

E-ISSN: 2707-6644

P-ISSN: 2707-6636

Impact Factor (RJIF): 5.43

www.computersciencejournals.com/ijcpdm

IJCPDM 2025; 6(2): 128-132

Received: 03-06-2025

Accepted: 05-07-2025

Mansi

Department of Computer
Science and Engineering, R. D.
Engineering College, Duhai,
Ghaziabad, Uttar Pradesh,
India

Ramender Singh

Department of Computer
Science and Engineering, R. D.
Engineering College, Duhai,
Ghaziabad, Uttar Pradesh,
India

Corresponding Author:**Mansi**

Department of Computer
Science and Engineering, R. D.
Engineering College, Duhai,
Ghaziabad, Uttar Pradesh,
India

Artificial intelligence in the military: An overview of the capabilities, applications, and challenges

Mansi and Ramender Singh

DOI: <https://www.doi.org/10.33545/27076636.2025.v6.i2a.121>

Abstract

This article explores current and future opportunities for developing artificial intelligence (AI) algorithms in military contexts. It focuses on seven key patterns of AI application, including object detection, robotics, military logistics, and the broader implications of AI use, such as global instability and nuclear risk. With the rise of the Fourth Industrial Revolution, AI has become a critical component of modern military systems, offering superior data processing and enhanced capabilities like self-control, self-regulation, and autonomous decision-making. AI is now integrated across nearly all military domains. Increased research and development support from defense agencies is expected to drive the growth of AI-powered military systems. This essay examines both the opportunities and threats posed by military AI, highlighting its potential for advancement as well as the risks of misuse or unintended consequences in times of instability.

Keywords: Artificial intelligence, military AI, enhanced capabilities

Introduction

Artificial intelligence (AI) has been gradually improving and becoming a more efficient method worldwide, thanks to advancements in data, computer processing power, and machine learning, particularly over the last two decades. As a result, Therefore, it should come as no surprise that AI has numerous applications in the military sector as well, spanning a vast range ^[1]. Military capability is the current measurement index when determining a country or nation's "Power." The U.S. Department of Defense defines military competence or capability as "the ability to achieve a certain combat objective (win a war or battle, destroy a target set)." It is directly or indirectly influenced by modernization, structure, preparedness, and sustainability. The equipment, arsenal, and level of technical sophistication largely determine the degree of modernization ^[2]. The Internet is replacing the conventional way of initiating war instigated from the start of the Second World War. According to researchers, modern autonomous systems and artificial intelligence (AI) are expected to play a crucial role in future military confrontations ^[3]. This type of enhancer helps in the military sector in various ways. It turns out to be the greatest weapon in developing military capability ^[4]. Data on a wide range of resources and capabilities (human resources combat and support vehicles, helicopters, cutting-edge intelligence, and communication equipment, artillery, and missiles) that can carry out complex tasks of various types, such as intelligence gathering, movements, direct and indirect fires, infrastructure, and transports, should be considered in military decisions ^[3, 5]. AI methods, such as the qualitative spatial interpretation of CoA diagrams and interleaved adversarial scheduling, among others, enhance the military world in various ways ^[6]. The study has the potential to inform policy and decision-making in this area, particularly about issues such as military modernization and preparedness. The research findings could potentially inform the development of guidelines and regulations for the responsible use of AI in military settings. Recall chess pieces better when arranged on a chess board in meaningful patterns than randomly arranged chess pieces ^[32, 33]. It has been demonstrated that people skilled in reading architectural plans, reading circuit diagrams, and deciphering X-ray images have the best ability to spot essential patterns in those fields ^[34, 35]. Therefore, it appears logical to speculate that the capacity to recognize key battlefield patterns is at least one element of the battle command experience.

Conversational Pattern

Reinforcement learning is a subset of the broader field of artificial intelligence that is both exciting and often underutilized. However, it has long been employed by the military. This technique serves as a valuable approach for teaching autonomous systems to perform complex military tasks. Unlike supervised learning, which relies on well-labeled data provided by humans, or unsupervised learning, where machines learn by discovering clusters of information, reinforcement learning operates through a trial-and-error method. It learns from environmental feedback and general objectives to iteratively improve towards success. This encompasses the interaction between humans and machines, as well as their reciprocal communication and exchange. This pattern's goal is to enable machines to interact with people in the same way that people do. Over the years, one of the significant advancements has been the

development of conversational agents based on conversational patterns, speech and object recognition, and natural language understanding [36]. A subset of the larger fields of AI (artificial intelligence) Reinforcement learning is one of the most exciting yet underutilized types of machine learning. However, the military has been using this technique for a long time now. A helpful approach to problem-solving for teaching autonomous systems to carry out challenging military tasks is reinforcement learning. Reinforcement learning tries to learn through trial-and-error, using environmental feedback and general goals to iterate towards success, as opposed to supervised learning approaches, where machines learn by being trained by humans with well-labeled data, or unsupervised learning approaches, where machines try to learn through the discover of clusters of information and other groupings [52].

