




Article

Evaluating the Role of Machine Learning in Defense Applications and Industry

Evaldo Jorge Alcántara Suárez ¹ and Victor Monzon Baeza ^{2,*} 

¹ Spanish Navy's Engineering Corps, Technical Officer Scale, 35003 Las Palmas de Gran Canaria, Spain; ealcsua@gmail.com

² SIGCOM Group, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, L-1855 Luxembourg, Luxembourg

* Correspondence: victor.monzon@uni.lu

Abstract: Machine learning (ML) has become a critical technology in the defense sector, enabling the development of advanced systems for threat detection, decision making, and autonomous operations. However, the increasing ML use in defense systems has raised ethical concerns related to accountability, transparency, and bias. In this paper, we provide a comprehensive analysis of the impact of ML on the defense sector, including the benefits and drawbacks of using ML in various applications such as surveillance, target identification, and autonomous weapons systems. We also discuss the ethical implications of using ML in defense, focusing on privacy, accountability, and bias issues. Finally, we present recommendations for mitigating these ethical concerns, including increased transparency, accountability, and stakeholder involvement in designing and deploying ML systems in the defense sector.

Keywords: machine learning; defense; military tactical environments; artificial intelligence; industry



Citation: Alcántara Suárez, E.J.; Monzon Baeza, V. Evaluating the Role of Machine Learning in Defense Applications and Industry. *Mach. Learn. Knowl. Extr.* **2023**, *5*, 1557–1569. <https://doi.org/10.3390/make5040078>

Academic Editors: Yoan Miche, Jianlong Zhou, Andreas Holzinger and Fang Chen

Received: 28 July 2023

Revised: 9 October 2023

Accepted: 20 October 2023

Published: 22 October 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In recent decades, the term machine learning (ML) has gained widespread popularity, extending beyond the scientific community. ML has been touted as a means to easily enhance the system in which it is implemented. In contrast to classical programming, ML leverages technological advancements such as increased computational capabilities and the collection of large amounts of data (Big Data) to facilitate the generation of algorithms that describe the relationship between inputs and outputs. These algorithms can then be utilized to predict the likelihood of future events statistically.

Technologies or techniques based on ML, or, in more general terms, in artificial intelligence (AI), have revolutionized many industrial sectors because of their numerous advantages, including:

- *Improved efficiency:* ML techniques can automate repetitive and time-consuming tasks, such as data entry and analysis, freeing up employees' time to focus on more complex and creative tasks [1].
- *Increased accuracy:* ML algorithms can analyze large datasets quickly and accurately, providing insights that would be difficult for humans to identify [2]. This can help businesses make more informed decisions, improve product quality, and reduce errors.
- *Cost savings:* By automating tasks and improving accuracy, ML can help businesses save money on labor and reduce waste [3].
- *Predictive maintenance:* ML can analyze data from sensors and other sources to identify when equipment is likely to fail, allowing businesses to perform maintenance before a breakdown occurs [4].
- *Fraud detection:* ML algorithms can detect patterns in data that may indicate fraudulent activity, such as credit card fraud or insurance fraud [5].

- *Improved supply-chain management:* ML algorithms can analyze data from across the supply chain to identify areas for improvement, such as reducing inventory levels or improving delivery times [6].

Currently, many renowned companies, such as Google, Netflix, Amazon, Twitter, Facebook, IBM, Apple, Microsoft, and Oracle, are investing significant financial resources in ML technology to analyze customer profiles and develop new products for the market. For instance, Netflix leverages machine learning to analyze user search data and recommend content on the home screen that aligns with user preferences [7]. Another example is Amazon's Alexa technology, which records user voices and sends the data to the cloud-based Alexa Voice Services for analysis using ML algorithms to interpret user commands and subsequently provide relevant outputs to the device [8]. These examples bring technologies from the civilian world to tactical or military scenarios, such as virtual assistants (Apple's Siri or Amazon's Alexa), speech recognition, and text-to-speech for transcription and translation. Overall, ML within AI can provide significant benefits to businesses and industries, including the defense industry, mainly from a security perspective. Other technologies in conjunction with AI and ML were analyzed in relation to defense in [9], such as neuromorphic processors for advanced computing, which help to process high-volume data. Also, new and evolved tactical scenarios were proposed using emerging technologies in [9,10].

In addition, the defense sector is closely related to Public Protection and Disaster Relief (PPDR) applications and Mission-Critical Services (MCSs) due to their shared objective of safeguarding public safety and security. Both the defense sector and PPDR/MCS entities are involved in emergency response and crisis management. They work to mitigate the impact of disasters, natural or human-made, and protect civilians from harm. The defense sector and PPDR/MCS agencies are responsible for safeguarding critical infrastructure [11] such as power plants, communication networks, transportation systems, government facilities, and water infrastructure. This protection is crucial for maintaining essential services during emergencies [12]. In this regard, ML and artificial intelligence techniques in general can help attain the technological innovation that both institutions require through cooperation and coordination for effective responses and resilience in the face of a wide range of challenges. Notable research, such as that of Petrov et al. in [13] on achieving end-to-end reliability for mission-critical traffic in 5G network software, Spantideas et al. in [14] on intelligent Mission-Critical Services over Beyond 5G networks with a focus on control loop and proactive overload detection, and Skarin et al. in [15] aiming towards mission-critical control at the edge and over 5G, exemplifies the cutting-edge contributions in this field. These studies paved the way for the integration of advanced ML techniques into the defense sector's critical operations. One can see that ML methods play a pivotal role in optimizing these applications. Their adaptability and effectiveness make them directly applicable to the defense sector, enhancing its capabilities significantly. ML applications were discussed in [16] in relation to a tool called DIVVA that verifies and validates disaster-related information on social media platforms. This work used an ML technique based on a bidirectional LSTM model that achieved 84% accuracy in information classification.

