

**SPOTLIGHT:**

# **Secure cloud networking: the key to multi-domain operations**



Sponsored by

**maximus**



# Secure cloud networking: the key to multi-domain operations

*Counter-UAS, ISR sensors, autonomous platforms all depend on truly secure cloud computing.*

BY BREAKING DEFENSE



*Maj. Huw Miller, 1st Cavalry Division current operations officer from the 3 (UK) Div., tracks and synchronizes operations during the Warfighter 23-04 exercise. 1CD fully integrated mission command systems including the Command Post Computing Environment to synchronize units across division battlespace for multi-domain operations. (U.S. Army photo by Lt. Col. Jennifer Bocanegra)*

With the award of JWCC (Joint Warfighting Cloud Capability) in late 2022, the Defense Department initiated foundational network infrastructure designed to let warfighters from all services conduct operations across multiple Areas of Responsibility.

With the cloud, they will ultimately be able to share data across all three security domains – Confidential, Secret, and Top Secret, which is a defining enabler of Combined Joint All-Domain Command and Control (CJADC2) and tactical operations at the edge. The cloud also lets them take advantage of modern software development and artificial intelligence.

“Cloud computing remains a fundamental component of the department’s global IT infrastructure and modernization strategy,” said DoD Chief Information Officer John Sherman, speaking in March before a House Armed Services subcommittee. “With battlefield success increasingly relying on digital capabilities, cloud computing provides the IT platform

needed to satisfy the warfighter’s requirements for rapid access to data, innovative capabilities, and assured support.”

That means modern cloud solutions like JWCC need to integrate with legacy on-premise and hybrid-cloud environments, while balancing security and compatibility across a wide range of maturity levels.

For the DoD, that translates into an imperative to accelerate cloud modernization efforts so that systems are interoperable and can take advantage of the latest cybersecurity, encryption, and intrusion-detection capabilities while also being hardened against future threats.

## Cybersecurity in the OCONUS cloud

In thinking about the possibilities of multi-domain operations, one of the key challenges that must be met for combined land, air, sea, space and cyber operations is encryption and segregation of data between security domains at the edge. The goal is cross-domain protection of data at rest and in transit while still giving operators the information they need for decision making.

“We’re dealing with threat actors that have advanced capabilities that can gain access to networks undetected and live off the land, blending in with normal network activity while conducting malicious activity,” said Michael Sieber, senior director of cybersecurity for defense at Maximus. “That means the posture an organization takes to protect and transport data to the tactical edge has to change.”

The edge systems most dependent on secure cloud computing and modern cloud applications include: counter-unmanned aerial systems; intelligence, surveillance, reconnaissance platforms, both crewed and uncrewed; and tactical communication systems that are crucial for operational success.

“These systems now face a very unique physical and cybersecurity threat from jamming, hacking, and exploiting systems that require active protection across the board,” said

*ON THE COVER: Fire Controlman 2nd Class Nathan Ritchie stands watch in the combat information center aboard the Arleigh Burke-class guided-missile destroyer USS Dewey (DDG 105) while conducting operations in the north Pacific Ocean, April 9, 2024. Dewey is forward-deployed and assigned to Destroyer Squadron (DESRON) 15, the Navy’s largest DESRON and the U.S. 7th Fleet’s principal surface force. (U.S. Navy photo by Mass Communication Specialist 1st Class Samantha Oblander)*

Sieber. “Cybersecurity in the cloud is about ensuring data is secure as it’s transported across networks.”

Moving data across the relatively secure transport pipes of the Continental U.S. is a challenge in itself. Outside the Continental U.S. (OCONUS), however, secure transport becomes an even higher priority – especially in the austere environments found in OCONUS.

“The current crisis in Ukraine and CJADC2 experiments demonstrate the need for rapid extension of enhanced edge computing capabilities globally to reduce network latency, enable advanced data processing such as AI, and improve operational resilience,” said Sherman, who noted that in the last year the DoD Office of the Chief Information Officer, in partnership with the Defense Information Security Agency, successfully deployed the initial OCONUS commercial cloud capability in support of U.S. INDOPACOM missions. The OCONUS cloud is designed for mission command, resulting in “improved agility, greater lethality, and improved decision-making at all levels,” according to Sherman.

Many of these investments in edge computing – especially in the U.S. Navy as no service operates more on the tactical edge than they – are also meant to unlock the potential benefit that DoD is putting into other areas like AI, machine learning, and automation.

“That means deploying those capabilities to process the data closer to the source to reduce latency and ensure real-time data analysis in field operations,” said Frank Reyes, cloud solutions leader at Maximus. “It helps to do as much of the data encryption, segregation, and threat intelligence as you can in the field to minimize latency and enhance responsiveness of applications in areas like real-time threat analysis for counter-UAS operations.”

### **Cloud computing leads to more standardization**

Cloud computing also plays an important role in standardizing data formats and protocols used in transport layers to move information quickly to the edge. Warfighters have to deal with a mixture of classified data, ISR feeds, and unclassified information that impacts missions. Standardization allows companies like Maximus to build tailored defense solutions that get the right information to decision makers.



*An MH-60S Sea Hawk assigned to the “Eightballers” of Helicopter Sea Combat Squadron (HSC) 8 takes off from the flight deck aboard the Arleigh Burke-class guided-missile destroyer USS Russell (DDG 59) during a trilateral exercise, April 11, 2024, among maritime forces from Japan, the Republic of Korea, and U.S. (U.S. Navy photo by Mass Communication Specialist 3rd Class John A. Miller)*

“Standardization is still the backbone from a data-transformation perspective,” said Seiber. “Much has changed in transport over the past decade and standardization needs to be in place when you are tailoring information so that the end user can access it immediately while addressing multiple security layers.”

The idea of standards isn’t new. For example, aircraft platforms have been equipped with the 1553 data bus for decades, which allow sensor suites, onboard avionics, and mission computers to communicate across to the aircraft. That’s how aviation platforms like the AC-130 gunship, which has been in operation since the 1970s, has been able to remain a relevant weapon by adding new missiles, bombs, and guns as they’re developed. They all are interoperable because they’re just systems that the computer sees, commands, and responds to.

“Bringing that mindset into the IT space is going to be key,” said Reyes, noting that everybody is already familiar with that model through commercial apps on smartphones. “There are nearly two million apps in the Apple app store and all of them use the same operating system standard, GPS standard, and accelerometer standard. Focusing on the interfaces, standards, and interoperability unlocks a lot of innovation if done right.”