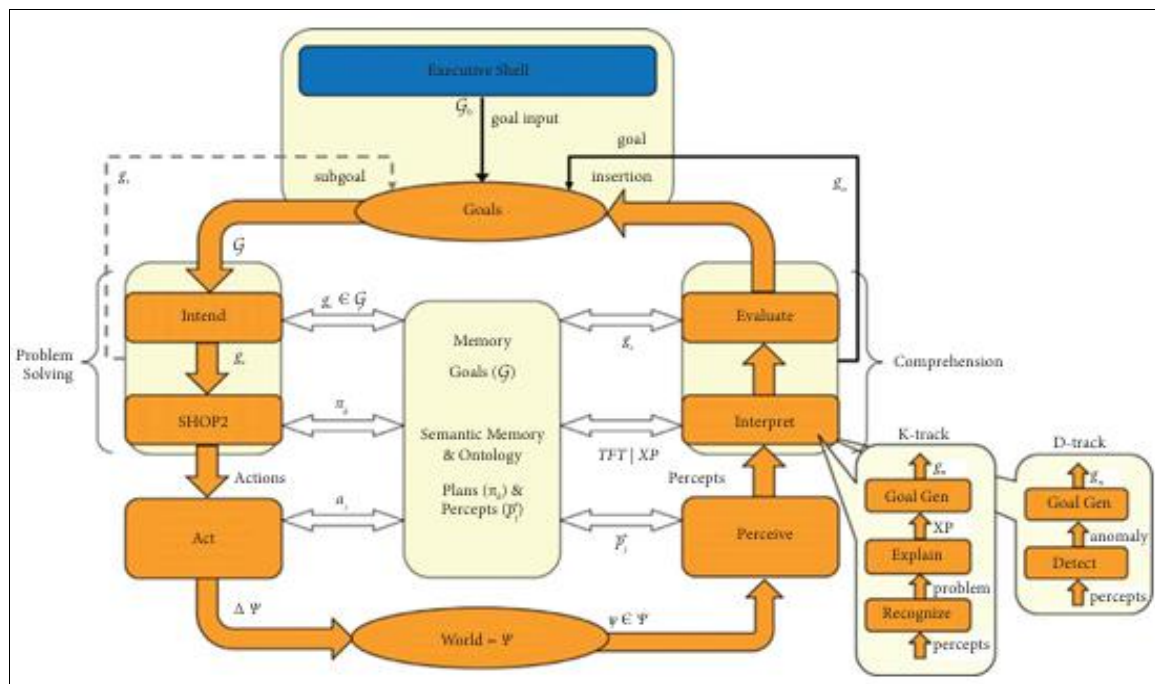


Fig 1: Metacognitive integrated dual-cycle architecture (MIDCA) object-level structure.

Autonomous Systems Pattern

This category includes both physical hardware and autonomous software systems, often referred to as software “bots.” The first automatically guided vehicle system was created in the 1950s by the American company Barrett Electronics. Between 2004 and 2007, the American Defense Advanced Research Projects Agency (DARPA) organized three Urban Challenges to advance this technology. The most influential reference control model for autonomous and self-adaptive systems operates on a feedback loop that controls and manages the Monitor-Analyze-Plan-Execute (MAPE) cycle using shared knowledge, as illustrated in Figure. The process is straightforward: the system's sensors gather data, and then it follows these stages in order: monitor, analyze, plan, and execute. The analysis and planning stages rely on rule-based policies. The most influential reference control model in the feedback loop for autonomous and self-adaptive systems controls and manages the monitor-analyze-plan-execute over shared knowledge (MAPE-K) in a subsystem, as shown in Figure. The work is simple: the program's sensor gathers data and

then performs the stage in the following order: monitor, analyze, plan, and execute. The analysis and plan part is rule-based policies. Any action that might involve autonomy should be carefully considered. With so many options, the autonomous pattern has a promising future.

Applications of Artificial Intelligence in the Defense Sector:

Practically every military application involves artificial intelligence, and growing military support for innovative and advanced AI technologies is anticipated to increase the demand for AI-driven systems in the military. As illustrated in Figure 10, this part of the paper largely focuses on the AI capabilities important to military operations for simplicity and their applications in defense sectors.

