Booz
Allen®

Written Statement for AI Insight Forum: National Security
Horacio Rozanski, CEO
Booz Allen Hamilton

December 6, 2023

Introduction

Thank you, Majority Leader Schumer, Senators Rounds, Heinrich, and Young for the opportunity to participate in the AI Insight Forum on National Security and address the transformational technology of AI and its impact on U.S. military capabilities.

Booz Allen is the leading provider of AI services to the federal government. We have decades of experience inserting new technologies into national priority missions. As AI continues evolving into a strategic opportunity for our nation, Booz Allen stands ready to meet the challenge as a proven U.S. government partner and innovation leader in AI.

Today, great power competition demands speed in the adoption of AI across every facet of the U.S. national security ecosystem. We must balance technological advancement with ethical considerations, ensuring that AI serves the interests of our nation while safeguarding our fundamental values. Booz Allen is working every day to move faster as we bring trusted AI solutions and other technologies to our nation's highest priority national security missions, at the scale and speed of relevance.

Through our work, we see three key takeaways related to the transformative power of AI on our nation's military capabilities.

First, there is no question that national security applications must utilize algorithms. More classical static algorithms have been embedded in defense systems for at least a century. Examples include: munitions (land mines), weapon systems (missiles), and intelligence (keyword searches). Today, the rise of AI has introduced more powerful dynamic algorithms to the national security landscape. Dynamic algorithms can learn and evolve by discovering patterns and making predictions. Thus, they can greatly accelerate decision making, and will be essential in defensive and offensive capabilities, especially with near-peer adversaries who are aggressively pursuing AI for national security objectives.

Second, AI doesn't operate in a vacuum. Its true potential is unleashed when paired with other technologies to amplify capabilities, identify anomalies, and accelerate transformational outcomes. In every corner of our technological landscape, the emerging implications of AI are vast and groundbreaking. For instance, AI is primed to boost the resilience and adaptability of cyber, space, and communications capabilities. The power is in 'AI&'. For example: AI&cyber; AI&space; AI&joint fires. The great opportunity in this family of technologies is that they can accelerate and amplify human cognitive processes through pattern discovery and information synthesis across a near-infinite set of inputs. This enables faster decision making and delegates the more routine tasks so humans can focus on judgement and creativity.

Third, the gap between the introduction of powerful new technologies and malicious exploitation is narrowing, and Adversarial AI is already here and real. Open-source intelligence shows that nation-states have successfully executed adversarial AI attacks against real AI models in the wild. We should expect these incidents and threat actors to multiply in both number and sophistication. Adversarial AI introduces five principal threats: Poisoning, Malware, Evasion, Inversion, and Theft. All five threat vectors work to either compromise AI models or exfiltrate sensitive information. And combined with the known and growing threat of Deepfakes – used to spread misinformation, manipulate public opinion, and impersonate public officials – this is an area of utmost importance to national security.

To effectively respond to both the opportunities and risks of AI, we need an all-of-nation approach. This requires changes to both the way the government and industry do business. The government must provide certainty of goals, resources, and incentives to enable the digital industrial base to best anticipate and meet the national security needs of the United States. Industry must transform how it will work together to leverage the best capabilities in support of our national security goals, especially to deliver secure scaled 'AI&' solutions that solve our nation's greatest challenges, at speed. This means industry needs to embrace more partnering, co-creating, and co-investing to develop and bring the best capabilities to bear in this perpetual race of techno-competition. This will unleash American industry to be an asymmetric advantage in great power competition.

We at Booz Allen understand this and have begun to reinvent ourselves to meet the mission.

Booz Allen's Commitment to Strengthening U.S. Leadership on AI

We are building the DoD's Data Foundation

DoD's Chief Digital and AI Officer (CDAO), Dr. Craig Martell, has continually stated that the Department must "get the data right" before it can effectively pursue delivering artificial intelligence. Booz Allen is privileged to play a key role in establishing the DoD's data foundation, through the management and integration of DoD's primary data platform, Advana. Critical to the recently released DoD Data, Analytics, and AI Adoption Strategy, Advana now hosts hundreds of authoritative data sources, delivers a scalable platform to >100,000 users across the Department, and serves hundreds of operational applications across the Pentagon and all 11 Combatant Commands, integrating data to power AI solutions for decision advantage. Advana is a national asset of strategic importance and is foundational to the DoD's AI journey.

