PROSPECTS OF ARTIFICIAL INTELLIGENCE INTEGRATION IN THE DEFENSE SECTOR

https://doi.org/10.59982/18294359-25.1-gs-04

Gevorg Smbatyan
PhD student
PAARA ,Chair of Administration
gevorgsmbatyan20hk@paara.am

Gegham Smbatyan
PhD student
PAARA, Chair of Administration
geghamsmbatyan20hk@paara.am

Abstract

The rapid advancement of Artificial Intelligence (AI) is transforming numerous sectors, especially in defense. Nations are actively exploring ways to utilize AI to strengthen their military capabilities, improve cybersecurity, and protect their citizens. The importance of AI in national security has become even more pronounced due to the challenges of modern warfare, including the rise of cyber threats, hybrid warfare strategies, and the increasing deployment of autonomous systems.

Ministries of Defense play a crucial role in ensuring national security by overseeing military operations, shaping defense strategies, and fostering collaboration with international partners. In this context, Artificial Intelligence (AI) technologies present opportunities to enhance operational efficiency, improve decision-making, and increase preparedness for the increasingly complex security challenges we face. This article explores the potential of AI in national security, emphasizing how the defense sector can leverage AI to tackle both traditional and emerging threats. It examines the worldwide application of Artificial Intelligence (AI) in the defense sector, highlighting crucial areas where AI technologies can be adapted and integrated into defense systems. The primary aim is to underscore the potential benefits of AI in improving existing national defense structures, as well as the challenges that must be addressed for the successful deployment of AI-driven systems.

***Keywords*:** Artificial Intelligence, Defense Sector, Armenia, National Security, Future States, Strategic Planning.

Introduction

1. The Role of Artificial Intelligence in the Context of National Security

In our current information-driven and technologically advanced society, national security has expanded to include much more than just military forces and operations. It now involves protecting critical infrastructure, responding to cyber threats, safeguarding sensitive data, and ensuring a country's political and economic stability [Greg and Chan]. Artificial Intelligence (AI) technologies have become vital in tackling these complex challenges. Today, AI is utilized to analyze vast amounts of data, which allows for quicker and more informed decision-making. This leads to enhanced situational awareness, improved threat prediction, and the automation of various operations [Herbert].

The use of Artificial Intelligence (AI) in national security encompasses autonomous systems, unmanned devices, and advanced cybersecurity measures, all of which are essential components of

modern defense strategies [Andrew et al.]. Implementing AI in autonomous drones or robotics can greatly improve territorial surveillance, minimize human casualties, and deliver real-time critical information needed for making accurate decisions during military operations [Gertz]. The significance of embracing and adapting these technologies is substantial, as they help modernize and enhance the efficiency of national security systems. This is crucial for maintaining competitiveness and security on a global scale [Russell and Norvig].

2. The Role of AI in the Military and Defense Sector

Today, the defense sector encounters a variety of strategic and operational challenges, many of which can be addressed through the use of artificial intelligence technologies. These challenges include optimizing resource management, improving military readiness, and ensuring quick responses to emerging threats [Tansley].

- **AI in Threat Detection for Cybersecurity:** One of the most promising uses of artificial intelligence in national security is in the realm of cybersecurity. AI-driven systems can sift through vast amounts of data and detect patterns of malicious activity much more quickly than human analysts [Rid]. These technologies are essential for safeguarding military networks, communications, and national infrastructure from cyber threats [Kissinger]. Additionally, AI systems can forecast potential attacks, allowing for proactive measures to be implemented ahead of time.
- **Autonomous Systems and Unmanned Aerial Vehicles in Defense:** The integration of AI-powered autonomous systems and unmanned aerial vehicles (UAVs) can greatly enhance defense surveillance capabilities, particularly in border regions and conflict zones. Autonomous drones equipped with AI can conduct reconnaissance missions in hazardous or inaccessible areas. They can also relay real-time information about enemy movements and positions, facilitating quicker and more effective military responses [Goodman]. The deployment of these technologies can provide a strategic edge in surveillance, intelligence gathering, and combat operations [Մկրտչյան].
- **Decision-Making and Strategic Planning:** AI technologies play a crucial role in decision-making by analyzing complex datasets and offering actionable insights [Webb]. These systems can sift through battlefield data, enemy strategies, and logistical details, assisting military leaders in making quicker and more precise decisions. Additionally, AI's capability to simulate different scenarios helps evaluate potential military situations and refine strategic planning [McFate]. Moreover, AI can foresee possible conflicts and crises, allowing for proactive measures to be put in place [Arquilla and Ronfeldt].

This underscores the vital importance of artificial intelligence in the defense sector, providing enhanced security and aiding in the resolution of strategic challenges.

