Hindawi
International Journal of Intelligent Systems
Volume 2023, Article ID 8676366, 31 pages
https://doi.org/10.1155/2023/8676366

Review Article

Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges

Adib Bin Rashid, Ashfakul Karim Kausik, Ahamed Al Hassan Sunny, and Mehedy Hassan Bappy

Industrial and Production Engineering Department, Military Institute of Science and Technology (MIST), Dhaka, Bangladesh

Correspondence should be addressed to Adib Bin Rashid; adib@me.mist.ac.bd

Received 7 February 2023; Revised 19 April 2023; Accepted 17 October 2023; Published 6 November 2023

Academic Editor: Yu-an Tan

Artificial intelligence (AI) has become a reality in today's world with the rise of the 4th industrial revolution, especially in the armed forces. Military AI systems can process more data more effectively than traditional systems. Due to its intrinsic computing and decision-making capabilities, AI also increases combat systems' self-control, self-regulation, and self-actuation. Artificial intelligence is used in almost every military application, and increased research and development support from military research agencies to develop new and advanced AI technologies is expected to drive the widespread demand for AI-driven systems in the military. This essay will discuss several AI applications in the military, as well as their capabilities, opportunities, and potential harm and devastation when there is instability. The article looks at current and future potential for developing artificial intelligence algorithms, particularly in military applications. Most of the discussion focused on the seven patterns of AI, the usage and implementation of AI algorithms in the military, object detection, military logistics, and robots, the global instability induced by AI use, and nuclear risk. The article also looks at the current and future potential for developing artificial intelligence algorithms, particularly in military applications.

1. Introduction

Artificial intelligence (AI) has been gradually improving and becoming a more efficient way worldwide with the help of data, computer processing power, and machine learning developments, especially during the last two decades. As a result, AI is being used increasingly and more frequently in the daily life of various sectors. A few of the various uses of this technology include speech recognition, biometric authentication, mobile mapping, navigational systems, transportation and traffic control, management, manufacturing, supply chain management, data collection, and control targeted online marketing. Therefore, it should come as no surprise that AI has many applications in the military sector also, in a vast range [1].

Military capability is the current measurement index when determining a country or nation's "Powerforce." 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. Studies show that hacking attacks on for-profit companies and governmental institutions around the AI sector are more common now. According to researchers, modern autonomous systems and artificial intelligence (AI) are expected to be crucial in future military confrontations [3].

Recent scientific publications show how prevalent neural network technology is today in the cyber fight. The development of intelligent transport systems (ITS) is one of the major examples, along with forecasting and assessing environmental phenomena, separating informational tweets from noninformational ones (containing information that are rumors or nondetailed irrelevant data), and forecasting dynamic FX conventional markets. This type of enhancer helps in the military sector in various ways and 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].

For instance, the decisional component necessitates an integrated framework that can carry out the necessary processes, from capturing a high-level course of action (CoA) to implementing a thorough analysis/plan of activities. One possibility is to build the approach on several AI methods, such as qualitative spatial interpretation of CoA diagrams and interleaved adversarial scheduling, and many others likewise enhance the military world in different paths [6].

The contributions of this paper are for the advancement of AI in the military capabilities, and the significance of this narrative review is to identify several key applications of AI in the military, including target recognition, surveillance, homeland security, cybersecurity, transportation and logistics, autonomous vehicles, and combat training. We have also highlighted the potential benefits of using AI in these areas, including increased efficiency, accuracy, and decision-making capabilities.

The paper also identifies several challenges and potential risks associated with using AI in the military, such as the potential for malfunction, hacking, and other forms of cyberattacks. The ethical and legal implications of using AI in the military are discussed in detail, particularly in relation to issues such as autonomous weapons and the potential for unintended harm.

The study has the potential to inform policy and decision-making in this area, particularly in relation to issues such as military modernization and preparedness. The research findings could potentially aid in developing guidelines and regulations for the responsible use of AI in military settings.

2. Seven Patterns of AI

There are many applications for AI, including chatbots, automated drones, facial recognition, virtual assistants, cognitive automation, fraud detection, autonomous vehicles, and applications for predictive analytics. However, regardless of how AI is applied, each of these applications has something in common. Despite the variety of applications, people who have created hundreds or even thousands of AI projects know that every AI use case falls into one or more of seven categories, as shown in Figure 1.

The seven patterns of artificial intelligence are goal-driven systems, autonomous systems, conversational/human interactions, predictive analytics, hyperpersonalization, and decision support. These seven patterns of AI have revolutionized military operations in recent years, offering new capabilities and applications for tasks such as object detection, decision support, and conversational interactions. Let's explore a tiny part of the seven patterns of AI in the military, highlighting recent innovations and research studies in each area. The current and future potentials for AI algorithms in the military are examined, with the hope of providing a comprehensive overview of the capabilities, applications, and challenges of using AI in this context (Table 1).

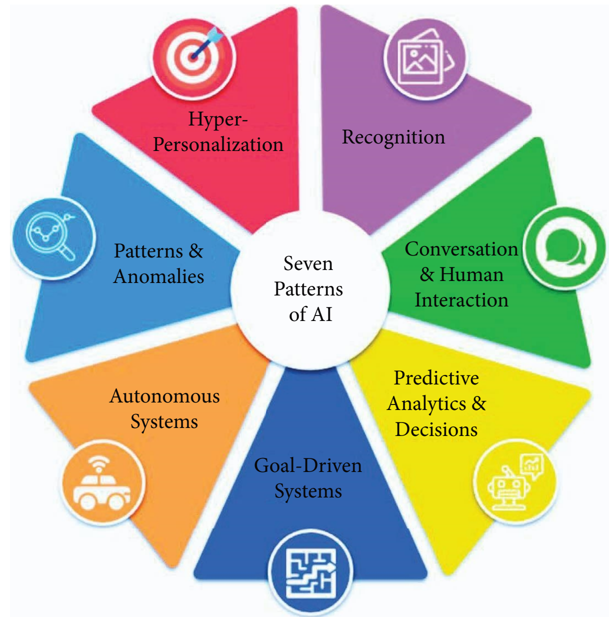


Figure 1: Seven patterns of AI.

Any personalized approach to AI will require programming and design because, no matter how these trends and the above innovations are blended, they all follow similar principles. Then, these seven patterns are employed alone or in various combinations, depending on the specific issue to that AI is being applied [22].

These seven AI patterns have undergone extensive study and are discussed below with an example.

2.1. Hyperpersonalization. The hyperpersonalization pattern is a way to use machine learning to create an individual profile and then have that profile learn and adapt over time for various purposes in processing, such as displaying relevant content, recommending appropriate products, and giving personalized recommendations. Treating each person individually is hyperpersonalization's main aim and objective. The four components of a hyperpersonalization plan are decision-making, data foundation, designing, and dissemination. The data foundation is the most crucial component because a hypercustomization approach depends on customer feedback to provide experiences, even though these components are important. A hyperpersonalization approach helps in building a client database. This will enable the delivery of hyperpersonalized experiences in the future [23].

Table 1: Summary of recent contributions of seven patterns of AI in innovations and military techs.

Patterns of AI	Modern-day innovative equipment/tech	Research paper
Goal-driven systems	Autonomous drones (e.g., MQ-9 reaper)	[7, 8]
Autonomous systems	Self-driving military vehicles (e.g., KF51 panther)	[9, 10]
Conversational/human interactions	Chatbots for military communication (e.g., US Army's Sgt. Star)	[11, 12]
Predictive analytics and decisions	Predictive maintenance for military equipment (e.g., F-35)	[13, 14]
Hyperpersonalization	GANs for personalized soldier training	[25–27]
Decision support	AI-assisted decision-making in military operations (e.g., SAGE)	[18, 19]
Pattern and anomalies recognition	Object detection in military surveillance (e.g., Raven drone)	[20, 21]

Implementing hyperpersonalization strategies can increase customer contact ability and consumer engagement as needed. To increase the number of clients who can receive highly customized experiences, it is essential to understand these techniques' impact, peak, and limit and the best moment to implement a new one [24]. Furthermore, rather than combining the two, most research concentrates on either traditional storefronts or e-commerce. This customer experience evaluation with the help of hyperpersonalization is almost similar to the military experience. Military teams can understand the best strategy and would be more effective through hyperpersonalization. It would enlighten them on what would increase their efficiency and teamwork most out of the many options available through machine analysis. Big data and hyperpersonalization are said to be the next big thing in the military art of war strategy buildup. Already AI augmentation with hyperpersonalization is poised to take over Europe and the US. The logistics department of the military sector worldwide most benefits from hyperpersonalization [25].

The decision-making component of the hyperpersonalization pattern alone plays a huge role in military capabilities. This component is particularly valuable in unmanned aerial vehicles (UAVs), commonly known as drones. UAVs are equipped with a wide range of sensors, cameras, and other data-gathering tools that allow them to collect vast amounts of data about the environment and potential targets. The decision-making component of hyperpersonalization can be used to analyze this data in real time, providing actionable insights into military commanders and allowing them to make more informed decisions [26].

For example, a drone equipped with hyperpersonalization algorithms could analyze data from a battlefield, such as the location of enemy combatants, the terrain, and the weather conditions, to determine the best course of action for a particular mission. The drone could provide real-time recommendations to commanders, such as where to deploy troops or which targets to prioritize, based on the unique characteristics of the mission and the environment [27].

In addition, there are also other utilizations of the same component in military applications, such as tanks, cars, military vehicles, and aircraft. For example, a tank equipped with hyperpersonalization algorithms could analyze data from its sensors and cameras to determine and make the best decision to choose the easiest route to a particular destination or the best tactics to use in a specific situation.

One example of recent innovation in hyperpersonalization for military decision-making is using neural networks to analyze UAV data. In a recent study, researchers used a neural network to analyze data from a UAV flying over a military training ground, identifying potential targets and providing real-time recommendations to military commanders. The neural network was able to locate targets accurately with a high degree of precision, improving the overall effectiveness of the mission [28].

GANs (generative adversarial networks), for instance, are neural network models for AI-augmented typical media that obtained the ability to enable the hyperrealistic synthesis of digital content of the modern work environment since the introduction of hyperpersonalization. In this machine learning (ML) model, GAN, two neural networks compete to make more accurate predictions. Examples include creating photorealistic photographs, voice cloning, facial animation, and image translation from one format to another. So, applying this technique in military warfare will let them know the best prediction through data evaluation and set a better strategy. A new AI-assisted brain imaging technique, fNIRS (functional near-infrared spectroscopy), can measure cortical hemoglobin concentration changes over time without being intrusive. Here, the near-infrared light is directed in the processing onto the surface of the body's skull and is primarily absorbed by two types of hemoglobin along with its propagation inside the cerebral cortex (HbR) that are oxygenated hemoglobin (HbO) and deoxygenated hemoglobin (HbD). By continuously observing light debilitation, fNIRS may reconstruct and establish the cortical concentration fluctuations of HbO and HbR; the local neuronal activity can be inferred from there. The physiological basis is almost similar and analogous to other imaging modalities techniques, such as functional magnetic resonance imaging (fMRI). However, because of its high cost, resilience, and portability advantages, it is best used at the bedside or in challenging clinical settings. If the cost can be minimized, the application of this system in the military from the perspective of better imaging of the enemy team would be more accurate and work great on the deciding factor to engage or not [25–27].

To train a generative model with GANs, the task is framed as a supervised learning problem with two submodels: the generator model, which everyone trains to create new instances, and the discriminator model, which tries to categorize examples as either real (from the domain) or fake (generated). In Figure 2, the process and function of that training are structured. Like in the figure, GAN training proceeds in alternate periods: the discriminator develops across several epochs. For one or more epochs, the generator practices. To continue training the generator and discriminator networks, steps 1 and 2 are repeated.

2.2. Pattern Recognition. Pattern recognition (PR) is a powerful computational method for objectively assessing visual data. In short, supervised machine learning is a distinctive machine-learning strategy in which the algorithm looks for significant patterns that divide into some divisional groups after being taught on samples. On the other hand, the unsupervised learning process is a technique used in machine learning and AI augmentation where the computer learns new types of patterns without relying on any examples from earlier training or operations. Typically, it is carried out by applying a set of predefined and predetermined rules. Unsupervised pattern recognition learning techniques clustering divides a dataset into different groups according to predetermined operations criteria, eventually developing a cluster or several clusters [29].

PR has a lot of advantages over other processes. Compared to a manual image processing setup, using PR process full images to identify image tiles on a grid without any

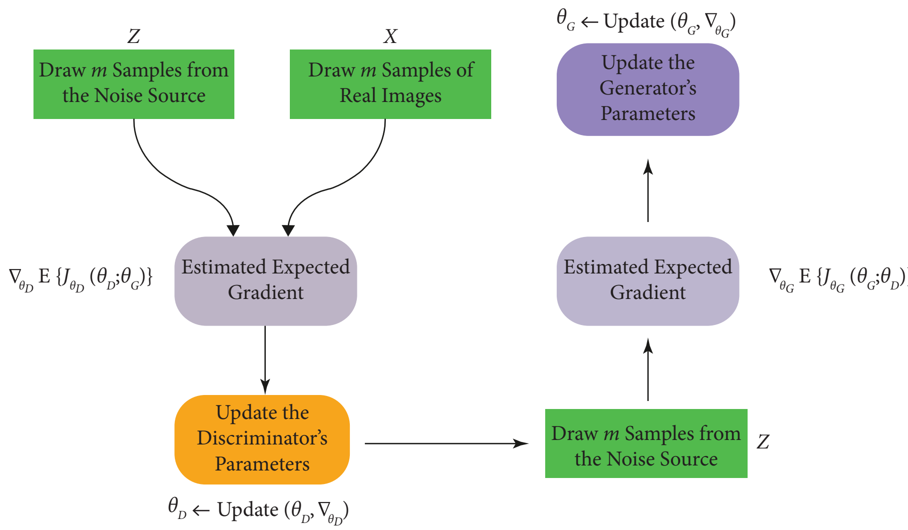


Figure 2: The main loop of GAN training [25].

preceding region identification phase is far more advantageous. It can be employed with segmentation algorithms to optimize the advantages of both strategies. In a limited sense, it is like evaluating confusion matrices in classification experiments. The quantitative data produced by these PR techniques differ from those produced by segmentation algorithms, which are better, more advantageous, and more efficient. Unlike the segmentation algorithm, PR can result in a better qualitative experimental finding, such as identifying the "hits" on a screen [30]. Because it is free from assumptions on the nature or existence of morphological changes in the imaging experiment, it is a suitable exploratory imaging test. The use of PR based on these advantages is trending right now in business and other industries. For example, let us see the utilizing stages of regions of interest (ROIs) to process PR.

As shown in Figure 3, the image is detected and captured to find the regions of interest (ROIs), and then, the data are divided into two parts: training and test sets. An ROI can be shown as a binary mask picture in the process. Pixels in the ROI are set to 1 in the mask picture, while pixels outside the ROI are set to 0. Through the next stages, the process is completed.

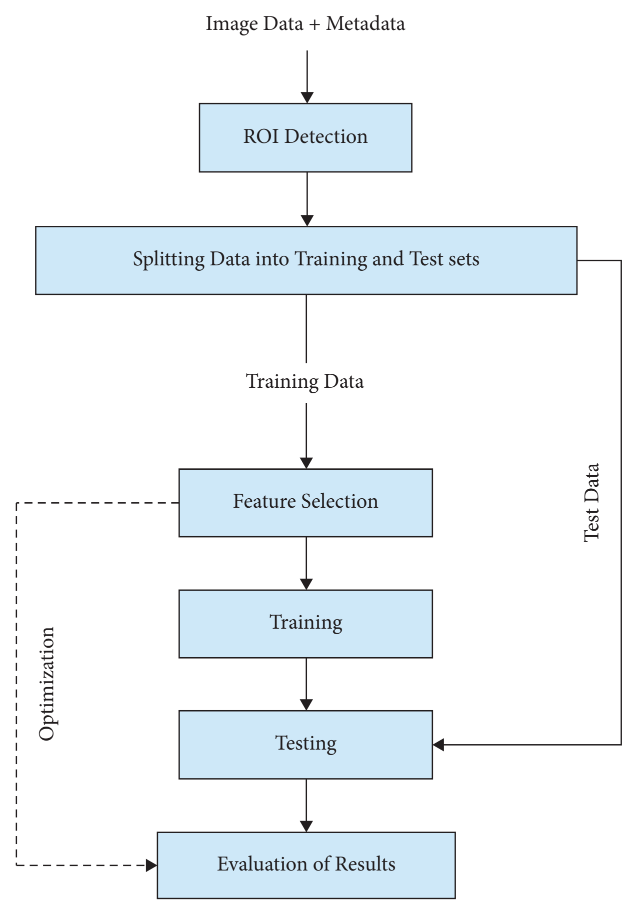


Figure 3: High-level architecture of bioimage analysis system [29].

