GovCIO
MEDIA & RESEARCH

SPRING 2024

DeepDives

Future JOINT OPERATIONS

INSIDE:

SPONSORED BY

verizon✓

GovCIO MEDIA & RESEARCH

From the editor's desk

Ross Gianfortune, Managing Editor

A Connected Future

Defense Department officials are steadfast in preparing now for a future force that is connected and advantageous. Technology and innovation will fuel these efforts.

Leaders are exploring how to integrate artificial intelligence into more combat operations to aid faster decision-making and enable more connectivity.

At Army Futures Command, having a tech-savvy future force is integral for American military superiority. Gen. James Rainey warned recently of "fundamental changes to warfare" on the horizon. Technology use cases in global hotspots like Ukraine and Israel have enabled the Army to innovate appropriately as the service prepares for Army 2040, the service's modernization strategy.

The Pentagon's Combined Joint All Domain Command and Control (CJADC2) concept already includes emerging technology in plans to bring together different services in even the most austere environments. While budget constraints hamper some efforts, Under Secretary for Research and Engineering Heidi Shyu said rapid prototyping, experimentation and exercises will be critical.

Future-proofing the fighting force is an ultimate Pentagon goal. In training, research, technology and innovation, the future of military operations is being written today.

Table of Contents

Ross Gianfortune,
Managing Editor

Jordan McDonald,
Staff Writer

GovCIO
MEDIA & RESEARCH

Army Leaders: The Future Force Will Be Tech-Savvy

AI and other technologies will enable military personnel to be better warfighters.

Six years into the Army's modernization plan, the service's leaders are deliberating on how to fully integrate emerging technology like artificial intelligence into the battlefield.

Transformation and IT modernization were key themes at AUSA's annual meeting, where Gen. James Rainey, commanding general of the Army Futures Command, said "deliberate modernization" of the service is progressing, reducing timelines and sticking to initial priorities.

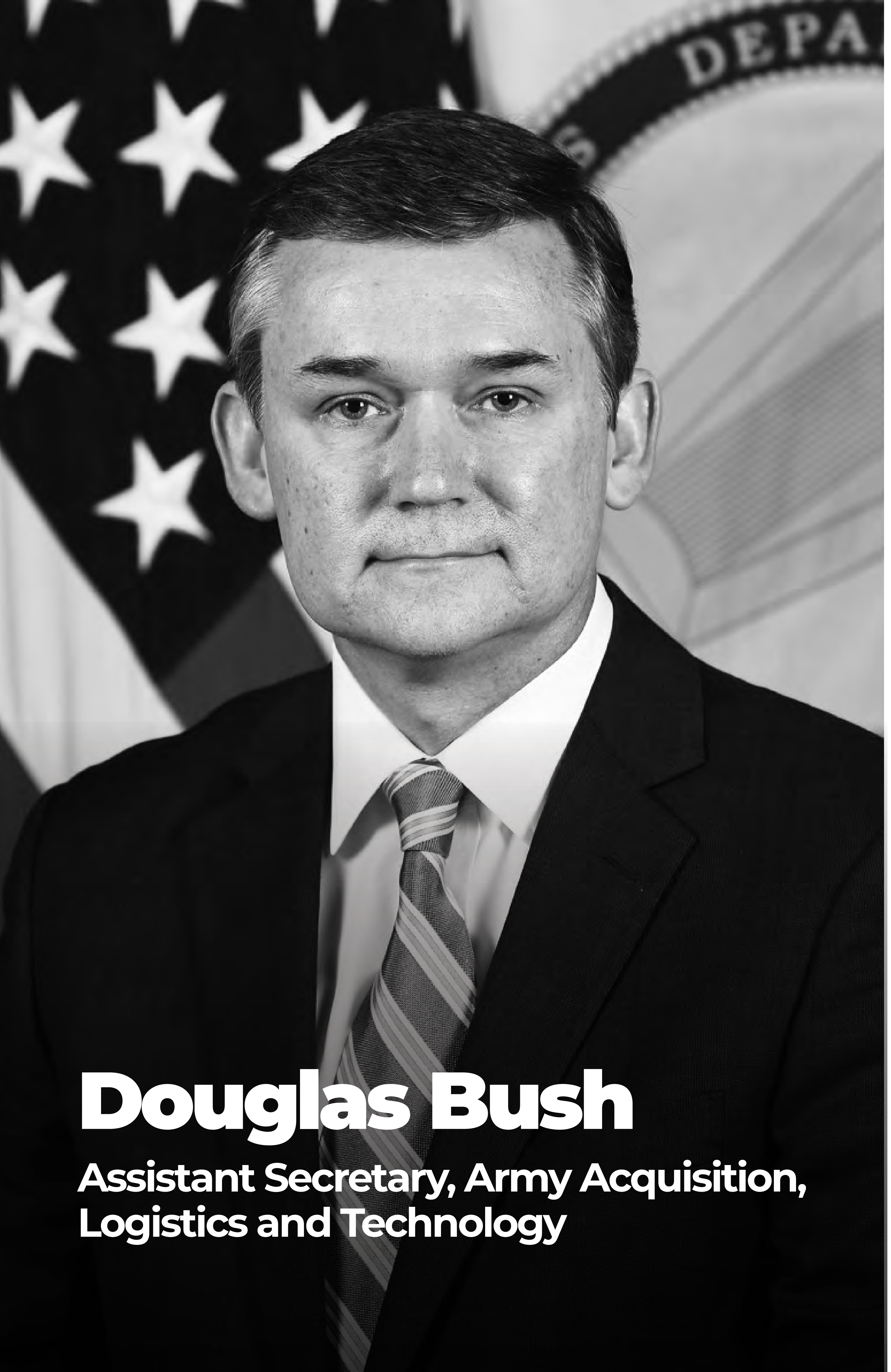
Rainey warned that there are "fundamental changes to warfare coming" on the horizon, and the time for the Army to adjust and adapt to them is now. According to Rainey, the Army's command-and-control warfighting system needs to be ready to integrate emerging technologies that have the "potential to be incredibly disruptive" — like AI, machine learning, large language models and quantum computing — as soon as possible ahead of 2040.