Literature Review

The use of artificial intelligence in national security has attracted considerable global interest, underscoring its essential role in defense, cybersecurity, and strategic planning [Angelina]. Research shows that AI holds significant promise for threat detection, data-driven decision-making, automated surveillance, and enhancing operational efficiency [Knake]. Autonomous systems and unmanned devices are particularly appreciated for their effectiveness in surveillance and reconnaissance, as they minimize human risk and improve the accuracy of real-time intelligence [Payne].

AI is also crucial for bolstering cybersecurity resilience. Machine learning algorithms can swiftly identify, predict, and respond to cyber threats, allowing for a more proactive and preventive strategy [Allan and Peter]. Further studies indicate that AI can be effectively utilized in border security. Autonomous drones and surveillance systems are particularly advantageous in scenarios

that require operations in hard-to-access or hazardous areas, providing monitoring, data collection, and reconnaissance that enhance the efficiency of defense agencies [Weiner].

Nonetheless, the integration of AI into the defense sector presents various challenges and ethical dilemmas. Adherence to international humanitarian law is especially important during military operations. Concerns arise regarding the legality and accountability of autonomous systems, particularly in situations where life-or-death decisions might be made without human oversight [Bankins]. The literature also highlights the necessity of developing policies and regulations that ensure the safe and ethical incorporation of AI in defense while simultaneously strengthening national security [Lin].

Research Methodology

This study uses a qualitative, multi-method approach to investigate the potential of artificial intelligence in national defense, focusing on both theoretical and practical dimensions. Given the complexities involved in integrating AI into the defense sector, the methodology ensures a thorough analysis of AI's possible applications and the challenges that come with them [Walsh].

The data for this research is gathered from two main sources:

- **Literature Review:** Analyzing both international and local literature on AI in defense provides essential context. It examines global trends, case studies from similar countries, and specific research on defense requirements. This review emphasizes the operational outcomes of AI applications as well as the challenges, including ethical, technological, and managerial issues that could impede the integration of AI into national security [Turobov].
- **Case Study Analysis:** The study draws on cases from countries facing comparable strategic and geopolitical challenges. It pays special attention to how these nations tackle infrastructure and regulatory hurdles. The policies they adopt, the technological solutions they implement, and the effectiveness of AI deployment are thoroughly analyzed.

This research relies exclusively on publicly available data and does not incorporate classified or restricted information. Despite its limitations, the combination of literature review and case study analysis offers a richer understanding of AI's role in national security. This methodology aims to enhance knowledge on AI applications, identify potential challenges, and suggest strategic solutions to improve the technological capabilities of national defense [Bostrom].

International Experience in Artificial Intelligence

Several nations, including the United States, China, and Russia, have made notable advancements in artificial intelligence research and its military applications.

The United States stands out as a frontrunner in incorporating AI into its national defense strategy. The Department of Defense has poured substantial resources into AI research, focusing on areas like autonomous systems, cybersecurity, and data analysis. Additionally, the U.S. has set up the Joint Artificial Intelligence Center to oversee AI integration across all military branches, showcasing a model for developing strategic programs, allocating resources, and ensuring the effective use of AI technologies [Davenport and Kirby].

China and Russia also prioritize the advancement of AI technologies in their defense strategies. China's military doctrine emphasizes AI as a crucial component of future warfare, with significant investments in AI-driven drones, robotic systems, and cyber warfare capabilities [Horowitz]. Meanwhile, Russia is concentrating on the application of AI in strategic planning, autonomous systems, and military robotics, positioning itself as a leader in using AI for military operations management [Andress and Winterfeld].

These nations exemplify how AI technologies can be seamlessly integrated into national security strategies.

Country Defense Strength Index: The Global Firepower ranking, which evaluates the defense capabilities of countries based on over 60 factors, including troop numbers, financial resources, logistical capabilities, and geographical considerations, assesses 145 countries [2025 Military Strength Ranking]. This ranking facilitates comparisons of defense strength across various categories. The findings indicate that effectively integrating AI technologies can greatly bolster a country's national security and defense capabilities, offering a strategic edge.

Table 1.

Country	Rank	Power Index
USA	1	0,0699
Russia	2	0,0702
China	3	0,0706
Israel	15	0,2261
Ukraine	20	0,3755
Greece	30	0,5337
Syria	64	1,2771

Defense Capabilities of Countries Among 145 Nations

The United States is at the top of the list, which makes sense given its enormous military budget, technological edge, and dominance in both naval and air power, along with its global reach. Russia comes in second, with military strength that is almost on par with the U.S., though the slight gap can be attributed to economic conditions, technological progress, and the impact of alliances. China also ranks highly due to its large military, sophisticated defense industry, and strategic influence.

