Testimony of Haniyeh Mahmoudian, Global AI Ethicist

Before the

U.S. House Armed and Services Committee

Subcommittee on Cyber, Information Technologies, and Innovation

Hearing on "Machine Learning and Human Warfare: Artificial Intelligence on the Battlefield"

Tuesday, July 18, 2023

Chair Gallagher, Ranking member Khanna, and the distinguished members of the Cyber, Information Technologies, and Innovation subcommittee:

Thank you for the opportunity to testify before the subcommittee on the critical issue of Machine Learning and Human Warfare: Artificial Intelligence on the Battlefield. My name is Dr. Haniyeh Mahmoudian, and I am an AI Ethicist. In my individual capacity, I am an advisory member of the National Artificial Intelligence Advisory Committee (NAIAC) and co-chair the AI future Working Group. I am currently employed as a Global AI ethicist at DataRobot. I am testifying today in my individual capacity and not on behalf of any entity or organization. My testimony and views I express today are my own and should not be contributed to any other organization, entity, or individuals.

My background is in machine learning and artificial intelligence (AI) and in the past five years, my focus has been on AI bias and more broadly responsible AI. In my capacity as a Global AI Ethicist at DataRobot, in addition to providing educational support on AI ethics, I have worked with engineering and product teams to incorporate principles of trustworthy AI into the product. The importance of incorporation of AI ethics and responsible AI frameworks in AI utilized in warfare cannot be overstated. Therefore, I am grateful for the committee's attention to AI governance and responsible use of AI in the military and for inviting me to share my insights and expertise.

Importance of AI

AI holds immense potential and is poised to revolutionize nearly every facet of our lives, from how we work, communicate, to how we solve complex problems. It's a field that has grown exponentially in recent years, underpinned by advances in computational power, data availability, and innovations in machine learning algorithms..

AI is increasingly becoming an essential component of modern military strategies and operations, holding the potential to revolutionize how nations prepare for and conduct military missions. AI's influence is seen across a broad spectrum of military applications, each profoundly impacting operational efficiency and decision-making.

In the realm of cybersecurity, AI can help protect military networks and systems against increasingly sophisticated cyber threats. By continually learning from new data, AI can identify and respond to novel cyber-attacks more effectively than traditional systems. Furthermore, AI can assist in offensive cybersecurity operations, identifying vulnerabilities in enemy networks and systems.

AI's role in predictive maintenance is another noteworthy application. By analyzing data from military equipment, AI can predict when parts might fail and recommend proactive

maintenance, improving the reliability and readiness of military hardware. This can lead to cost savings and increased operational efficiency by minimizing unplanned downtime and preventing catastrophic failures.

AI also plays a crucial role in injury prediction and prevention among military personnel. Using data gathered from sensors worn by soldiers and machine learning algorithms, AI can effectively track real-time physical fatigue and potential injuries. This could aid in prevention of musculoskeletal injuries (MSK) and other bodily injuries. According to the U.S. Army Public Health Center, musculoskeletal injuries among active-duty soldiers result in over 10 million restricted-duty days each year, and constitute more than 70% of the medically non-deployable population. These types of injuries, along with their subsequent impacts, are a major reason for medical disability and consequent discharge from service.[1]

Text analysis is another area where AI can rapidly review and analyze intelligence reports, swiftly translating or decoding local or coded languages. It can detect trends, specific words, or phrases and extract key information rapidly. AI's ability to process and analyze vast amounts of data from various sources surpasses human capacity. It helps identify patterns, detect real-time threats, and highlight only the most relevant information, enhancing the speed and effectiveness of military decision-making.

It is imperative that the United States expedite the adoption of AI to sustain our strategic advantage, especially in the military. While these benefits are significant, it is crucial to ensure that the use of AI in military contexts adheres to legal and ethical guidelines, particularly regarding decision-making in lethal operations. As AI continues to evolve, it will undoubtedly play a more prominent role in shaping the future of military strategy and operations.

Why Ethical and Responsible AI Matter

As technology has advanced, the ethical and moral considerations of its application have always been a topic of discussion. These concerns have intensified due to the swift progress in AI, its widespread adoption, and larger impact on our lives. In recent years, insufficient scrutiny and evaluation of AI systems, coupled with a limited comprehension of AI's potential adverse effects, have led to numerous instances where AI, despite being developed with noble intentions, ended up harming the vulnerable individuals and communities it was designed to help or inadvertently discriminated against marginalized groups. This suggests that considerations of AI Ethics have often been relegated to a secondary concern when building and deploying AI systems.

[1] https://militaryembedded.com/ai/machine-learning/using-sensors-and-ml-to-prevent-warfighter-injury

To fully leverage the power of AI, particularly in governmental applications such as the military, it's crucial to garner public trust by ensuring AI is effective, reliable, and ethically built and operated. This necessitates the establishment of ethical and responsible AI frameworks for the creation and implementation of AI systems. Such measures should protect civil liberties and rights, guarantee fairness, and instate a robust AI governance system with accountability at its core.

It is encouraging that the Department of Defense has taken initiatives to develop AI ethics principles that will apply to both combat and non-combat functions and assist the U.S. military in upholding legal, ethical, and policy commitments in the field of AI. As former Secretary Esper has remarked, "AI technology will change much about the battlefield of the future, but nothing will change America's steadfast commitment to responsible and lawful behavior. The adoption of AI ethical principles will enhance the department's commitment to upholding the highest ethical standards as outlined in the DOD AI Strategy, while embracing the U.S. military's strong history of applying rigorous testing and fielding standards for technology innovations"[2].

