

OVERCOMING THE CHALLENGES OF AI ADOPTION WITH IBM WATSONX

Generative AI for the Department of Defense

With the formation of the AI Rapid Capabilities Cell (AIRCC) in December of 2024, the Chief Digital and Artificial Intelligence Office (CDAO) in partnership with the Defense Innovation Unit (DIU) has signaled enhanced efforts to accelerate and scale the deployment of cutting-edge AI-enabled tools.

However, the U.S. Department of Defense (DoD) faces a wider range of unique issues than commercial or other non-governmental organizations face in the adoption of generative AI. These challenges stem from technical, security, and operational complexities. Some of these challenges include:

⚠️ DATA CHALLENGES

DoD networks often house vast amounts of data, much of which is unlabeled due to the sheer volume and complexity of the data sources. Additionally, significant portions of this data reside on classified networks, which pose challenges for accessing, labeling, and processing the data, particularly for advanced AI applications. Supervised learning algorithms require labeled datasets to understand the relationship between features and output. Without labels, it becomes difficult to train models effectively.

⚠️ INTEGRATION WITH LEGACY SYSTEMS

Many mission-critical applications and datasets in current use run on legacy systems that are not easily compatible with modern data platforms needed for adoption of generative AI. Typically, migrating these applications and data is technically difficult and expensive.

“The pace of technological change is accelerating. That’s a given. The challenge is how we in the Department of Defense can harness it to maintain our strategic advantages.”

– **Ash Carter**
Former Defense Secretary

⚠️ EXPLAINABLE AI REQUIREMENTS

While AI can enhance tactical and strategic decision-making, decisions made by the AI system can have significant consequences. Ensuring these systems are transparent and can explain their reasoning can help establish trust among human operators and stakeholders and is essential for accountability. It also enables analysts to identify and rectify potential biases in AI systems, leading to better outcomes.

⚠️ **CYBERSECURITY RISKS**

The U.S. Department of Defense (DoD) is addressing cybersecurity risks associated with AI systems through several strategic initiatives, such as the AI Cyber Defense Pilot Programs and the Risk Management Framework for AI to ensure the security of data training and AI models to prevent data poisoning or backdoor attacks.

⚠️ **VENDOR CONCERNS AND COLLABORATION**

Developers often fear that their intellectual property rights could be threatened or that their platforms or applications could be reverse engineered. In addition, achieving interoperability between government-owned platforms and industry-developed tools is a challenge due to vendors locking data in silos rather than adopting open standards for shareability.

⚠️ **CULTURAL AND BUREAUCRATIC BARRIERS**

Almost any new technology adopted by any organization may face resistance to implementation due to the attitudes of individuals who are comfortable with the status quo or concerned that the new technology may make them redundant. While processes such as Authority to Operate (ATO) are essential to ensure that information systems are secure, effective, and compliant with regulations and standards, they add barriers that can slow the adoption of generative AI.

⚠️ **BUDGETARY CONSTRAINTS**

The DoD's long budgetary cycles do not align with the rapid pace of AI innovation, making it difficult to fund emerging technologies that were not anticipated years in advance.

⚠️ **CONCERNS ABOUT VERIFICATION BEFORE DEPLOYMENT**

With potential adversaries such as China and Russia going all in on generative AI, there is pressure on the DoD to maintain competitiveness in these technologies, which can create accelerated adoption cycles that could put our warfighters at risk.

⚠️ **OVERCOMING THE CHALLENGES OF AI ADOPTION**

If, the DoD is going to achieve and maintain an advantage in the adoption of AI against potential adversaries, it will have to avoid technological missteps and build on a proven enterprise data platform that offers the performance, security, scalability, and flexibility needed to meet the complex needs of our nation's military.







Executive Summary

- The U.S. Department of Defense (DoD) faces a wider range of unique issues than commercial or other non-governmental organizations face in the adoption of generative AI. These issues stem from technical, cultural, operational, and bureaucratic complexities.
- Technical challenges include unlabeled and classified data, integration with legacy systems, scalability, and requirements for explainable AI.
- Cybersecurity risks, such as data poisoning and back door attacks.
- Cultural and bureaucratic barriers such as resistance to change or Authority to Operate Procedures
- Budget issues, appropriation cycles, and long procurement processes.
- IBM watsonx is a proven enterprise data platform that offers the performance, security, scalability, and flexibility needed to meet the complex needs of our nation's military.
- IBM watsonx is a comprehensive portfolio of AI products that accelerate the impact of generative AI in core workflows. IBM watsonx offers several distinct advantages for the DoD compared to other data platforms, in areas of decision-making, security, and scalability.