Autonomous Weapons and Target Recognition

These are some exquisite examples of the application of AWS and target recognition in the defense sector worldwide.

However, there is a rising case due to the extensive use of AI in the military sector. Most AI-based AWS prospects are considered dangerous and under their governments' control. Many of them are recognized as being of public importance.

These examples and points highlight how risky and irresponsible these AWS ideas can be in the wide open if not followed by the LAWS (ethical codes for AWS), as mentioned.

Cybersecurity

Cybersecurity research has affected the whole world, while the United States, China, Germany, India, Japan, Australia, and most European nations have advanced the most. They employ artificial intelligence (AI) technology in the form of intelligent agents to defend against other cyberattacks and stop distributed denial of service (DDoS) attacks. Also, this prospect is not only for businesses and industries; it has developed and enhanced in the defense sector far more.

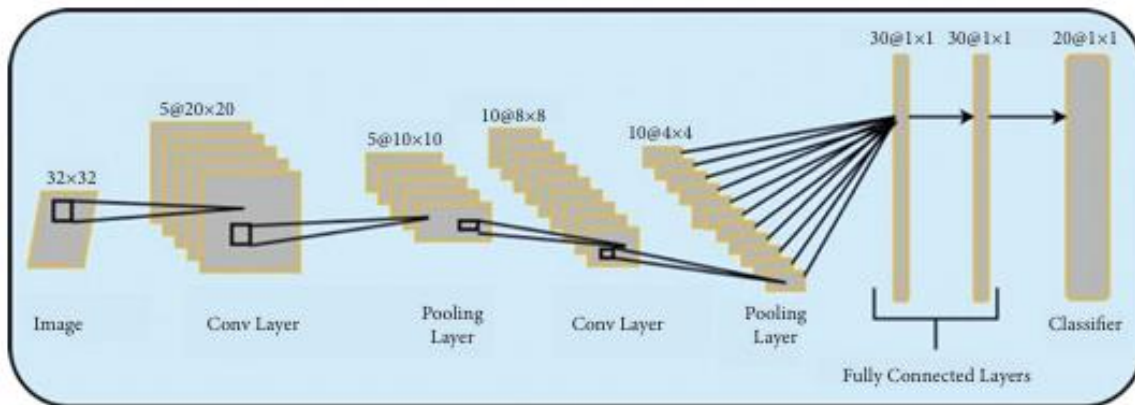


Fig 2: Basic convolutional network architecture

Figure 2 illustrates the functioning process of neural networks in detection. In actuality, AI stagnated and only evolved into a subset of specific application domains of the defense sector, such as data processing algorithms. The training subfield of AI created it. Providing a thorough or partial analysis of all the choices might not be possible. The effectiveness of AI techniques was demonstrated in a reasonably quick evaluation. Instead, it divided up the pathways and architecture into different categories. Discoverability is globally constrained for neural networks, knowing systems, intelligent agents, search, machine learning, and other areas.

Impact and Influence of Artificial Intelligence on Worldwide Strategic Stability and Nuclear Risk

AI capabilities have a significant impact because they are responsible for international strategic stability. A single choice might upset this delicate equilibrium, impacting the strategic stability between the world's major military powers. Their trait may impact strategic stability and make warfare less reliable.

There are five clear global risks of AI in the modern era:

1. Program bias introduction to the decision-making process
2. Lack of traceability in AI implementation
3. Black box algorithms and lack of transparency
4. Data gathering & sourcing and privacy infractions or violations of personal data
5. Uncertain legal liability or identification of authority

The risks associated with using AI systems rise along with their advantages. The following inquiries will be addressed in this section: potential hazards of artificial

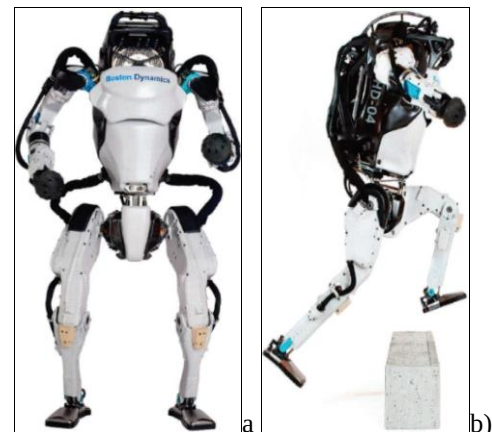


Fig 3: Atlas: (a) overall look and (b) jumping over an obstacle

There are more than enough ways that AI applications can cause global devastation within a second without any right consequences. A strategic instability or a nuclear threat could occur just because of some miscalculations by human-controlled AI operators or software-based AI operators or due to misinformation led by any third parties.

