

DOD Takes on

AI

INSIDE:

- Space Force to Rebuild IT Infrastructure for AI ... 3
- Infographic: DOD's Principles of Ethical AI 6
- Pentagon Needs Trustworthy AI to Support Warfighters..... 11

SPONSORED BY



Red Hat

From the editor's desk



Amy Kluber, Editor-in-Chief

DOD's AI Journey Leans on Partnerships

The Defense Department has been on a long journey to leverage capabilities that artificial intelligence is poised with all aspects of the defense mission.

The journey to get there is challenging. DOD leaders are working on new frameworks to ensure AI is created and used ethically. Plus, services like the Space Force are working to rebuild legacy systems to accommodate AI. The services are seeing varying uses for the technology.

Most importantly it'll unlock personnel and service members to better carry out mission-critical tasks that ensure national security.

The partnerships that are enabling these capabilities require close attention to the data management side of the house to help process data at the edge more quickly. This will help the department meet its vision toward Joint All-Domain Command and Control (JADC2). 🌸

Table of Contents



Amy Kluber,
Editor-in-Chief



Anastasia Obis,
Staff Writer/
Researcher

ARTICLE

Space Force to Rebuild IT Infrastructure for AI, Digital Twins

Old infrastructure is a major roadblock for the Space Force Technology and Innovation Office responsible for the service's digital transformation efforts.

BY ANASTASIA OBIS

INFOGRAPHIC

DOD's Principles of Ethical AI

There are many challenges in building ethical and trustworthy AI, but doing so is more critical than ever. The Defense Department developed five AI ethical principles to ensure the agency develops and deploys the powerful technology in a responsible manner.

PARTNER INTERVIEW

Automation is Key to Processing Data Faster at the Edge

As defense systems increasingly require faster data processing, tools like AI and machine learning have promising potential.

Michelle Davis, Director, Solution Architects, Federal Division, Red Hat

ARTICLE

Pentagon Needs Trustworthy AI to Support Warfighters

Defense leaders are eyeing better governance and risk management as policy around ethical AI shapes up.

BY ANASTASIA OBIS

Space Force to Rebuild IT Infrastructure for AI, Digital Twins

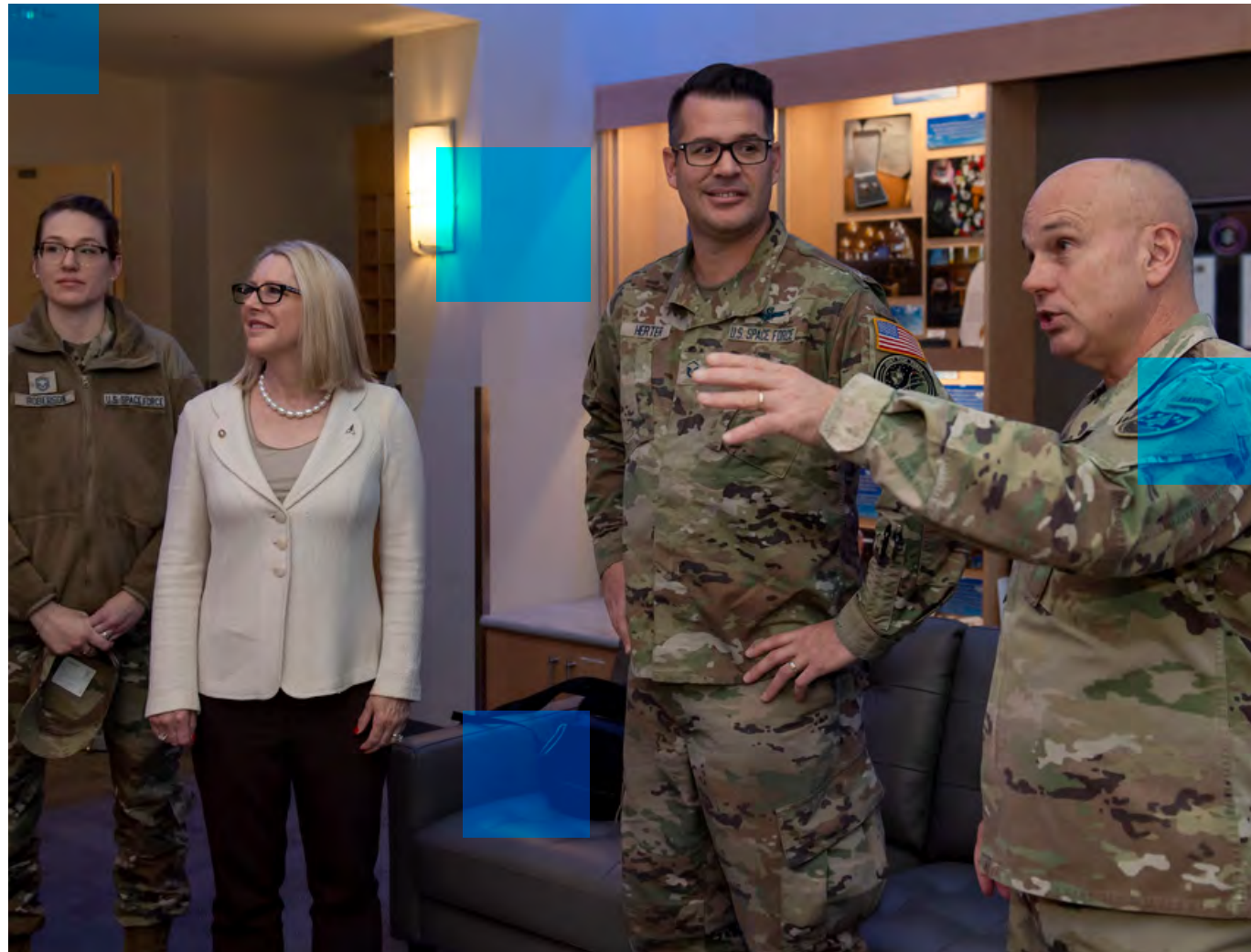
Old infrastructure is a major roadblock for the Space Force Technology and Innovation Office responsible for the service’s digital transformation efforts.