Likewise, in industrial privileges, the military is also being enhanced by the pattern recognition process. Effective battle command requires commanders to read visual cues like maps and overlays quickly, so pattern recognition is crucial for the best and most efficient command on the ground. Army officers are given the guidelines and procedures for efficient command but not specific instructions on deciphering and applying battlefield patterns. The knowledge that commanders have amassed in the form of patterns may be the cause of their expertise. Skillful pattern recognition is a sign of expertise, according to research from the past 20 years. Expert programmers, for instance, can replicate important patterns of program code more effectively than code that does not adhere to acknowledged programming conventions [31]. Master chess players can 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 important 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.

2.3. Conversational Pattern. Over the years, various cutting-edge solutions have been created based on one of the most general conversational AI patterns. The modern workplace of the twenty-first century is filled with social robots and AI-augmented living helpers. In many industries, including the military, the significance of interactions between humans and robots is becoming increasingly apparent. With AI technology's help, this interaction is termed as conversational pattern. This is characterized as conversational forms of engagement and information spread across various mediums, including voice, text, and image formats, between machines and humans. This covers the interaction between humans and machines and their back-and-forth communication. This pattern's goal is to make it possible for 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) and NLP (natural language processing) is natural language interpretation (NLI) which is a profound invention in the sector of conversational patterns of AI. Most Internet users have probably unknowingly encountered NLP technology through machine translation tools and search engines, as well as AI (artificial intelligence) unintentionally using financial resources and video game programs [36]. To create and develop language-related software, natural language processing (NLP), a subfield of computer science, investigates the structure and operation and arranges language use into computational models based on conversational patterns.

One of the first chatbots was the traditional ELIZA, another conversational pattern created in 1966. The first exemplary AI conversational pattern resembles a chat with a Rogerian psychotherapist. ELIZA produced a discursive environment that required essentially no real-world expertise from the software. The ALICE bots was one of the most effective chatbot implementations of conversational patterns and artificial linguistic computer entity on the Internet. It has already achieved great success in AI (artificial intelligence). ELIZA's evolutionary offspring, ALICE, possesses all of its ancestor's skills but has not undergone any significant changes [38].

Figure 4 is the first chat between a human and ELIZA, followed by pattern matching and substitution methodology to simulate and continue the conversation. In short, it just mimics human conversation. It was just the primitive version of "Jarvis" from the movie Iron Man.

But the ALICE, which is mostly expressed as A.L.I.C.E (artificial linguistic Internet computer entity) and termed as ALICE bots, was a conversational bot that was more effective and influencing as ELIZA but followed almost the same way of interacting, just with some new modifications. The programming code of the bot was rewritten to Java code again in 1998 for better output. Program D is the Java implementation as it is right now. The application uses the AIML (artificial intelligence markup language) XML Schema to express the heuristic dialogue rules. The current system architecture of ALICE is shown in Figure 5.

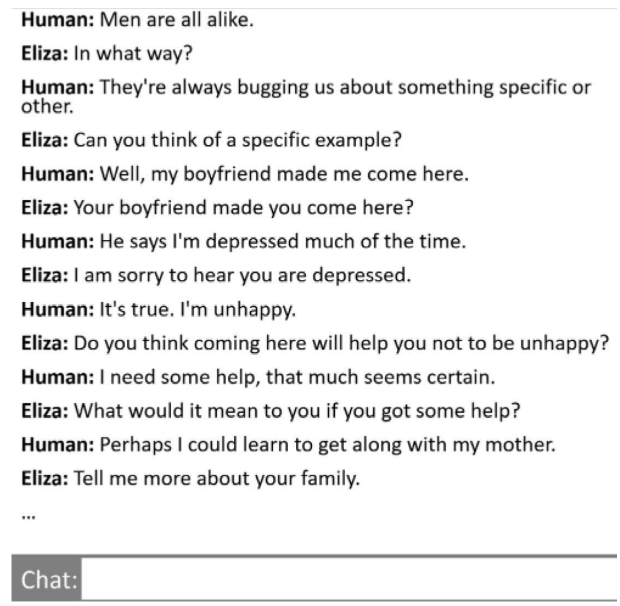


Figure 4: A conversation between ELIZA and a human [37].

The modern era brought some more revolutionary chatbots, which are exemplary when it comes to the discussion of conversational patterns of AI. WeChat is one of those modern revolutions in conversational pattern establishment.

WeChat is a major instant messaging system in a few influencing and digital countries. It was initially released in 2011. Along with basic functions like chatting, it also created specific services for its consumers. A group created by Artificial BudDy U Love that is known as ABDUL in 2008 is a connective conversational agent as a resource for Internet information that currently offers access to the Thai language and information resources. ABDUL uses the Instant Messaging (IM)-based protocol to enable connections from various gadgets and platforms [40]. The system and the user can converse using natural language. ABDUL works as a linguist and information specialist right now.

Like industry and business pilgrims, these chatbots based on conversational patterns have been developing quite an influence on military capability. Conversational agents or bots have emerged and will likely influence more as AI has grown. No datasets in military communication are as precise as the datasets found with the help of conversational patterns. For example, military soldiers will require information about their surroundings and instructions to complete their tasks in an unknown location. The study on conversational patterns for the military mostly concerns creating conversational systems for similar situations. Many countries have been making advancements in the field based on these data on military scenarios using conversational patterns. Additionally, by deploying a conversational military agent, soldiers will get prompt, pertinent responses while working on repetitious chores with less effort and expense [41].

2.4. Predictive Analytics. It was estimated that by 2025, the price of software for business information and data analytics in the United States alone might reach a maximum of USD 191.60 billion [42]. American firms are spending more on this money because one of the seven patterns of AI, predictive analysis, is ensuring a new dawn on the eve of Industry 4.0. Because of the massive development in digital data generated by consumers and the resulting services sector now holds the highest part of the market for predictive analytics software due to the necessity to extract strategic, vital information, investors are focusing more and more on this prospect of AI. For businesses to analyze consumer behavior and develop niche marketing strategies, predictive analytic AI is more essential than ever. Also, people can create fruitful, enduring friendships if IoT (Internet of things) technology, another predictive analytic software prospect, is used to obtain engagement insights. IoT has already shown a great prospect of application in the military sector, as it is illustrated in Figure 6.

The above figure illustrates the many applications of predictive analytics technology like IoT shortly. When it comes to gathering battlefield data, as mentioned in the figure, military teams can scan and keep an eye on the battlefield with unmanned drones, cameras, and sensors with the help of IoT. These armed drones can provide real-time data to the command center, capture live photos, and track the enemy's location and terrain. These same techs would help them to determine and identify enemies. Enemies can enter military installations with stolen badges or pose as civilians [43]. IoT sensors may collect fingerprints, iris scans, and other biometric data to identify people and those who might be a threat. Another part of the figure depicts smart bases; military bases can use IoT sensors and devices to enhance their equipment and services' functionality, performance, and comfort. The help of IoT in determining and monitoring soldiers' health is very common now in every country's military force. Sensors are inserted inside their uniforms to track or centrally monitor the soldiers' physical and mental well-being. Heart rate, body temperature, thermal distribution, and some behavioral traits like speech patterns can all be monitored by sensors. A successful military operation depends on the effective delivery of personnel and ammunition and the routine maintenance of military vehicles [44]. IoT technology's connected sensors and analytics make it possible to trace goods from their point of origin to the locations on the battlefield where they are needed. These are all the major applications of IoT, as mentioned in Figure 6; aside from that, they have other applications in the military sector.

The military has always been at the forefront of cutting-edge or enhanced technology. Internet is one of the most significant daily applications created by or with military

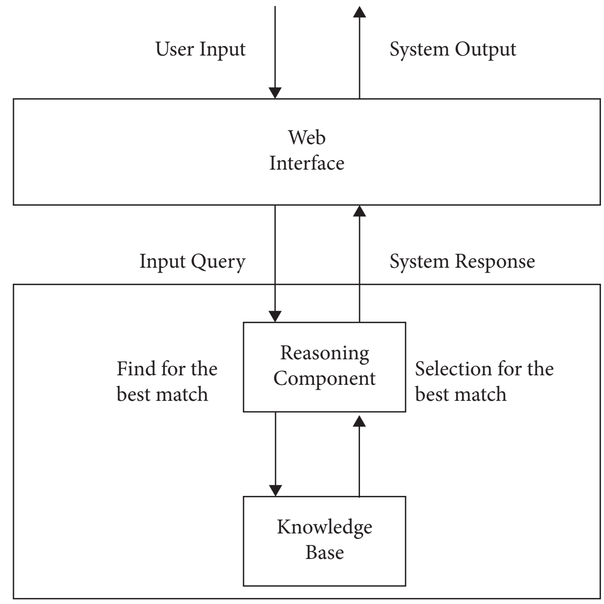


Figure 5: ALICE system architecture [39].

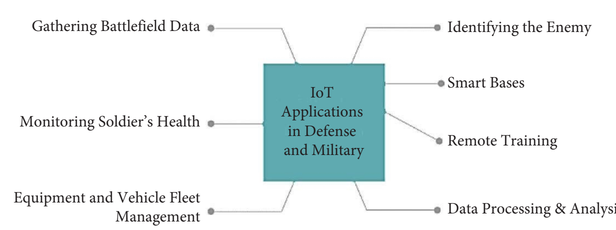


Figure 6: Applications of the Internet of things (IoT) in defense and military [39].

use in mind. Having said that, the military is implementing predictive analytics at a slower rate than the rest of the business and industry, as was indicated above. However, there may be additional uses for the technology that they prefer not to promote. Predictive analytics' core function is to make predictions based on the past [45]. It is not always necessary to use machine learning or artificial intelligence. In its most basic form, all that is required is a little common sense. Most individuals can probably forecast rain or even a storm depending on the intensity of the indicators if clouds are darkening the sky and there is a strong breeze.

These are the military areas that can be influenced by predictive analytics of AI and would be sufficient to make the military more capable:

(1) Estimating a soldier's effectiveness in an actual combat situation or the direct battlefield based on their performance in a virtual environment
(2) Predictive maintenance is sometimes known as predicting when a vehicle will need repairs and replacement parts
(3) Estimation of the amount of instruction and care that soldiers will require in a specific combat situation

Whether on the battlefield or not, the military employs various vehicles for its operations, which rely heavily on AI augmentation and datasets. This may not be as simple as it may seem because routine maintenance alone may not be sufficient to maintain their condition throughout the active operation. Due to the frequent use of military vehicles, parts can break without warning, and AI software could malfunction if not intended with regular maintenance. The military could reduce vehicle malfunction and failure during operations with predictive analytics. Predictive maintenance is what is meant here. Vehicles may collect data using various methods, from specialized sensors to telltale emissions that frequently go undiscovered [46].

The latter is true for a test run of Uptake Technologies' predictive analytics software for several Bradley M2A3 assault vehicles. The Bradley M2 is an extensively armored transport vehicle from BAE (British Aerospace Engineering) systems [47]. By monitoring and analyzing the data gathered from current sensors and telematics, such as GPS, while the vehicle is in operation, the objective is to predict the failure of the vehicle and/or its parts. Installing new sensors would not be necessary to find and gather the data. Uptake defends this strategy by citing its prior success in applying it to manufacturing and industrial machinery. Berkshire Hathaway Energy, Caterpillar, and Boeing are a few of its accomplishments.

This was just one example of using AI (predictive analytics) to modernize military capability. Different governments invest more than a hundred million all over the globe to enhance their military with the help of predictive analytics.

2.5. Goal-Driven Systems Pattern. One of the core patterns of AI is the "goal-driven systems pattern" out of the seven patterns of AI. Like the others, this type of artificial intelligence is used to address a common set of issues that would otherwise require human cognitive ability. Finding the best answer to an issue is the challenge that machines must deal with in this specific pattern. The issue could be navigating a maze, streamlining a supply chain, or minimizing idle time and travel routes. Regardless of the precise need, the power we seek is discovering the greatest solution through trial and error, even if it is not obvious.

A unique concept of AI is goal-driven autonomy (GDA), which gives autonomous agents total autonomy. The agent searches for problems within the context of its current goals and purpose rather than randomly recognizing abnormalities. The metacognitive integrated dual-cycle architecture, short, "MIDCA," known as "action-perception" cycles, takes place at both the cognitive and metacognitive levels [48]. This is a perfect example of a goal-driven system pattern. Figure 7 illustrates the function of the system in a structural drawing.

For several reasons, the requirements engineering process must explicitly articulate goals in AI. Goals offer the basis which identifying conditions that support their proposal elucidating to clients the justification behind those requirements, identifying and eventually resolving requirements conflicts, and supplying criteria for the requirements specification's completeness (if every objective is achieved, then the specification is finished), and typically acting as the most reliable data in the specifications. So, in short, it is clear that the main objective of this system is to act spontaneously in a greater capacity in a dynamic environment and to manage any unexpected events that are very common on the battlefield. These systems based on goal-driven system patterns would make things easier for the armed forces [49].

The KAOS method, which stands for "knowledge acquisition in automated specification" or "keep all objectives satisfied," is one of the most prominent examples of goal-driven system patterns in the contemporary area of AI in the modern world. The KAOS technique assists with the complete explanation of the requirements process, from the high-level objectives that the composite system has to achieve to the actions, objects, and restrictions the software component must adhere to. It is a method for requirements engineering that focuses on capturing goal-oriented software requirements. A "composite system" includes the intended program and its surroundings in this context. So, for a better perspective of the battlefield environment or to understand the attackers' regions, this is a great help. KAOS offers a better capturing of enemy approach than any other typical programs in the military. It even can share information across a good number of diverse teams. The technique consists of a language for its specifications to elaborate its procedure and high-level information that is given during procedure local advice implementation [50]. This method has been implemented in the military sector for a certain time now for better output, and the system works just fine with it functioning better in operations.

Distributed artificial intelligence (DAI) has been utilized to capture a common environment, similar to KAOS, consisting of groups of intercommunicating agents and behavioral circumstances. The effectiveness of list processing (LISP) in terms of space and time execution when attempting to operate as a goal-oriented autonomous system is still up for debate, even though LISP-based languages have made substantial advancements [51]. Industries and businesses look forward to making a fast impact with the help of this goal-driven system pattern software. In the military sector, the AI-assisted goal-driven pattern system DAI has been used for the collection, archiving, retrieval, analysis, and visualization of spatial data to enhance decision-making from the perspective of battlefield objectives.

Reinforcement learning is one of the most exciting but least used types of machine learning. However, the military has been using this technique for a long time now. A useful 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 discovery of clusters of information and other groupings [52].