Realize the Promise of AI with IBM watsonx

IBM watsonx is a comprehensive portfolio of AI products that accelerate the impact of generative AI in core workflows. IBM watsonx offers several distinct advantages for the DoD in areas of decision-making, security, and scalability, compared to other data platforms.

THE IBM WATSONX PORTFOLIO INCLUDES:

-  **watsonx.AI** – an enterprise AI studio designed to empower builders to construct powerful AI solutions
-  **watsonx.data** – a hybrid, open data lakehouse to power AI and analytics with all relevant data, anywhere it resides
-  **watsonx.governance** – an end-to-end toolkit for AI governance to manage risk compliance and the entire AI lifecycle
-  **watsonx Orchestrate** – an enterprise ready solution that helps create, deploy and manage AI assistants and agents to automate processes and workflows
-  **watsonx Code Assistant** – accelerates code production and increases developer productivity with generative AI
-  **watsonx Assistant** – enables you to build better virtual agents to drive enterprise productivity

SUPPORT FOR ENHANCED DECISION-MAKING

IBM watsonx integrates advanced AI models, such as the IBM Granite model, with Retrieval-Augmented Generation (RAG) capabilities. This allows defense leaders to access high-quality, real-time data for situational analysis, operational decision support, and mission planning. For example, it can generate comprehensive reports and assist with scenario modeling to anticipate challenges and mitigate risks.

By leveraging trusted AI principles, IBM watsonx ensures that its outputs are explainable and reliable. The ability to easily understand the reasoning behind the relevant AI models enables defense leaders and warfighters to act quickly with high confidence in the outcomes.

DATA SECURITY AND COMPLIANCE

IBM watsonx is designed to meet DoD's strict security requirements, making it well-suited for handling classified and sensitive data. Unlike public-facing AI platforms like OpenAI's GPT models, IBM watsonx emphasizes privacy and ensures data stays within secure environments through on-premises or hybrid cloud deployments.

IBM also provides IP indemnification for its AI models, reducing legal risks associated with their use.



OPERATIONAL READINESS AND PREDICTIVE CAPABILITIES

IBM watsonx builds on IBM's history of predictive maintenance solutions used by the U.S. Army for vehicles like the Stryker fleet. By analyzing sensor data, watsonx has demonstrated the ability to predict maintenance needs, reducing downtime and improving mission readiness.

The platform's ability to analyze structured and unstructured data enhances logistics planning and asset management across large-scale military operations.

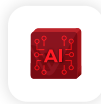


SCALABILITY AND FLEXIBILITY

The Department of Defense and all its component organizations operates one of the largest, and most complicated, data enterprises across the globe.

IBM watsonx supports hybrid deployments, allowing the DoD to manage its infrastructure on-premises or in a secure cloud environment. This flexibility ensures compatibility with existing IT systems while providing enterprise-grade reliability, disaster recovery, and zero downtime options.

It can scale from small proof-of-concept projects to enterprise-level implementations, making it adaptable to various defense use cases.



AI GOVERNANCE FOR RESPONSIBLE USE

IBM watsonx governance provides tools to monitor bias, fairness, and compliance in AI models. This ensures ethical AI usage while mitigating risks associated with automated decision-making—a critical factor for the DoD as it integrates AI into its operations.

Strong governance also facilitates collaboration across departments and allied nations by ensuring consistent standards for data sharing and analysis.



SUPPORT FOR COMPLEX MILITARY APPLICATIONS

IBM watsonx can assist with advanced applications like wargaming simulations, operational planning, and resource prioritization by combining analytics, visualization tools, and AI-driven course-of-action analysis. These capabilities expand commanders' decision-making space in real-time scenarios to adapt quickly to changing conditions and enemy actions.

IBM and V3Gate

IBM watsonx is available from V3Gate, a recognized IT solutions provider for the U.S. Public Sector, healthcare, and education. Founded in 2007, V3Gate is a Service-Disabled Veteran-Owned Small Business (SDVOSB) and Minority-Owned Business Enterprise (MBE).

Contact V3Gate to discuss how IBM watsonx can accelerate your adoption of generative AI.

To learn more, visit v3gate.com/partners/ibm