BY ANASTASIA OBIS

To reach digital maturity, the U.S. Space Force is rebuilding IT systems, some of which are more than 30 years old, to accommodate artificial intelligence (AI) capabilities and digital twin models. Space Force tech leaders hope to release a new strategy soon to guide these efforts.

“Fundamentally, Space Force is ... three years old, and we have a vision to be a digital service,” Lisa Costa, the U.S. Space Force chief technology and innovation officer, said at an event this year. “A large part of what we’re doing is focusing on shoring up and rebuilding the infrastructure so that the AI, the ... digital twins that sit on top of that infrastructure can operate well and in a way that our Guardians are used to accessing technology when they pick up their phone.”

The Space Force Technology and Innovation Office is currently



developing a model-based systems engineering strategy and implementation guide to establish standards, policies and guidance for how the service will develop and use digital models.

Model-based systems engineering, which keeps track of complex contemporary systems, accelerates transformation and reduces costs, is widely used across the Defense Department. Last year, the U.S Army awarded five rapid prototyping other transaction agreements for the Future Tactical Unmanned Aircraft System

Increment 2 effort, which will utilize model-based systems engineering to align unmanned aircraft systems to higher-level architectures.

“You can imagine if you’re contracting for different digital models, different digital twins, you can imagine all of the different standards that might be used ... the different inputs, the different measurements,” Costa



Lisa Costa

Chief Technology and
Innovation Officer, U.S.
Space Force

said. “The different processing, the different outputs, we want to be able to control for error ... we want to be able to ensure that we’re not vendor locked, and we’re able to run those models on very different systems because we may have different capabilities at different locations.”

Costa said the Space Force is working on an integrated operations network (ION), which will provide high bandwidth and low latency for essential capabilities, like AI or improvements to its Unified Data Library (UDL).

“One of the things we’re really trying to do is make sure as we build out ION, which is that base infrastructure that we are providing left and right limits for all the things that will sit on top of it like digital engineering, AI or enhanced UDL, putting out those standards to reduce regret over time,” Costa said.

For the past three years, the Space Force has been building “vertical infrastructures,” developing acquisitions, the Space Warfighter Analysis Center, the Space Training and Readiness Command and the Space Operations Command.