Escalation of Global Instability via "Deep Fakes"

A significant issue that emerged throughout the use of AI was the capacity of third parties to manipulate alert systems and insert misleading information to trick human technology operators. A previously undisclosed nonstate entity named The World Peace Guardians posted fake photos and videos on social networks to make it look like a few soldiers of American Special Forces were gassed to death in Syria during a clash with Russian military instructors. Some US analysts argued that using tactical nuclear weapons as retaliation was justified.

Distorted Early Warning Assessments

Mathematical coefficients obtained from extensive metadata analysis carried out at the time of the testing and training phases of the program Unified Platform appear to have skewed the dubious claims.

During the exercise, the United States crew was conscious of the variety of possible issues caused by the artificial intelligence-based evaluations offered by the United States Cyber Authority's Unified Platform. The Russian systems for

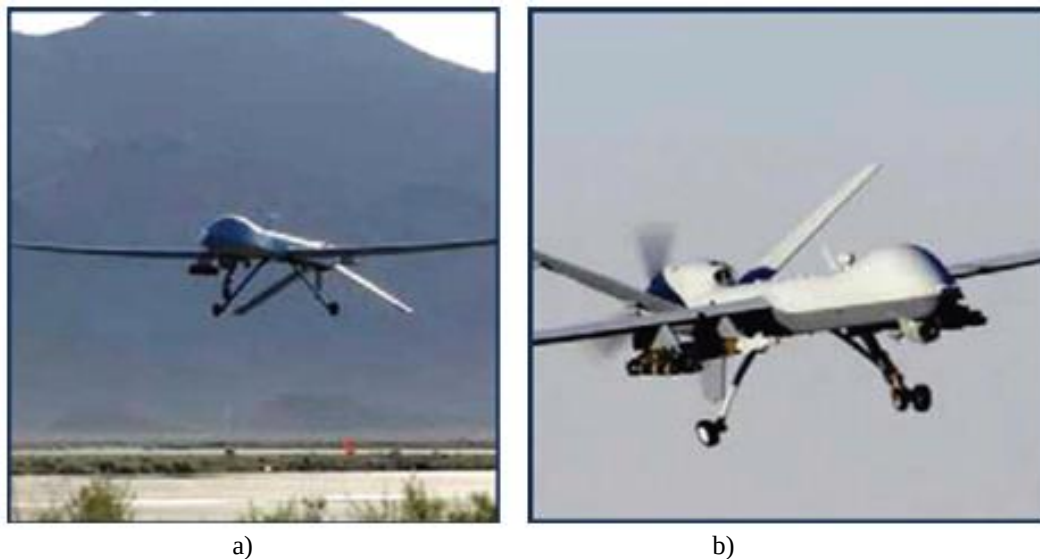


Fig 4: (a) MQ-1 predator and (b) MQ-9 reaper

The Overall Uncertainties, Threats, and Challenges of AI: Overall, aside from its own challenges, it can also create challenges of its own which could be termed as threats. For a better summarization, let us explore and highlight the major uncertainties, threats, and challenges of AI in the current domain of military applications and implementations

- 1. Cybersecurity:** AI systems in the military are often interconnected with other systems and, therefore, are vulnerable to cyberattacks. The malicious use of AI can cause significant harm to the military's infrastructure, personnel, and operations. Moreover, AI-powered cyberattacks could be difficult to detect and prevent.
- 2. Adversarial attacks:** Adversarial attacks are a type of attack that can cause AI systems to produce incorrect results by manipulating the input data. In a military context, adversarial attacks could cause an AI system to misidentify targets or provide misleading information.
- 3. Training:** Developing and training AI systems for military applications requires significant resources and expertise. Moreover, the quality and quantity of data available for training can be limited, making it difficult to create accurate and reliable AI models.
- 4. Integration:** Integrating AI systems with existing military infrastructure and processes can be challenging. This requires significant changes to existing systems and processes, which can be time-consuming and expensive.
- 5. Public perception and conception:** The use of AI in military applications raises concerns among the public about the potential for machines to replace human soldiers, reduce accountability, and increase the risk of harm to civilians.

Conclusions

This paper aims to represent the main sectors of utilization and the possibility of using AI augmentations and AI al-

gorithms in the military sector, especially in cybersecurity, object detection, robotics, and logistics.