In [17], one can find a list of ML techniques that can be used in disaster detection from six areas of interest: early warning damage, damage assessment, monitoring and detection, forecasting and predicting, post-disaster coordination and response, and long-term risk assessment and reduction. Artificial neural networks are the most promising approach today for the detection of, for example, earthquakes, according to [17]. However, a traditional Support Vector Machine (SVM) has been used in research to detect changes in images, allowing for a classification process. Likewise, a variety of mission-critical applications are emerging for critical infrastructures and missions. Within public networks based on 5G and future 6G technologies, centralized deep reinforcement learning (CDRL) and federated DRL (FDRL) are ML solutions for critical services [18].

All these solutions, when the defense sector comes into play, must be analyzed from an ethical and legal point of view due to the human involvement required. In this context, our contribution arises.

Our Contribution

The pervasive influence of machine learning (ML) has extended its transformative reach across various industries, and the defense sector is unequivocally emblematic of this paradigm shift. However, the defense sector is more delicate due to the nature and repercussions that decisions can have on human lives. For this reason, in the literature, several works have proposed the use of artificial intelligence and machine learning in tactical scenarios or military systems. On the other hand, no work has assessed the repercussions that this could have from an ethical and legal point of view. In this work we extend the contribution of the authors in the work [19].

This paper provides the following contributions:

- An assessment of the implications of using ML algorithms and integrating them into defense systems from an ethical and legal perspective.
- A presentation of the requirements of a framework for carrying out ML–defense integration from an ethical and legal point of view.
- The challenges, advantages, and disadvantages of including ML in defense systems are analyzed, including an example of a project that has implemented ML.

The introduction provides a brief overview of the growing interest in leveraging ML technologies for defense purposes and outlines the paper’s objective to uncover potential problems and roadblocks.

2. Method

The methodology followed was based on the authors’ extensive military experience and real-world encounters with ML applications. We intended to identify and discuss the inherent issues of utilizing ML in military applications in order to inform a better-informed decision-making process for using ML effectively in this sector.

- **Data Collection:** The authors collected data through a combination of structured technical research and real projects. They engaged with fellow military personnel, defense technologists, and ML experts to gather insights and anecdotes related to the challenges faced during the deployment of ML systems. The projects are not described in their entirety for confidentiality reasons given the military environment.
- **Case-study selection:** The authors selected a case study involving various ML applications within the defense sector. This case study was the SALAs project (Section 6) and included examples from a survey regarding opinions on the use of lethal autonomous weapon systems.
- **Problem identification:** The collected data were systematically analyzed to identify recurring challenges across our own experiences. The authors categorized the challenges into technical, ethical, operational, and strategic dimensions to provide a holistic view.
- **Comparative analysis:** The authors performed a comparative analysis of the identified challenges in order to create a framework. Although the challenges could be interpreted as applying to artificial intelligence in general, they focused on the military perspective.

The authors mainly drew from their collective experience some practical recommendations for mitigating challenges and advancing the successful integration of ML in defense. These recommendations encompass legal and ethical aspects that have not been considered so far in the literature or any research.

3. ML and Defense Sector

The usage of ML in defense has the potential to enhance security, improve decision making, and increase efficiency. The examples mentioned above for the civil world can

be extended for applications in defense. The tactical landscape would be completely transformed, including new technologies. This transformation was explained in [9], where ten use cases were proposed involving emerging technologies such as 5G and future 6G networks. ML algorithms arose decades ago. However, their implementation in real systems has not been possible. Today, 5G and future 6G communication systems bring with them techniques that improve processing and the amount of data that can be used, making it possible to introduce ML into various systems. For this reason, it is time to address the dilemma that the use of ML in defense could pose. Virtual assistants recognize and respond to spoken commands, allowing for the hands-free operation of devices and appliances and also providing automated responses to common questions or issues. This increases and guarantees the security of soldiers on the battlefield. Speech-to-text technology converts spoken language into text, enabling the real-time transcription of speeches, lectures, and meetings, which improves communications and, again, the security and safety of humans. However, using these technologies for military purposes also raises significant legal and ethical concerns that must be carefully considered. For several reasons, assessing AI and ML's legal and ethical implications in the defense industry is essential. Firstly, the use of these technologies in defense is subject to national and international legal frameworks that regulate the development, production, and use of weapons. For example, developing and deploying autonomous weapons systems raises concerns about accountability, transparency, and human control. These issues are critical for ensuring compliance with international law and maintaining global peace and security.

Secondly, AI and ML applications in defense can lead to unintended consequences, including biases, errors, and discrimination. For example, facial recognition technologies used in defense can perpetuate racial and gender biases. As such, it is essential to establish a legal framework that takes into account the potential risks and harms associated with these technologies.

Thirdly, ethical considerations must be taken into account when using AI and ML in defense. These technologies raise questions about the moral responsibility of individuals and institutions, the value of human life, and the protection of human rights. For example, the use of AI and ML in decision-making processes may lead to decisions that conflict with ethical principles, such as fairness, justice, and equality.