Rainey said modernization has created opportunities for the Army to observe technology use cases in emerging hotspots like Ukraine and Israel, allowing the Army to turn those observations into "real capability in our formations."

Rainey said that while the Army will still be able to adapt to technology as it arrives, it will require "commanders who are as good at leveraging technology as they are at reading terrain, doing combined arms maneuver and understanding the enemy."

Army Acquisition, Logistics and Technology Assistant Secretary Douglas

Photo credit: Pfc. Brandon Perry, U.S. Army/DVIDS



Douglas Bush

Assistant Secretary, Army Acquisition, Logistics and Technology

Bush said at the event that Congress' support and flexibility has allowed the Army to acquire better technology on a faster scale, but added that congressional oversight is still very necessary to keep priorities in line.

Bush said mechanisms are being put in place to build government capacity to "understand AI and work with industry to evaluate it and field it quickly. There's a government responsibility to understand what we're buying and what we're deploying, especially with a new technology that potentially is so transformational."

Bush stated that the Army is taking steps to build its institutional knowledge of emerging technologies through efforts such as rotating officers with private industry to better understand how private industry tech can integrate with the Army.

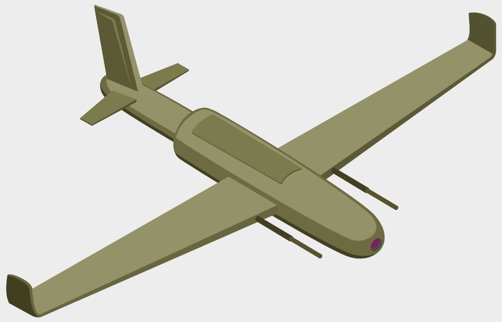
However, Rainey believes that while the Army can build up its knowledge and understanding of AI and other emerging technologies, it shouldn't try to compete with private industry.

"I think industry is always going to be better at and ahead of the Army and the military on AI," Rainey said. "I think as we design the command-and-control warfighting system of the future that we need to get not one company, not vendor lock, but we need to get a handful of cutting edge companies integrated into that system as a service doing AI, doing ML, and making sure that we are always one step ahead of the enemy and we're being predictive."

Photo Credit: Stokkete/Shutterstock

“We need to get a handful of cutting-edge companies integrated into that system as a service doing AI, doing ML, and making sure that we are always one step ahead of the enemy and we’re being predictive.”

Douglas Bush, Assistant Secretary,
Army Acquisition, Logistics and Technology



CJADC2 Guiding Principles

The Defense Department's Combined Joint All Domain Command Control (CJADC2) concept includes a set of these key overarching principles.

CYBERSECURITY

Joint Force Command and Control must employ a layered defense spearheaded by a strong cyber defense to deter malicious activity that would threaten enterprise operations. The department must adopt a wartime mindset during day-to-day operations—e.g., train as we fight—and develop knowledgeable leaders and staffs trained to employ the tools and authorities at their disposal.