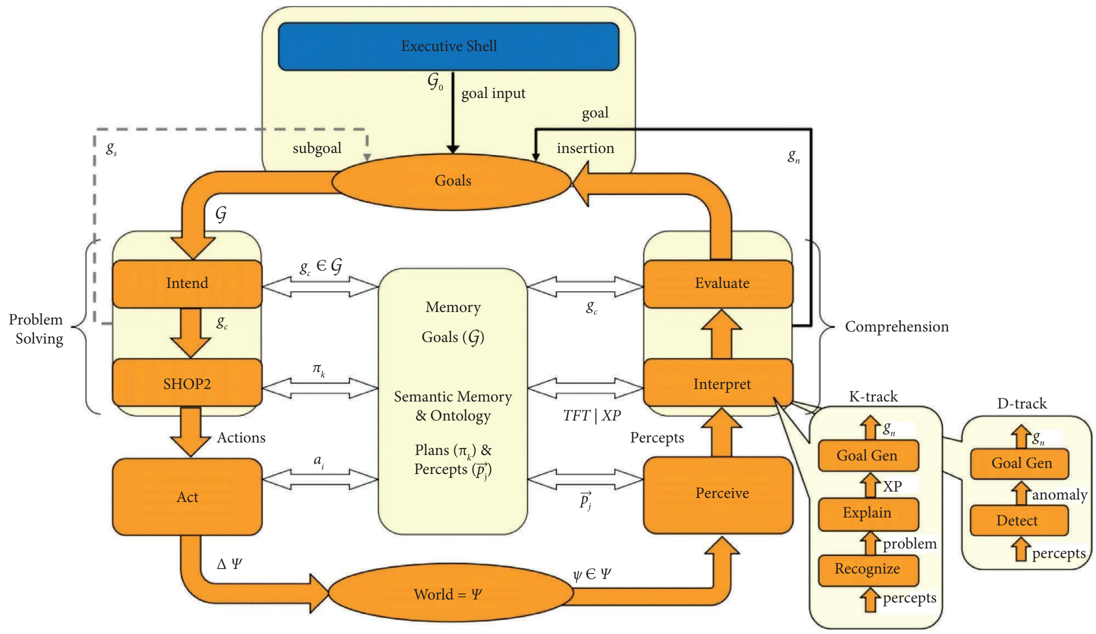


Figure 7: Metacognitive integrated dual-cycle architecture (MIDCA) object-level structure [48].

Without AI, businesses rely on people to develop programs and rule-based systems that instruct software and hardware on how to function. Although policies and procedures can be fragile and restrictive, they can be useful in managing finances, personnel, time, and other resources. The machines are not learning; the systems are only as robust as the rules humans design. Instead, what makes the system function is the human intelligence built into the rules.

2.6. Autonomous Systems Pattern. Autonomous intelligence, or the autonomous system pattern, is the most sophisticated type of AI, in which procedures are automated to produce the intelligence that enables computers, bots, and systems to behave independently of human interaction. This AI class may have the most use in the military sector worldwide. Autonomous systems are capable of carrying out a task, achieving a goal, or interacting with their surroundings with little human intervention. These systems must also be able to anticipate events, make plans, and be aware of their surroundings, which make more sense as to why these are used to fulfill military aims and objectives. This covers both physical hardware and autonomous software systems (software "bots").

The reduction or abolition of human labor is the main goal of the pattern of the autonomous system. The users must ensure that the autonomous system performs as nearly at the human level as possible when a human is removed from the equation. As a result, it is clear why this is one of the trickier patterns to apply. Since autonomous systems are designed to reduce the need for human work, they must be dependable, consistent, and of exceptionally high caliber [53].

One of the most important uses of artificial intelligence (AI) is in unmanned autonomous systems with intelligence. The development of such systems significantly promotes developments in AI technology. Intelligent human-designed machines that can be transported utilizing cutting-edge technology to carry out tasks or manage without human intervention are known as unmanned autonomous systems (UAS) [54]. It is the prime example of an autonomous system pattern in the modern world. Also, this is the fastest advanced and most invested pattern of AI in the military sector worldwide.

Improvements in the study of unmanned autonomous systems have led to the development of numerous impressive applications. The research community has been astonished by unexpected advancements in autonomous ground and aerial vehicles for commercial and security purposes, some of which have even come to pass. For instance, Google has made its driverless vehicle available for purchase in California even while Tesla and other manufacturers' products are still undergoing testing. Unmanned aerial vehicles (UAVs) are frequently used on the battlefield for several purposes and in search and rescue operations. In these systems, AI algorithms are applied on a large scale. For tasks like trajectory planning, radio/radar signal identification, and vision, large-scale implementations of models like long short-term memory (LSTM) and attention are developed in the inner network [2]. These improvements save both the economy and lives. Deep reinforcement learning developments also ushered in a new era of gaming when Lee Sedol, a well-known Korean player, was defeated by AlphaGo with a final score of 4 : 1. This is when humans started to pay attention to their robot competitors. AlphaGo is recognized as the most difficult game ever created by humans.

In 1950s, the American company Barrett Electronics created the first automatically guided vehicle system. The American Defense Advanced Research Projects Agency (DARPA) organized three UV challenges between 2004 and

2007, which aided in the speedy development of UV technologies. The National University of Defense Technology of China created the Hongqi CA7460 autonomous driving car with autopilot in China. It has a top speed of 130 km/h and can reach highway speeds up to 170 km/h [54]. The car could overtake other moving objects on the road.

Google developed the first fully functional UV prototype on December 22, 2014, and the real road testing started in 2015, another exemplary autonomous system pattern advancement. Since then, they have driven 1.4 million kilometers testing cars. Thanks to wireless firmware that has been updated to version 7.1.1 due to the help of Tesla's UV has accumulated 780 million miles of test data and is capable of collecting one million miles of data every 10 hours [55].

Almost every corporation worldwide is drawn to the UAV boom, particularly in the military sector. Military unmanned aerial vehicles (UAVs) are generally used for attack and damage assessment, as well as for battle surveillance and reconnaissance, electronic countermeasures, and damage assessment. Compared to their military counterparts, civilian UAVs can be used for a wider range of jobs, including disaster search and rescue, railway and transmission line inspections, resource exploration, agricultural surveying, traffic control, weather forecasting, aerial photography, and environmental monitoring.

However, these control loops are insufficient for a system to move around, behave appropriately, and operate in various real-world open contexts. Sense-decide-act or monitor-analyze-plan-execute (MAPE)-style controllers are usually called autonomous. "Agents" are the basic behavioral elements of an autonomous system [56, 57]. They are the ones who developed, coded, or constructed them during the system's development. Agents take the initiative and strive toward set goals that may change over time; how the self-adaptive software or unmanned autonomous software functions is shown in Figure 8.

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 8. 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.

Cobots, also known as collaborative robots, are another type of autonomous system. In case many are not familiar with the idea, cobots are machines that work alongside and close to people to complete jobs. On the other hand, industrial robots are physically segregated from people and caged off. Cobots are designed to function independently of humans even while they are close by, even though they can act in an augmented intelligence capacity [59].

Even though the AI's autonomous patterns system is likely the most difficult to construct regardless of whether it is in the case of the military sector or industry and business sectors, it may have a considerable influence when done well with the proper development and enhancement. Any action that might involve autonomy should be carefully considered. With so many options, the autonomous pattern has a promising future.

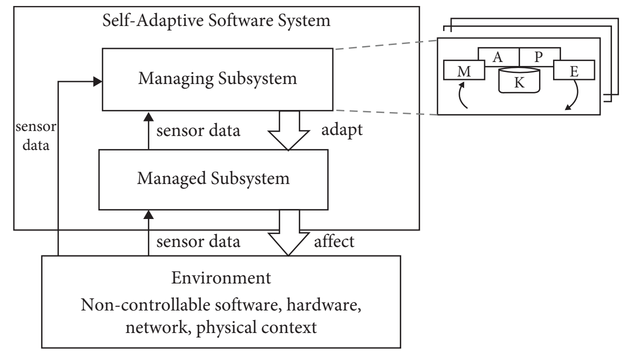


Figure 8: An MAPE architecture [58].

2.7. Identifying Patterns and Anomalies. The patterns and anomalies is one of the seven AI patterns which are most frequently used in different industries worldwide, and the military sector is no different. Anomaly detection for advanced military aircraft with the help of AI-augmented neural networks and machine learning is very common now. Machine learning is especially adept at swiftly shifting through huge amounts of data to detect patterns, abnormalities, or outliers. One of those AI uses, known as "pattern-matching," tends to crop up repeatedly, and with good reason—it has a wide range of uses. The basic aim and objective of AI's patterns and anomalies pattern are to understand patterns in the data and find higher-level connections between that data using machine learning and other cognitive approaches. Finding what fits with the current data and what does not requires determining whether a given data point matches an existing pattern or is an outlier or anomaly. There are numerous ways to apply this design, one of the more popular patterns [60].

Applications of this pattern include fraud and risk detection to determine whether events are unusual or consistent with expectations. Finding ways to data and assisting in reducing or correcting human error are further applications. Predictive text is another example of this pattern; it can look at speech and language patterns to propose words to write more efficiently. This helps the armed forces a lot for a better understanding of the battlefield and what the environment of the battlefield may look like. Most countries now implement this AI technique in their military sector to teach their trainee soldiers and cadets to train tactically and strategically. Some of them even have distinct learning on pattern recognition and identifying anomalies.

To find trends and anomalies, running applications in virtual machines rather than hardware-based devices are quickly gaining popularity across all industries. This brings down the cost while also making the service more easily accessible. Many military powers worldwide have accepted and already practiced these techniques for over a decade for better privilege in the combat zone. The adoption of the OpenStack cloud environment is expanding in academia and industry because it provides open-source cloud services to execute the application in research and production environments. The next generation of cyberwarriors is being trained in numerous nations using this open-source

OpenStack cloud platform. Even the most powerful military forces worldwide have ditched their legacy training model for this AI-augmented built-up training. One of the issues with a cloud system is locating anomalies and foreseeing them before they occur. Any military power that can address and eliminate this issue by identifying patterns and anomalies would be unstoppable [61].

The traditional approach involves manually checking for anomalies by monitoring heart rate and threshold levels. The use of machine learning algorithms to detect problems before they occur has been the subject of recent investigations.

While discussing the applications, let us start with network function virtualization. Network function virtualization is the process of virtualizing network services on dedicated hardware. Academics and business professionals closely observe how network function virtualization (NFV) is applied. Service providers can more easily incorporate network services into software that can operate on common servers by using NFV. With the help of NFV, switches and routers can be operated as virtual network services on a single server. The military forces have been able to reduce the cost of the hardware. As a result, other industries benefit, too [62].

Some forecasting methods, such as autoregressive integrated moving average (ARIMA), rely on historical data to produce predictions. However, these tactics are ineffective if the data lack discernible patterns and exhibit high levels of random volatility [62, 63]. Machine learning and deep learning algorithms are much more efficient and dependable than earlier approaches. ARIMA excels in pattern prediction over shorter time horizons but fails over longer horizons. Forecasting is a great weapon from a military perspective. It is all about accuracy and fastness; the better these two issues, the more advanced they are considered. In many countries, ARIMA is considered the most accurate and fast forecast program, and the military sector continues to implement it till now. For example, countries like China forecast their military spending based on this program.

DeepLog is right now the most prominent use of AI patterns in the case of identifying patterns and anomalies. DeepLog learns patterns from typical execution and can spot anomalies when they differ from patterns with typical execution. This model is to be regularly updated so that it might recognize new log patterns in the future. DeepLog can also show how the observed patterns behave [62, 64]. This makes it easier for model users to identify the main cause of the anomaly. This model performed better than more traditional methods in finding anomalies in logs. Most military powers worldwide recognize and accept it as their initial system for identifying patterns and anomalies. The modern architecture of DeepLog is shown in Figure 9.

This pattern of AI also helps in the following:

(1) Digging deeper into the data
(2) Predictive typing in smartphone devices or any computers
(3) HR departments can handle job applicants and find patterns among them

There are numerous techniques to see AI's patterns and oddities in action. AI is being used to observe patterns, including intelligent monitoring, recognizing flaws or errors, and making modifications as necessary, cybersecurity applications, and stock market analysis.

However, it is important to be cautious about the data on which this AI pattern was trained, just like anything else that learns from it. After it was uncovered that their AI recruiting tool preferred men for technical jobs a few years ago, Amazon came under fire. Biased datasets can especially affect the patterns and anomalies of AI, such as hyper-personalization and recognition patterns. It should not be surprising that pattern recognition systems will display the same type of bias as the training data if bias data were used to train the systems–no matter if the system is used in the military sector or for industrial purposes. The whole training program and strategy build-up could be unacceptable if biased datasets occur during the military training program initiation.

3. Applications of Artificial Intelligence in the Defense Sector

Artificial intelligence (AI) is becoming more prevalent in battlegrounds. Like industries and businesses, the military is also day by day starting to be more AI-focused when it comes to advancement and development. AI-powered military systems can process large volumes of data more efficiently than conventional systems. Additionally, AI enhances fighting systems' self-control, self-regulation, and self-actuation through innate calculation and decision-making abilities. 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 [65]. 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.

3.1. Autonomous Weapons and Target Recognition. The Cuban Missile Crisis during the Cold War, which nearly resulted in the nuclear war, provides the finest illustration of the impact and exceptional significance of autonomous weapon systems (AWS) and target recognition [66]. This one piece of technology–the US Naval Forces' Autonomous Weapons System and Target Recognition–could have prevented this scenario. The United States and the Soviet Union focused more on deterrence and wartime stability after learning from the outcome of the conflict, such as by making AI-controlled military decisions less predictable and achieving machine-like accuracy. World Wars initiated the application of AI in the defense sector, but it started progressing in situations like the above.

Increased investments in uninhabited ground vehicles (UGV) like the Russian Platform-M and AWS like the MQ-9 Reaper (Figure 11(a)) resulted from these advancements. In

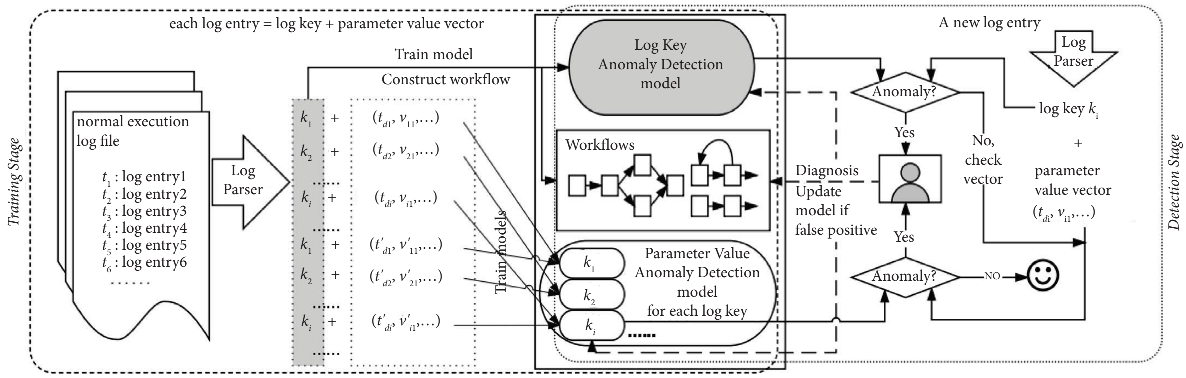


Figure 9: DeepLog architecture [60].

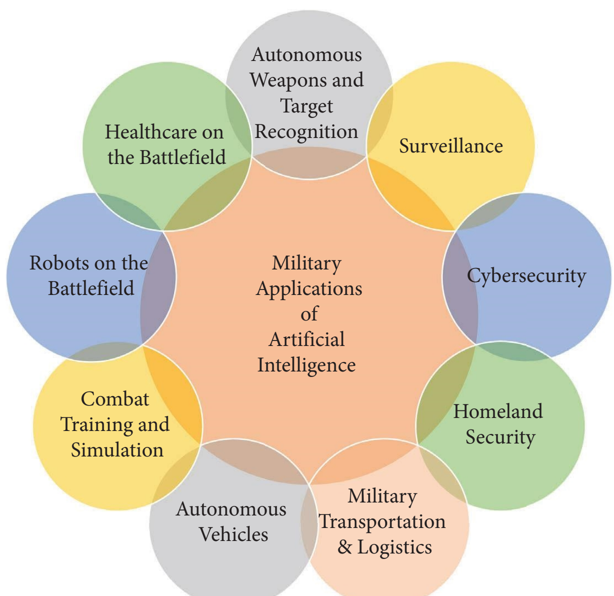


Figure 10: Applications of artificial intelligence in the defense sector.

these technologies, a drone pilot's sensor system for weapon detection and launch may even be the same as a pilot's sensor system in the cockpit of an inhabited aircraft [71].

