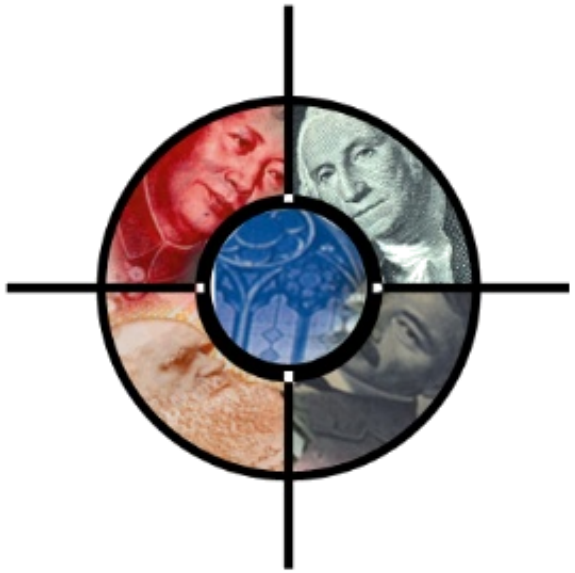
AI and National Security

Jan 4, 2020



Schulte-Research

Paul Schulte, MA, MALD
Paul@schulte-research.com
www.schulte-research.com
(+852) 9705 0777

Mirza Muhammad
mirza@schulte-research.com

Introduction

No.	How important is being at the forefront of AI & what are the implications of using AI for defense
1	Chinese Govt stated that it will take the lead in AI by 2030, Russian govt also very keen in being the leader as it understands that the leader in this field will "rule the world", U.S. released a statement in 2018 where it admitted that AI is key in ensuring success in warfare.
2	U.S. military already working on incorporating AI with its combat tech; Project Maven – Uses AI to identify insurgents in Iraq & Syria. What are the limits of using AI in warfare?
3	AI became prevalent and a topic of keen interest after 2010 due to: (1) the availability of "big data" sources, (2) improvements to machine learning approaches, and (3) increases in computer processing power.
4	Current AI is Narrow AI: machine learning, which involves statistical algorithms that replicate human cognitive tasks by deriving their own procedures through analysis of large training data sets.
5	VCs had invested about 8 billion in AI in 2018 and the Department of Defense has also increased investments in this field from $600 million in 2016 to $927 million by 2020.

Issues for Congress

No.	Why is AI apt to be used in National Security
1	First, AI has the potential to be integrated across a variety of applications, improving the so-called "Internet of Things".
2	Secondly, AI applications are dual-use, meaning they have both military and civil application.
3	Thirdly, AI is a relatively transparent enabling capability, meaning that its integration into a product may not be immediately recognizable
4	Congress's subcommittee chair called for a "national level effort" to preserve a technological edge in the field of AI as "this is not something the Pentagon can fix by itself.".
5	Initiatives by Congress to address issues relating to AI: • a Joint Artificial Intelligence Center (JAIC) - "coordinate the efforts of the Department to develop, mature, and transition artificial intelligence technologies into operational use" • strategic roadmap for AI development and fielding, as well as guidance on "appropriate ethical, legal, and other policies for the Department governing. • National Security Commission on Artificial Intelligence to conduct a comprehensive assessment of militarily relevant AI technologies and provide recommendations for strengthening U.S. competitiveness
6	Lack of Funding: Lieutenant General John Shanahan, the director of the JAIC stated that a major issue impeding AI advancements and competitiveness in comparison to competitor countries would be a lack in funding. Experts argue that the $1.75 billion six-year budget and the Defense Advanced Research Projects Agency's (DARPA's) $2 billion multiyear investment in over 20 AI programs is still insufficient and will cause "innovation deficit".