Despite its small size, Israel (0.2261 score, 15th position) is recognized as a formidable defensive state, boasting advanced technologies, strong allies (notably the U.S.), and an effective military. Ukraine (0.3755 score, 20th position) currently maintains a robust position, particularly because of the ongoing conflict in recent years. Its military strength index has improved, although it still does not make it into the top 10.

Even as a NATO member, Greece (0.5337 score, 30th position) has a significantly lower military capability compared to the leading nations. Syria (1.2771 score, 64th position) is considerably weaker, a situation that can be attributed to years of civil war, economic turmoil, and limited military resources.

It can be concluded that the U.S., Russia, and China have nearly equal military strength, fueled by substantial technological advancements and large defense budgets. Israel and Ukraine possess significant military potential but lag behind the top nations. Greece and Syria do not have the same level of resources, which restricts their defensive capabilities.

This ranking illustrates that the global distribution of military power is influenced by both economic strength and advancements in military technology, as well as diplomatic relationships.

Conclusion

This article presents a scientific novelty that examines the intersection of artificial intelligence (AI) and national security. It provides a forward-looking analysis of how AI integration can revolutionize the defense sector by enhancing decision-making efficiency, improving threat detection

accuracy, refining surveillance mechanisms, and boosting the overall coordination of military operations.

This research is innovative for several key reasons:

- **Adapting AI Applications to Different Countries' Defense Needs:** While global discussions often center on technologically advanced nations like the U.S., China, and Russia, this article investigates how AI can be beneficial for countries with smaller or medium military and technological capabilities. It emphasizes the role of AI in cybersecurity, hybrid warfare, and autonomous surveillance systems, considering the unique challenges and opportunities faced by each nation.
- **Enhancing Strategic Planning Through AI:** The article illustrates how artificial intelligence can enhance defense strategic planning by analyzing complex data, modeling various conflict scenarios, and offering actionable insights. This method can enable a more flexible and rapid response to both traditional and emerging threats while ensuring resources are used efficiently.
- **Interdisciplinary Approach to AI and Defense:** The article adopts an interdisciplinary perspective, merging defense strategy, data science, and international law to tackle the ethical and practical challenges of AI integration. It pays special attention to ensuring that AI usage aligns with international humanitarian law principles and geopolitical realities.
- **Need for Infrastructure and Human Capital Development:** The research highlights the need for infrastructure and human resource development for effective AI integration. It suggests collaborative strategies among governments, academic institutions, and the private tech sector to lay the groundwork for training specialists and enhancing technological capabilities.

AI has the potential to enhance national security standards, making them more adaptable, predictive, and technologically advanced. To realize this potential, it is essential to create policies and strategies that strike a balance between innovation, security, and adherence to international norms.

The use of artificial intelligence in national security presents significant opportunities for a country's defense systems. It improves threat detection, automates surveillance and reconnaissance, and aids in strategic decision-making. AI can greatly boost defense efficiency by delivering real-time intelligence and enabling rapid response capabilities [Հովհաննիսյան]:

Integrating AI necessitates careful planning, substantial investments in infrastructure, and the cultivation of human talent. Many nations can draw lessons from the experiences of countries like the United States, China, and Russia, which have made AI technology development a priority. The insights gained from these leading nations can help tailor AI technologies to meet specific defense requirements [Calo et al].

However, despite the promise of AI, its implementation in the defense sector may encounter various challenges.

Technical and Infrastructure Limitations: The effective use of artificial intelligence systems relies on advanced technological infrastructure, including powerful computing resources, data storage capabilities, and access to high-quality datasets. Many countries may need substantial upgrades to their technological frameworks to effectively integrate AI into their defense sectors. Furthermore, AI systems require extensive data processing and management capabilities, necessitating investments in advanced solutions for data collection, processing, and management [Johnson, 1-23].

Human Capital and Expertise: Another significant challenge is the lack of skilled professionals needed to implement AI technologies. AI is a highly specialized field that demands experts who can design, deploy, and maintain complex systems. To cultivate such specialists,

collaboration among academic institutions, private tech companies, and international partners is essential to create a reliable pool of talented professionals.

Ethical and Legal Concerns: The use of AI in military operations also raises ethical and legal concerns. Autonomous systems may participate in decision-making processes, including critical decisions that are not directly overseen by humans. It is vital to thoroughly examine the implications of employing such technologies and ensure their use aligns with international humanitarian law and the rules of armed conflict [Brundage].