According to some, the best autonomous weapons with the greatest capacity to detect targets with machine accuracy are the Patriot missile system (Figure 11(b)), the Phalanx weapon system (Figure 11(c)), the AEGIS naval weapon system ((Figure 12), and a few more [84]. However, this system's object-detecting component still needs much room for improvement. 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. There are more than a hundred arguments in favor of banning these dangerous AI-based AWS. However, no country plans to stop using or abandon this remarkable technology; on the contrary, it is being developed and advanced continuously. In that case, global organizations tightened the constraints on AWS since innovation and advancement cannot be stopped, and they did this to make the rules as moral as possible. Moral standards constructed the AWS for the lethal autonomous weapon system (LAWS) [85].

Now why these ethical codes are necessary? For example, the Israeli Harpy drone (Figure 11(d)) is one of the most deadly and sophisticated autonomous AWS used today. They are trained to move and think in a certain area for specified targets. These AI-based AWS employ the "Fire and Forget" high-explosive warhead, which could be dangerous in certain scenarios. What if, instead of attacking the enemy, these AI bots start to attack the civilians or fail to acquire the exact target? These are also called "Slaughterbots" internationally [66]. However, the development and deployment of AWS in military operations raise several ethical and moral concerns. Some potential dangers of AWS include the following:

(1) Malfunction: Autonomous weapons systems rely on AI algorithms to make decisions, and if there is a malfunction, the system may target the wrong individuals or groups. This could result in unintended casualties and human rights violations.
(2) Lack of Accountability: Since AWS is designed to operate without human intervention, assigning responsibility for any errors or violations during their operation becomes challenging. This lack of accountability could lead to impunity for individuals responsible for errors or violations.
(3) Hacking: AWS could be hacked, making them vulnerable to unauthorized use. This could result in the system being used against the country that created them or other unintended targets.
(4) Lack of Human Control: AWS does not require human intervention to operate, raising concerns about losing human control over military force. This lack of control could have significant implications for the conduct of warfare.

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 in Table 2.

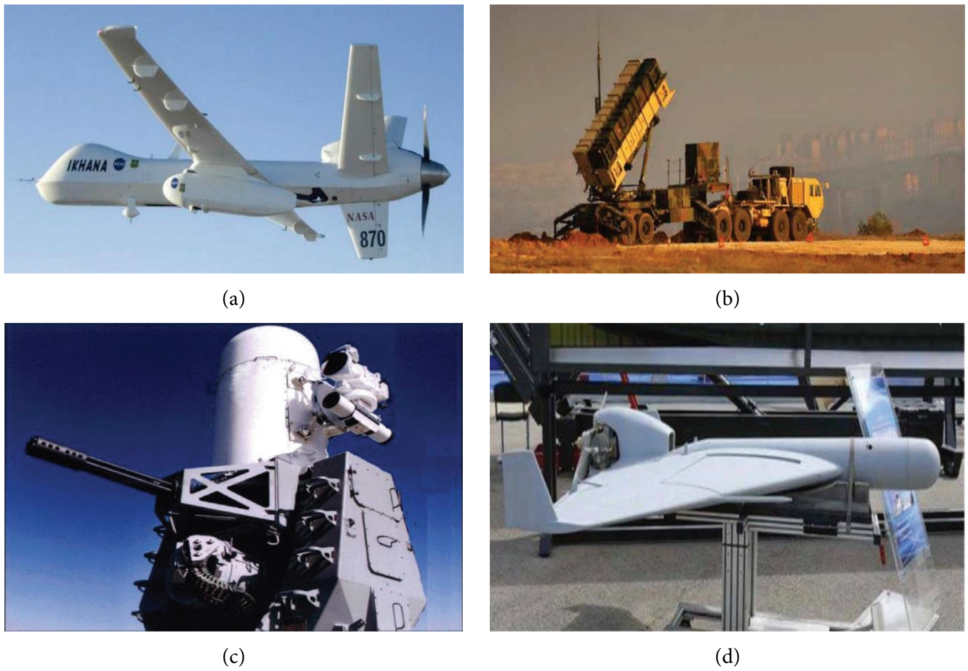


Figure 11: (a) MQ-9 reaper [67], (b) patriot missile system [68], (c) PHALANX block 1B system [69], and (d) the harpy drone [70].

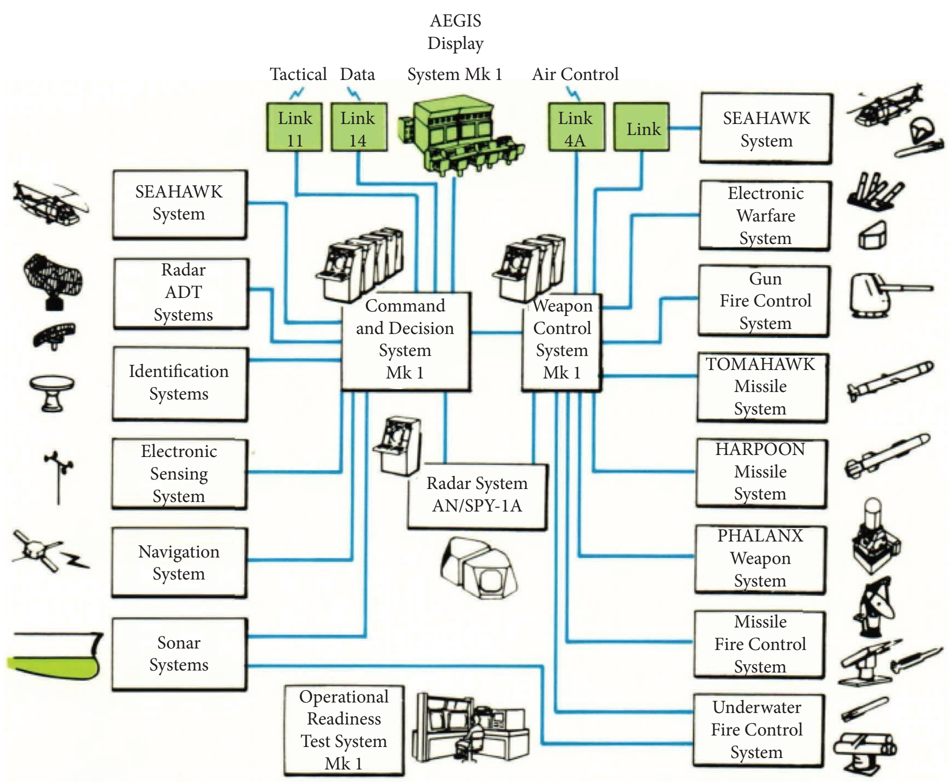


Figure 12: The major elements of the AEGIS combat system [83].

3.2. Surveillance. Day by day, the use of AI in the surveillance sector is improving and becoming more likely to be applied in every industry. There were over 23,000 new AI-related patents in 2008; by 2018, there were about 78,000 on surveillance with the help of AI [86]. The defense sector alone is taking a great part in applying and implementing AI-augmented surveillance systems. Many programs are already in effect in this sector worldwide, and more will likely occur shortly. Any country not following this trend is expected to get dominated and stay below the quality of

Table 2: Summary of key principles in AI-controlled AWS ethical codes.

Ethical codes	Human dignity	Privacy	Human autonomy	Fairness
A14PEOPLE	Benevolence fosters overall well-being and protects the environment on a global scale	No secrecy	Human agency and autonomy	Maintaining and advancing justice and solidarity
EAD2	Putting the growth and well-being of everyone first	N/A	Human rights	Objectivity and accountability
MONTREAL	Putting the general welfare first	Privacy and intimacy are protected	A fully autonomous and responsible human being	Fairness and diversity inclusion/solidarity
COMISION UE	Respecting a robot's decision to refuse care	Defending any human against harm and granting them complete freedom in the face of any violations of their privacy	Defending against the threat of robot manipulation	Preventing the severance of social relationships
UK LORDS	N/A	Intelligibility/explainability/transparency	N/A	Education, social and political cohesiveness, and inequality
ACM	Overall personal and societal well-being	Full privacy	N/A	Fairness/Nondiscrimination
GOOGLE	Socially beneficial	Users' safety and privacy	N/A	Be responsible for human role equity and refrain from fostering unfair bias
COMEST	Human dignity	Privacy/do not harm	Human autonomy	Responsibility

other military forces that use surveillance with AI's help. These innovations in this sector are proving to be more beneficial, making the military capability more stable and accurate. For example, the location of underwater mines is one of the crucial areas of object detection in military applications affecting the sense of security for civilians and the military. Another example is an AUV with a dead-reckoning (DR) navigation method based on neural networks, called NN-DR, perfect for rapidly changing conditions and decisions. This helps the defense sector to find a better and almost accurate decision.

The AI sector has created various methods for locating difficult problems that require human intellect. Some of these methods have matured so that precise algorithms can support them. Some methods have become so well-known and extensive that they are no longer considered for the assistance of humans. Instead, AI is doing the work far better with quality and efficiency.

Traffic centers have already started using 5G IT-based infrared temperature monitoring to track passenger circumstances in various cities. Regarding B5G digital media, it is possible to create an emergency plan for B5G cloud live streaming and, using the 5G+ fiber optic dual gigabit network; several hospitals can be continuously live-streamed on the CCTV website, which users have referred to as the communication with the widest audience [87].

The epidemic brought about a new level of AI revolution in the surveillance industry. The military of different nations is also considering applying this technology to strengthen their military capability. B5G enabled low-latency, high-quality video streaming for military medical staff to efficiently diagnose patients remotely, greatly improved regional access to medical information, allowed doctors outside of locked-down epicenters to recognize CT and X-ray specimens, and assisted in reducing the burden of diagnostic pressure on local doctors. Additionally, it could reduce the number of people exposed to the disease, particularly remote medical workers and high-risk people with chronic diseases who would have acquired a diagnosis [88].

Thanks to advanced AI algorithms, humans can now benefit from new capabilities like autonomous driving and the automated detection of dangerous situations. Deep learning (DL), a very sophisticated technology that could replace conventional algorithms to enhance visual object detection and recognition, is one such AI-based approach. Numerous recent works have examined DL models' complex intricacies [89]. This research focuses on incorporating DL methods for object recognition and image processing in autonomous detection and monitoring systems installed at railway crossings (physical intersections between rail and road traffic) employing arrays of sensors. Currently, many railroad crossings use typical security measures, including sensors, cameras, road signs, traffic signals, and physical barriers, to prevent unsafe and risky circumstances brought on by people accessing the railway crossing area when an approaching train is crossing [90]. All of these are directly or indirectly coming in benefit of military surveillance, for example, tracking enemy footprints, learning their potential next step and taking decisions accordingly, establishing a distinction between civilians and military for better decision making, finding the right direction, statistical benefit, and many others. However, these benefits depend a lot on the data collection and the algorithm used for the surveillance method.

Numerous studies and research papers discuss how modern telecommunication surveillance technology can increase safety at railroad crossings. For example, to warn drivers using a human-machine interface (HMI), Singh, through his thoughts and theories, proposed a cooperative ITS system for railroad crossings that are based on already-existing technologies such as the global positioning system (GPS) and the dedicated short range communication (DSRC) [90]. Zang demonstrates the recognition of a vehicle's license plate using deep learning and a visual attention model. Kim studies deep convolutional neural network (DCNN) applications for recognizing license plates, while DCNN applications for car logo recognition systems are studied by Soon (Figure 13). Numerous studies have examined various methods for detecting obstacles using deep learning and image processing [90].

Due to the rigidity of these processes, networks can be maintained statically with significant constraints. Networks used for military surveillance and other purposes administered statically by static scripts or commands are less effective and have less automatic resource provisioning. Applying software-defined networking has been suggested to improve network management in any type of military aspect, most recently in a good number of researches (SDN). Among these, the RFC 7149 and the IETF describe SDN as a collection of methods for facilitating network services' deterministic, dynamic, and scalable design, provision, and operation [92]. The use of these technologies definitely will create a differential between two military parties on the battlefield. They implement many rules about the traffic flows that pass through the network through the SDN controller, enabling the building of adaptive networks. SDN generally allows users to operate networks more effectively and affordably [92].

Data association and target state estimate are the two main components of a typical target-tracking application for surveillance. Thus, measurement-to-measurement connection, measurement-to-track association, track evaluation, and multiple hypothesis tracking are additional divisions of data association (MHT). Each of these components and subcomponents has the potential to be entirely or partially carried out by AI in the military sector [86].

3.3. 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 [56]. Also, this prospect is not only for businesses and industries; it has developed and enhanced in the defense sector far more.

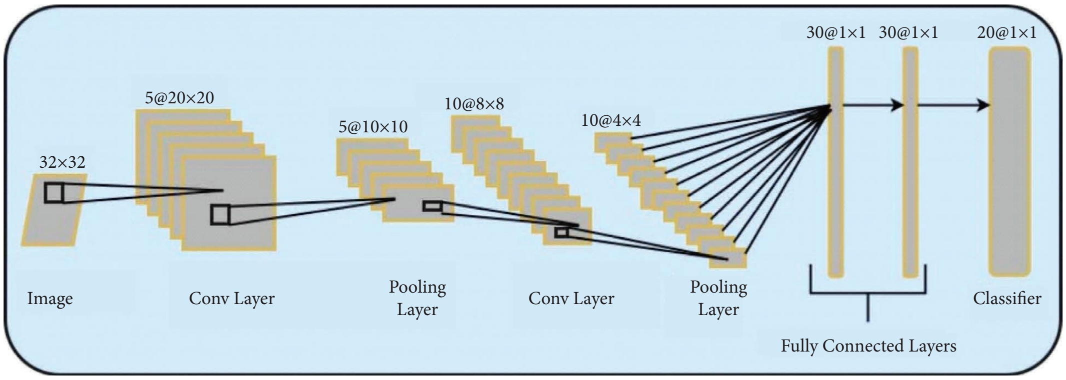


FIGURE 13: Basic convolutional network architecture [91].

Frank Rosenbelt's groundbreaking use of neural networks for pattern recognition is renowned for its efficiency. It can quickly pick up new information from military data, tackle challenging problems, and defend against a constrained number of cyberattacks from the enemy. To detect and prevent any intrusion, neural nets support software and hardware installation [82].

Figure 14 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 [84]. Here, these classes were defined and provided with references to several cyber security applications (Table 3), which are now on the way to enhancement in the military sector.

The potential for AI in cyber security is enormous and vast. By influencing people's behavior, social engineering uses people to gain access to a system. As a result, a security environment's weakest link is the human mind, which an attacker can easily exploit. Different military nations use artificial intelligence to enhance the security and effectiveness of their systems to prevent this. The third world war is considered a cyberattack, not any on-field war. This shows how important for every nation to improve its cyber security with the help of AI.

System security of any military of any country can be increased by utilizing expert systems, neural networks, and other methods. A good AI system can predict the nature of upcoming attacks and prevent them using the attack records from previous assaults. It might be feasible to reach a degree of security in the future, making hacking very challenging [85].

3.4. Homeland Security. Although several civilian agencies are generally in charge of reacting to domestic catastrophes such as terrorist attacks, the U.S. Army has always played a part in bridging gaps in civilian capability. Every other nation follows the same system. To enhance this option, AI is coming in help at a great length. Hundreds of countries prefer AI-assisted software to zone out the areas that require military support the most. Data collection and data analysis with the help of suitable software play an important role in this case. Three important national security goals can be defeated in six crucial homeland security mission areas by implying the national defense sector using AI [88].

Leaders in homeland security and the national armed forces of all nations will have endless chances with the help of AI to support their communities better and run their organizations. Some of the major strategic rivals worldwide have made considerable expenditures in AI for their countries' security. Similarly, the Department of Defense (DOD) is spending billions on creating and incorporating AI into defensive systems for military capability enhancement. The kinds of artificial intelligence (AI) that the DOD employs range from automating straightforward business processes (such as processing financial data) and foreseeing mechanical problems in weapon systems to carrying out intricate analyses to support its mission of waging wars. Many nations' DOD's warfighting mission depends on several AI capabilities still under development. Examples include improving military systems (like drones and robotic ships), assessing intelligence data (like facial recognition), or making suggestions on the battlefield (such as where to target missile strikes) [86].