ENTERPRISE DESIGNED AND SCALED INFORMATION SHARING

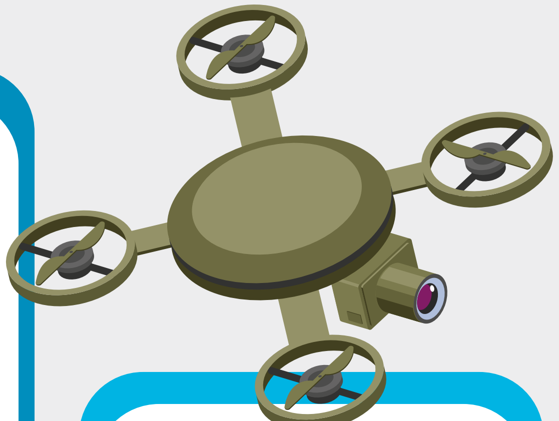
Continuous information sharing must be designed and operated at an enterprise level. CJADC2 will depend on enterprise nodes and supporting communications networks to provide connectivity with the bandwidth, functionality and security needed to bring vital information to the Joint Force Commander.

DATA AND INTEROPERABILITY STANDARDS-DRIVEN

The Joint Force data fabric must consist of efficient, evolvable, and broadly applicable common data standards and architectures, with standardized key interfaces and services to access, aggregate, manage, store, process, and share data across a large environment with a wide variety of partners and operational uses.

RESILIENT IN A DEGRADED ENVIRONMENT

The Joint Force must be able to operate with minimum guidance within a degraded or contested C2 environment, and commanders and staffs must train aggressively in conditions where sensing and communications are severely impacted or completely disabled, and where adversary intentions are ambiguous.



UNITY OF EFFORT IN CAPABILITY DEVELOPMENT

DOD must improve its C2 capability development and implementation processes to more readily adopt cross-domain priorities and solution options.

DELIVERING CJADC2 CAPABILITIES WITH SPEED

The Department must continue to evolve its current approach to C2 development and acquisition, and adapt existing methodologies to more rapidly produce needed capabilities.

Source: Defense Department

GovCIO
MEDIA & RESEARCH

verizon✓

Creating an Agile Infrastructure for Defense

Zero trust and microsegmentation play key roles in revolutionizing global, high-speed connectivity.

What are the challenges the DOD faces regarding network connectivity around the globe?

Rouse DOD's decision to officially sunset the legacy Joint Regional Security Stack (JRSS) in 2021 and move toward secure access service edge (SASE) cloud architecture and zero trust architecture means that all the military services are coping with a fundamental shift in network connectivity.

This is causing them to rethink how they operate their networks and pushing them toward a truly software-defined networking architecture (SDN).

The services are all developing advanced applications and looking at how artificial intelligence (AI) and machine learning (ML) are being incorporated into everything they do. The impact of these changes is that all the services are having to invest in high-

Chris Everich
Distinguished Architect,
Verizon

David Rouse
Senior Director,
Defense and National
Security, Verizon

performance infrastructure that will be agile enough to handle the demands of advanced applications and massive increases in the amount of data transmitted and processed.

They are also challenged to overcome existing technical debt in their present systems. There is a lot of excellent work being done in the test and evaluation domains to address these issues, but the challenge will be whether these solutions can function at the immense scale needed by the services.

The underlying reality is that funding for advanced infrastructure that can deliver the agility and performance needed for uses including warfighting, logistics, cybersecurity and communications has not been fully addressed in current budget appropriations.

To manage the investment needed to deploy the advanced connectivity now and in the future, government and industry will have to work collaboratively.

Can you list out the ways such a network can maintain the levels of security the DOD requires?

Everich Complementing SASE is the incorporation of zero trust access architectures. Rather than operating one's IPSec VPN tunnel wide open to any authenticated user, zero trust access provides fine grained control through microsegmentation at the edge.

Both military and civilian experts now seem to expect the network at the edge to be compromised. Microsegmentation has the potential to isolate the compromise, minimize the potential damage, while in theory allowing the rest of the mission systems to continue to operate. Microsegmentation is a security technique that breaks data centers and cloud environments into segments down to the individual workload level. Organizations implement microsegmentation to reduce attack surface, achieve regulatory compliance

> **"There is a lot of excellent work being done in the test and evaluation domains to address these issues, but the challenge will be whether these solutions can function at the immense scale needed by the services."**
>
> **— David Rouse, Senior Director, Defense and National Security, Verizon**

and contain breaches.