“Those are verticals of excellence that we need to integrate horizontally,” Costa said. “The way they are integrated is based on older networking technology and so the CTIO office is heavily engaged in building and bringing to Space Force by ION, the integrated operations network, which focuses on integrating across those verticals so that they’re able to pass off digital models to one another.”systems,” NIST Information Technology Laboratory Chief of Staff Elham Tabassi told GovCIO Media & Research. 🌟

“A large part of what we’re doing is focusing on shoring up and rebuilding the infrastructure so that the AI, the ... digital twins that sit on top of that infrastructure can operate well and in a way that our Guardians are used to accessing technology when they pick up their phone.”

**— Lisa Costa, Chief Technology and Innovation Officer,
U.S. Space Force**

DOD's Principles of Ethical AI

There are many challenges in building ethical and trustworthy AI, but doing so is more critical than ever. The Defense Department developed five AI ethical principles to ensure the agency develops and deploys the powerful technology in a responsible manner.

01 Responsible

Exercising appropriate levels of judgment and care when implementing AI capabilities, while being responsible for the development, deployment and use of AI.

05 Governable

Designing AI capabilities in a way that fulfills their intended functions while also possessing the ability to detect and avoid unintended consequences, as well as deactivate systems that demonstrate unintended behavior.

02 Equitable

Taking deliberate steps to minimizing unintended bias when deploying AI systems.

03 Traceable

Possessing an understanding of the technology, its development processes, and operational methods applicable to AI capabilities such as transparent and auditable methodologies, data sources and design procedure.

04 Reliable

Having explicit and well-defined uses of AI capabilities and the safety, security and effectiveness of those capabilities are subject to testing and assurance.



Automation is Key to Processing Data Faster at the Edge

As defense systems increasingly require faster data processing, tools like AI and machine learning have promising potential.

What are some of the biggest challenges around AI in defense technology?

Davis Artificial intelligence is transforming our everyday lives, including war. At its core, AI is all about the data, which makes collection and analysis of that data a great challenge.

From a defense perspective, data is collected from sensors on a variety of endpoints including ships, aircraft, unmanned aircraft systems and satellites — collecting information in a quest for maintaining battlefield advantage and decision dominance.

Despite the vast opportunities this amount of data presents, there are many limitations. Because of the critical roles smaller form-factor devices are playing in the future of technology, we need to adapt how we process data in these changing conditions. This is mainly due to limitations in size, weight and power (SWAP) and in internet connectivity. (ctd.)



Michelle Davis
Director, Solution Architects,
Federal Division, Red Hat

“Having parts of your command-and-control system run where best suited, and being able to move from cloud to a private cloud and back to on premise, are competitive advantages.”

— Michelle Davis, Director, Solution Architects, Federal Division, Red Hat

 **What are some of the successes or use cases for AI you've seen helping?**

Davis With the rise of containerization, Kubernetes and AI in the commercial world, we have seen the ability to field new capabilities more quickly in as little as 24 hours. These include applications that can do things from proactively predicting weapon mechanical failures to dynamically adjusting trajectories based on situational awareness.

We have seen success not only in these deployments being faster, but also they are much more rich, resilient, secure and agile. The portability of workload and applications have opened new avenues of information sharing and faster decision-making. Having parts of your command-and-control system run where best suited, and being able to move from cloud to a private cloud and back to on premise, are competitive advantages.

The new computer server is a cluster, and this distributed cluster can be made up of public, private and hybrid-cloud architectures. This cluster also includes automated failover of stored data in times of crisis and operational disruptions like cyberattacks, infrastructure degradations or outages.

Furthermore, security is always paramount for DOD systems and applications. The concept of starting with trusted parts, which is an important element of containerization and Red Hat's enterprise Kubernetes platform OpenShift, places security to the left in the software development lifecycle. Software is never done, and adding AI to the mix requires continual innovation, training and feedback. (ctd.)

 **What do you look forward to over the next year?**

Davis I look forward to the day when AI drives automation as well as developer and operations activities. With natural language, we can instruct computers to perform both common and complex tasks.

Imagine code rebasing automatically based on past processing (and human) experiences. Imagine models being created and trained based on

changes in infrastructure or environment. Imagine within minutes we can have a push-button collaboration environment with enterprise security, compliance and credentialing solutions in place.