Issues for Congress

No.	Why is AI apt to be used in National Security
7	Other issues: • National security community also argue that it would not be a responsible use of taxpayer money to duplicate efforts devoted to AI R&D in the commercial sector when companies take products 90% of the way to a useable military application. • Lack of an exact definition for AI and hence investments into AI is vague and not very specific. • Pace of AI technology development is moving faster than the speed of policy implementation. • A key question that surrounded the use of AI in wartime was "What role do we want humans to play in wartime decision making?. What are the ethical boundaries of using fully automated machinery during wartimes?
8	Protecting the AI innovations of the U.S.: • Chinese government is reported to be aggressively pursuing AI investments in the United States. • U.S. blocked a Chinese firm from acquiring Lattice Semiconductor, a U.S. company that manufactures chips that are a critical design element for AI technology.
9	Balance between data protection and AI exploration: • Much of this data is classified, access controlled, or otherwise protected on privacy grounds. However, for AI to be sustainable and 'better' it needs to run through and study countless data sets; as much as possible.
10	Safety:. • AI algorithms are vulnerable to bias, theft, and manipulation, particularly if the training data set is not adequately curated or protected
11	Increased training in intellectual property rights for acquisitions professionals and a pilot program for intellectual property valuation in the procurement process. This is to ensure companies are not hesitant in partnering with DOD over fears of losing intellectual property rights.

AI Applications for Defense

No.	Why is AI apt to be used in National Security
1	Intelligence, Surveillance, and Reconnaissance: • Project Maven team is incorporating computer vision and machine learning algorithms into intelligence collection cells that would comb through footage from uninhabited aerial vehicles and automatically identify hostile activity for targeting. • IARPA is sponsoring several AI research projects - developing algorithms for multilingual speech recognition and translation in noisy environments, geo-locating images without the associated metadata, fusing 2-D images to create 3-D models, and building tools to infer a building's function based on pattern-of-life analysis.
2	Logistics: • Use in Aircrafts - Instead of making repairs when an aircraft breaks or in accordance with standardized fleet-wide maintenance schedules, the Air Force is testing an AI-enabled approach that tailors maintenance schedules to the needs of individual aircrafts. • The Army's Logistics Support Activity will analyze shipping flows for repair parts distribution, attempting to determine the most time- and costefficient means to deliver supplies.
3	Cyberspace Operations: • Conventional cybersecurity tools look for historical matches to known malicious code, so hackers only have to modify small portions of that code to circumvent the defense. AI-enabled tools, on the other hand, can be trained to detect anomalies in broader patterns of network activity, thus presenting a more comprehensive and dynamic barrier to attack
4	Information Operations and "Deep Fakes": • deep fake technology could be used against the United States and U.S. allies to generate false news reports, influence public discourse, erode public trust, and attempt to blackmail diplomats. • Media Forensics (MediFor) project, which seeks to "automatically detect manipulations, provide detailed information about how these manipulations were performed, and reason about the overall integrity of visual media."

AI Applications for Defense

No.	Why is AI apt to be used in National Security
5	Command and Control: • Multi-Domain Command and Control (MDC2), which aims to centralize planning and execution of air, space, cyberspace, sea, and land-based operations. This is aimed at allowing "any sensor to provide data to any shooter from any service, ally, or partner … to achieve effects against any target."
6	Semi-autonomous and Autonomous Vehicles: • AI may enable the "loyal wingman" to accomplish tasks for its inhabited flight lead, such as jamming electronic threats or carrying extra weapons.
7	Lethal Autonomous Weapon Systems (LAWS): • A special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system. • General Paul Selva stated, "I do not think it is reasonable for us to put robots in charge of whether or not we take a human life."

Military AI Integration Challenges

No.	Why is AI apt to be used in National Security
1	Technology: • The military variant of a vehicle would need to be able to operate in locations where map data are comparatively poor and in which GPS positioning may be inoperable due to adversary jamming. Moreover, semiautonomous or autonomous military ground vehicles would likely need the ability to navigate off-road in rough terrain—a capability not inherent in most commercial vehicles
2	Process: • A failure rate deemed acceptable for a civilian AI application may be well outside of tolerances in a combat environment. • Commercial technology companies are also often reluctant to partner with DOD due to concerns about intellectual property and data rights
3	Personnel: • Challenges when it comes to recruiting and retaining personnel with expertise in AI due to research funding and salaries that significantly lag behind those of commercial companies. • DOD "would pay for advanced technical education in exchange for two days a month of training with government systems and two weeks a year for major exercises."
4	Culture: • 80% of participants rated the commercial technology community's relationship with DOD as poor or very poor.119 This was due to a number of factors, including process challenges, perceptions of mutual distrust, and differences between DOD and commercial incentive structures. • Companies are refusing to work with DOD due to ethical concerns over the government's use of AI in surveillance or weapon systems.