The human face and gait are the major and dominating biometric traits that can be exploited in visual surveillance systems in the modern homeland security industry. Through motion detection, tracking, and behavior comprehension, a single-camera visual surveillance system is sufficient for recognizing and identifying people. However, AI-based numerous cameras are more advantageous when considering homeland security.

The majority of segmentation techniques in homeland security involve either spatial or temporal information during the picture processing; the most widely used techniques are [87] as follows:

(1) Temporal differencing
(2) Background subtraction
(3) Optical flow

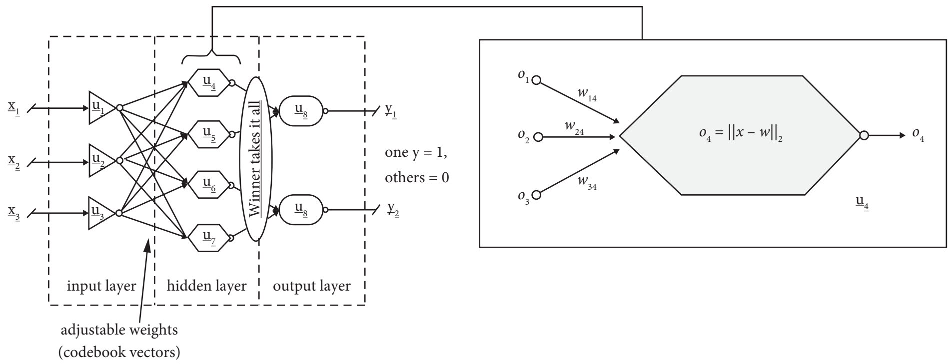


Figure 14: An LVQ neural network to detect DDoS [83].

The IT and TST (transducer science and technology) research testing is an essential and advisable component of the contemporary workplace and might be an integrated solution to handle related issues in these fields.

(1) Domestic Counterterrorism: information technology (IT) specialists can improve information access, interchange, and municipal, state, and federal law enforcement officers' capacity for crime analysis.
(2) Intelligence and Warning: IT specialists can help create new information-gathering, intelligence-gathering, and analysis capabilities to spot terrorist attacks in the future.
(3) Critical Infrastructure and Key Assets: the creation of analytical, modeling, and simulation tools for critical infrastructure (such as transportation systems), cyberspace vulnerability and risk assessments, and protection can be aided by TST and IT researchers.
(4) Border and Transportation Security: researchers in IT and TST can help create "smart borders" by developing identity management and deception detection techniques. TST and IT researchers can also contribute to enhancing the security of international shipping and developing effective and efficient strategic and operational models for infrastructure protection related to transportation.
(5) Defending against Catastrophic Threats: IT researchers can assist in developing simulation, detection, and alerting procedures for potential catastrophic threats, such as chemical and biological assaults. By focusing on the transportation needs for carrying out such attacks, TST researchers can contribute to these efforts.
(6) Emergency Preparedness and Response: IT researchers can help first responders by enhancing information sharing and communication interoperability before and after disasters. TST researchers can contribute by creating tools to aid in logistical decision-making that will increase the effectiveness of response operations [88].

With the use of AI that was developed based on the IT and TST studies, 224 internal terrorist organizations in the US, as well as 440 foreign terrorist organizations, were found, which represents a significant advance and impact of AI in this sector. This tech made a differential for the armed forces in catching terrorists worldwide. Recently, homeland security issues have been brought up in international research on antiterrorist and anticrime technologies. The tools and methods developed by IT and TST for AI-built security include data integration, data analysis, text mining, image and video processing, and evidence combining, to name just a few. However, issues still need to be addressed about their suitable application in the intelligence and security domains with the aid of the initial data and their efficient application in national security mission domains [89].

Numerous artificial intelligence subdisciplines must be thoroughly researched and improved to convert raw homeland security data into actionable intelligence. These subdisciplines include data mining, text mining, web mining, natural language processing, planning, reasoning, dispute resolution, link analysis, and search algorithms.

3.5. Military Transportation and Logistics. Military aircraft use AI systems like HITL systems (Figure 15), which can produce the best possible decision-making results. These particular AI designs are made only for better output on the battlefront, which cannot be accumulated in other ways. Their operations and functions are different and use big data for fast result output. These AI-augmented techs help in the military by enabling the process of numerous and various types of unmanned aerial systems (UAVs) and other intelligence, surveillance, and reconnaissance (ISR) platforms (Figure 16) of the twenty-first century [4]. As mentioned, even the modern military of different nations sets the most effective routes for drivers by AI-assisted vehicles.

Virtual reality and air combat simulations are the most popular training programs for new military recruits. The Marine Corps allocated roughly $7.1 million for unmanned warning systems that can provide commanders with a greater perspective on the battlefield, while the US Air Force invested over $87 on developing AI wargames [4].

Table 3: Application of cyber security [82].

Inventors	Proposal	Functions
Harini and Dharani	A system that makes use of expert systems, intelligent agents, and neural networks	Based on the information and knowledge they have been given, they work on two sections and an interference-using engine. This method can identify any harmful code that might lead to the installation of malware on the user's PC. Intelligent agents use actuators and sensors to provide defense against any DDoS assault
Shwapnil Ramesh Kumar	A system that applies data mining approaches to image processing, pattern identification, and fuzzy systems	Phishing and fraudulent auctioning can be stopped through data mining. Image processing is mostly used when any form of malware invasion occurs, and pattern matching uses fingerprint, voice, and facial recognition as a security
Enn Tygu	A system that makes use of neural network-based software applications and cyber protection approaches	The algorithm for solving constraint problems aids in resolving the constraints. Since the neural network is ineffective in all situations, an application can sometimes be used as a defense strategy
Arockia panimalar	A specific, one-of-a-kind system that employs technologies like export systems to provide the best performances	The solutions would provide the highest level of mobility and instantly identify DDoS attacks

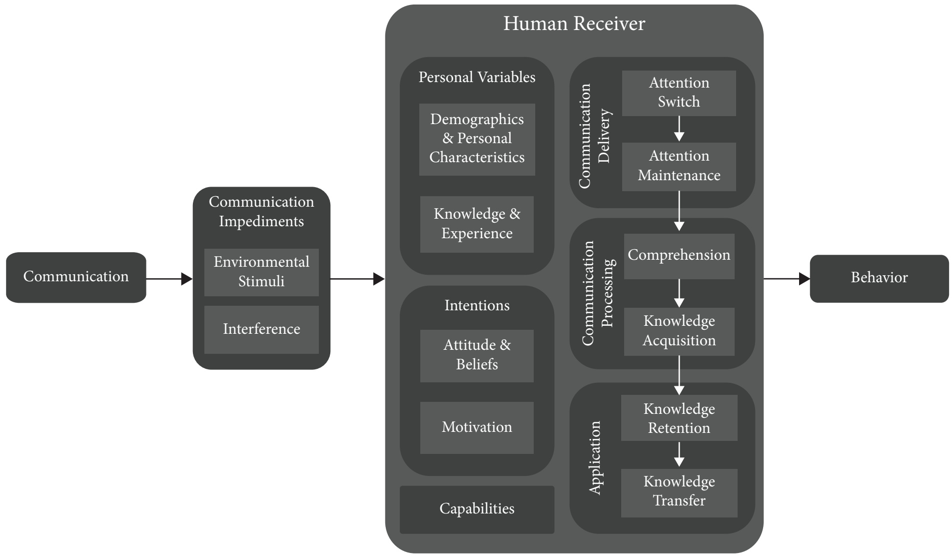


Figure 15: The HITL framework [90].

The use of AI neural networks in military applications and consequences holds immense promise and the potential to open up several doors in almost every industry, including logistics and transportation. The automatic identification system (AIS), which gives a wealth of data regarding sea traffic but necessitates a sizable volume of processed data, has recently gained significant military clout. Using fuzzy ARTMAP by AIS greatly aids the cause [92].

The water mines seriously endanger the movement and transportation of battleships. With the aid of unmanned airborne vehicles (UAV) and unmanned underwater vehicles (UUV), also known as autonomous underwater vehicles (AUV), which were created specifically for this purpose, this threat might almost be nullified and help in improved transportation for the marine personnel [93].

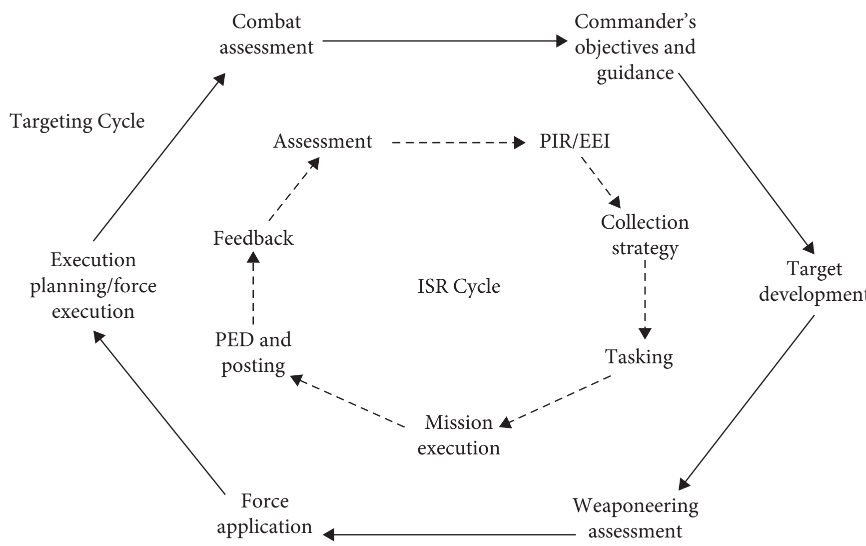
Any nation's navy can become more responsive, adaptable, mobile, and ultimately more lethal than ever with the help of AI alone. The quantity of people needed is a significant drawback to naval power. Without such, a team cannot beat its opponent even with the appropriate equipment. However, it appears that AI can be helpful in this field. AI systems are now used to support administration, quick information relay, planning, logistics, crisis response, force protection, force infrastructure, training, direction, and intelligence in movement. AI will consider all options and select the best one for each [6].

Most of the world's biggest cities struggle with logistics, traffic, and transportation issues. This is brought on by the rapidly growing human population and the rising number of vehicles on the road. The use of technology in the planning and administration of a sustainable transportation system could be very beneficial. Cities are battling traffic congestion. Therefore, artificial intelligence (AI) solutions that use a single user interface to receive real-time data from moving vehicles for traffic control and to take advantage of mobility on demand for trip planning have emerged. The secure integration of AI-based decision-making, traffic management, routing, transportation network services, and other mobility optimization tools are possibilities for efficient traffic management.

Some of the AI technologies that help transportation include Artificial Neural Networks (ANN), Genetic Algorithms (GA), Simulated Annealing (SA), Fuzzy Logic Model (FLM), and Ant Colony Optimizer (ACO). Implementing these tactics in transportation management aims in the military and other sectors worldwide to lessen congestion, increase the predictability of commuter travel times, and enhance the economics and productivity of the system as a whole [93].

3.6. Autonomous Vehicles. Autonomous vehicles, sometimes known as mobile robots, are being deployed in both the military and the private sector. Unmanned ground vehicles (UGV), unmanned spacecraft, unmanned aerial vehicles (UAV), and unmanned underwater vehicles are some of these (UUV). Most current systems are only partially autonomous and depend on frequent human interaction. Beyond this capability, sophisticated yet adaptable software systems will be needed [94]. Based on very simple, fundamental AI software technologies like Lockheed Martin provides an unmanned ground vehicle (UGV) for transporting big platoons' gear, guns, medical supplies, and rations. Likewise, there is also BAE system software in the US military which is still an improvement that transports more than one wounded soldier on an unmanned medivac vehicle.

The NN of Sales and Correa, which is utilized to perceive and quickly learn the surroundings and suggests unmanned machines for navigating AVs under urban road conditions, is one of the good uses of object detection and pattern recognition learning. Akemi has done similar work regarding the path planning of AVs using sliding mode control mode [95]. Autonomous vehicles (AVs) use AI techniques such as NN (RNN), LSTM, and RL for better path clearance in various situations. Although their ability to recognize objects has greatly improved in recent years, they now accomplish much more.



NOTE: PED = processing, exploitation, and dissemination.

Figure 16: The ISR cycle [91].

The Spot is another swift quadruped that can cross any surface and environment. The robot has cameras and sensors on the front, back, and sides, enabling SLAM (simultaneous localization and mapping) navigation. SLAM techniques are often employed for tasks like item localization, pedestrian recognition, and locating the UAV that calls for updating a map of an ambiguous region while keeping an eye on a moving object [95].

In some research and development, BMW used a personal computer and a real-time embedded computer (RTE PC) that combined sensor output data to better perceive the surroundings through pathway detection [96].

Since 2003, the 8-wheeled fighting vehicle known as the Stryker has been produced and used by the American military to bridge the capability gap between the Abrams and Bradley, which are heavily armored vehicles, and the High Mobility Multi-Purpose Wheeled Vehicles, which are lightly armored vehicles (HMMWV)- both of these are AI-augmented. The Stryker's engine, transmission, hydraulics, wheels, and tires are shared by various vehicle types, enabling reconfiguration to carry out various duties (mobile gun system, infantry carrier, mortar carrier). Germany, Lithuania, Australia, and the Netherlands have used the Boxer, a multi-purpose armored fighting vehicle, since 2011. Two essential components comprise the Boxer: the platform and the detachable mission module [97].

3.7. Combat Training and Simulation. One of the best instances of the addition of artificial intelligence to combat training and simulation is automated intelligent pilots for military use. The best AI-based aircraft are STOW "97" and Roadrunner "98", both stationed at Wissard Laboratory on the Ocean Naval Air Station in Virginia Beach [98]. These demonstrate and assess the relevant technology and ongoing network infrastructure testing.

An Office of Naval Research program, Virtual Training & Environments (VIRTE), creates immersive virtual trainers for military operations in urbanized terrain (MOUT). In this exercise, four-man fire squads of US Marines will be stationed in a simulated urban area and tasked with clearing a building that could house enemy soldiers. Virtual opponents are necessary to fill the environment and test the trainees.

A commercial computer game series called AI-augmented MOUTbot incorporates simulations now employed in military innovation. MOUTbot is a more practical and effective option for combat training than real-time initiation for countries with highly developed militaries. This technological procedure uses 25 operators across its 800 production rules and 25 key data structures [99].

The following abilities are necessary for MOUTbots to carry out their assigned missions:

(1) Situational awareness
(2) Sort the situation according to variables such as the enemy, health, medical attention, ammo, equipment, and amount of incoming fire
(3) Collecting and managing information about threats and ally units
(4) Identifying tactically important topology
(5) Mobility/movement
(6) Moving across the space, passing through doorways to get from one door to another (run and walk)
(7) Calculating the routes between different rooms and figuring out which rooms are visible
(8) Investigate structures and draw a map of the inside
(9) Management and handling of weapons
(10) Unjamming and reloading guns
(11) Adapt your weapon choice to the circumstances

(12) The performing ability for specific missions
(13) When instructed to do so by the supervisor or leader, change the mission
(14) Leave the mission
(15) Appropriate tactical and mission response
(16) Use a rifle, grenade, or rocks to attack
(17) Retrench, conceal, and emerge
(18) Protect a space
(19) Roam
(20) Keep an eye out for enemy entry
(21) Surrender
(22) Communication and coordination through realistic messages

The MOUTbots' (Figure 17) AI augmentation uses a data structure to retain situational awareness during execution in any environment. For instance, the threat data structure keeps a superior and secure knowledge of the enemy.

