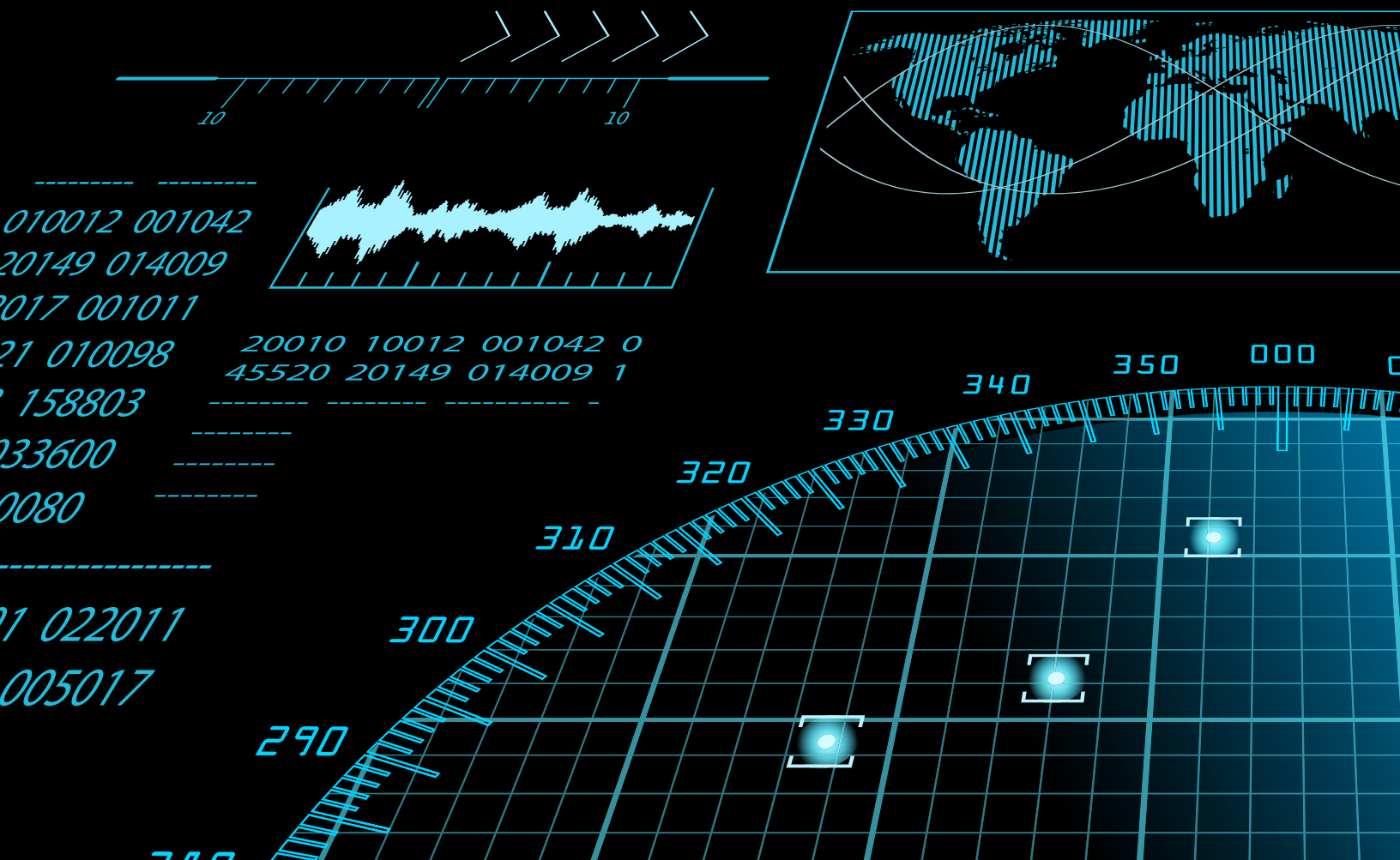
vmware

3 Essential Criteria for

Securing the Future of Warfare and Decision Superiority



As threats become more dynamic, the military needs integrated, accurate information in the right hands to achieve the mission. In a recent roundtable featuring experts from the U.S. Department of Defense and VMware, participants sought to define the future of warfare and how JADC2 can give the U.S. an edge, by outlining three vital attributes for future operations.

The battlefield is evolving quickly — due in part to emerging technologies — and as warfare changes, the Department of Defense is reshaping its approach to leverage data dynamism to enable decision superiority within the arena.

"Rapid advances in unmanned systems, robotics, data processing, autonomy, networking, and other enabling technologies have the potential to spur an entirely new warfighting regime," notes the Center for A New American Security, underscoring the need for the DoD to consider how to best use and defend against these new tools.

Spurring further urgency is the realization these new technologies will no doubt be adopted by state and non-state actors seeking to gain a competitive advantage over U.S. operations. If the U.S. military wants to retain its operational superiority, it needs to leverage emerging technologies to implement a new warfighting regime.

Enter, Joint All-Domain Command and Control (JADC2): The Defense Department's embrace of these emerging technologies, which aims to improve security while giving the U.S. a competitive and tactical edge.

In previous decades, each agency under the Department of Defense followed different guidelines around data management. In a recent Congressional Research Report, analysts found that, "traditionally, each of the military services developed its own tactical network that was incompatible with those of other services (i.e., Army networks were unable to interface with Navy or Air Force networks)."

JADC2 attempts to reconcile this incompatibility and provide the DoD with the integrated, accurate information it needs — compiling data from across disparate sources — ultimately informing real-time, machine-assisted decision making. Reconciling these different ways of operating, however, will take some effort.

