University of Florida
AI Policy Guide #2

AI and National Security:

Barriers to Securing the Future

Damon L. Woodard

Director, Florida Institute for National Security
Professor, Electrical and Computer Engineering Department
University of Florida

AI and National Security:
Barriers to Securing the Future

Damon L. Woodard
Director, Florida Institute for National Security (FINS)

Executive Summary

Artificial Intelligence (AI) transforms national security by enhancing capabilities in intelligence analysis, cyber defense, autonomous operations, and strategic planning. As AI becomes an integral part of defense, intelligence, and homeland security efforts, it offers the potential to increase agility, improve decision-making, and respond more effectively to both conventional and non-traditional threats. However, the path to realizing this potential is obstructed by significant technical, operational, ethical, and governance challenges.

This report identifies four critical barriers to the responsible adoption of AI in national security. First, AI systems are often hampered by poor data quality, limited interoperability, and a lack of robustness in unpredictable environments. Second, there are persistent difficulties in integrating AI tools into legacy systems and cultivating a skilled national security workforce capable of managing AI technologies. Third, the ethical and legal implications of deploying AI, especially in surveillance and autonomous systems, necessitate stronger accountability mechanisms and clearer legal frameworks. Fourth, the fragmented nature of current AI governance across federal agencies impedes coordination and risks inconsistent implementation, both domestically and internationally.

To address these challenges, the report outlines a set of interlocking policy recommendations. These include investing in secure and scalable technical infrastructure, reforming acquisition pathways to support agile development, expanding AI-specific training and workforce pipelines, institutionalizing rigorous ethical and legal review processes, and creating unified governance structures supported by international cooperation. Together, these actions will ensure that the United States can safely and effectively integrate AI into its national security enterprise while upholding democratic principles and maintaining global leadership.

Overview

Artificial Intelligence (AI) is rapidly becoming a central component of national security strategy, fundamentally reshaping how defense, intelligence, and homeland security institutions plan and execute operations. The integration of AI into national security missions enables more agile, data-driven, and predictive capabilities, enhancing the responsiveness and efficiency of government agencies. From surveillance and reconnaissance to logistics optimization and cyber defense, AI-driven systems are already being used to support critical functions, thereby transforming how threats are detected, analyzed, and addressed.

Across the national security landscape, foundational AI technologies, including deep learning, natural language processing, computer vision, and large language models, are being deployed in ways that enhance decision-making and situational awareness. These tools are being used to enhance intelligence analysis,

detect cyber threats, enable autonomous systems, and support strategic scenario planning. AI is also influencing domains beyond traditional military and intelligence contexts, including infrastructure resilience, disaster response, and public health security. This broad integration reflects a growing consensus that AI is no longer an emerging technology of the future; it is now a critical enabler of national defense and public safety.

As the pace of AI development continues to accelerate, national security stakeholders are embracing its potential to optimize resource allocation, enhance operational readiness, and respond more effectively to an increasingly diverse range of threats. These threats include not only conventional military risks but also asymmetric and non-traditional challenges such as cyberattacks, misinformation campaigns, and climate-induced disasters. However, despite the significant promise of AI, its full realization within the national security enterprise remains hindered by a range of interrelated barriers. These include technical limitations, institutional inertia, legal and ethical concerns, and a lack of cohesive governance structures. The following assessment examines these challenges in greater depth, laying the groundwork for a set of policy recommendations designed to ensure the safe, responsible, and effective use of AI in national security.

Assessment

While artificial intelligence offers transformative potential for enhancing national security capabilities, its adoption and operationalization across defense, intelligence, and civilian agencies has been inconsistent and fraught with challenges. These difficulties are not merely technical; they also reflect deeper organizational, strategic, and societal issues that must be addressed to ensure that AI tools can be deployed in ways that are both mission-effective and ethically sound.

Technical Foundations Require Strengthening

The successful deployment of AI systems in national security contexts is heavily dependent on the availability, quality, and reliability of the data used to train and operate these systems. However, mission-relevant data is often fragmented across different agencies, stored in incompatible formats, or restricted by classification levels that impede access and sharing. This fragmentation significantly reduces the utility of data for training robust and generalizable AI models. When AI systems are deployed in environments that differ substantially from their training conditions, performance often degrades, leading to unpredictable or suboptimal outcomes.