Significant shortcomings remain despite the need to establish a legal framework and address ethical considerations when using AI and ML in defense. Many legal frameworks are outdated and do not fully account for the unique challenges posed by AI and ML applications in defense. Additionally, ethical considerations are often neglected, and there is a lack of consensus as to which ethical principles should guide the development and use of these technologies.

Given the basic idea behind how ML works and the use that large companies are currently making of it in various fields, this article analyzes the ethical and legal issues involved in applying this technology in projects related to a country's defense sector, as well as the disadvantages, challenges, and advantages it entails. It should be understood that when talking about the defense of a country or a war, it is not only necessary to think of those physical events with destructive results involving tangible materials. We must also think of computer attacks, the hacking of networks, terrorism, social alarm and insecurity, piracy, uncontrolled immigration, threats from space, and any other action or omission that provokes a situation of hostility at the national level.

We extracted a series of advantages and disadvantages regarding the introduction of ML in different defense systems, as shown in Figure 1. The union of ML with defense technologies offers several advantages. Firstly, it enables the simulation of possible war scenarios, allowing defense agencies to evaluate different strategies and develop effective countermeasures. Additionally, machine learning enhances the training of troops by providing realistic and dynamic simulations, improving their decision-making abilities and situational awareness. Furthermore, ML algorithms can analyze historical data to extract valuable insights, helping operators understand and respond to complex contextual

situations more effectively. By processing vast amounts of information, these algorithms can also provide operators with additional and useful intelligence, assisting in decision-making processes and enhancing overall operational efficiency. Another benefit is the potential for early warning and the prevention of future incidents. These algorithms can analyze patterns and anomalies in data to identify potential risks, enabling proactive measures to be taken to mitigate or prevent potential threats.

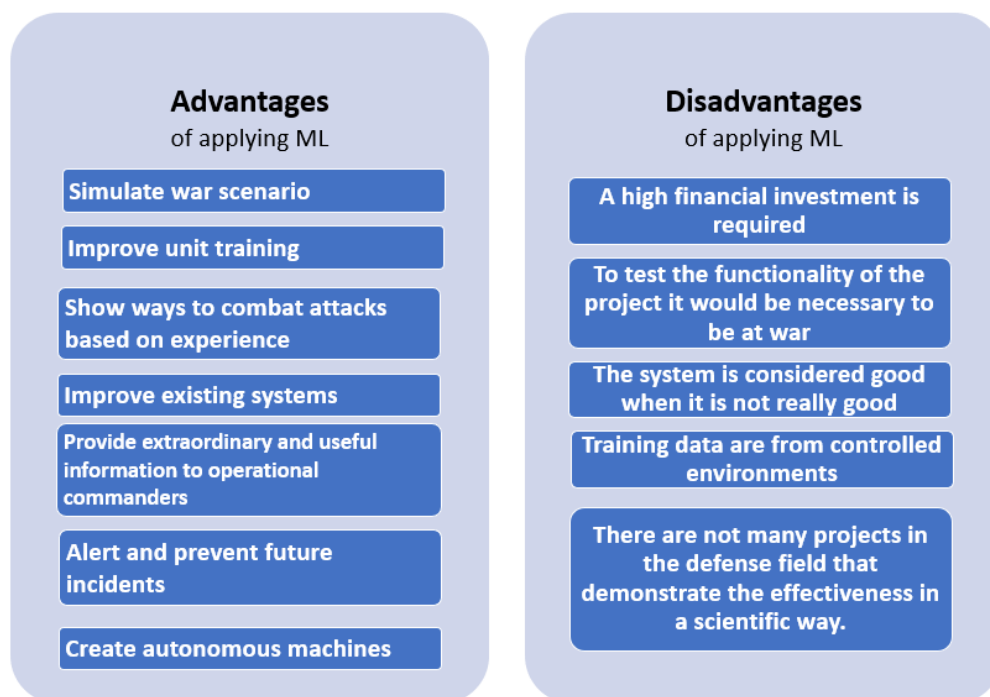


Figure 1. Advantages and disadvantages of applying ML in military environments.

However, there are also notable disadvantages to consider. Implementing machine learning in defense systems requires a significant financial investment, as it involves developing and maintaining robust infrastructure, acquiring advanced technologies, and training personnel. Obtaining relevant data to train machine learning algorithms can also be challenging, as it often requires extensive and diverse datasets that accurately represent real-world scenarios.

4. Defense Systems for Integrating ML

Various systems in defense already include ML-based technologies. We collected the main candidates that have been selected as pioneers in the application of these techniques to evolve defensive technologies, as follows:

1. **Autonomous systems:** These include unmanned aerial vehicles (UAVs) or ground vehicles, which leverage ML algorithms to enable them to navigate and complete missions without direct human control. For example, Ref. [20] proposed an autonomous network using multi-agent reinforcement learning for early threat detection, which is an increasingly important part of the cybersecurity landscape given the growing scale and scope of cyberattacks.
2. **Predictive maintenance:** ML algorithms are used to analyze data from sensors and other sources to predict when equipment may fail, allowing maintenance to be performed before a breakdown occurs. The SOPRENE project [21] proposed the use of ML for predictive maintenance.
3. **Cybersecurity:** ML can analyze network traffic to detect anomalies and potential threats, enabling faster response times and reducing the risk of cyber attacks [22].

