Written Testimony of Lieutenant General John (Jack) N.T. Shanahan (USAF, Ret.)
AI Insight Forum: National Security
Wednesday, December 6, 2023, 3:00 PM EST

Majority leader Schumer, Senators Rounds, Heinrich, and Young, thank you for the opportunity to participate in today's AI Insight Forum on National Security.

My testimony reflects my unique background as the only senior military officer responsible for standing up and leading two organizations in the DoD dedicated to fielding AI capabilities: Project Maven, also known as the Algorithmic Warfare Cross-Functional Team, and the DoD Joint AI Center (JAIC).

It is becoming increasingly evident that the unfolding Artificial Intelligence (AI) era holds the potential to rival the agrarian and industrial revolutions in terms of its long-term consequences, even as those consequences are still unknowable and, I contend, largely unpredictable. As a general-purpose enabling technology, AI is already exhibiting signs of its potential far-reaching impacts on national security and economic strength. What most distinguishes this era is the unprecedented pace of change, the breadth and depth of diffusion, and the rate of adoption of AI capabilities. All three characteristics are poised to continue accelerating for the foreseeable future.

A state that rapidly and comprehensively adopts AI is expected to gain significant, perhaps even decisive national security and economic advantages. Such states could wield considerable influence in shaping the global future. It is already evident that AI will fundamentally alter the landscape of warfare and impact national security on a grand scale. The geopolitical and geoeconomics ramifications are profound.

Despite the still-extensive gap between current capabilities and the desired future performance of AI-enabled systems, many of the world's militaries and intelligence services, led by the United States and China, are actively pursuing the integration of AI with the expectation that it will bring dramatic improvements in effectiveness and efficiency. The adoption of AI for military and intelligence is envisioned to generate substantial qualitative and temporal advantages over competitors and adversaries.

AI-enabled platforms, sensors, decision-support systems, and analytic tools are poised to play a pivotal role in future military and intelligence operations, spanning from undersea to outer space, across cyberspace and the electromagnetic spectrum, and for everything else in between to include back-office administrative functions. AI, in the forms of machine learning, deep learning, and generative AI, holds immense potential to accelerate information retrieval, analysis, and decision-making; sort through vast troves of data; automate dull, dirty, and dangerous tasks; uncover signals in noise; recognize patterns; identify anomalies; issue threat warnings; fuse data; discern vital correlations across all domains that might elude human perception; optimize logistics, medical support, and talent management; and help with operational planning at every level.

Ultimately, the aim should be for AI to assist humans in making more informed decisions and, where appropriate and feasible, for AI-enabled systems to take actions based on human-defined conditions. The latter potentially includes the employment of weapons.

The performance of Ukrainian forces against Russia provides an early indicator of how AI might shape future conflicts. This war offers persuasive evidence that the side that adapts the fastest, to include rapidly updating fielded software and AI models, stands to gain a battlespace advantage. Operations in Ukraine underscore another prevailing reality: for the foreseeable future, the DoD must grapple with the coexistence of so-called legacy hardware systems and cutting-edge AI capabilities. It is not AI or Javelins; it is AI and Javelins, and even AI in Javelins.

Ukraine provides a much-needed wakeup call. While not all lessons will apply equally to every future crisis and conflict, we ignore the technology-centric lessons of the Russia-Ukraine conflict at our peril. The trends are clear: smaller, smarter, cheaper, attritable, swarming or networked, self-sustaining, robust, and resilient systems. Moreover, once again quantity has a quality all of its own.

The DoD has made demonstrable progress on AI adoption during the six years since Project Maven was established. In general, the Department is moving faster, and DoD leaders have implemented myriad changes to accelerate AI integration. Despite some positive signs, however, the DoD and the rest of the national security enterprise continue to struggle to scale AI projects. This remains a vexing problem for the institutional bureaucracies of the federal government, which were built as industrial-age hardware organizations that are becoming progressively more sclerotic in today's software-centric digital age.

I present several recommendations to accelerate and scale AI across the DoD.