Game manuals and instructional scenarios are insufficient to teach new players how to play sophisticated games, such as highly realistic tactical simulations of contemporary battlefields. Adding postgame after-action reports is beneficial, but they infrequently offer guidance for the entire work and frequently concentrate on quantitative criticism rather than specifics about what the player did incorrectly and how to improve. A higher degree of engagement and a more in-depth qualitative analysis are provided by the intelligent teaching system (ITS) technology to aid players while playing. AI technology is applied by combining an ITS component with the tactical simulation armored task force (ATF), creating the virtual combat training center (V-CTC). In V-CTC, the Army's Fort Irwin combat training facility instructors, or observers/controllers, are mimicked. The ATF game has been modified to send an event stream over TCP-IP connections to the ITS component, which analyzes the events and takes the necessary action. The military environment, including the classroom, the battlefield, and embedded deployments, was the primary focus of V-development. CTCs, on the other hand, tutors (or nonplayer characters performing that role) in nonmilitary games may greatly enhance players' gaming experiences. Alternatively, these players might experience frustration while learning particularly challenging games or be unaware of the tactical alternatives and depth of strategy accessible in a well-designed game [100].

3.8. AI-Assisted Robots on the Battlefield. Protecting soldiers' health and lives on the battlefield is one of the main goals of modern technology. One strategy that is commonly brought up in this context is "bringing the machines onto the battlefield." Using bioinspired robots in military operations might quickly replace conventional weapons in the conflict. Robots can tolerate harsh temperatures, a lack of food and drink, and life-threatening weariness.

Boston dynamics, an American corporation, is the market leader in mobile robots. The robots can move around freely, find and avoid obstacles, follow a predetermined itinerary, and recognize and act upon cues from their surroundings. Two examples of bioinspired AI-assisted robots that can be employed on the battlefield are Spot (Figure 18) and Atlas (Figure 19) [92]. Figure 20 illustrates robotic systems for casualty extraction, evaluation, and evacuation. Figure 21 represents the unmanned ground vehicles (UGV) extraction platforms with chemical, biological, and explosive (CBE) detection systems based on Raman spectroscopy so that they have the operational ability to identify environmental toxins and provide force protection.

3.9. Healthcare on the Battlefield. Wearable technology with AI capabilities may now assess medical data from soldiers and help with difficult diagnoses. For real-time health monitoring of physiological and biomedical parameters, including body temperature, heart rate, EEG, and ECG, a body sensor network (BSN) made up of physiological and biomedical sensor nodes located close to or inside a human body can be employed [102, 103].

A soldier cannot identify an incoming missile as quickly as the helmet in the illustration. To alert soldiers to approaching bullets, bombs, or damaging waves, it is integrated with the sensors of other soldiers, battlefield IoT devices, and overhead assets. Consequently, these smart helmets and clothing can shield soldiers against traumatic brain injury (TBI) (Figure 22). Health experts can access a soldier's healthcare information to continually monitor and compare health status so that real-time responses can be applied as necessary thanks to the integration of smart helmet, smart uniforms, and smart eyewear sensors [104].

AI can be combined with robotic surgical systems (RSS) and robotic ground platforms (RGPs) to perform remote surgical support and rescue operations in war zones. Teleradiology consulting could be offered through an automated platform. The graphic shows how a radiologist from Spain used an ultrasound probe to help patients get abdomen and echocardiograms while they were in Afghanistan.

Two seven-degree-of-freedom arms, motion scaling (1 : 10), tremor filtering, and haptic feedback are shown on a military surgery robot in Figure (a). End-effectors for the robot are easily replaceable and can even be equipped with a laser tissue welding tool. The robot only has solid-state memory drives because the controller was designed to function in various climates. Software for the M7 (Figure 23) has recently been adjusted to meet teleoperation needs [101] better.

A mini-robot was created by Rentschler et al. and placed within the abdominal cavity. The wireless concept was further refined in the model, and a robot is positioned utilizing a platform resembling a single-incision laparoscopic port. Similar to the flexible-tip laparoscopes on the robotic arms of the da Vinci model, the robot's surgical arms have a wide range of motion (Figure 24(a)). Once the port is deployed locally, as depicted in (Figure 24(b)), the scope and arms can be controlled wirelessly from anywhere in the world [107, 108].

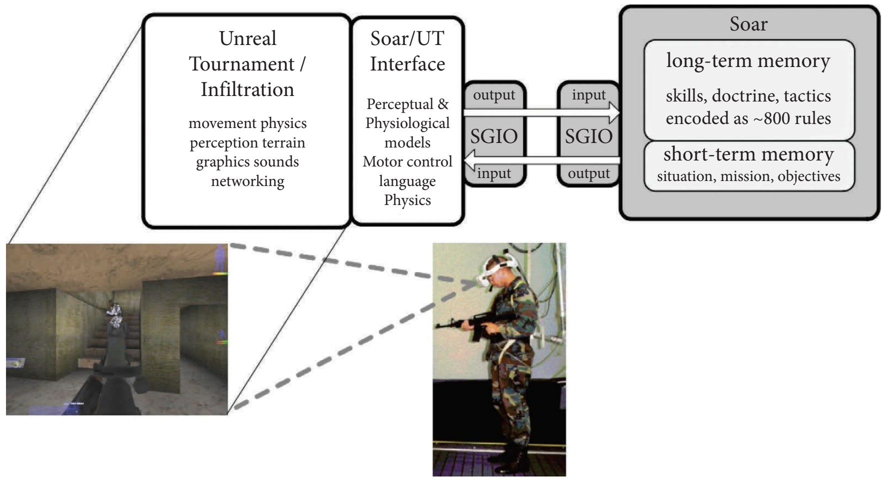


Figure 17: The MOUTBot system architecture [99].

(a) (b)

Figure 18: Spot: (a) overall look and (b) climbing stairs [92].

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

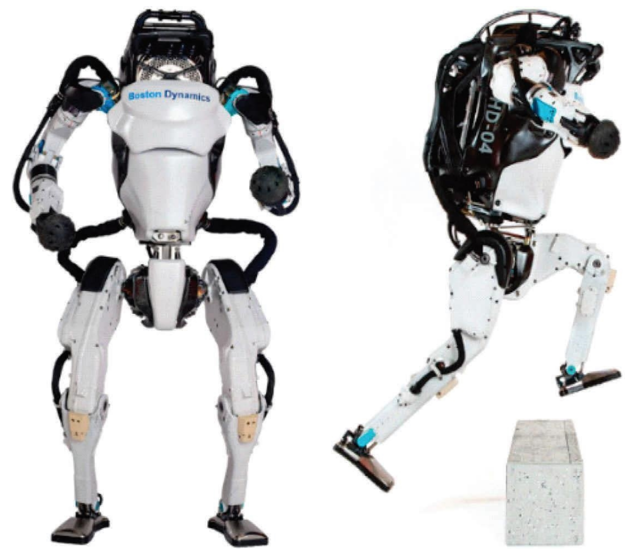
Artificial intelligence (AI) is the trending buzz that makes it simple to exaggerate the benefits and minimize the risks associated with its development and application in the military. Strategic stability may be compromised by the mixing and entwining of nuclear and nonnuclear capabilities and the escalating tempo of war. The things offered to the world by the new technologies predict and indicate that the likelihood of military escalation, particularly unintentional and unintended escalation, will increase technological advancement in AI-assisted typical possible capabilities. Military artificial intelligence's capacity to raise those hazards is not highlighted, even though the concerns of inadvertent escalation posed by developments in military technology were cited in the previous literature [109].

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. Certain AI-based weaponry and recently developed technologies are so effective and cutting-edge that they may be able to neutralize their effects. The absence of many weapons that threaten stability is a good thing. Loitering attack munitions (LAM), sometimes known as suicide drones, are weapons that engage targets without human interaction. Using preprogrammed sensors to sense the object and launch an attack, they pursue objects such as ships, tanks, and enemy radar. LAMs are more dangerous and lethal than cruise missiles since they are AI-augmented, allowing them to fire down any projectiles faster than human operators and stay in the air longer [110]. Their trait may impact strategic stability and make warfare less reliable (Figure 25).

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

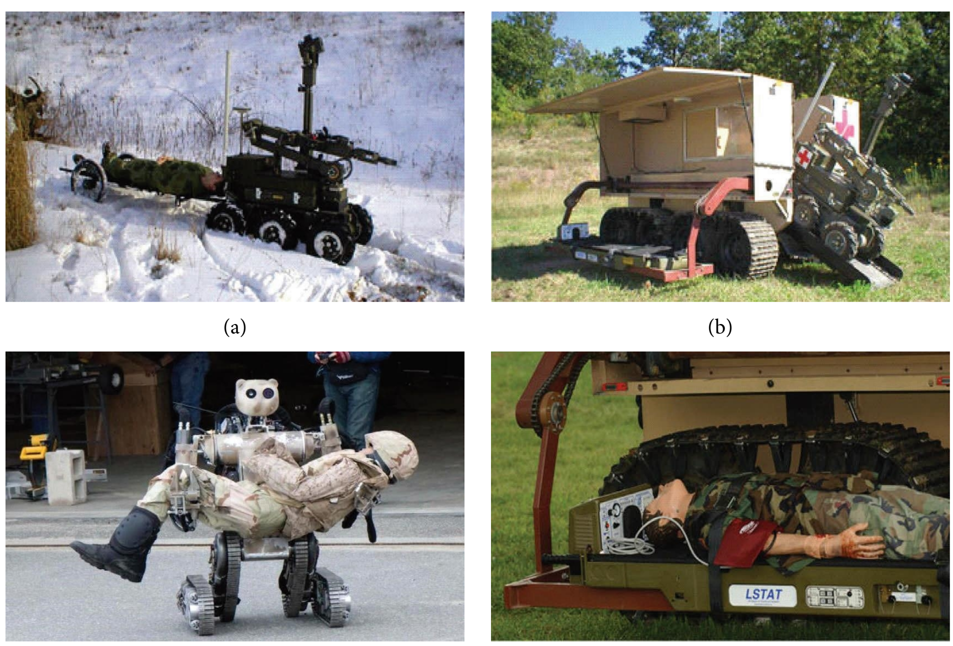
(1) Program bias introduction to the decision-making process
(2) Lack of traceability in AI implementation
(3) Black box algorithms and lack of transparency
(4) Data gathering & sourcing and privacy infractions or violations of personal data
(5) Uncertain legal liability or identification of authority

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



(a) (b)

Figure 19: Atlas: (a) overall look and (b) jumping over an obstacle [92].



(a) (b) (c) (d)

Figure 20: (a) Robotic extraction (REX), (b) robotic evacuation vehicle (REV), (c) battlefield extraction assist robot (BEAR), and (d) life support for trauma and transport (L-STAT) integrated with REV [101].

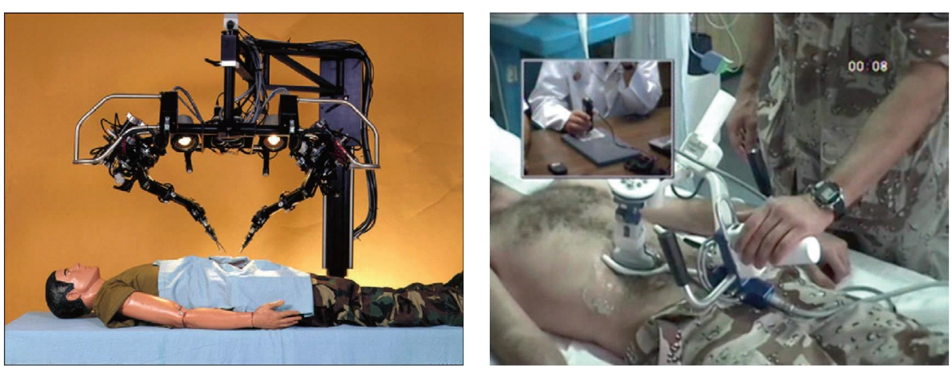
intelligence, whether the advantages exceed the drawbacks, and how they affect nuclear risk and global stability.

AI-augmented conventional capabilities may impact the strategic stability between major military powers. The complex, varied interactions between this new technology and various sophisticated conventional weapons could jeopardize nuclear capabilities, multiplying their potential disruptive impacts. Even in heavily fortified areas like China's east and coast, in a swarming sortie, hundreds of AI and ML-powered autonomous drones might well be able to avoid and outnumber an adversary's highly developed defenses [112]. On the contrary, a US F-35 stealth fighter would not be seriously threatened by a relatively inexpensive and solitary unmanned aerial vehicle (UAV). These tiny electromagnetic jammers and cyberweapons can interfere with communication networks and the adversary's targeting sensors, eroding the defenses of the adversary's multitiered air system in readiness for long-range stealth bomber offensive attacks and drone swarms. For instance, in 2011, in

(a) (b)

Figure 21: Robotic Raman spectroscopy chem/bio/explosive detector: (a) ARES robot and (b) Talon robot [101].

Figure 22: Traumatic brain injury (TBI) helmet concussion sensors [104].



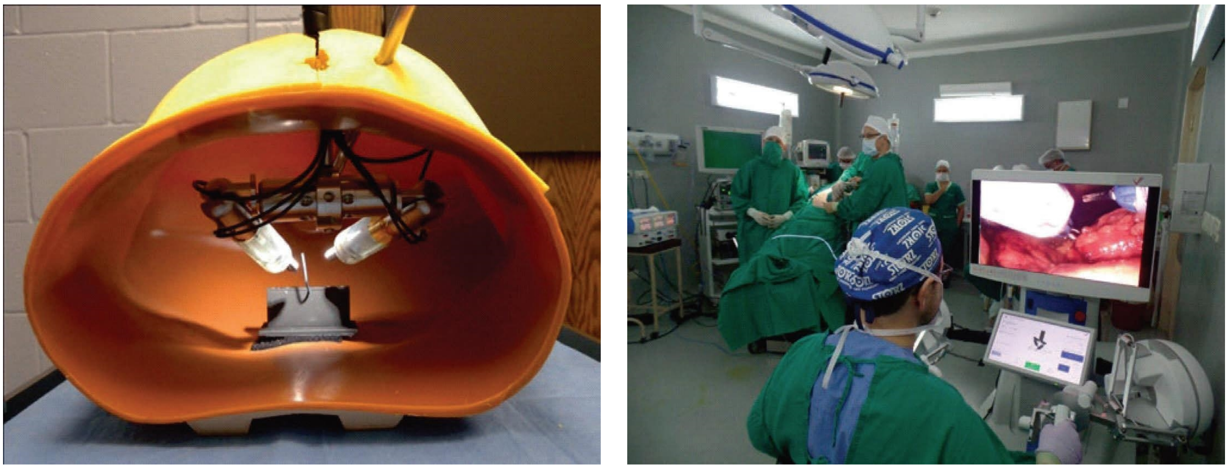
(a) (b)

Figure 23: (a) The M7 lightweight surgical robot for military and space applications [105] and (b) teleradiology consultation using a robotic platform [106].

the Middle East, compromised MQ-1 (Figure 26(a)) and MQ-9 (Figure 26(b)) drones exposed the susceptibility of US subsets of systems to offensive cyberattacks. To prevent (or decrease) this threat, future generations of AI technology may be included in stealth aircraft like the F-35. Artificial intelligence will soon be able to control small drone swarms that conduct sensing, reconnaissance, and targeting missions close to manned F-35 aircraft, coupled with defenses against swarm attacks. In the future, UAV and support platform endurance improvements may enhance drone swarms' resistance to such countermeasures [110].

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.

4.1. 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



(a) (b)

Figure 24: (a) Robot platform is inserted into the abdomen and (b) the console surgeon conducts the operation at a remote location via wireless connectivity [106].

Figure 25: Three examples of standard launch methods for loitering munitions [111].

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.

The families of several notable US leaders were subsequently seen rapidly leaving Washington, DC, in doctored recordings that surfaced on American and Chinese media outlets. Other eyewitness reports over social networks said that the missile bases had been on high alert in the western US and that their two-person operators had already unlocked the entrances to the silos' AI nuclear command and control systems. Due to such and several other signs employed by Russian artificial intelligence-based spatial awareness programs, Moscow's tactical monitoring systems told the Russian authorities that an American airstrike was likely to occur. The President of China warned the US not to launch a nuclear attack against any nation in the initial situation report produced by the control team. He also stated that if the US did not offer convincing proof that it was not preparing for war, China would be forced to take uncertain countermeasures, which is quite really a shocking example of the impact and influence of artificial intelligence on worldwide strategic stability.