The possibilities and applications of AI in the military, such as autonomous weapons and target recognition, surveillance, cybersecurity, military transportation and logistics, homeland security surveillance, cyber security, autonomous vehicles, and combat training and simulation, are described, discussed, and evaluated in our paper. The doing of reconnaissance with the use of partially autonomous vehicles in the military and sensor systems' utilization for betterment along with threat assessment in air defense systems with high time requirements, the emerging patterns intelligence analysis, education and training, and command and control systems from a military perspective are additional potential applications.

However, military uses of AI should take into account the following challenges

1. Vulnerabilities that could significantly harm the performance of the system
2. Transparency to guarantee model performance in line with military specifications
3. Inadequate machine learning (ML) training data
4. Effects of AI on nuclear risk and global strategic stability

We require more data and research for further retention on any decision regarding AI in the military and its capabilities. More study is needed on applying data, machine learning, and social science research to improve AI explainability in military contexts and enhance their capabilities appropriately.

References

1. Chauhan S, Singh D, Singh AK. Artificial intelligence in the military: an overview of the capabilities, applications, and challenges. J Survey Fish Sci.

- 2022;9(2):984-991.
<https://doi.org/10.53555/sfs.v9i2.2911>
2. Kiran, Singh D, Goyal N. Analysis of how digital marketing affect by voice search. J Survey Fish Sci. 2023;30(2):407-412.
<https://doi.org/10.53555/sfs.v10i3.2890>
 3. Tyagi Y, Singh D, Singh R, Dawra S. Analysis of the most recent trojans on the Android operating system. Educ Adm Theory Pract. 2024;30(2):1320-1327.
<https://doi.org/10.53555/kuey.v30i2.6846>
 4. Singh S, Singh D, Chauhan R. Manufacturing industry: a sustainability perspective on cloud and edge computing. J Survey Fish Sci. 2023;10(2):1592-1598.
<https://doi.org/10.53555/sfs.v10i2.2889>
 5. Sharma P, Sarma KK, Mastorakis NE. Artificial intelligence aided electronic warfare systems - recent trends and evolving applications. IEEE Access. 2020;8:224761-224780.
 6. Heller CH. The future navy—near-term applications of artificial intelligence. Nav War Coll Rev. 2019;72.
 7. Zhang Y, Dai Z, Zhang L, Wang Z, Chen L, Zhou Y. Application of artificial intelligence in military: from projects view. In: Proceedings of the 2020 6th International Conference on Big Data and Information Analytics (BigDIA); 2020 Dec; Shenzhen, China.
 8. Heller CH. Near-term applications of artificial intelligence. Nav War Coll Rev. 2022;72.
 9. Scharre P. Army of none: autonomous weapons and the future of war. New York: WW Norton & Company; 2018.
 10. Vaidya VR, Lyle M, Miranda WR, *et al.* Long-term survival of patients with left ventricular noncompaction. J Am Heart Assoc. 2021;10(2):e015563.
 11. Gillath O, Ting A, Branicky MS, Keshmiri S, Davison RB, Ryan S. Attachment and trust in artificial intelligence. Comput Human Behav. 2021;115:106607.
 12. Pradhan P, Satapathy A. Physico-mechanical characterization and thermal property evaluation of polyester composites filled with walnut shell powder. Polym Polym Compos. 2019;30.
 13. Lee D, Yeo S. Developing an AI-based chatbot for practicing responsive teaching in mathematics. Comput Educ. 2018;191:104032.
 14. Hu J, Emile-Geay J, Nusbaumer J, Noone D. Impact of convective activity on precipitation $\delta^{18}\text{O}$ in isotope-enabled general circulation models. J Geophys Res Atmos. 2018;123(23):13595-13610.
 15. Dalzochio J, Kunst R, Barbosa JLV, *et al.* Predictive maintenance in the military domain: a systematic review of the literature. ACM Comput Surv. 2023;55:135.
 16. Creswell A, White T, Dumoulin V, Arulkumaran K, Sengupta B, Bharath AA. Generative adversarial networks: an overview. IEEE Signal Process Mag. 2018;35(1):53-65.
 17. Wicaksono AS, Afif A. Hyper parameter optimization using genetic algorithm on machine learning methods for online news popularity prediction. Int J Adv Comput Sci Appl. 2018;9(12).
 18. Feng K, Han H, Tang K, Wang J. Statistical tests for replacing human decision makers with algorithms. arXiv preprint arXiv:2306.11689. 2019.