4. **Situational awareness:** ML algorithms can analyze data from a variety of sources, including sensors, cameras, and social media, to provide real-time situational awareness to military personnel [23]. The automated detection of refugee dwellings from satellite imagery using multi-class graph-cut segmentation and shadow information was presented in [24].
5. **Logistics and supply-chain management:** ML algorithms can optimize logistics and supply-chain management by analyzing data on inventory levels, shipping times, and other factors to improve efficiency and reduce costs [25].
6. **Threat detection:** ML algorithms can be used to detect potential threats, such as explosives or weapons, at security checkpoints or during cargo inspections [20].

Overall, ML-based technologies have the potential to significantly enhance the capabilities of defense systems and personnel, improving efficiency, accuracy, and safety.

5. Legal Framework

As history has shown, novel technologies often emerge and gain widespread use among the population, leading to legal and political interventions to regulate their usage. Such regulations may take the form of ethical, health-related, or social recommendations. The advent of ML techniques and their ability to deliver automated decisions without human intervention is no exception to this trend, as their regulation has only been considered in recent years while they materialized from a purely theoretical concept into practical applications. The European Commission (EC) published a “White Paper” in Brussels in February 2020 [26], which was the first significant document on the legal regulation of AI at the European level. Its primary goal was to create an ecosystem of excellence that can support the development and adoption of artificial intelligence across the EU economy and public administration by leveraging the strengths of industrial and professional markets and the huge volume of digital data produced worldwide.

According to an official statement from the EC [27], there are seven essential requirements for AI legislation:

- Human action and oversight.
- Technical soundness and security.
- Privacy and data management.
- Transparency.
- Diversity, non-discrimination, and fairness.
- Social and environmental well-being.
- Accountability.

Additionally, special concern has been expressed about the protection of fundamental rights, such as personal data protection, privacy, and non-discrimination, as well as the civil and criminal liability of actions performed by autonomous systems or machines utilizing machine learning.

Based on these considerations, a member country of the European Commission launched a regulatory pilot project on AI called “sandbox” in June 2022 [28]. Sandbox will serve as a tool to carry out a first regulatory project based on the experience of legislative authorities and companies developing AI to identify the best practices for the implementation of this technology. This pilot project is expected to be the starting point for the European Regulation on AI and is anticipated to be implemented within the next two years.

6. Ethical Framework

The ethical dilemmas that AI or the use of ML algorithms can raise have been discussed in many fields. For example, UNESCO addressed in [29] the ethical dilemmas of AI in different sectors, such as the automotive, legal, and art sectors. However, the defense sector has not yet been taken into account, which further justifies our analysis. An important point today is meeting the Sustainable Development Goals [30]; likewise, the Defense sector and its applications must analyze these requirements and consider their implications.

Unquestionably, the use of warfare systems must comply with International Humanitarian Law (IHL), which establishes a set of rules aimed at limiting the effects of armed conflicts for humanitarian reasons (Hague Law). To this end, it is crucial that human leaders supervise war actions to establish an adequate level of discrimination and precaution, depending on the tactical situation, in order to ensure that the risks to non-combatants are proportional to the military objectives' importance. However, in a war situation where the enemy could use autonomous and lethal weapon systems, the semi-automatic establishment of appropriate levels may not be compatible with protecting the units activated on the battlefield and the mission's success.

While military AI can be appropriate for its speed, determination, and accuracy, it can also be concerning due to its making of decisions without temperance, meditation, or adaptation to the various mazes of warfare. Factors such as identifying combatants, peaceful populations, civilians, and military allies; attacks with inordinate intensity; threats; system failures; impersonations; and insufficiently experienced deployed systems could promote an escalation in the war situation and increase the risk instead of providing advantages. It is challenging for a machine to automatically attend to and evaluate the principles of distinction and proportionality, such as distinguishing between a terrified civilian and a dangerous combatant in an urban scenario or applying just defensive force in the face of aggression, which requires a quantitative, qualitative, and ethical assessment.

Other essential aspects are accountability and human dignity. Responsibility serves as a deterrent against unconscionable actions, as a guarantor of law enforcement, and as a moral punishment. Human dignity is crucial from a moral standpoint because a human death chosen by a completely autonomous algorithm can lead to understanding human life as an object. The decision to eliminate a life should involve at least a prior moral judgment.

A recent example of the ethical challenges posed by the use of ML in military tactical environments is Google's decision not to renew Project Maven with the US Pentagon. This decision was controversial, with more than 4000 employees requesting the project's cancellation, suggesting a lack of confidence in the government's use of this system [31].

Finally, it is important to note that in 2015, the Open Roboethics Institute (ORI) conducted an international survey in which it received responses from more than 1000 people from 54 different countries. Among other aspects, this survey asked for opinions on the use of lethal autonomous weapon systems (SALAs) [32]. The results from the SALAs survey [32] are collected and shown in Table 1.

Table 1. Opinion survey on the use of SALAs.

Response Rate	Comment
67%	All types of SALAs should be banned internationally.
56%	The use and development of SALAs should be prohibited.
85%	SALAs should not be used for offensive purposes.
71%	Remotely operated weapon systems should be used instead of SALAs.
60%	The respondent would prefer to be attacked by remotely operated systems rather than SALAs.

Based on the data presented in Table 1, it seems that from an ethical point of view, the development and use of SALAs were not very well received by the respondents. For example, 67% of the respondents thought that all types of SALAs should be banned internationally. Moral and ethical factors prevailed over war strategies and successful operations, refuting the famous expression "all is fair in war".