The case presented a plausible illustration of third parties escalating a situation. A nonstate entity created a convincing enough deep fake to precipitate a nuclear crisis involving two nations. According to a background study, the psychological distance between the adversary and its victim can be increased to a great extent because of the aggressive AI capabilities [114].

4.2. Distorted Early Warning Assessments. Deep fakes perpetrated by foreign entities could have been amplified by artificial intelligence tools that are misused to produce false positives. In this case, just three months before the emergency, the United States Cyber Authority's "Unified Platform," which oversees and coordinates integrated information, electronic as well as cyber warfare functions, was producing statistically unusual results concerning spatial awareness evaluations about the advanced indication of chosen persistent advanced threat sets of data connected to Russian cyber actors. 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

(a)

(b)

Figure 26: (a) MQ-1 predator and (b) MQ-9 reaper [113].

tactical alert would be biased in the same way, which concerned them very much. This could have led to a direct nuclear war between two militarily strong countries and led to global warfare [115].

Attacks using data poison the ability of an AI system to discern between good and bad data can be weakened by adding distorted inputs to the training samples for such an artificial intelligence ML procedure. Content creation, feedback weaponization, man-in-the-middle, and disturbance-injecting attacks are the most common methods for these operations.

4.3. Through False-Positive Safety Alerts. Few years ago, the AI-driven management software at four commercial nuclear power reactors in heavily populous Chinese regions started reporting falsified safety alarms. In each instance, sensors detected structural issues within the plant, prompting management bodies to implement emergency protocols that halted operations even though engineering examinations indicated neither structure damage nor human injury. However, frequent interruptions regarding electricity generation through these significant power stations were hurting the economy.

In response, the operating authorities asked GaiaForce, an AI software vendor, to modify the detecting functions so that further structural stability degradation was needed before the automated breakdown measures were initiated. This made every affected power station possible to run at or close to complete capacity. GaiaForce could not locate any functional issues with the code. During the initial rounds, it was not obvious whether the false positives were due to malicious activity [114].

4.4. Malfunctioning Navigational Systems. A slight change in how the game was played could have led to a significant power struggle caused by various faulty sensors. In the case of a fictional build-up with a scenario of crisis, a destroyer of the United States Navy engaged in an exercise called freedom-of-navigation in South China Sea territorial waters claimed by China came dangerously close to bumping with another vessel of the PLA Navy due to serious problems with its automated navigational systems. It was unknown where the antagonistic inputs had come from, although they might have been implanted into the vessel's artificial intelligence system. Malware classification for PDFs, spam filtration, distributed DoS threat detection, and worm signature creation are few examples of system classifiers that can be bypassed in an attack on cyber security.

These inputs can potentially lead an artificial intelligence system towards an incorrect picture classification by slightly changing the pixels or patterns of the image—changes that may be invisible to human sight and lead to unfortunate circumstances [114].

4.5. Hijacking the Private-Sector Technology. One of the most eye-opening flaws the exercise showed was the potential for another nonstate actor to steal private-sector technology advancements for malicious purposes, with disastrous repercussions for strategic stability. The Defense Advanced Research Projects Agency awarded contracts to the US technology company QuantumAI for its cutting-edge magnetometers and gravimeters. The two companies collaborated to launch quantum-sensing satellites in four open sources that used AI to measure minute variations in the Earth's magnetic and gravitational fields. Subscribers started using the new technology to locate hazardous metallic effluents from industrial sites, sunken ships, and new mining prospects. The Wassenaar Arrangement and the US International Traffic in Arms Regulations placed export controls on QuantumAI's technology, which is only traded to the NATO nations that are government-approved researchers.

In round one, reportedly from sources connected to QuantumAI, satellite images of the South China Sea were posted online, rendering the water transparent and revealing the whereabouts of three Chinese submarines. The US team was concerned that whoever posted this information online may also divulge the position of US submarines, while the Chinese team believed that the US government was to blame. That is what happened in round two. The same website that provided geographic information about Chinese submarines now has a global map with extra markers for nuclear submarines from the US and Russia. Undermining the second-strike potential offered by stealthy nuclear-armed submarines represented a risk to strategic stability [114].

There are many other ways that AI could breach global stability, especially between the powerful nations in the military, and result in severe nuclear risks. A new generation of AI-augmented advanced conventional capabilities will exacerbate the risk of accidental escalation caused by the blending of nuclear and strategic nonnuclear weapons (or conventional counterforce weapons) and the escalating speed of warfare, undermining strategic stability, and increasing the likelihood of nuclear conflict. Because no one fully controls and understands AI, it cannot be trusted fully (possibly never).

In a competitive and contested multipolar nuclear environment like now, which is likely to amplify the potentially destabilizing influence of AI, there will undoubtedly be a greater risk of major military forces unintentionally escalating their conflict to a nuclear level. Therefore, in the current multipolar geopolitical order, asymmetric alternatives to undercut the deterrence and resolve of a sophisticated military will appeal to more people. These choices include the absence of a robust normative and legal framework, uncertain rules of engagement, and relatively low-risk and inexpensive AI-augmented AWS capabilities. AI-augmented conventional weapon systems may make it more difficult to control the level of escalation during future crises or conflicts by obstructing efficient and dependable information, and communication flows between enemies and allies as well as inside military organizations.

4.6. 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. The paper has already discussed how AI could be used for worldwide instability and can bring so much chaos in the same field of military capabilities, which has been helping the globe to develop for a long time. AI in the military can be a double-edged sword if not implied following global ethics (Table 2 is one of the examples) and not observed frequently with the right moderators and evaluators. A slight misguidance and negligence can lead any nation's military to the verge of collapse resulting in global instability or an alarming scenario that no one expected. 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) Ethical concerns: The use of AI in the military raises several ethical concerns, including the potential for autonomous weapons systems to make life-or-death decisions without human oversight. There is a need to ensure that the use of AI in military applications aligns with ethical standards and principles.

(2) Reliability: One of the main challenges of using AI in military applications is ensuring its reliability. The accuracy of AI models heavily depends on the quality and quantity of data used for training, and there is always a risk of errors and bias in the data. Any inaccuracies in the output of an AI system could have severe consequences, particularly in military operations.

(3) 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.

(4) 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.

(5) 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.

(6) 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.

(7) 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.

Last but not least, the rectitude of AI augmentation and processing systems are particularly susceptible to deception, even though it is a persistent intelligence and strategic issue that predates the cyber age. Reliance on AI coupled with malicious actors' exploitation of technology could significantly exacerbate the disruptive consequences of disinformation operations. Establishing legislative frameworks that determine how new technology interacts with the current arsenal of disinformation tools, such as social media, should be a crucial responsibility of governments. Time constraints prevented a more thorough investigation of an AI system's vulnerability, but the tabletop exercise was riddled with indications and suspicions of AI-related espionage. They will probably endure in the real world as well. These AI-related facts must be considered since they threaten world peace and stability [116, 117].

5. Conclusions

This paper aims to represent the main sectors of utilization and the possibility of using AI augmentations and AI algorithms in the military sector, especially in cybersecurity, object detection, robotics, and logistics. Overall, the seven patterns of AI are paving their way in military capabilities enhancement. The discussion of their impact on people's sense of security is also portrayed. One of the key technological advancements of the future is that AI has the best possibility to significantly impact the transformation and advancement of contemporary society along with military capability. An exciting new phase of rapid development has begun for AI technology. It is now acknowledged as having the most potential to alter the disruptive technology landscape in the future. Also, using them to improve national strategies and assets like applications in the military has become very common. However, we must be cautious about how we use it and what the circumstances will be short. Progression is our expectation and reason for our build-ups with the help of AI; if it has a bad impact on the next generation, it is better to stop those specific innovations.

The AI component in military decision-making provides a robust backbone capable of generating intuitive sketch-based user interfaces that specialists may utilize with little training. Users requested an integrated framework that simultaneously records CoA sketches and statements and offers a single map-based user experience for both operations. The goal is to provide a framework that can express the sketches of CoA with visual comprehension.

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

In terms of everything, if AI is not implemented correctly with the help of the right hand in the military sector, it will likely become a double-edged sword that could cut both ends and destroy a nation instead of doing good. Nevertheless, a more detailed requirements analysis is required to comprehend the utilization. Regarding risk, data quality, and regulatory constraints, military needs may differ significantly, and some forms of openness may not even be applicable. 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.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Das, A. Dey, A. Pal, and N. Roy, "Applications of artificial intelligence in machine learning: review and prospect," *International Journal of Computer Application*, vol. 115, no. 9, pp. 31–41, 2015.
[2] M. L. Cummings, *Artificial Intelligence and the Future of Warfare*, Institute of International Affairs London, London, UK, 2017.
[3] P. Sharma, K. K. Sarma, and N. E. Mastorakis, "Artificial intelligence aided electronic warfare systems- recent trends and evolving applications," *IEEE Access*, vol. 8, pp. 224761–224780, 2020.
[4] C. H. Heller, "The future navy—near-term applications of artificial intelligence," *Naval War College Review*, vol. 72, 2019.
[5] Y. Zhang, Z. Dai, L. Zhang, Z. Wang, L. Chen, and Y. Zhou, "Application of artificial intelligence in military: from projects view," in *Proceedings of the 2020 6th International Conference On Big Data And Information Analytics (BigDIA)*, Shenzhen, China, December 2020.
[6] C. H. Heller, "Near-term applications of artificial intelligence," *Naval War College Review*, vol. 72, 2022.
[7] R. Arkin, *Governing Lethal Behavior in Autonomous Robots*, CRC Press, Boca Raton, FL, USA, 2009.
[8] P. Scharre, *Army of None: Autonomous Weapons and the Future of War*, WW Norton & Company, New York, NY, USA, 2018.
[9] V. R. Vaidya, M. Lyle, W. R. Miranda et al., "Long-term survival of patients with left ventricular noncompaction," *Journal of the American Heart Association*, vol. 10, no. 2, Article ID e015563, 2021.
[10] O. Gillath, A. Ting, M. S. Branicky, S. Keshmiri, R. B. Davison, and S. Ryan, "Attachment and trust in artificial intelligence," *Computers in Human Behavior*, vol. 115, 2021.
[11] P. Pradhan and A. Satapathy, "Physico-mechanical characterization and thermal property evaluation of polyester composites filled with walnut shell powder," *Polymers and Polymer Composites*, vol. 30, 2019.
[12] D. Lee and S. Yeo, "Developing an AI-based chatbot for practicing responsive teaching in mathematics," *Computers & Education*, vol. 191, 2018.
[13] J. Hu, J. Emile-Geay, J. Nusbaumer, and D. Noone, "Impact of convective activity on precipitation δ18O in isotope-enabled general circulation models," *Journal of Geophysical Research: Atmospheres*, vol. 123, no. 23, pp. 13595–13610, 2018.
[14] J. Dalzochio, R. Kunst, J. L. V. Barbosa et al., "Predictive maintenance in the military domain: a systematic review of the literature," *ACM Computing Surveys*, vol. 55, 135 pages, 2023.
[15] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial

networks: an overview," *IEEE Signal Processing Magazine*, vol. 35, no. 1, pp. 53–65, 2018.
[16] R. Sharma, A. Kumar, and C. Chuah, "Turning the blackbox into a glassbox: an explainable machine learning approach for understanding hospitality customer," *International Journal of Information Management Data Insights*, vol. 1, no. 2, Article ID 100050, 2021.
[17] A. S. Wicaksono and A. Afif, "Hyper parameter optimization using genetic algorithm on machine learning methods for online news popularity prediction," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 12, 2018.
[18] K. Feng, H. Han, K. Tang, and J. Wang, "Statistical tests for replacing human decision makers with algorithms," arXiv.2306.11689, 2019.
[19] S. Dai, A. Bechtel, C. Eble et al., "Recognition of peat depositional environments in coal: a review," *International Journal of Coal Geology*, vol. 219, 2020.
[20] C. J. Chiu, J. C. Hu, Y. H. Lo, and E. Y. Chang, "Health promotion and disease prevention interventions for the elderly: a scoping review from 2015–2019," *International Journal of Environmental Research and Public Health*, vol. 17, no. 15, p. 5335, 2020.
[21] H.-M. Chuang and D.-W. Cheng, "Conversational AI over military scenarios using intent detection and response generation," *Applied Sciences*, vol. 12, no. 5, p. 2494, 2022.
[22] A. Brisson, G. Pereira, R. Prada et al., "Artificial intelligence and personalization opportunities for serious games," *Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment*, vol. 8, no. 5, pp. 51–57, 2021.
[23] P. Pataranutaporn, V. Danry, J. Leong et al., "AI-generated characters for supporting personalized learning and well-being," *Nature Machine Intelligence*, vol. 3, no. 12, pp. 1013–1022, 2021.
[24] J. M. Valdez Mendia and J. J. A. Flores-Cuautle, "Toward customer hyper-personalization experience—a data-driven approach," *Cogent Business & Management*, vol. 9, no. 1, Article ID 2041384, 2022.
[25] S. Barnes, "Understanding virtual reality in marketing: nature, implications and potential," *SSRN Electronic Journal*, vol. 52, 2016.
[26] L. Gao, Y. Chen, B. Zhang, and Y. Gao, "A real-time target detection and recognition system for UAVs based on improved YOLOv3 and ST-C3D," *IEEE Access*, vol. 7, pp. 35028–35036, 2019.
[27] K. Qian, C. Liu, B. Yang, and J. Wang, "Hyperpersonalized UAV intelligence based on machine learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, 2021.
[28] J. Sha, Y. Chen, Y. Gao, and X. Li, "Deep neural networks-based target detection and recognition for UAV," *IEEE Access*, vol. 9, pp. 92960–92968, 2021.
[29] L. Shamir, J. D. Delaney, N. Orlov, D. M. Eckley, and I. G. Goldberg, "Pattern recognition software and techniques for biological image analysis," *PLoS Computational Biology*, vol. 6, no. 11, Article ID e1000974, 2010.
[30] F. Valafar, "Pattern recognition techniques in microarray data analysis," *Annals of the New York Academy of Sciences*, vol. 980, no. 1, pp. 41–64, 2002.
[31] M. T. H. Chi, R. Glaser, and M. J. Farr, *The Nature of Expertise*, Psychology Press, London, UK, 2014.
[32] W. G. Chase and H. A. Simon, "The MIND'S eye in chess," in *Visual Information Processing*, pp. 215–281, Elsevier, Amsterdam, The Netherlands, 1973.
[33] A. D. Groot, "Perception and memory versus thought: some old ideas and recent findings," *Problem Solving*, vol. 30, pp. 19–50, 1966.
[34] D. E. Egan and B. J. Schwartz, "Chunking in recall of symbolic drawings," *Memory & Cognition*, vol. 7, no. 2, pp. 149–158, 1979.
[35] A. Lesgold, H. Rubinson, P. Feltovich, R. Glaser, D. Klopfer, and Y. Wang, "Expertise in a complex skill: diagnosing x-ray pictures," in *The Nature of Expertise*, pp. 311–342, Lawrence Erlbaum Associates, Inc, Mahwah, NY, USA, 1988.
[36] S. Hussain, O. Ameri Sianaki, and N. Ababneh, "A survey on conversational agents/chatbots classification and design techniques," in *Web, Artificial Intelligence and Network Applications*, L. Barolli, M. Takizawa, F. Xhafa, and T. Enokido, Eds., vol. 927,pp. 946–956, 2019.
[37] H. Shum, X. He, and D. Li, "From Eliza to XiaoIce: challenges and opportunities with social chatbots," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 1, pp. 10–26, 2018.
[38] V. L. Rubin, Y. Chen, and L. M. Thorimbert, "Artificially intelligent conversational agents in libraries," *Library Hi Technology*, vol. 28, no. 4, pp. 496–522, 2010.
[39] V. Sharma, M. Goyal, and D. Malik, "An intelligent behaviour shown by chatbot system," *International Journal of New Technology and Research*, vol. 3, no. 4, p. 3, 2017.
[40] L. C. Klopfenstein, S. Delpriori, S. Malatini, and A. Bogliolo, "The rise of bots: a survey of conversational interfaces, patterns, and paradigms," in *Proceedings of the 2017 Conference on Designing Interactive Systems*, pp. 555–565, Edinburgh, Scotland, June 2017.
[41] H. M. Chuang and D. W. Cheng, "Conversational AI over military scenarios using intent detection and response generation," *Applied Sciences*, vol. 12, no. 5, p. 2494, 2022.
[42] S. Zulaikha, H. Mohamed, M. Kurniawati, S. Rusgianto, and S. A. Rusmita, "Customer predictive analytics using artificial intelligence," *Singapore Economic Review*, vol. 12, 2020.
[43] F. T. Johnsen, Z. Zielinski, K. Wrona et al., "Application of IoT in military operations in a smart city," in *Proceedings of the 2018 International Conference On Military Communications And Information Systems (ICMCIS)*, Warsaw, Poland, May 2018.
[44] A. Akbar, A. Khan, F. Carrez, and K. Moessner, "Predictive analytics for complex IoT data streams," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1571–1582, 2017.
[45] G. Shmueli and O. R. Koppius, "Predictive analytics in information systems research," *MIS quarterly*, vol. 21, 2011.
[46] R. Saha, M. T. Tariq, and M. Hadi, "Deep learning approach for predictive analytics to support diversion during freeway incidents," *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2674, no. 6, pp. 480–492, 2020.
[47] K. L. Rich and M. S. Salter, "Bradley m2a3/m3a3 embedded training system (bets): initial user assessment: defense technical information center," *Army Research Inst for the Behavioral and Social Sciences Alexandria VA*, vol. 14, 2002.
[48] M. Paisner, M. T. Cox, M. Maynord, and D. Perlis, "Goal-driven autonomy for cognitive systems," *Proceedings of the Annual Meeting of the Cognitive Science Society*, vol. 36, 2014.
[49] P. Deadman and R. H. Gimblett, "A role for goal-oriented autonomous agents in modeling people-environment