Techno-Economic Net Assessments. The national intelligence community and defense intelligence enterprise, in coordination with other federal Departments and Agencies, must allocate resources to develop comprehensive, continuously-updated techno-economic net assessments comparing the United States against China and Russia. These comparative assessments must include not only all critical elements of the AI stack along with corresponding funding levels, but also how the People's Liberation Army (PLA) and Russian military forces may be organizing differently to integrate AI into their forces, as well as their progress in developing new operational warfighting concepts based on the integration of AI and other disruptive technologies.

Digital modernization. The DoD and the rest of the federal government will never succeed in applying AI at scale without accelerating digital modernization of their respective organization's underlying information technology architecture and infrastructure, with a particular emphasis on data management. The JAIC's first Chief Technology Officer, Mr. Nand Mulchandani, and I co-wrote a paper titled *Software-Defined Warfare: Architecting the DoD's Transition to the Digital Age*. This paper, which

is based on commercial software industry best practices, provides a useful framework for the DoD's digital modernization.

Big bets. The study of warfare is a study of asymmetric technology advantage and disadvantage. It is time for the DoD to make bigger AI bets, or risk ending up on the wrong side of the asymmetry equation. The Small Business Innovation Research and Small Business Technology Transfer (SBIR/STTR) programs and others like them have been relatively successful for individual AI pilot projects, but AI funding levels across DoD neither match the rhetoric of Department leaders nor reflect the rapid pace of private sector AI advances. AI funding should be increased substantially, although the leaders of the military Services must demonstrate alignment between requested funding and the National Defense Strategy and the Data, Analytics, and AI Adoption Strategy.

Program of Record Integration. As we learned with Project Maven and other AI projects at the JAIC/CDAO, there are inherent limitations in adding AI as a 'sidecar' to legacy weapon and decision support systems. To the maximum extent possible and where it makes sense operationally, the military Services should integrate AI requirements into programs of record as early as possible during system development, via the System Program Offices (SPO) and Program Executive Officers (PEO).

Chief Digital and AI Office (CDAO). Combining the JAIC, Defense Digital Service (DDS), and OSD Chief Data Officer (CDO) was a laudable initiative. It is now worth reviewing the CDAO's mandate, with the goal to reassess the balance of effort between technology integration and provision of AI enablers that support the military Services and combatant commands. Regardless of any adjustments to this ratio, I recommend that the CDAO prioritize solving the combatant commands' top problems.

Government-industry-academia cooperation. The future success of America's national security enterprise will depend on forging and maintaining stronger bonds between the government, private industry, and academia, and expanding public-private partnerships. With limited exceptions, the DoD should adopt a 'commercial first' approach to adopting emerging and disruptive technologies. The goal should be rapid adaptation, not trying to recreate what already exists in industry. DoD leaders should strive not only to accelerate adoption of capabilities offered by the nation's best startup and established technology companies, but also foster greater cooperation between these national security innovation network companies and traditional Defense Industrial Base (DIB) companies. These companies have certain inherent advantages – such as personnel and facility security clearances, understanding of the government's contracting and acquisition processes, and the ability to produce weapon systems at scale – that will be indispensable in accelerating and scaling AI adoption across the Department.

Workforce development. Workforce development comprises training, education, certification, and talent management. Since there are already many initiatives underway designed to foster government-wide AI education and training, I will only underscore that AI-related education and training need to begin at accession, and continue through

separation or retirement for all personnel – from general/flag officers and senior civilian executives all the way down to entry-level personnel. The JAIC's congressionally-directed *2020 Department of Defense AI Education Strategy* provides an excellent framework for Department-wide AI education and training. Department leaders should mandate career-long tracking and management of personnel with AI skills, and accelerate and scale initiatives that place experts from commercial technology companies into the federal government (and vice versa).

Reorganization. While individual technologies may play crucial roles in wartime, the greatest advantages will be reaped by military forces that reorganize bureaucratically to effectively assimilate emerging and disruptive technologies. This transformation will include the development of innovative warfighting operational concepts that revolve around AI-enabled systems. The Joint Staff's Joint Warfighting Concept should serve as a guide for the Services and combatant commands to consider how to organize differently for an AI-enabled future, and for evaluating new organizational concepts through exercises, experiments, and wargames. These should progress from small-scale single-Service events, through large-scale joint and combined exercises and wargames. I encourage members of the Senate and House Armed Services Committees to invite DoD leaders to discuss potential new organizational designs.