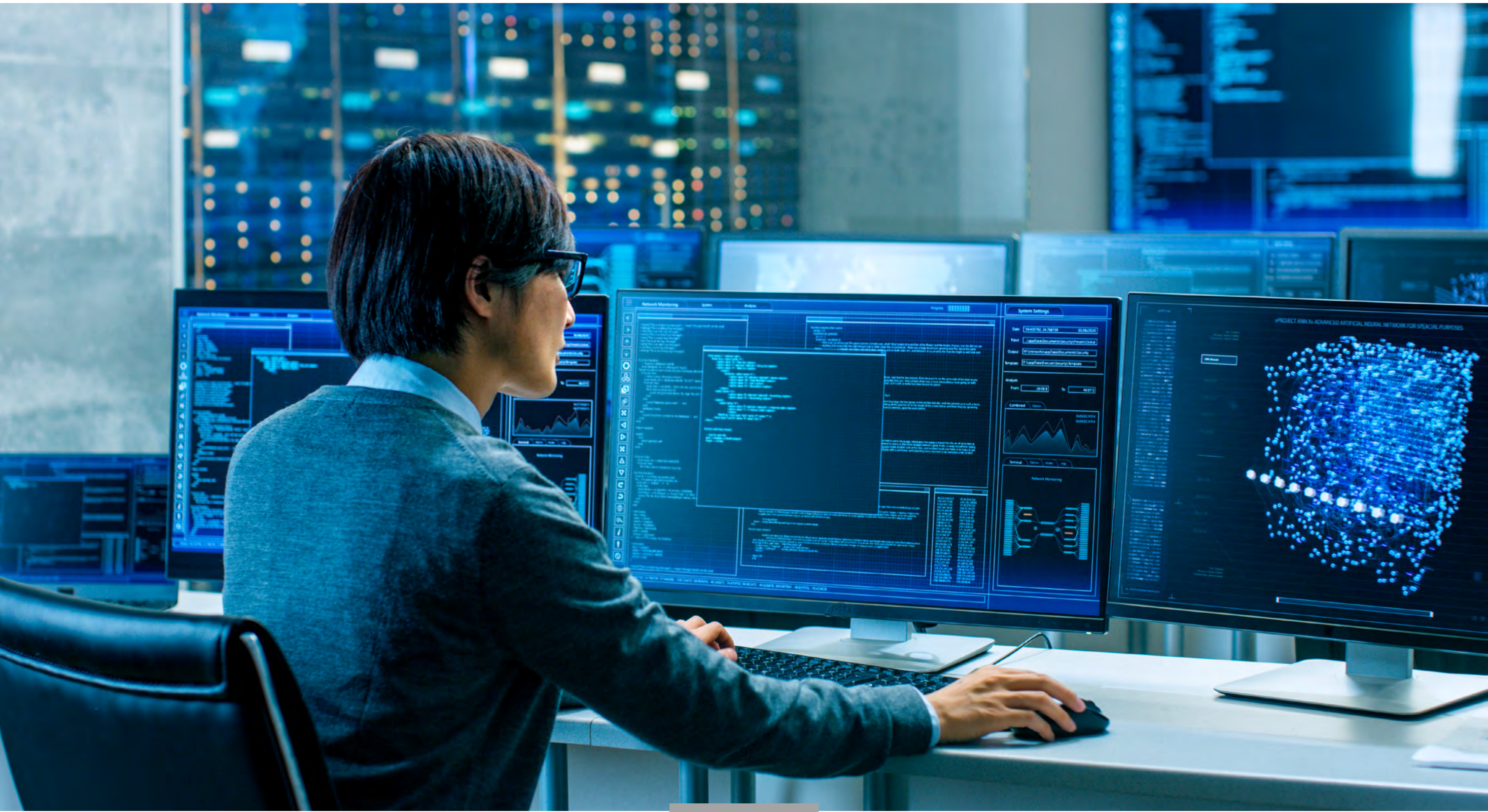
DOD's competitive advantage today and tomorrow relies on the right data at the right times for the right folks. These innovations will not only give us a competitive advantage, but it also will ultimately shorten the kill cycle. 