7. Example of ML Application in Defense: ATLAS

The *Advanced Targeting and Lethality Automated System* (ATLAS) project [33] pursued as a primary goal the equipment of US combat tanks with AI and ML capabilities, allowing them to identify and attack targets three times faster than conventional methods. Therefore, from an AI and ML point of view, the ATLAS project focused on developing a learning algorithm capable of processing a large volume of data collected by sensors. Its purpose was to detect and identify threats automatically and assign the corresponding orientation and elevation to weapon systems so that they can proceed with an attack [34]. In addition, an ML algorithm capable of directly assigning the best weapon from those available to shoot down the detected target was also implemented. In pursuit of this objective, ATLAS concentrated on advancing the following technology areas:

- Data collection regarding possible types of military targets and the pre-training of the ML algorithm used.
- Image processing, where we should highlight the capacity for the detection, classification, recognition, identification, and tracking of targets that can be achieved by applying ML techniques for this purpose.
- Trigger control—in this area, advanced targeting algorithms, the automation of the firing process, and the recommendation of the weapon to be used according to the identified target are very important.
- The technical support integrated into the combat vehicle, since a high-voltage power supply system (600 Vdc) and the integration of sensors and electronics are necessary.
- Sensors—in order to carry out this automation and to provide the ML algorithm with real-time working data, the tanks are equipped with image sensors in the visible, NIR (near-infrared), SWIR (short-wave infrared), MWIR (medium-wave infrared), and LWIR (long-wave infrared) wavebands; gyro mechanisms that make possible the continuous 360° rotation of the sensors and rangefinder; and LADAR (laser detection and ranging)/LIDAR (light detection and ranging)-type lasers.

8. Challenges in the Defense Sector

ML has great prospects in applications related to military environments. However, to create reliable products, it is still necessary to resort to simulation systems, knowledge, and data engineering, according to reference [35]. The main challenges that emerged from this evaluation are summarized in Figure 2.



Figure 2. Challenges of applying ML in military environments.

- **Possible friendly fire:** There is a possibility of fire between units of the same side due to the misidentification of assets, confusion between allies and hostile units, errors in communicating the nature of identified assets, or insufficient contextualization during objective development. The automation of tasks is associated with a lack of tactical patience or even pre-action meditation, which can result in unassessed collateral damage.
- **Adversarial attacks against ML models:** With the passage of time and the widespread use of this technology, the emergence of methods for attacking or interfering with these systems (adversarial evasion attacks) has led to the need to study the reliability, privacy, and security of these algorithms. For example, in imaging systems, noise imperceptible to the human eye could be inserted in such a way as to induce a reliable classification error during jamming. Of note are “white-box” attacks, which occur when the enemy knows how the algorithm (of the deep neural network) works, and “black-box” attacks, which occur when the adversary knows only the type of input and output of the system. Researchers at Stony Brook University (New York) and IBM developed the ARES evaluative framework [36] based on reinforcement learning for adversarial ML, allowing researchers to explore system-level attack/defense strategies and re-examine target defense strategies as a whole.
- **Transparency:** As in safety-critical systems, these types of applications require high transparency, high security, and building user trust. Regarding transparency, the challenges are to improve user confidence in the recommendations given by the system; identify previously unknown causal relationships that can be tested with other methods; determine the limits of system performance; ensure fairness to avoid systematic biases that may result in unequal treatment for some cases; and improve model interoperability, so that users can predict the system recommendations, understand the model parameters, and understand the training algorithm.
- **Ethics in decisions made by machines:** There is a degradation of “humanization” in the decisions made. A machine does not consider the death of civilians as collateral damage or take into account the morality of annihilating the life of an enemy combatant, even when they have indicated their surrender. Thus, it is a major challenge for a machine to learn and contemplate this criterion in its decision algorithm.
- **The scarcity of data and the lack of values:** The performance of an ML algorithm depends mainly on the quality of the samples, the availability of large amounts of samples or data, and whether the data are optimal or meaningful for the exercise. For example, in the case of the US Army, which is a great power with a great deal of combat experience and a very large amount of recorded data, it may be considered that the number of samples is insufficient for the application of ML in a real, substantial, and imminent confrontation. On the one hand, there is a large amount of unknown data on the adversary, and on the other hand, obtaining data in real-time during combat is difficult due to the impossibility of computing and processing the extracted information. If the existing database originates from exercises, it will definitely be limited to certain levels of security and costs and will therefore be substantially different from a real battle. As a solution, it has been proposed to fill this data gap through very arduous fieldwork, taking all possible real values and then identifying them, labeling them, and creating a database with labels according to the needs of the ML algorithm. Another option would be to sample using real-time strategy games, where the commander can play various roles in different scenarios and thus accumulate experience in the form of data.
- **Failures in the evaluation criteria:** The ultimate goal in developing ML algorithms is creating a system that aids decision making based on accumulated experience and experience gained in new scenarios. However, the main challenge is to determine the extent to which the algorithm is valid and reliable for decision making and to make it extensible to other scenarios. Therefore, the decision-making process of the created system requires a large number of experiments and simulations to test its effectiveness.

- **The complexity of modeling a tactical environment:** A large amount of information is relevant concerning a battlefield, among which the state of the combat units and weapons present is of relative importance. The situation is complex due to the difficulty of controlling the behavior of the units, modeling the battlefield environment, intuiting the mechanisms of action, and identifying the evaluation criteria. To all this, we must add the determination of factors such as the efficiency and cost of the war; the damage produced and the need to sustain the resources deployed; and the need to take over air, land, or sea space.

