. **Johnson, J. (2019).** Artificial intelligence & future warfare: implications for international security. Defense & Security Analysis, Vol. 35, No. 2, pp. 147–169. DOI: 10.1080/14751798.2019.1600800.
12. **Johnson, J. (2020).** Artificial intelligence, drone swarming and escalation risks in future warfare. The RUSI Journal, Vol. 165, No. 2, pp. 26–36. DOI: 10.1080/03071847.2020.1752026.
13. **Johnson, J. (2020).** Artificial intelligence: A threat to strategic stability. Strategic studies quarterly, Vol. 14, No. 1, pp. 16–39.
14. **Koch, W. (2022).** AI for aerospace and electronic systems: Technical dimensions of responsible design. IEEE Aerospace and Electronic Systems Magazine, Vol. 38, No. 1, pp. 106–111. DOI:10.1109/MAES 2022.3228300.
15. **Lamnabhi-Lagarrigue, F., Samad, T. (2023).** Social, organizational, and individual impacts of automation. In: Nof, S.Y. (eds) Springer Handbook of Automation, pp. 61–75. DOI: 10.1007/978-3-030-96729-1_3.
16. **Laudien, T., Ernst, J., Schmerwitz, S. (2023).** Bringing a colored head-down display symbology heads up: display fidelity review of a low-cost see-through HMD. Artificial Intelligence and Machine Learning for Multi-

Domain Operations Applications, Vol. 12538, pp. 191–197. DOI: 10.1117/12.2664840.

17. **Márquez, J. (2021).** Internet de las cosas (IoT) y grandes datos frente ataques de denegación de servicio distribuido (DDoS). UMNG, VI Congreso Internacional de Administración de la Seguridad y Salud en el Trabajo. Gestión del riesgo: una visión global e integral. Editorial Neogranadina. pp. 189–235. DOI: 10.18359/litgris.6278.

18. **Márquez, J. (2020).** Virtual world as a complement to hybrid and mobile Learning. International Journal of Emerging Technologies in Learning, Vol. 15, No. 22, pp. 267–274. DOI: 10.3991/ijet.v15i22.14393.

19. **Yang, C., Wang, X., Lu, Y., Liu, H., Le, Q., Zhou, D., Chen, X. (2023).** Large language models as optimizers. Google DeepMind, pp. 1–42. DOI: 10.48550/arXiv.2309.03409.

20. **Márquez, J. (2021).** Dronica as an option for the security and defense of cities. Academia Letters, No. 861, pp. 1–3. DOI: 10.20935/AL861.

21. **Márquez, J. (2023).** Desarrollos tecnológicos e implicaciones de los drones autónomos militares: perspectivas en la geopolítica mundial. Revista Tecnológica, Vol. 35, No. 1, pp. 137–151. DOI: 10.37815/rte.v35n1.1018.

22. **Maschmeyer, L. (2022).** Subverting skynet: the strategic promise of lethal autonomous weapons and the perils of exploitation. 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), Vol. 700, pp. 155–171. DOI: 10.23919/CyCon55549.2022.9811008.

23. **Montasari, R. (2023).** National artificial intelligence strategies: A Comparison of the UK, EU and US approaches with those adopted by state adversaries. Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity, Vol. 101, Cham: Springer International Publishing, pp. 139–164. DOI: 10.1007/978-3-031-21920-7_7.

24. **Müller, O., Rotter, S. (2017).** Neurotechnology: Current developments and ethical issues. Frontiers in Systems Neuroscience, Vol. 11, No. 93, pp. 1–5. DOI: 10.3389/fnsys.2017.00093.

25. **Nadibaidze, A. (2022).** Great power identity in Russia's position on autonomous weapons systems. Contemporary security policy, Vol. 43, No. 3, pp. 407–435. DOI: 10.1080/1352 3260.2022.2075665.

26. **Pekarev, J. (2023).** Attitudes of military personnel towards unmanned ground vehicles (UGV): a study of in-depth interview. Discover Artificial Intelligence, Vol. 3, No. 1, pp. 24. DOI: 10.1007/s44163-023-00058-4.

27. **Qian, S., Liu, M., Dou, Y., Fink, Y. Yan, W. (2023).** Una ley de Moore para fibras permite tejidos inteligentes. Revista Nacional de Ciencias, Vol. 10, No. 1, DOI:10.1093/nsr/nwac202.

28. **Quirión, R. (2023).** Brain organoids: are they for real? Frontiers in Science, Vol. 1, p. 1148127. DOI: 10.3389/fsci.2023.1148127.

29. **Raaijmakers, S. (2019).** Artificial intelligence for law enforcement: Challenges and Opportunities. IEEE Security & Privacy, Vol. 17, No. 5, pp. 74–77.

30. **Rani, V., Nabi, S. T., Kumar, M., Mittal, A., Kumar, K. (2023).** Self-supervised learning: A succinct review. Archives of Computational Methods in Engineering, Vol. 30, No. 4, pp. 2761–2775. DOI: 10.1007/s11831-023-09884- 2.

31. **Sattler, S., Pietralla, D. (2022).** Public attitudes towards neurotechnology: Findings from two experiments concerning brain stimulation devices (BSDs) and brain-computer interfaces (BCIs). PloS One, Vol. 17, No. 11, p. e0275454. DOI: 10.1371/journal.pone.0275454.

32. **Scollick, A. (2023).** The Irish defence forces in the drone age. The EU, Irish Defence Forces and Contemporary Security, Cham: Springer International Publishing, pp. 295–314. DOI: 10.1007/978-3-031-07812-5_15.

33. **Smirnova, L., Morales, P. I., Hartung, T. (2023).** Organoid intelligence (OI) the ultimate functionality of a brain microphysiological system. ALTEX Alternatives to animal experimentation, Vol. 40, No. 2, pp. 191–203. DOI: 10.14573/altex.2303261.

34. **Speith, T., Speith, J., Becker, S., Zou, Y., Biega, A., Paar, C. (2023).** Expanding explainability: From explainable artificial intelligence to explainable hardware. DOI: 10.48550/arXiv.2302.14661.

35. **Taddeo, M., Blanchard, A. (2022).** Accepting moral responsibility for the actions of autonomous weapons systems: A moral gambit. Philosophy & Technology, Vol. 35, No. 3, p. 78. DOI: 10.1007/s13347-022-00571.

36. **Yamin, M., Ullah, M., Ullah, H., Katt, B. (2021).** Weaponized AI for cyberattacks. Journal of Information Security and Applications, Vol. 57, p. 102722. DOI: 10.1016/j.jisa.2020.102722.

Article received on 16/08/2023; accepted on 19/02/2024.

[*] Corresponding author is Jairo Eduardo Márquez-Díaz.