Photo Credit: Gorodenkoff/Shutterstock



A path to modern day software delivery

- DevSecOps
- Automated governance
- Trusted software supply chain

redhat.com/dod



Pentagon Needs Trustworthy AI to Support Warfighters

Defense leaders are eying better governance and risk management as policy around ethical AI shapes up.

BY ANASTASIA OBIS

As the Defense Department accelerates use of advanced technologies such as artificial intelligence (AI), the need to build trustworthy AI systems is more critical than ever, especially when applying these technologies in the military realm.

For fiscal year 2024, DOD is seeking \$1.8 billion to adopt and deliver AI capabilities. DARPA has been conducting AI research for more than 60 years and invested more than \$2 billion in AI advancement over the past several years.

Recognizing the potential that AI can bring to the battlefield, defense leaders are pushing for good governance, risk management, regulations and policy in place as it is increasing the use of this technology to support mission-critical activities.

“We reach for the opportunity that AI provides us with what we need to reach with the other hand and manage the risks that will come with the application of that disruptive technology,” Coast Guard Vice Adm. Kevin Lunday, who commands the Atlantic Area, said at the 2023 Sea-Air-Space conference at National Harbor,



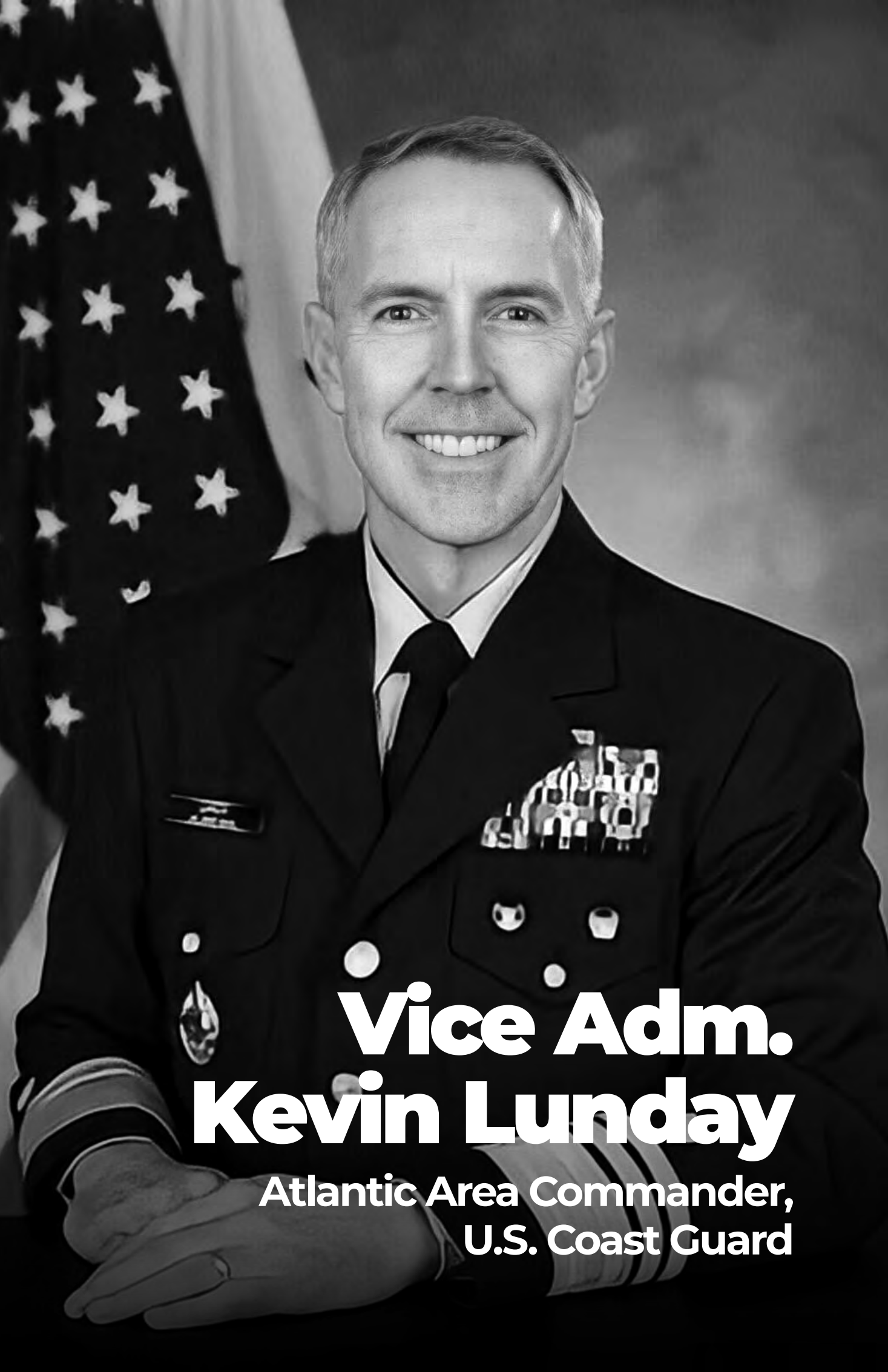
Maryland. “When we train our officers ... the first rule is one hand for yourself and one hand for the ship. ... So that’s how I think about risk management as we reach for the opportunity.”