On the other hand, political and economic factors also exist, since military objectives often represent political decisions. Therefore, on some occasions, regardless of the outcome of a battle, if political and economic containment is achieved, the consequences could be positive and valid as a strategy for a tactical environment. All this makes it difficult to build the upper layers of the modeling system.

- **Limited and uncertain information:** During a battle, the information received may be incomplete, and the source may not be certain. Therefore, making decisions with these obstacles may not guarantee profit. Because of this, it is imperative to consider how to discretize time and action, create temporary windows of advantage, and seize the initiative in order to attain military or strategic objectives. Command staff who make decisions according to routines or prescribed protocols will be at a tactical disadvantage. Ideally, they should pay attention to contingencies and innovate their tactics as needed.

However, the transfer of historical knowledge by military experts in the form of facts and rules is an indisputable premise to begin the development of an ML algorithm to be applied in tactical environments. As a basis, the system must know what is meant by the military domain; the performance of the weapons used; the models of warfare (asymmetric, symmetric, hybrid, destructive, nuclear, etc.), the relevant decision models (political, economic, securing civilians, the conquest of territory, etc.); the rules in armed conflicts; and the rules of operation between combatants or between allies.

Following on from the above information, the challenges faced in [37] during war simulation to predict the winning warship using Random Forest are presented as an example. The example study is presented in Table 2, alongside the challenges proposed.

Table 2. Example of a training data challenge.

Challenges	Warfare Simulation Predicting Battleship Winner Using Random Forest [37]
Possible friendly fire	In this case, this challenge did not apply, since the algorithm did not have to identify friendly or enemy units—it only predicted the winner.
Adversarial attacks against ML models	The enemy could match the disposition of dummy weapons. One would have to check whether this could affect the training data and the final result.
Transparency	In order for the command to completely trust the prediction of the algorithm, it should be aware of all sources and constraints. In this case, the information appeared transparent but was also very simple.
Ethics in decisions made by machines	In this case, this challenge did not apply since the algorithm did not make decisions. It only predicted the winner.
The scarcity of data and the lack of values	The reference used 9660 battleship datasets, but there were confidential data such as possible secret weapons or novel defense systems that were not covered.
Failures in the evaluation criteria	Without battlefield data and with the limitation of training data, one would not be sure whether the algorithm was valid and reliable in a real scenario.

Table 2. *Cont.*

Challenges	Warfare Simulation Predicting Battleship Winner Using Random Forest [37]
The complexity of modeling the tactical environment	The study did not consider the scenario in which the battle would take place nor the initial state of the combat units. It only took into account the size, speed, capacity, number of crew, attack, additional attack, and defense of the ships.
Limited and uncertain information	The study offered only one final winner. It was necessary to discretize the time and action in case there was, for example, a misfire or weapon limitation. This would change the situation.

9. Conclusions

Machine learning (ML) has become a pervasive force, revolutionizing industries far and wide, and defense is no exception. Its implementation offers a spectrum of advantages, encompassing heightened efficiency, substantial cost savings, adept fraud detection mechanisms, and the refined management of intricate supply chains. However, the incorporation of ML into defense operations unearths a host of intricate legal and ethical concerns that loom large. Currently, there is a discernible void in terms of comprehensive legal and ethical frameworks capable of governing these novel technologies. This void poses an imminent risk, as the absence of clear guidelines could inadvertently pave the way for unforeseen perils to emerge. The urgency of instituting a comprehensive legal framework is paramount, primarily to pre-emptively address the latent threats and potential harms that ML might introduce into defense systems.

Ethical considerations similarly cast a lengthy shadow over the unbridled integration of ML within defense. These span the realm of both individual and institutional moral responsibilities. The ethical conundrums expand when confronted with matters of safeguarding human life and protecting the rights that underpin human dignity. One of the most striking and controversial aspects revolves around the delegation of decision-making authority to autonomous machines bolstered by ML capabilities, operating without the capacity for moral discernment. While this marks a departure from the norm, it remains a distinctive issue demanding earnest contemplation.

The nexus of legal and ethical implications underscores the urgency of contemplating the application of AI and ML in defense contexts. International laws must be meticulously adhered to and human rights vigilantly safeguarded, necessitating the establishment of robust ethical precepts. However, for all the efforts to underscore the need for these frameworks, tangible gaps persist, reminding us that the path to their implementation is intricate and multifaceted.

Therefore, in this work, we carried out a crucial assessment to determine the requirements and weaknesses related to the creation of future legal and ethical frameworks. These frameworks must take into account the conditions of human nature that surround the defense sector and tactical scenarios. In this analysis, we found a limitation in the lack of information due to the confidential nature of the sector. This, in turn, became the central pillar for defining such frameworks. While establishing a legal framework and addressing ethical concerns pose challenges, taking advantage of potential benefits and minimizing risks and harms is necessary. At the same time, this analysis included the advantages of strengthening defense systems with ML, such as improving training systems for combatants or tactical situation prediction that guarantees the success of the mission. The disadvantages include the difficulty of carrying out the testing phase for systems and the initial deployment barriers. In addition, the challenges of the application of ML in defense projects were studied and identified, such as complexity reduction and faster recovery from failures. These ongoing challenges and potential opportunities highlight possible research directions for advancing the application of machine learning in defense while also addressing legal, ethical, and operational considerations.

