International Journal of Trend in Research and Development, Volume 10(4), ISSN: 2394-9333
www.ijtrd.com

AI and Cyber Security with Reference to Military/ Defense

Mahak Bhardwaj
FY BBA LLB (Hons.), Narsee Monjee Institute of Management Studies (NMIMS), Kirit P. Mehta School of Law, Mumbai, India

Abstract: Cyber security and Artificial Intelligence (AI) are two quickly developing fields that are playing abigger role in military and defense operations. The use of AI has become essential to detecting andpreventing assaults as a result of the increasing sophistication of cyber threats. In this study, the state-of-the-art in cyber security and AI as well as how these fields overlap in the context of war and defense is discussed. The research starts out by giving a summary of the AI methods utilizedin cyber security, including machine learning, natural language processing, and anomaly detection.The use of AI in enhancing military and defense system security, including the identification of cyber threats and the safeguarding of vital infrastructure, is then covered. The possibility for adversarial attacks and the difficulty of interpreting results produced by AI are some of the difficulties related with the use of AI in cyber security that we then explore. Also, some of the ethical problems with using AI in military and defense activities, such as challenges with accountability, prejudice, and transparency are discussed. Lastly, attention is drawn to some of theresearch needs in the area, including the need for better AI algorithms that can adapt to shifting threats and the expansion of study into the long-term implications of AI on military/defense operations. Overall, this paper offers a thorough analysis of the current state of artificial intelligence (AI) and cyber security in military/defense, and it identifies some of the major difficulties and promising areas for further study.

Keywords: *Cyber Security, Artificial Intelligence, Military, Adversarial Attacks, Transparency*

I. INTRODUCTION

The rapid advancement of deep learning in artificial intelligence (AI), in particular, has had a significant impact on a number of industries as well as ongoing changes to conventional manufacturing processes and way of life. The evolution of machine intelligence is mostly a resultof the innovation of AI theory and practice, from passive learning with computer capacity to autonomous learning and enhanced learning. Both human wisdom and machine intelligence are necessary to prevail in a military conflict. As a result, human-machine collaboration would complement each other's shortcomings and capabilities, which is essential for success in the increasingly complicated environment of modern warfare. There are numerous difficulties to takeinto account, notwithstanding the potential uses of AI in the military.

Since it has been shown that even if an AI technique is unknown, it may still be vulnerable to minute changes in input data, developing trustworthy and stable AI systems can be challenging. High risks necessitate transparent military AI-systems; yet, this is difficult because many AI techniques are black boxes with little openness, making it difficult to win over decision makers and aid risk assessments.

Predictions for military AI

The next 10 years will see the definition or re-definition of several key advanced military technologies, according to predictions about the usage of AI in military applications. AI solutionswill become primarily intelligent through the fusion of analytical and knowledge-focused abilities. Afterward, the AI solutions will be interconnected in order to make use of the network of physical and virtual domains, which will include sensors, organisations, people, and autonomous agents, aswell as to fully exploit the benefits of blockchain technology in terms of maintaining data integrity. They will be spread out over a significant region in order to make use of large-scale, decentralisedsensor networks, storage, and processing. They will also digitally combine the physical, informational, and human realms to support new disruptive effects. (In line with predictions made by the NATO Science and Technology Organization for the year 2020).

Uses of AI in defense to develop proactive cyber protection strategies

AI can be utilised in a variety of ways in the military and other organisations involved in defence to develop and put into practise proactive cyber defence strategies. These strategies can be developed in the context of the military. The following is a list of some of the most significant potential applications for artificial intelligence:

1. Threat Detection and Analysis: AI can be used to detect and analyse cyber threats in real time, enabling defence organisations to swiftly identify and respond to potential attacks. This is made possible by the use of threat detection and analysis. The capacity of AI to recognise andassess dangers in the here and now makes this outcome conceivable. AI can also be used to monitor the behaviour of users and networks in order to detect anomalies, such as those that may indicate a cyber attack is being planned. This can be accomplished by using a combination of machine learning and deep learning techniques.
2. Predictive Analysis: AI can be used to analyse large amounts of data, identify patterns, and forecast future cyberattacks. This type of analysis is known as predictive analytics. The term "predictive analytics" refers to this particular kind of analysis. In their efforts to take preventative measures or measures to mitigate the effects of potential attacks, defence organisations may find this to be of assistance.
3. Training and Simulation in Cyberspace: Training and Simulation in Cyberspace Members of the armed forces and those working in the defence industry can benefit from the use of artificial intelligence when it comes to receiving cyber training and simulation. This can be helpful in improving the cyber awareness and skills of personnel, and it also makes it possible to test a variety of cyber defence

strategies in an environment that is both safe and under control.