Defining what constitutes a trustworthy system is challenging, as trust is a multifaceted concept. Earlier this year, the National Institute of Standards and Technology (NIST) released the AI Risk Management Framework (AI RMF) to help federal agencies responsibly develop and deploy AI systems.

NIST defines a trustworthy AI system in 11 words: valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced and fair with harmful bias managed.

“There’s a lot of meaning behind every single one of those 11 words,” Lunday said.

Experts say the path to trustworthy AI systems is long and complex, including factors such as improving resiliency to adversarial attacks or building the infrastructure to support these systems. Defining what it means to have a



Vice Adm. Kevin Lunday

Atlantic Area Commander,
U.S. Coast Guard

trustworthy system and how to measure success is fundamental to this journey.

“Human-to-machine interaction — that’s fundamental to trust; being able to define what do you mean by trust? ... There are definitions out there in the research community,” DARPA Information Innovation Office Deputy Director Matt Turek said at Sea-Air-Space. “What are the levels of resources that we need to build state-of-the-art AI systems? What’s the impact on energy and climate from filling those large systems? How do we have AI systems that anticipate what humans need and are in alignment with human values? All of these, I think, are core challenges that we need to get out there and ultimately get highly trustworthy AI systems.”

While DOD seeks to take advantage of industry solutions, defense leaders say there are problems that the private sector will not have the answers for as industry’s needs are fundamentally different from national security needs.

“I think part of that is because there’s a fundamental misalignment between what the industry is doing and what DOD ultimately needs,” Turek said. “I think there are many compelling capabilities, ... but industry isn’t focused on those sorts of life-and-death problems. They also have access to massive amounts of data and compute, and that’s not always the case for the sorts of problems we work on in the DOD. We care a lot about unusual events. Sometimes those are the ones we might care the most about, by definition, and there’s not a lot of training data available.”

Working through the challenges of defining what constitutes trustworthy systems or how to measure success hampers organizations from providing appropriate oversight and policies around the technology.

“I think one of the challenges from a policy perspective is, how do we construct regulations appropriately? I go back to that foundational science of how you measure and evaluate AI systems. You don’t have some of that foundational science,” Turek said. “It’s not like you say you need to have this level of trust score operating in this particular domain ... so I think that creates



challenges for policymakers.”

Guidance such as NIST’s framework equip organizations with resources to manage risks associated with development and deployment and promote responsible use of this technology. In creating this guidance, NIST worked with a wide range of experts, including psychologists, philosophers and legal scholars, to better understand the impacts AI has in real life.

“During the different stages of AI lifecycle through the design, development, deployment and regular monitoring of the systems, it’s really important to reach to a very broad sense of expertise ... the tech community, but also ... psychologists, sociologists, cognitive scientists to be able to help us understand the impact of the systems,” NIST Information Technology Laboratory Chief of Staff Elham Tabassi told GovCIO Media & Research. 🌟

When we train our officers ... the first rule is one hand for yourself and one hand for the ship. So that's how I think about risk management as we reach for the opportunity.”

**— Vice Adm. Kevin Lunday, Atlantic Area Commander,
U.S. Coast Guard**