Author Contributions: All authors contributed material to the paper based on their different research directions and projects. All authors contributed to the ideas that generated the original papers referenced herein. All authors contributed to writing and reviewing the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: All authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Loubiri, O.; Maag, S. Automated Web Testing using Machine Learning and Containerization. In Proceedings of the 2022 26th International Conference on Circuits, Systems, Communications and Computers (CSCC), Crete, Greece, 19–22 July 2022; pp. 113–121. [\[CrossRef\]](#)
2. Dhakal, A.; Kulkarni, S.G.; Ramakrishnan, K.K. ECML: Improving Efficiency of Machine Learning in Edge Clouds. In Proceedings of the 2020 IEEE 9th International Conference on Cloud Networking (CloudNet), Piscataway, NJ, USA, 9–11 November 2020; pp. 1–6. [\[CrossRef\]](#)
3. Dhirawani, P.; Parekh, R.; Kandoi, T.; Srivastava, K. Cost Savings Estimation for Solar Energy Consumption Using Machine Learning. In Proceedings of the 2022 11th International Conference on Renewable Energy Research and Application (ICRERA), Istanbul, Turkey, 18–21 September 2022; pp. 42–49. [\[CrossRef\]](#)
4. Liulys, K. Machine Learning Application in Predictive Maintenance. In Proceedings of the 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 25 April 2019; pp. 1–4. [\[CrossRef\]](#)
5. Wei, Y.; Qi, Y.; Ma, Q.; Liu, Z.; Shen, C.; Fang, C. Fraud Detection by Machine Learning. In Proceedings of the 2020 2nd International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI), Taiyuan, China, 23–25 October 2020; pp. 101–115. [\[CrossRef\]](#)
6. Rao, U.A.; Nalinipriya, G.; Jangirala, S.; Poonguzhali, I.; Azahad, S.; Samatha, B. Improved Food Supply Chain Forecasting Management Using IoT and Machine Learning. In Proceedings of the 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 16–17 October 2022; pp. 1–4. [\[CrossRef\]](#)
7. Sudharsan, B.; Kumar, S.P.; Dhakshinamurthy, R. AI Vision: Smart speaker design and implementation with object detection custom skill and advanced voice interaction capability. In Proceedings of the 2019 11th International Conference on Advanced Computing (ICoAC), Chennai, India, 18–20 December 2019; pp. 97–102. [\[CrossRef\]](#)
8. Ramadhan, G.; Setiawan, E.B. Collaborative Filtering Recommender System Based on Memory Based in Twitter Using Decision Tree Learning Classification (Case Study: Movie on Netflix). In Proceedings of the 2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS), Bandung, Indonesia, 23–24 November 2022; pp. 1–6. [\[CrossRef\]](#)
9. Monzon Baeza, V.; Concha Salor, L. New horizons in tactical communications: An overview of emerging technologies possibilities. *IEEE Potentials* **2023**, *42*, 1–8. [\[CrossRef\]](#)
10. Concha Salor, L.; Monzon Baeza, V. Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications. *Telecom* **2023**, *4*, 709–731. [\[CrossRef\]](#)
11. Villar Miguelez, C.; Monzon Baeza, V.; Parada, R.; Monzo, C. Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks. *Smart Cities* **2023**, *6*, 728–743. [\[CrossRef\]](#)
12. Parada, R.; Monzon Baeza, V.; Barraca-Ibort, D.N.; Monzo, C. LoRa-Based Low-Cost Nanosatellite for Emerging Communication Networks in Complex Scenarios. *Aerospace* **2023**, *10*, 754. [\[CrossRef\]](#)
13. Petrov, V.; Lema, M.A.; Gapeyenko, M.; Antonakoglou, K.; Moltchanov, D.; Sardis, F.; Samuylov, A.; Andreev, S.; Koucheryavy, Y.; Dohler, M. Achieving End-to-End Reliability of Mission-Critical Traffic in Softwarized 5G Networks. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 485–501. [\[CrossRef\]](#)
14. Spantideas, S.; Giannopoulos, A.; Cambeiro, M.A.; Trullols-Cruces, O.; Atxutegi, E.; Trakadas, P. Intelligent Mission Critical Services over Beyond 5G Networks: Control Loop and Proactive Overload Detection. In Proceedings of the 2023 International Conference on Smart Applications, Communications and Networking (SmartNets), Istanbul, Turkey, 25–27 July 2023; pp. 1–6. [\[CrossRef\]](#)
15. Skarin, P.; Tärneberg, W.; Årzen, K.E.; Kihl, M. Towards Mission-Critical Control at the Edge and Over 5G. In Proceedings of the 2018 IEEE International Conference on Edge Computing (EDGE), Washington, DC, USA, 1–3 May 2018; pp. 50–57. [\[CrossRef\]](#)
16. Bongirwar, V.; Mishra, S.S.; Bisen, A.; Mundhada, S.; Singh, U. Disaster Information Verification and Validation Application Using Machine Learning. *Int. J. Next-Gener. Comput.* **2022**, *13*. [\[CrossRef\]](#)