How can AI-based military and defense cyber security concerns be mitigated?

There are both possible benefits and potential threats involved with the use of artificial intelligence (AI), and the use of AI can give major benefits to military and defence cyber security. Using AI in military and defence cyber security may expose users to a number of significant hazards, including the following:

1. Bias: Artificial intelligence systems can be biassed towards specific sorts of attacks, whichcan lead to blind spots in the defences against cybercrime. Either the data that were used to train the system or the architecture of the algorithms that were utilised could be to blamefor this bias.
2. Attacks of an adversarial nature: Artificial intelligence (AI) systems can be susceptible to attacks of an adversarial nature, in which an adversary purposefully manipulates the system to create inaccurate or malicious results. This can be especially harmful in the context of cyber security, since an adversary could utilise an AI system to circumvent the security mechanisms that are in place.
3. Inability to provide explanations: Because some AI systems are difficult to explain, it mightbe challenging to comprehend the basis for the conclusions they generate. This can make it challenging for individuals responsible for cyber security to place their trust in the resultsproduced by AI systems, and it may also make it more difficult to investigate instances ofcyber attack.
4. Human Error: Errors caused by humans can occur in AI systems, and these might range from poor configuration to inappropriate use. Because of this, a network's protections against cyberattacks may become vulnerable.

The military and other defence organisations can take a few different initiatives to decrease these risks, including the following:

Create AI systems that are both transparent and explainable: Companies should strive to create AI systems that are both transparent and explainable. This will allow cyber security employeesto understand how the systems make decisions and uncover any potential biases or vulnerabilities.

Test and evaluate AI systems on a regular basis: Artificial intelligence (AI) systems should betested and evaluated on a regular basis by organisations to detect any vulnerabilities or faults and to ensure that they are performing as intended.

Employ many levels of protection: To guarantee that their cyber security defences are robust and successful, businesses should employ numerous layers of defence, which should include both artificial intelligence (AI) technologies and human specialists.

Training personnel in AI systems: Companies should offer their cyber security professionals with the training they need to comprehend and effectively use AI systems, as well as to identify and handle any possible concerns that may occur. This training should focus on providing personnel with an understanding of AI systems.

It is possible for military and defence organisations to ensure that their defences are effective and robust by implementing these actions, which will lower the risks connected with utilisingAI in cyber security and make it possible for them to mitigate those risks.

Advantages and Disadvantages of AI in the Military Field

	Benefits and Potential Advantages	Disadvantages and Risks
Strategic Decisionmaking	- More precise, faster situation assessments and analyses - Offsetting emotions and prejudices - Rational behavior in crisis situations	- Low crisis stability due to acceleration of decisions - Prejudices can be inherent in algorithms - Problems regarding the balance of power within states, for example between the military and the civilian leadership.
Training and Organization of Armed Forces	- Personalized training, fair assessments and promotions - More realistic exercises, maneuvers and simulations - Credible simulations of future technologies and their applications	- Overestimation of AI-generated results - Cultural and personnel problems due to incompatibility between military culture and values held by specialized personnel - Military cast system due to higher technical specialization
Military Operations	- More efficient processing of data from different sources - Reduction of administrative and staff work through forward-looking logistics - Reduced risks for troops through autonomous logistics - Improvement of support and reconnaissance systems	- Potential dependencies that cannot be replaced in the field - Risks in supply chains due to lack of inventories and reserves - Unclear whether autonomous vehicles can be used in complex scenarios - Reduction of strategic stability

Research Questions

1. How can AI be used in military and defense organizations to create and implement pro-active cyber defense strategies?
2. What potential risks could arise from using AI to military and defense cyber security, andhow might such risks be reduced?
3. How can AI be applied to help military and defense organizations establish strong identity and access management solutions?