"We have folks that have been around a long time and are used to doing things their way," said Dan Derick, Chief Data Officer of USSTRATCOM, during the recent roundtable with VMware and Government Executive Media Group, in which industry and military leaders gathered to discuss the future of warfare.

With these roadblocks in mind, what must the DoD do to move past today's silos toward a more collaborative way of using data and, in turn, secure decision superiority? At the recent roundtable, discussion centered around these roadblocks, with participants brainstorming solutions and narrowing in on three key criteria to ensure JADC2 succeeds.

1. Think Small to Go Big While Iterating Toward "Bomb-Proof Architectures"

To address data and information silos, Service branches need to move data to meet individuals on various edge devices and provide them with unfettered access to information. Liberating information, though, is easier said than done. During the roundtable discussion, experts discussed how the DoD could best provide the right data to the right person at the right time under JADC2.

One of the most promising ideas, championed by Major General Bob Stevenson J0, J3, and EMS of USSTRATCOM, focused on creating an application to allow individuals to request information on an as-needed basis, similar to how the ride-sharing app Uber works. By providing individuals with information at the critical moment of need, the Defense Department would be able to quickly and efficiently address data silos. Those familiar with Uber know, though, that the platform is susceptible to ransomware attacks, network outages, and a whole host of problems.

"Uber is an open architecture system that could easily be hacked," said Stevenson, noting that if the DoD were to use a similar approach, they would have to "robust it for a combat-contested environment."

Robust, "bomb-proof architectures" that Stevenson alludes to often require massive amounts of time, financial investment and human capital – all of which pose tremendous challenges to Services who are already strapped for time, cash and talent. As JADC2 is implemented across the Services, decision-makers need to focus on investing in methods and applications that bridge the gap to achieve mission outcomes in the short term, allowing warfighters to leverage data for critical mission threads now while iterating toward a more robust distributed data-mesh architecture for the long term. This point was emphasized by Rear Admiral Ronald Fritzemeier, Director, NC3 Enterprise Center at USSTRATCOM, who said, "We need to think small to go big."

Ensuring that the right data is transmitted to the right person at the right time is a process that will take time and effort. However, by delivering small, targeted amounts of mission-enabled data at the edge early and often, the DoD will better prepare itself to wield decision superiority against malign state and non-state actors.

2. Leverage Both Legacy and Modern Applications to Optimize Operations

While it's necessary to adopt modern technologies to facilitate a more integrated approach to data and to make JADC2 a reality, upgrading applications and operations is no easy task. The good news is that adopting completely new software and data capabilities isn't necessary — or even advised.

"The Army is a really, really big army. We cannot possibly modernize the entire Army all at the same time. It would break the bank and the entire department," said Major General Peter Gallagher, director of the network cross-functional team for Army Futures Command, speaking during the roundtable about the U.S. Army's own JADC2 modernization initiatives.

Instead, the DoD should rely on highly automated, software-defined and virtually consistent infrastructure environments across public cloud, operations centers and edge environments to reduce IT operations complexity and enable a combination of legacy and modern applications through a virtual single pane of glass. A combined approach to data management in this ecosystem will allow the Services to provide greater security, reliability and resilience around legacy applications while also tapping into the power and flexibility of modern cloud-native applications.

Moreover, by beginning to blend modern tools with legacy ones, the DoD can move strategically to new technologies, ensuring they don't adopt an architecture that's unmanageable. By moving toward modernization at a steady pace and maximizing use of open-standard, software-defined IT components with out-of-the-box managed service automation, Services can retain control of IT operations while ensuring they won't adopt an

“COVID brought to light the absolute need to invest in technology that allows all individuals to be able to work together remotely — it forced the DoD to find a way to securely communicate and video conference no matter where you are. We have to get out of our own way and work together.”

Katherine Escobar, Deputy Division Chief of the Data and Services Division for Cyber and Command, Control, Communications and Computers Integration (DD C5I), Joint Staff J6

out-of-the-box managed service automation, Services can retain control of IT operations while ensuring they won't adopt an infrastructure that requires them to add and maintain legacy components ad infinitum.

Gallagher notes that the Army has focused on scale and scope, modernizing at a strategic pace toward an architecture that can help to improve compatibility and security for the long term.

“We're working our way through, making sure that as we modernize, we're taking guidance from the G-3/5/7 and really trying to modernize what we can, when we can. To ensure that we've got the best solutions out there, but maintain some semblance of backward compatibility and forward compatibility so we can constantly evolve,” said Gallagher, referencing the U.S. Army's Operations, Plans, and Training directive, which focuses on defining approved training methods for multi-domain operations.

3. Collaborate, Collaborate, Collaborate!

Collaboration is by far the most important aspect of preparing for the future of warfare under JADC2, but it's also the most challenging and complex. In a recent Partnership for Public Service report, researchers found the majority of government agencies still struggle to collaborate internally. This is largely due to underlying systemic structures that encourage or mandate data silos.

However, according to Katherine Escobar, Deputy Division Chief of the Data and Services Division for Cyber and Command, Control, Communications and Computers Integration (DD C5I), Joint Staff J6, that might be changing thanks to the recent pandemic.

“COVID brought to light the absolute need to invest in technology that allows all individuals to be able to work together remotely — it forced the DoD to find a way to securely communicate and video conference no matter where you are. We have to get out of our own way and work together,” said Escobar during the roundtable.

Indeed, greater collaboration can help the DoD create the data sharing and problem-solving pathways it needs to make JADC2 successful.

By collaborating across teams, agencies and commercial partners like VMware, the DoD can command the expertise and information it needs to craft the robust, bomb-proof architectures and hybrid applications needed to secure decision superiority under JADC2.

Click the link to learn more about how VMware can help your agency prepare for the future of warfare under JADC2, or email us at JADC2@vmware.com