17. Arinta, R.R.; Andi W.R., E. Natural Disaster Application on Big Data and Machine Learning: A Review. In Proceedings of the 2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 20–21 November 2019; pp. 249–254. [\[CrossRef\]](#)
18. Liu, Y.; Deng, Y.; Nallanathan, A.; Yuan, J. Machine Learning for 6G Enhanced Ultra-Reliable and Low-Latency Services. *IEEE Wirel. Commun.* **2023**, *30*, 48–54. [\[CrossRef\]](#)
19. Alcántara Suárez, E.J. Análisis de la aplicación de machine learning en sistemas de defensa. Master's Dissertation, Universitat Oberta de Catalunya, Barcelona, Spain, 2023.
20. Campbell, R.G.; Eirinaki, M.; Park, Y. A Curriculum Framework for Autonomous Network Defense using Multi-agent Reinforcement Learning. In Proceedings of the 2023 Silicon Valley Cybersecurity Conference (SVCC), San Jose, CA, USA, 17–19 May 2023; pp. 1–8. [\[CrossRef\]](#)
21. Fernández-Barrero, D.; Fontenla-Romero, O.; Lamas-López, F.; Novoa-Paradela, D.; R-Moreno, M.D.; Sanz, D. SOPRENE: Assessment of the Spanish Armada's Predictive Maintenance Tool for Naval Assets. *Appl. Sci.* **2021**, *11*, 7322. [\[CrossRef\]](#)
22. Kseniia, N.; Minbaleev, A. Legal Support of Cybersecurity in the Field of Application of Artificial Intelligence Technology. In Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 7–11 September 2020; pp. 59–62. [\[CrossRef\]](#)
23. Yongcui, Z. Situation Awareness and Target Recognition of Marine Big Data Battlefield based on Deep Learning. In Proceedings of the 2022 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 24–26 June 2022; pp. 430–435. [\[CrossRef\]](#)
24. Ergünay, Ü.S.K.; Kahraman, F.; Ates, H.F. Automated detection of refugee dwellings from satellite imagery using multi-class graph-cut segmentation and shadow information. In Proceedings of the 2014 22nd Signal Processing and Communications Applications Conference (SIU), Trabzon, Turkey, 23–25 April 2014; pp. 1591–1595. [\[CrossRef\]](#)
25. Korecki, Z.; Smrž, V.; Pecháček, T. Support of the logistics chain by small aircraft in times of emergency. In Proceedings of the 2020 New Trends in Aviation Development (NTAD), Stary Smokovec, Slovakia, 17–18 September 2020; pp. 136–141. [\[CrossRef\]](#)
26. European Commission White Paper: On Artificial Intelligence—A European Approach to Excellence and Trust. Brussels. 2020. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065> (accessed on 27 July 2023).
27. European Commission Ethics Guidelines for Trustworthy AI. 2020. Available online: <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html#:~:text=The%20Ethics%20Guidelines%20for%20Trustworthy%20Artificial%20Intelligence%20%28AI%29,as%20part%20of%20the%20C2%A0AI%20strategy%20announced%20earlier%20that%20year> (accessed on 27 July 2023).
28. Truby, J.; Brown, R.; Ibrahim, I.; Parellada, O. A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications. *Eur. J. Risk Regul.* **2022**, *13*, 270–294. [\[CrossRef\]](#)
29. UNESCO. Artificial Intelligence: Examples of Ethical Dilemmas. 2023. Available online: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics/cases> (accessed on 27 July 2023).
30. Tarazona Lizarraga, C. Análisis de las necesidades de una Smart City en el marco de un desarrollo sostenible. Master's Dissertation, Universitat Oberta de Catalunya, Barcelona, Spain, 2020.
31. Wakabayashi, D.; Shane, S. Google Will Not Renew Pentagon Contract That Upset Employees. *The New York Times*, June 2018. Available online: <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html> (accessed on 27 July 2023).
32. Roldán Tudela J.M. Artificial Intelligence Application in Defence. Spanish Institute of Technological Studies, June 2018. p. 166. Available online: https://www.ieee.es/Galerias/fichero/docs_trabajo/2019/DIEET0-2018La_inteligencia_artificial.pdf (accessed on 27 July 2023).
33. Breaking Defense. BD Checks Out Army's Robotic Gun: ATLAS 2020. Breaking Defense, Land Warfare, Networks/Cyber. 2020. Available online: <https://breakingdefense.com/2020/10/bd-checks-out-armys-robotic-gun-atlas/> (accessed on 27 July 2023).
34. Strout, N. How the Army Plans to Revolutionize Tanks with Artificial Intelligence. C4ISRNET, Artificial Intelligence, October 2020. <https://www.c4isrnet.com/artificial-intelligence/2020/10/29/how-the-army-plans-to-revolutionize-tanks-with-artificial-intelligence/> (accessed on 27 July 2023).
35. Wang, W.; Liu, H.; Lin, W.; Chen, Y.; Yang, J.A. Investigation on Works and Military Applications of Artificial Intelligence. *IEEE Access* **2020**, *8*, 131614–131625. [\[CrossRef\]](#)
36. Ahmed, F.; Vaishnavi, P.; Eykholt, K.; Rahmati, A. Ares: A System-Oriented Wargame Framework for Adversarial ML. In Proceedings of the 2022 IEEE Security and Privacy Workshops (SPW), Francisco, CA, USA, 22–26 May 2022; pp. 73–79. [\[CrossRef\]](#)
37. Intizhami, N.S.; Husodo, A.Y.; Jatmiko, W. Warfare Simulation: Predicting Battleship Winner Using Random Forest. In Proceedings of the 2019 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), Makassar, Indonesia, 1–3 August 2019; pp. 30–34. [\[CrossRef\]](#)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.