Expect the coupling of SDN, the means to maneuver the network with AI/ML tooling to defend the network. The military can learn how to not just block the network intrusion, but also reroute the network in an agile fashion to continue the mission.

List out some examples and use cases where enhanced network capabilities can assist the DOD's mission now and in the future.

Rouse Artificial intelligence (AI) and machine learning (ML) are tools. If you think about what our agencies do, there are billions of transactions in seconds within our systems.

AI and ML allow us to aggregate tons of data and see what's going on without human intervention. These tools will allow us to understand large data sets, look for anomalies and then use this understanding to make continuous improvements in cybersecurity. These are necessary technologies that offer real advantages to agencies that can apply them properly.

But AI and ML also can be used maliciously in creating dynamic exploits that can be customized down to specific areas that make it hard to detect. This brings us back to the importance of reducing the risk to your attack surface.

That means that our best opportunities to deter AI and ML-created exploits force us to employ AI and ML to understand the anomalies within our huge data sets so that they can be quickly mitigated.

Photo Credit: Senior Airman Stephen Pulter, U.S. Air Force

verizon

DOD's Heidi Shyu Points to Joint Capabilities for AI Agility

The department is targeting rapid prototyping and joint exercises as it fields critical technology for warfighter readiness.

Interoperability among military service branches is key to strengthening readiness of joint capabilities the Defense Department is hungry to fund like artificial intelligence, Defense Department Under Secretary for Research and Engineering Heidi Shyu said at a recent event in March 2024.

"We're focusing on contested logistics, and on multi-domain command and control," she said. "Based on the specific scenarios, we started looking for AI prototypes that will accelerate and pull through."

Funding issues stand in the way of moving forward with timely research and testing, Shyu noted. A two-year budget cycle currently restricts the department's ability to rapidly prototype and purchase promising new technologies from industry. Shyu also cited the Congressional budget process and the cycle of continuing resolutions as roadblocks to DOD accelerating capabilities and developments.

"The adversary doesn't have the same constraints," she said.

Since 2022, DOD funded $10 million and $20 million for 25 companies as part of its Accelerate the Procurement Fielding of Innovative Technologies program. The investments spanned a broad range of capabilities, including unmanned service vehicles that have a modular payload, giving them the flexibility of carrying munitions, missiles and other cargo.

Other investments include research for unmanned aerial vehicles to take off and land vertically on ships and night-vision goggles that are lighter weight, have higher resolution and provide double the field of view.

"That's what we've been focusing on: rapid prototyping, experimentation, exercises — and pull it quickly into production for the joint fight," she said. "The other thing that's important to notice is that we also fund the comparative testing program. We have 98 projects ongoing with 26 countries. And this is where I'm leveraging their technology that they have matured."

If it works, she will buy it, she said. "Why should we reinvent? If it could

Photo Credit: AFCEA International

Heidi Shyu

Under Secretary for Research and Engineering, Defense Department

accelerate capability by definition is going to be interoperable,” Shyu explained.

It’s important that the new technologies can be deployed across all theaters, she said. These include Indo-Pacific Command, Communications-Electronics Command and Strategic Air Command.

“The technologies that we develop, for example, contract unmanned aircraft systems, direct energy [and] lasers, are going to apply no matter where you are,” she said. “There’s a broad spectrum that we’re developing that’s applicable, independent of the theater we’ll be putting it on.”

She also said that she is working to facilitate and foster a better working relationship between government, industry and academia to enhance intelligence, surveillance and reconnaissance. She met with Indopacom Chief Adm. Sam Paparo, who called for cutting edge AI systems like unmanned warships.

She emphasized the importance of holistically evaluating portfolios and integrating science and technology investments to drive future success.

“We’re tying the pieces together,” she said. “Now we’re tying the [security and privacy] piece to a huge area we’re investing in that could change the future. So all that is starting to integrate together.”

Shyu stressed to the audience of private industry professionals that the DOD is their partner. Entry points to working with the department include the Small Business Innovation Research / Small Business Technology Transfer or the rapid prototyping capabilities of the Rapid Defense Experimentation Reserve, she said.

“We are a sticky customer. Namely, once we know you can produce a good product, we have you for a long, long time,” she said. “The first piece is trying to figure out how to get to us.”

“We’re focusing on contested logistics and on multi-domain command and control. Based on the specific scenarios, we started looking for AI prototypes that will accelerate and pull through.”

—Heidi Shyu, Under Secretary for Research and Engineering, Defense Department