interactions in forest recreation," *Mathematical and Computer Modelling*, vol. 20, no. 8, pp. 121–133, 1994.
[50] R. Darimont and A. van Lamsweerde, "Formal refinement patterns for goal-driven requirements elaboration," *ACM SIGSOFT Software Engineering Notes*, vol. 21, 1996.
[51] R. E. Stepp and R. S. Michalski, "Conceptual clustering of structured objects: a goal-oriented approach," *Artificial Intelligence*, vol. 28, no. 1, pp. 43–69, 1986.
[52] Y. Li, "Deep reinforcement learning: an overview," 2018, http://arxiv.org/abs/1701.07274.
[53] P. Bourgine, "Towards a Practice of Autonomous Systems," *Towards a practice of autonomous systems. Proceedings of the first european conference on artificial life*, vol. 7, 1992.
[54] T. Zhang, Q. Li, C. Zhang et al., "Current trends in the development of intelligent unmanned autonomous systems," *Frontiers of Information Technology & Electronic Engineering*, vol. 18, no. 1, pp. 68–85, 2017.
[55] D. Harel, A. Marron, and J. Sifakis, "Autonomics: in search of a foundation for next-generation autonomous systems," *Proceedings of the National Academy of Sciences*, vol. 117, no. 30, pp. 17491–17498, 2020.
[56] H. Abbass, J. Harvey, and K. Yaxley, "Lifelong testing of smart autonomous systems by shepherding a swarm of watchdog artificial intelligence agents," 2018, http://arxiv.org/abs/1812.08960.
[57] R. Haddal and N. Hayden, *Autonomous Systems Artificial Intelligence and Safeguards*, Sandia National Lab.(SNL-NM), Albuquerque, NM, USA, 2018.
[58] P. Arcaini, E. Riccobene, and P. Scandurra, "Modeling and analyzing MAPE-K feedback loops for self-adaptation," in *Proceedings of the IEEE/ACM 10th International Symposium On Software Engineering For Adaptive And Self-Managing Systems*, Florence, Italy, May 2015.
[59] M. Peshkin and J. E. Colgate, "Cobots," *Industrial Robot: International Journal*, vol. 26, no. 5, pp. 335–341, 1999.
[60] M. Du, F. Li, G. Zheng, and V. Srikumar, "DeepLog: anomaly detection and diagnosis from system logs through deep learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, November 2017.
[61] Y. Himeur, K. Ghanem, A. Alsalemi, F. Bensaali, and A. Amira, "Artificial intelligence based anomaly detection of energy consumption in buildings: a review, current trends and new perspectives," *Applied Energy*, vol. 287, Article ID 116601, 2021.
[62] L. Girish and S. K. N. Rao, "Anomaly detection in cloud environment using artificial intelligence techniques," *Computing*, vol. 20, 2021.
[63] P. V. de Campos Souza, A. J. Guimarães, T. S. Rezende, V. J. Silva Araujo, and V. S. Araujo, "Detection of anomalies in large-scale cyberattacks using fuzzy neural networks," *AIDS*, vol. 1, no. 1, pp. 92–116, 2020.
[64] A. Mishra and P. Yadav, "Anomaly-based ids to detect attack using various artificial intelligence & machine learning algorithms: a review," in *Proceedings of the 2nd International Conference On Data, Engineering And Applications (IDEA)*, pp. 1–7, Bhopal, India, February 2020.
[65] M. Taddeo, D. McNeish, A. Blanchard, and E. Edgar, "Ethical principles for artificial intelligence in national defence," *Philosophy & Technology*, vol. 34, no. 4, pp. 1707–1729, 2021.
[66] M. C. Horowitz, "When speed kills: lethal autonomous weapon systems, deterrence and stability," *Journal of Strategic Studies*, vol. 42, no. 6, pp. 764–788, 2019.
[67] M. Pestana, *Flying unmanned aircraft: a pilot's perspective*, Infotech@Aerospace 2011, St. Louis, MI, USA, 2011.
[68] D. J. K. Hawley, *Automation And The Patriot Air And Missile Defense System*, Center for a New American Security, Washington, DC, USA, 2017.
[69] M. R. Chaparro, *An Analysis Of Spending Patterns Associated With the PHALANX Close-In Weapon System (CIWS) Program*, Defense Technical Information Center, Fort Belvoir, VA, USA, 2003.
[70] R. Bogue, "Robot ethics and law: Part one: ethics," *Industrial Robot: International Journal*, vol. 41, no. 4, pp. 335–339, 2014.
[71] M. C. Haas and S.-C. Fischer, "The evolution of targeted killing practices: autonomous weapons, future conflict, and the international order," *Contemporary Security Policy*, vol. 38, no. 2, pp. 281–306, 2017.
[72] J. D. Flanagan and G. W. Luke, "Aegis: newest line of navy defense," *Johns Hopkins APL Technical DigestBhopal, India*, vol. 2, no. 4, p. 6, 1981.
[73] J. Haner and D. Garcia, "The artificial intelligence arms race: trends and world leaders in autonomous weapons development," *Global Policy*, vol. 10, no. 3, pp. 331–337, 2019.
[74] A. Gomez de Agreda, "Ethics of autonomous weapons systems and its applicability to any AI systems," *Telecommunications Policy*, vol. 44, no. 6, Article ID 101953, 2020.
[75] A. Wrabel, R. Graef, and T. Brosch, "A survey of artificial intelligence approaches for target surveillance with radar sensors," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 7, pp. 26–43, 2021.
[76] M. S. Hossain, G. Muhammad, and N. Guizani, "Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics," *IEEE Network*, vol. 34, no. 4, pp. 126–132, 2020.
[77] E. Alajrami, H. Tabash, Y. Singer, and M.-T. E. Astal, "On using ai-based human identification in improving surveillance system efficiency," in *Proceedings of the 2019 International Conference On Promising Electronic Technologies (ICPET)*, Gaza, Palestine, October 2019.
[78] M. T. Nguyen, L. H. Truong, T. T. Tran, and C.-F. Chien, "Artificial intelligence based data processing algorithm for video surveillance to empower industry 3.5," *Computers & Industrial Engineering*, vol. 148, Article ID 106671, 2020.
[79] P. Sikora, L. Malina, M. Kiac et al., "Artificial intelligence-based surveillance system for railway crossing traffic," *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15515–15526, 2021.
[80] N. Aloysius and M. Geetha, "A review on deep convolutional neural networks," in *Proceedings of the International Conference On Communication And Signal Processing (ICCSP)*, Chennai, India, April 2017.
[81] A. Rego, A. Canovas, J. M. Jimenez, and J. Lloret, "An intelligent system for video surveillance in IoT environments," *IEEE Access*, vol. 6, pp. 31580–31598, 2018.
[82] B. S. Sagar, S. Niranjan, N. Kashyap, and D. N. Sachin, "Providing cyber security using artificial intelligence– a survey," in *Proceedings of the 2019 3rd International Conference On Computing Methodologies And Communication (ICCMC)*, Erode, India, March 2019.
[83] J. Li, Y. Liu, and L. Gu, "Ddos attack detection based on neural network," *2010 2nd international symposium on aware computing*, vol. 4, 2010.
[84] D. P. Patil, *Artificial Intelligence in Cyber Security*, 2016.
[85] A. Anwar and S. I. Hassan, "Applying artificial intelligence techniques to prevent cyber assaults," *International Journal of Computational Intelligence Research*, vol. 8, 2017.

[86] M. C. Horowitz, G. C. Allen, E. Saravalle, A. Cho, K. Frederick, and P. Scharre, *Artificial Intelligence and International Security*, Center for a New American Security, Washington, DC, USA, 2018.

[87] T. Ko, “A survey on behavior analysis in video surveillance for homeland security applications,” in *Proceedings of the 2008 37th IEEE Applied Imagery Pattern Recognition Workshop*, Washington, DC, USA, October 2008.

[88] H. Chen and F. Y. Wang, “Guest editors’ introduction: artificial intelligence for homeland security,” *IEEE Intelligent Systems*, vol. 20, no. 5, pp. 12–16, 2005.

[89] H. Chen, F.-Y. Wang, and D. Zeng, “Intelligence and security informatics for homeland security: information, communication, and transportation,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, no. 4, pp. 329–341, 2004.

[90] L. F. Cranor, *A Framework For Reasoning About the Human in The Loop*, Carnegie Mellon University, Pittsburgh, PA, USA, 2008.

[91] C. Rhodes, J. Hagen, and M. Westergren, *A Strategies-To-Tasks Framework for Planning and Executing Intelligence, Surveillance, and Reconnaissance (ISR) Operations*, RAND, Santa Monica, CA, USA, 2007.

[92] M. Bistron and Z. Piotrowski, “Artificial intelligence applications in military systems and their influence on sense of security of citizens,” *Electronics*, vol. 10, no. 7, p. 871, 2021.

[93] L. S. Iyer, “AI enabled applications towards intelligent transportation,” *Transport Engineer*, vol. 5, Article ID 100083, 2021.

[94] L. N. Long, S. D. Hanford, O. Janrathitikarn, G. L. Sinsley, and J. A. Miller, “A review of intelligent systems software for autonomous vehicles,” *IEEE Symposium on Computational Intelligence in Security and Defense Applications*, vol. 54, pp. 69–76, 2007.

[95] Y. Ma, Z. Wang, H. Yang, and L. Yang, “Artificial intelligence applications in the development of autonomous vehicles: a survey,” *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 2, pp. 315–329, 2020.

[96] Z. Liu, H. Jiang, H. Tan, and F. Zhao, “An overview of the latest progress and core challenge of autonomous vehicle technologies,” *MATEC Web of Conferences*, vol. 308, Article ID 06002, 2020.

[97] X. Li and B. I. Epureanu, “AI-based competition of autonomous vehicle fleets with application to fleet modularity,” *European Journal of Operational Research*, vol. 287, no. 3, pp. 856–874, 2020.

[98] R. M. Jones, “Automated intelligent pilots for combat flight simulation,” *AI magazine*, vol. 16, 1999.

[99] R. E. Wray, J. E. Laird, A. Nuxoll, D. Stokes, and A. Kerfoot, “Synthetic adversaries for urban combat training,” *AI magazine*, vol. 16, 2004.

[100] W. R. Murray, “Intelligent tutoring systems for commercial games: the virtual combat training center tutor and simulation,” in *Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment*, Salt Lake City, Utah, October 2006.

[101] J. Rosen, B. Hannaford, and R. M. Satava, *Surgical Robotics*, Springer US, Berlin, Germany, 2011.

[102] A. Gondalia, D. Dixit, S. Parashar, V. Raghava, A. Sengupta, and V. R. Sarobin, “IoT-based healthcare monitoring system for war soldiers using machine learning,” *Procedia Computer Science*, vol. 133, pp. 1005–1013, 2018.

[103] H. B. Lim, D. Ma, B. Wang, Z. Kalbarczyk, R. K. Iyer, and K. L. Watkin, “A soldier health monitoring system for military applications,” in *Proceedings of the 2010 International Conference on Body Sensor Networks*, pp. 246–249, Singapore, June 2010.

[104] J. Farroha and B. Farroha, “Enabling intelligent battlefield healthcare through secure cyber medicine,” in *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2019*, R. Suresh, Ed., vol. 11015,p. 19, 2019.

[105] T. Haidegger and Z. Benyo, “Surgical robotic support for long duration space missions,” *Acta Astronautica*, vol. 63, no. 7–10, pp. 996–1005, 2008.

[106] R. B. Lim and D. Oleynikov, “Robotics in the military,” in *Robotic-Assisted Minimally Invasive Surgery*, S. Tsuda and O. Y. Kudsi, Eds., Springer International Publishing, pp. 323–327, Berlin, Germany, 2019.

[107] M. Reichenbach, T. Frederick, L. Cubrich et al., “Telesurgery with miniature robots to leverage surgical expertise in distributed expeditionary environments,” *Military Medicine*, vol. 182, no. 1, pp. 316–321, 2017.

[108] M. E. Rentschler, S. R. Platt, K. R. Berg, J. Dumpert, D. R. Oleynikov, and S. M. Farritor, “Miniature *in vivo* robots for remote and harsh environments,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 1, pp. 66–75, 2008.

[109] J. Cox and H. Williams, “The unavoidable technology: how artificial intelligence can strengthen nuclear stability,” *The Washington Quarterly*, vol. 44, no. 1, pp. 69–85, 2021.

[110] J. Johnson, “Artificial intelligence in nuclear warfare: a perfect storm of instability?” *The Washington Quarterly*, vol. 43, no. 2, pp. 197–211, 2020.

[111] M. Voskuijl, “Performance analysis and design of loitering munitions: a comprehensive technical survey of recent developments,” *Defence Technology*, vol. 18, no. 3, pp. 325–343, 2022.

[112] J. S. Johnson, “Artificial intelligence: a threat to strategic stability,” *Artificial Intelligence*, vol. 24, 2020.

[113] C. Don, G. Josh, and I. Chris, *Environmental Assessment for the MQ-1 Predator and MQ-9 Reaper Unmaned Aircraft System (UAS) Second Formal Training Unit (FTU-2) Beddown*, 2009.

[114] M. Fitzpatrick, “Artificial intelligence and nuclear command and control,” *Survival*, vol. 61, no. 3, pp. 81–92, 2019.

[115] L. M. Hough, N. K. Eaton, and M. D. Dunnette, “Criterion-related widities of personality constructs and the effect of response distortion on those widities,” *Journal of applied psychology*, vol. 75, 1990.

[116] A. Anastassov, “Artificial intelligence and its possible use in international nuclear security law,” *BAS Humanities and Social Sciences*, vol. 1, 2021.

[117] R. Legvold and C. F. Chyba, “Introduction: the search for strategic stability in a new nuclear era,” *Dædalus*, vol. 149, no. 2, pp. 6–16, 2020.