Research Objectives

1. The creation of AI-based solutions to assist in the creation of strong identity and accessmanagement systems for military and defense organizations.
2. To assess the potential of AI-based technologies in boosting situational awareness and threat identification in military and defense cyber security.
3. To recognize the difficulties in incorporating AI into the current military and defense cyber security infrastructure and to suggest solutions for a seamless integration

Hypothesis

H1: AI's usage in military and defence cyber security will improve the discovery and mitigation of online threats, improving the security of infrastructure and critical data.

H2: The development of transparent and comprehensible AI systems, regular testing and evaluation, and the deployment of several layers of defence can all help to reduce the potential hazards connected with the use of AI in military/defense cyber security.

H3: Artificial intelligence (AI) can swiftly spot possible risks and vulnerabilities that human analysts might overlook.

II. LITERATURE REVIEW

1. AI has the potential to improve cyber security, but it also creates new vulnerabilities and risks. This highlights the possibility that AI systems could be hacked or manipulated, the possibility that AI could be used in offensive cyber operations, and the risk of unintended consequences. Before deciding to implement AI in military cyber security, it is recommended that decision-makers give careful consideration to both the potential risks and benefits of

doing so. (Thomas Rid and Ben Buchanan, 2018)

2. "There are various types of AI, and they can be used to recognise and address online dangers. The application of AI in a military setting faces a number of difficulties, includingthe necessity for trustworthy data, the danger of bias, and the possibility of human error." (Daniel J. Lohrmann, 2019)
3. There are various forms of artificial intelligence, such as machine learning and deep learning, and numerous ways in which these forms of AI can be utilised to identify and respond to cyber threats. There is a potential for bias as well as concerns associated with employing AI in cybersecurity, such as the requirement for data that can be trusted and thepossibility of bias. Artificial intelligence has the potential to transform cyber security, butit is vital to carefully assess both the risks and the rewards (Seyedali Mirjalili, Seyed Mohammad Mirjalili, and Alireza Ghaffari, 2019)
4. "Artificial intelligence has the potential to improve military cyber security by increasing situational awareness, detecting threats, and automating responses." It is necessary to consider the difficulties associated with putting artificial intelligence to use in a military setting, such as the requirement for interoperability and the possibility of cyber assaults on AI systems. (Commander William J. Knarr, 2020)
5. In a military conflict, human wisdom is just as important as artificial intelligence. Collaboration between humans and machines would so complement each other's shortcomings and combine their strengths, which is essential for success in the increasingly complicated environment of modern warfare. (ZHANG Zhi-min, SHI Fei-fei, WAN Yue-liang, XU Yang, ZHANG Fan, NING Huan-sheng, 2020)

III. RESEARCH METHODOLOGY

In the current study's research approach, the "Doctrinal Method" is used to identify facts,circumstances, and reasons that are pertinent to the research subject. We used a lot of secondary sources when compiling the study report, which is why we went with this method of data collection. It was chosen because secondary data could be obtained more quickly than main data. The research is conducted through secondary sources, which include publications, papers, newspaper articles, sites, academic papers, statutes, and other significant resources that are readilyavailable in relation to the study's topic.

IV. DISCUSSION

Given the potential uses of AI in this configuration, the hypothesis that using AI in military and defence cyber security will lead to more effective and efficient identification and mitigation of cyber threats is a plausible one. This will lead to improved protection of sensitive information andinfrastructure. The ability to evaluate massive amounts of data in real time is one of the key benefitsof utilising AI in military and defence cyber security. This can assist to swiftly identify potential threats and weaknesses, which is a significant advantage. This may be of utmost significance in the context of military and defence enterprises, which frequently face a significant number of cyberattacks and threats to their networks. In addition to this, artificial intelligence can also provide extra levels of security through the implementation of technologies such as continuous monitoringand multi-factor authentication. This can assist to guarantee that only authorised users are able toaccess important information and systems, and that any suspicious behaviour is discovered and dealt with in real time. In addition, this can help to ensure that only authorised users are able to access sensitive information and systems.