In addition to data challenges, many AI models exhibit poor reliability under operational stress. These systems are vulnerable to performance failures, particularly in contested or rapidly changing environments where latency, bandwidth constraints, and limited computational resources are prevalent. Furthermore, a lack of explainability in many AI models complicates efforts to validate their outputs, identify the sources of errors, or build user trust. Without a clear understanding of how and why an AI system produces a given result, operators may be hesitant to rely on it in critical missions. Addressing these issues requires significant investment in data infrastructure, algorithmic robustness, and system transparency.

Operational and Workforce Integration Remains Uneven

Translating AI research and demonstration projects into fully operational capabilities has proven to be a significant hurdle. One of the most persistent barriers is the difficulty of integrating AI systems into existing platforms and workflows. Many national security organizations continue to rely on legacy infrastructure and software environments that are not conducive to the seamless deployment of modern AI technologies.

Security requirements, software incompatibilities, and procedural complexities often delay or derail integration efforts, even when the AI tools themselves perform well in testing.

The challenge is compounded by a shortage of technical talent within the federal workforce. AI professionals are in high demand across all sectors, and national security agencies face stiff competition from private industry, where compensation packages and work environments are often more attractive. Even when skilled personnel are hired, bureaucratic structures and risk-averse cultures can limit their ability to innovate or influence strategic decisions. In addition to hiring challenges, there is a pressing need to improve AI literacy among policymakers, military officers, and operational staff. Ensuring that decision-makers understand the capabilities, limitations, and appropriate uses of AI is essential for effective integration.

Ethical and Legal Safeguards Need Reinforcement

The deployment of AI in national security contexts raises significant ethical and legal questions that must be addressed to preserve public trust and compliance with democratic norms. The use of autonomous systems, AI-enabled surveillance, and predictive analytics requires careful consideration of their potential impacts on civil liberties, privacy, and human rights. While the Department of Defense has taken essential steps in articulating ethical principles for AI, the practical implementation of these principles across the wide range of national security operations remains uneven.

Concerns about algorithmic bias, lack of transparency, and the phenomenon of automation bias highlight the importance of maintaining human oversight and accountability. Misclassifications by AI systems could result in the targeting of innocent individuals, misidentification of threats, or flawed resource allocation decisions. To mitigate these risks, robust ethical governance structures must be established. These should include mandatory impact assessments, independent oversight mechanisms, rigorous testing procedures, and formal processes for reviewing, pausing, or terminating AI systems that pose unacceptable risks. Active engagement with civil society organizations can also help ensure that public interests and values are adequately represented in the development and deployment of AI technologies.

Governance and Strategy Require Greater Cohesion

The current approach to AI governance within the national security sector is highly decentralized, with different agencies pursuing independent initiatives, strategies, and standards. While decentralization can foster innovation, it also introduces challenges related to coordination, interoperability, and consistency. Without a unified governance framework, agencies risk duplicating efforts, applying inconsistent standards, and overlooking cross-cutting risks. This fragmentation undermines the potential for AI systems to be effectively scaled and trusted across different parts of the national security enterprise.

Internationally, the United States faces growing pressure to lead in establishing global norms for the development and use of AI in military and security contexts. Strategic competitors such as China are aggressively pursuing AI capabilities, often without the same level of ethical or legal restraint. This competitive environment may incentivize rapid deployment at the expense of safety and accountability. To address this, the United States must play a proactive role in building international coalitions, shaping multilateral agreements, and supporting joint research initiatives with allies. Establishing clear standards for the lawful and ethical use of AI, both domestically and internationally, will be crucial to maintaining strategic stability and global leadership.

Policy Recommendations to Advance Responsible AI Adoption

The United States must adopt a strategic policy to maximize the benefits of AI and minimize its risks. The following recommendations are designed to address the challenges outlined in the previous section and ensure that AI serves as a force multiplier for national security without compromising democratic principles.

- **Strengthen Technical Infrastructure and Data Foundations**

  The federal government should prioritize the development of secure, interoperable, and mission-relevant data ecosystems that support both classified and unclassified operations. Investments in shared data repositories, standardized data formats, and data labeling protocols are crucial for enhancing the quality and accessibility of training data. Efforts should also focus on expanding access to scalable computer resources through the deployment of cloud and edge computing platforms tailored to national security use cases. In parallel, dedicated test and simulation environments must be created to evaluate AI systems under realistic operational conditions. These environments should facilitate stress testing, adversarial analysis, and red teaming to identify vulnerabilities and ensure resilience. Research funding should be directed toward the development of explainable, energy-efficient, and context-aware AI models that can operate in resource-constrained environments.