Human-Machine Teaming. Optimizing the integration of humans and AI-enabled machines, which in turn depends on redesigning the interfaces between humans and machines and recalibrating human and machine roles and responsibilities, will be one of the most important and defining features of future military operations in the digital age. The DoD will have to change how systems are designed and developed, how humans are trained to work with 'smart' machines that are unlike any previous military systems, and how AI-enabled systems adapt to human interaction and intervention. The failure to prioritize user interface/user experience (UI/UX) in many legacy military hardware and software, which in the past might have been considered an annoyance rather than a systemic shortcoming, will become a debilitating condition in a future environment characterized by AI-enabled systems whose maximum benefits can only be achieved through dedication to the design of superior human-system integration.

Despite the hype and allure, AI will not miraculously dissipate the fog and friction of crisis and conflict. War will forever be characterized by uncertainty, ambiguity, complexity, non-linearity, and chaos. In future conflicts, however, I contend that the advantage will go to those who understand how to optimize the integration of humans and smart machines. The proverbial military genius who uses AI effectively is likely to defeat the military genius who does not.

Risk acceptance. Understandably, the DoD has traditionally been a risk-averse organization. The current exponential pace of technological change is uncomfortable for many people. Yet in today's rapidly-changing, disruptive, and disorienting world, risk aversion leads down a path toward irrelevance and even obsolescence. DoD leaders should nurture a culture of adaptability and agility, and grow a new generation of tech-

savvy leaders who are comfortable operating in highly uncertain and amorphous environments. Risks will inevitably increase with exponential rates of change, but they can be managed through the concept of fielding minimum viable products (MVP), continuous interaction between developers, testers, and end-users, and by integration of new technologies in experiments, wargames, and exercises. Effective risk management depends on understanding risks, assessing those risks, and knowing who can accept what risks (and at what level). Future DoD leaders do not need to be technology experts, but they must have a greater understanding of AI's strengths, limitations, benefits, costs, and risks when integrated into military operations.

AI assurance. AI assurance combines the principles of test and evaluation (T&E), to include red teaming, and the tenets of responsible AI. It must be treated as an integral part of the entire AI lifecycle. While AI is viewed as software, test and evaluation is as important for AI-enabled systems as it is for any other DoD military hardware or software system. Or, at this early stage of AI development, even more important. The is no inherent contradiction here: the national security enterprise can move at the speed of relevance while still adhering to the principles of AI assurance.

AI Dialogues. The rapid speed at which AI is advancing, often accompanied by exaggerated claims of its capabilities and significant misunderstandings and uncertainties regarding the actual state of other nations' military AI advancements, are fueling a dangerous cycle of mutual suspicion and misinterpretation. Leaders in China and the United States are convinced that the other side is rapidly developing AI-enabled military systems. Over time we can expect a mutually destabilizing environment, risking a rapid and uncontrolled escalatory spiral in which the United States and China continually strive for an advantage through the rushed deployment of AI technologies that may be untested, unproven, and potentially unsafe. It is imperative to prevent a reckless 'race to the bottom' in AI development. I advocate for pursuing focused AI dialogues between states, beginning with the United States and China, at both the informal Track II and formal Track I levels. These dialogues should involve defense representatives who possess hands-on experience and expertise with AI.

Finally, there are no shortcuts to integrating AI into national security. I firmly dismiss any notion that the United States has 'lost' the AI race against China. From my experiences, it is evident that China faces similar challenges to the DoD in scaling AI within the PLA. Still, the United States cannot afford to slow down. It is essential that our national security leaders sustain their unwavering commitment to advancing AI integration, despite the inevitable challenges and frustrations along the way, while diligently assessing and mitigating the diverse spectrum of risks involved.

I am optimistic that this forum, and similar initiatives, will play a pivotal role in maintaining America's status as the global leader in AI for national security. I express my gratitude to the members of this bipartisan AI Insight Forum for their efforts in bridging the critical gap between technology and policy, and for your willingness to implement decisive measures to accelerate the widespread adoption of AI for national security.