Yet, there are also possible hazards connected with the use of AI in military and defence cyber security, such as bias, adversarial assaults, and a lack of explainability. These risks could potentially compromise the integrity of the system. Because of the possibility that these dangers will result in weaknesses in the network's defences, addressing them may need for more resources and personnel with specialised knowledge. It's possible that military and defence organisations will need to invest in the development of AI systems that are visible and explainable, as well as intesting and evaluation on a regular basis and the employment of many levels of defence, in order to avoid these dangers. This can assist to ensure that any possible problems are discovered and treated in a timely and effective manner, which can help to guarantee that there are no problems. In general, the application of artificial intelligence (AI) in the field of military and defence cyber security has the potential to greatly improve the safety of sensitive information and infrastructure.To ensure that AI is used successfully and safely in this context, it is essential to thoroughly analysethe potential hazards and to take the proper measures to reduce these risks. Only in this way can one guarantee that AI will be utilised.

Limitations of the Study

The primary shortcoming of this paper was its emphasis on the direct impacts of advertising and sales promotion on consumer behaviour. Newspaper stories, websites, and academic papers are the only sources used in this study.

CONCLUSION

There is no doubt that AI is expanding the possibilities for defence technology. There are great hopes for the use of AI techniques in a number of military fields; nevertheless, there are still challenges and problems that need to be resolved in order to live up to those expectations.

To conclude, artificial intelligence has the potential to improve cybersecurity measures in militaryand defence activities. It is possible for it to increase capabilities such as threat detection, response speed, and decision-making, hence assisting in the prevention of successful cyber attacks. The development of more reliable and secure systems to safeguard sensitive data and infrastructure canalso be facilitated with the help of AI. Yet, the adoption of AI technology necessitates careful planning and attention because it presents new threats to data security. There is a possibility that the technology might be exploited through hacking or manipulation, and there is also a possibilitythat it could be used to conduct cyber attacks. As a result, it is of the utmost importance to formulatesuitable safeguards and laws in order to guarantee that AI is utilised in a responsible and ethical manner within military and defence contexts. In general, a comprehensive strategy that takes intoconsideration the various technical, organisational, and human variables is required for the efficient use of AI in cybersecurity. It is possible for military and defence companies to improve their ability to detect and respond to cyber attacks by implementing AI technology into their cybersecurity policies. At the same time, these organisations can protect their important assets and infrastructure.

References

[1] Szabadföldi,I.(2021).Artificial Intelligence in Military Application – Opportunities andChallenges. Land Forces Academy Review,26(2) 157-165.

[2] ZHANG Zhi-min, SHI Fei-fei, WAN Yue-liang, XU Yang, ZHANG Fan, NING Huan- sheng. Application progress of artificial intelligence in military confrontation[J].
[3] J. -H. Eom, N. -U. Kim, S. -H. Kim and T. -M. Chung, "Cyber military strategy for cyberspace superiority in cyber warfare," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)
[4] M. Karaman , H. Ã‡atalkaya and C. Aybar , "Institutional Cybersecurity from Military Perspective",
[5] Van Den Bosch, K., & Bronkhorst, A. (2018, July). Human-AI cooperation to benefit military decision making. NATO.
[6] Apiecionek, Ł., Makowski, W., Biernat, D., & Łukasik, M. (2015, June). Practical implementation of AI for military airplane battlefield support system.
[7] Masuhr, N. (2019). Ai in military enabling applications.
[8] Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018, May). Possibilities and challenges for artificial intelligence in military applications.
[9] Rasch, R., Kott, A., & Forbus, K. D. (2003). Incorporating AI *Intelligent Systems*, *18*(4),18-26.
[10] Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review Selma Dilek , Hüseyin Çakır and Mustafa Aydın (2015)
[11] Vacca, W. A. (2011). Military culture and cyber security.
[12] O'Connell, M. E. (2012). Cyber security without cyber war.
[13] Tikk-Ringas, E., Kerttunen, M., & Spirito, C. (2014). Cyber security as a field of militaryeducation and study.
[14] Karaman, M., Hayrettin, Ã., & Aybar, C. (2016). Institutional cybersecurity from militaryperspective.
[15] Lewis, L. (2017). Insights for the Third Offset: Addressing challenges of autonomy and artificial intelligence in military operations.