- **Accelerate Operational Integration and Workforce Development**

  To transition research innovations to practical use, modernize acquisition processes for agile development and rapid prototyping. Provide AI pilot projects structured pathways for scale-up, including funding, technical support, and performance evaluation criteria. Cross-agency innovation hubs and public-private partnerships can facilitate knowledge sharing and accelerate the adoption of innovative solutions Building a skilled and diverse national security AI workforce is equally critical. This requires the expansion of AI-specific fellowships, scholarships, and rotational programs targeting military personnel, intelligence analysts, law enforcement officers, and emergency responders. Professional development curricula should include instruction on AI ethics, human-machine teaming, and operational risk management. Partnerships with historically underrepresented institutions, community colleges, and technical training programs will help broaden the talent pipeline and ensure alignment with mission needs.

- **Institutionalize Ethical, Legal, and Accountability Frameworks**

  Consistent and enforceable ethical frameworks must govern the use of AI in national security. These frameworks should mandate comprehensive risk assessments, transparency audits, and accountability protocols for all high-impact systems. Legal standards must be clarified regarding the responsibility for AI-assisted decisions, including the roles of developers, operators, and decision-makers. AI tools in domestic use must adhere to nondiscrimination, proportionality, and due process standards to protect civil liberties. Independent oversight bodies, including congressional committees and inspector generals, should be empowered to monitor compliance and investigate incidents involving the misuse of artificial intelligence. Ongoing consultation with legal scholars, ethicists, and civil society stakeholders will enhance the legitimacy and social acceptability of AI systems deployed for security purposes.

- **Enhance Governance, Oversight, and International Collaboration**

  A unified national security AI governance framework should be established to align agency efforts, streamline standards, and promote interoperability. This framework could be supported by interagency working groups tasked with developing shared policies, metrics, and best practices. Additionally, establishing an independent AI Safety and Accountability Board would provide a mechanism for cross-sector oversight, incident response, and policy guidance. At the international level, the United States should lead initiatives to develop norms and treaties governing the responsible use of AI in military and civilian contexts. These efforts should address issues such as autonomous weapons, cross-border surveillance, cyber operations, and digital influence campaigns. Engagement with allies and multilateral organizations will be essential to promoting transparency, building trust, and ensuring that AI technologies support shared security objectives.

Conclusion

Artificial intelligence represents both a strategic opportunity and a complex governance challenge for the United States. By taking deliberate steps to strengthen technical foundations, modernize integration pathways, reinforce ethical safeguards, and coordinate governance structures, policymakers can ensure that AI enhances national resilience and operational effectiveness. The recommendations outlined in this document provide a roadmap for achieving these objectives while upholding the nation's democratic values and legal principles. In this time of rapid technological change, thoughtful and proactive leadership will be essential to securing the future of national security in the age of artificial intelligence.

About the Florida Institute for National Security

The Florida Institute for National Security (FINS) is dedicated to providing federal and state government entities with cutting-edge, applied Artificial Intelligence (AI)-driven and data science-based solutions for the most prevailing national security challenges.
Further, we aim to produce a robust talent pipeline of AI and data science knowledgeable professionals equipped with the expertise needed to advance this mission and drive the critical research it entails forward.

About the author

Damon Woodard

Dr. Woodard currently serves as the Director of the Florida Institute for National Security (FINS). He is a Professor within the Electrical and Computer Engineering Department at the University of Florida and directs the Applied Artificial Intelligence Group. He is an IEEE Senior Member, an ACM Senior Member, a National Academy of Science Kavli Frontiers Fellow, and a member of the Association for the Advancement of Artificial Intelligence (AAAI). Before becoming a faculty member, Dr. Woodard was a Director of Central Intelligence postdoctoral fellow. Dr. Woodard received his Ph.D. in Computer Science and Engineering from the University of Notre Dame, his M.E. in Computer Science and Engineering from Penn State University, and his B.S. in Computer Science and Computer Information Systems from Tulane University.

Dr. Woodard's research interests include a broad range of applied artificial intelligence topics. These include but are not limited to:

- Adversarial Artificial Intelligence
- AI-enabled Hardware Assurance & Security
- Counter Artificial Intelligence
- AI Hardware Acceleration
- Multi-modal Artificial Intelligence
- Explainable Artificial Intelligence (XAI)