We are focused on future technology at the intersection of mission, and transitioning AI capabilities from the lab to real-world operations

American industry – its depth, breadth, industriousness, and diversity – represents an asymmetric advantage in the great power competition. These very strengths mean that no one company can do this alone – nor should it. However, harnessing all of industry has proven difficult in the past due to challenges many companies experience in navigating procurement processes, understanding mission applications, and managing uncertainty and funding (particularly in the start-up community, where often only 1 in 10 survive). As such, Booz Allen has developed a robust technology scouting practice and venture capital arm to identify and accelerate new entrants into the digital industrial base, investing in promising companies that bridge critical capability gaps for our clients to integrate into mission solutions, while shepherding them through the "valley of death." With these and other technology partners we are charting entirely new tech and mission stacks to solve generational challenges with AI. As an example:

- Synthetaic – one of our corporate venture capital partners – found the "needle in the haystack" as it analyzed millions of square miles of satellite imagery to determine the path of the Chinese spy balloon in early 2023.
- To train the computer vision model, Synthetaic fed it a hand-drawn sketch of how the balloon likely appeared from satellite images; the model found the balloon in 2 minutes.
- From there, the learning began with the real satellite images and delivered 12 instances of the balloon, revealing both its origin and path as it transited the Pacific.

Combining the power of AI, space-based capabilities, innovation, and human expertise can be a game-changer for National Security.

Recommendations for Congress

The answer (to some questions) is, obviously, Generative AI

You will undoubtedly hear today about the amazing potential of Generative AI to impact America's National Security apparatus, and Booz Allen agrees with this fundamental premise. What Generative AI has done is to create a way for humans to program AI and receive feedback in a natural language format – unlocking the power of AI in a way that GUI unlocked the power of the PC. As a result, Generative AI has the potential to act as a force multiplier across a variety of agency missions and business operations. With organizations as large as U.S. Government agencies, even incremental productivity gains could yield billions of dollars of efficiencies on an annual basis. Congress should direct and fund both pilot and adoption activities like the CDAO's Task Force Lima to prioritize the use cases that are most ripe for application of this novel technology. Some of those include:

- **Administrative / Operations** – those tasks which are heavily manual and frequently repeated where Generative AI could augment government and contractor staff (e.g., Policy Review and Development, Security Classification Review).
- **Intelligence Analysis and Reporting** – augmentation and acceleration of the IC's intelligence analysis and reporting functions.
- **IT / Software Engineering** – acceleration of legacy code conversion and new code development through co-pilot capabilities which speed code creation, testing and deployment.
- **Command and Control (C2) Decision Support** – acceleration and enhancement of the DoD's C2 processes. Notably, this domain is not ready for deployment of this technology, but we should continue experimentation efforts like the CDAO's Global Information Dominance Experiment (GIDE) series.

Congress and U.S. Government agencies should continue to monitor the commercial industry for successful paths to organizational adoption of this technology, potentially soliciting RFIs to understand best practices and proven techniques to manage this transition most effectively.

New operational concepts must be prioritized

The emergent behavior that is produced by human-machine systems is one of the most critical – and underinvested – research priorities in national security. We must understand with clarity how these systems work, what capabilities and behavior will emerge as they learn and operate, and what specific actions or commands trigger these outcomes. And, most importantly for national security, we must understand both how to control these systems and leverage their maximum potential in operational scenarios. This is especially urgent for autonomous applications and warfighter augmentation. Congress should direct the cabinet level agencies to harness diverse research communities to develop new operational concepts for human-machine teams, including: behavioral scientists, human factors engineers, roboticists, and Responsible AI practitioners.

Test & Evaluation will be the biggest bottleneck in procurement of new AI-enabled systems

New technologies or operational concepts have always presented a challenge to the Test & Evaluation community, but AI and Autonomy are emerging as the most novel and complex ever seen. The gap between tinkering with, and the trustworthy deployment of, these capabilities is massive, and there is no easy checklist to help navigate this path. DoD Test & Evaluation entities need guidance, direction, and funding from Congress to organize for the coming wave of AI-enabled and autonomous systems that will require their approval for operational deployment.