Building Trust into AI

Responsible AI encompasses the ethical approach to designing, building, and deploying AI systems. Its aim is to utilize AI in a manner that prioritizes safety, trustworthiness, transparency, and more broadly ethical considerations. Embracing responsible AI practices promotes transparency and addresses concerns related to AI bias, thereby ensuring a more equitable and reliable application of AI technology.

Implementing responsible AI frameworks and fostering trust in AI systems requires consideration of people, processes, and technology. Various stakeholders participate in the AI lifecycle. It is crucial that individuals involved in the process of building, deploying, and using AI systems have AI literacy. The AI Initiative Act of 2020 (NAIIA) instructs the President, via the National AI Initiative Office, to continually uphold AI research and development. This includes promoting AI education and worker training schemes, endorsing interdisciplinary AI study and educational programs, and arranging and coordinating Federal interagency AI efforts[3]. "The National AI Initiative Act calls for agencies to prioritize fellowship and training programs to help American workers gain AI-relevant skills through skills programs, fellowships, and education in computer science and other growing Science, Technology, Engineering, and Math (STEM) fields"[4]. In Addition, to ensure the responsible use of AI, stakeholders should be provided with educational resources relevant to their roles and responsibilities on AI ethics and

[2] DOD Adopts Ethical Principles for Artificial Intelligence > U.S. Department of Defense > Release
[3] ABOUT - National Artificial Intelligence Initiative (ai.gov)
[4] EDUCATION AND TRAINING - National Artificial Intelligence Initiative

practical approach to apply the Department of Defense's AI ethics principles in their workflow and use cases.

AI governance refers to the system of rules, policies, and procedures designed to manage and oversee the development, deployment, and ongoing use of AI technologies. It's an approach to regulate the lifecycle of AI, which includes stages such as data collection and processing, model development, training and testing, deployment, and continuous monitoring. Implementing an AI governance framework and standardizing the AI lifecycle can help agencies work more effectively, and to proactively address the concerns inherent in their operations. AI governance is critical for several reasons. It establishes a structure for ethical AI use, ensuring that the development and application of AI technologies are aligned with societal values and norms, manages risk, and mitigates potential harm. AI can have unintended consequences, and strong governance can provide processes to evaluate, monitor, and mitigate these risks. In this regard, the National Institute of Standards and Technology (NIST) has made notable contributions by developing AI risk management frameworks and has recently released its AI Risk Management Framework 1.0[5]. In its first report, the National AI Advisory Committee (NAIAC) recommends that the White House encourage Federal agencies to implement NIST or similar processes to address risks associated with AI in its lifecycle with appropriate evaluations and monitoring[6]. In addition, governance ensures compliance with laws and regulations and promotes accountability and transparency. It ensures there are clear lines of responsibility for AI systems and their outcomes, and that these systems and their decision-making processes are transparent and explainable. In essence, AI governance can serve as a roadmap for the Department of Defense, guiding them on how to responsibly develop and use AI while managing risks and ensuring public trust. As the use of AI grows and evolves, the importance of robust AI governance will only continue to increase.

Human-centered design is a crucial principle in developing technology, including AI systems. This approach places the needs, behaviors, and experiences of people at the heart of the design process, ensuring that the resulting technology is accessible, understandable, and beneficial to its users. The technology should be developed in a way that respects and protects human rights, privacy, and dignity. This means that AI systems should be designed to operate transparently, so that users understand how decisions are being made, and to prevent and mitigate any potential harm or bias. In addition, the technology should be developed with robust oversight and control mechanisms. This involves the capability to monitor AI systems effectively, to track their decision-making processes, and to intervene or correct the system's course as needed. Human-centered AI technologies should support continuous learning and adaptation. Given that AI technologies are rapidly evolving, the design of these systems should facilitate ongoing

[5] AI Risk Management Framework | NIST
[6] National Artificial Intelligence Advisory Committee Year 1 Report 2023 (ai.gov)

updates and improvements based on user feedback, changing societal norms, and legal and regulatory developments. This also includes being able to adapt to changes in the environment or context in which the AI system operates. It is worth noting that methods and techniques required to ensure proper implementation of human-centered design such as the identification and mitigation of bias, the explanation of AI's decision making process, privacy preserving techniques, and continuous monitoring already exist today. But these methods have not been widely employed in AI development and deployment workflows.

Conclusion

Mr. Chairman, and members of the subcommittee, AI holds transformative potential across sectors. In the military, AI plays critical roles in cybersecurity, predictive maintenance, injury prediction and prevention, text analysis, intelligence, surveillance and reconnaissance (ISR), and autonomous systems. These applications enhance operational efficiency and decision-making while minimizing risk and downtime.

However, alongside these benefits, the use of AI raises important ethical and moral considerations. Hence, it is vital to establish practical ethical and responsible AI frameworks that ensure effectiveness, reliability, and ethical use, especially in high-stake applications in the military.

Investment in AI literacy for military personnel at all levels is a key step to ensuring responsible use of AI. It is critical to educate different stakeholders about AI and AI ethics. To successfully adopt and leverage AI at scale, the Department of Defense should implement a comprehensive AI governance framework and adapt risk management processes to manage and mitigate the risks associated with AI. Moreover, the technology implemented or acquired by the Department of Defense should be designed to support people and processes, including considerations for explainable AI and risk mitigation tools.

One of the challenges in adopting AI in the government, in particular the Department of Defense, is the slow procurement process. AI is an evolving space and long procurement cycles and delays can lead to obsolete AI tools that will require retraining due to changes in data over time. Therefore, it is paramount to expedite the procurement cycle while ensuring proper evaluation of the AI tools with robust governance processes.