Looking ahead, ongoing collaboration between governments, private tech companies, and international organizations will be crucial to fully leverage the potential of AI in national security. Additionally, as AI technologies continue to advance, it is important to develop flexible and adaptive strategies to embrace innovations that can significantly improve defense efficiency. Addressing these challenges and ensuring the responsible integration of AI can profoundly enhance each country's defense capabilities and security.

References

1. Allen Greg, Taniel Chan, Artificial Intelligence and National Security. Belfer Center for Science and International Affairs, Harvard Kennedy School, 2017, 132 p.,
2. Allan Friedman, Peter W. Singer, Cybersecurity and Cyberwar: What Everyone Needs to Know, January 3, 2014, Oxford University Press, pp. 110-156,
3. Andress J., S. Winterfeld, The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. 2012, Publisher by Syngress, 169 p.,
4. Angelina N., Cybersecurity and International Relations, 2024, Research Paper, 26 p.,
5. Andrew P. Williams Paul D., Scharre, Autonomous Systems: Issues for Defense Policymakers. Printed by: NATO Communications and Information Agency, 2021, 21 p.
6. Arquilla J., & Ronfeldt D., Swarming and the Future of Conflict. RAND Corporation, 2020, National Defense Research Institute, 103 p.,
7. Bostrom N., Superintelligence: Paths, Dangers, Strategies. Oxford University Press, 2014, pp. 1-4,
8. Brundage M., Shahar Avin, et al, The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation, Oxford University Press, 2018, 101 p.,
9. Calo R., Froomkin M., & Kerr I., Robot Law. Edward Elgar Publishing, 2016, 424 p.,
10. Davenport T., & Kirby J., Only Humans Need Apply: Winners and Losers in the Age of Smart Machines. Publisher: Harper Business, 2016, 288 p.,
11. Gertz B., War and Peace in the Information Age, Threshold Editions, 2017, 384 p.,
12. Goodman M., Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About It. Publisher: Doubleday, 2015, 464 p.,
13. Herbert Lin, Cyber Threats and Nuclear Weapons. Stanford University Press, 2021, 216 p.,
14. Horowitz M. C., Artificial Intelligence and the Future of Warfare, Research Paper, 2018, pp. 1-18,
15. James Johnson, Artificial intelligence & future warfare: implications for international security, 2019, Defense and Security Analysis 35(2): pp.1-23.
16. Kissinger H., World Order: Reflections on the Character of Nations and the Course of History, Penguin Books, 2018, 432 p.,
17. Knake R., Cyber War: The Next Threat to National Security and What to Do About It, Publisher: Ecco HarperCollins, 2011, pp.458-460,

18. Lin P., Robot Ethics: The Ethical and Social Implications of Robotics. Massachusetts Institute of Technology Press, 2014, 27 p.,
19. McFate S., The New Rules of War: Victory in the Age of Durable Disorder, William Morrow Paperbacks, 2019, 336 p.,
20. Payne K., Artificial Intelligence: A Revolution in Strategic Affairs?, 2018, pp. 7-32,
21. Rid T., Cyber War Will Not Take Place, Journal of Strategic Studies, 2013, 30 p.,
22. Russell S. & Norvig P., Artificial Intelligence: A Modern Approach (4th Edition), Publisher: Pearson, 2020, 1166 p.
23. Sarah Bankins, The Ethical Implications of Artificial Intelligence (AI) For Meaningful Work, Journal of Business Ethics, 2023, pp. 725-740,
24. Tansley J., István S., AI in Military Applications: Opportunities and Challenges. Land Forces Academy Review, 2021, pp. 157-165,
25. Turobov A., Artificial Intelligence and Security: Transformation and Consistency, 2022, pp. 1-41,
26. Walsh T., Machines that Think: The Future of Artificial Intelligence, Publisher: Prometheus Books. 2018, 336 p.,
27. Webb A., The Big Nine: How the Tech Titans and Their Thinking Machines Could Warp Humanity, Publisher: PublicAffairs, 2019, 336 p.,
28. Weiner A., Cyber Power: The Strategic Use of Technology in National Defense. Harvard University Press, 2020, 85 p.,
29. 2025 Military Strength Ranking, https://www.globalfirepower.com/countries-listing.php, (March 10, 2025)
30. Մկրտչյան Հ., Հայաստանում Արհեստական Բանականության Օգտագործման Հնարավորությունները Ազգային Անվտանգության Համար, Տիգրան Մեծ հրատարակչություն, 2021, էջ 5-10:
31. Հովհաննիսյան Գ., Արհեստական Բանականության Զարգացումը և Ազգային Անվտանգությունը Հայաստանում, ԵՊՀ հրատարակչություն, 2017, էջ 16-18:

Ներկայացվել է՝ 12.03.2025թ.
Ուղարկվել է գրախոսման՝ 06.05.2025թ.