MPEs gain momentum for sharing data with allied partners

By Scoop News Group Staff

DOD efforts to establish ‘Mission Partner Environments’ with allied partners take on new urgency as global conflicts and national security policy require data interoperability.

Military readiness in an era when security challenges rarely respect borders increasingly demands new and more advanced levels of collaboration and coordination among a diverse and often ad hoc coalition of partners.

U.S. Defense Department leaders have long recognized the need for more unified information-sharing platforms across the military services. However, efforts to overcome the technical barriers that separate disparate information enclaves among NATO allies and other coalition partners are taking on new urgency and momentum.

Central to those efforts is the renewed vision for creating interoperable “Mission Partner Environments” (MPEs) that allow the military and its trusted partners to communicate and share sensitive information securely and in real-time with allied partners.

That vision represents a logical extension of the DOD’s Combined Joint All-Domain Command and Control (CJADC2) strategy to federate, jointly access and act upon relevant situational data. The DOD’s decision to rebrand the CJADC2 strategy last May by adding “combined” reflects a renewed focus on working with international partners as well as different military commands.

It is also fueling a new level of commitment to integrate mission and coalition partners into evolving technical standards, capabilities and policies — and toward a global IT environment rather than a U.S.-centric environment. That, and a combination of other factors, is bringing greater attention to the need for global MPEs and the pathways for achieving them.

THE INTEROPERABILITY IMPERATIVE

The nature of global conflicts and the need to work jointly with allied military and nonmilitary organizations has put increasing pressure on U.S. and Pentagon officials to overcome the technical and policy obstacles that shackle information sharing.

Danielle Metz, now chief information officer and director for information and management in the Office of the Secretary of Defense, made that point bluntly more than a year ago when she told a defense industry audience, “The combatant commanders have been screaming for the need to be able to seamlessly collaborate not only internally ... but across the mission partners.”

“And that mission partner can mean anything to anybody, depending on where you are located and depending on what that actual mission is,” she explained. “Quite frankly, the department has struggled for years to be able to articulate what was meant by ‘mission partner environments’ and then to be able to transition from a very physically network-centric type environment to a more cloud-based one,” Metz said.

Since then, the conflict in Ukraine has added new urgency to the need for near real-time information exchange across multiple domains. It has also heightened how modern warfare has taken on new dimensions in contrast to previous conflicts, including:

- Hybrid Warfare Challenges — Conventional military tactics are being fused with cyber and information warfare. This blending of domains necessitates seamless data sharing to counter and respond to such multifaceted threats effectively.
- Information Warfare and Disinformation — Adversaries in the Ukraine conflict extensively employed disinformation campaigns to shape perceptions and destabilize regions. Interoperable systems enable partner nations to collectively analyze and counter such narratives, ensuring a more comprehensive and coordinated response.
- Dynamic Battlefield Tactics — The conflict has underscored the rapid evolution of the battlefield, where situational awareness is paramount. Interoperability enables partners to share real-time intelligence, adjust strategies and respond swiftly.
- Civil-Military Coordination — The Ukraine conflict has also highlighted the importance of integrating civilian and military efforts in a comprehensive approach. Interoperable systems facilitate coordination among various agencies, ensuring a more cohesive and effective response.
Enhanced Situational Awareness: Mission partner environments provide a comprehensive and real-time view of the operational landscape, enabling all partners to make informed decisions based on a common operating picture.

Faster Decision-Making: By facilitating rapid data exchange, these environments expedite decision-making, ensuring timely responses to emerging threats or opportunities.

Optimized Resource Allocation: Interoperable systems enable efficient allocation of resources by avoiding duplication and ensuring that each partner’s capabilities are strategically integrated.

Cross-Domain Collaboration: Mission partner environments break down silos between military domains, promoting cross-domain collaboration essential for countering hybrid threats.

Future-Proofing: By adopting interoperable systems, coalition partners future-proof their capabilities, ensuring adaptability to evolving technologies and threat landscapes.

THE SHIFT TO DATA-CENTRICITY
One of the critical challenges to accelerating the exchange of information across the services and with trusted allies lies with the need to standardize how data is managed, according to U.S. Marine Corps Lt. Gen. (Ret’d) Dennis Crall, who last served as Director for Command, Control, Communications and Computers/Cyber and CIO of the Joint Staff (J6).

“We live the consequences of not getting everyone on the same page,” said Crall at one of his last press briefings. “The risk is, continuing the current trajectory apart from JADC2.”

Years ago, he recalled, the idea of bringing information together primarily focused on the network. “We were going to mesh ourselves to make sure information had a pathway. And then, we started getting focused on application centricity. It was all about the application. That went on for a few years… and finally, the latent discovery for us was data. Data is the element that we were pursuing.”

“And data-centricity has three parts to it. The first is people. We hardly ever speak of this because we are so focused on the second tenant, which is technology. And then the third piece is process or policy. If you want to capture data-centricity, you’ve got to line all three of those up. I am confident that we will solve the technical pieces of JADC2. There is a way to do this. I also believe that process and policy, under the right pressures, will form around the needs of the department, and we will find ways to do things in an efficient and safe way.”

APPROACHING MPEs DIFFERENTLY
The concept of mission partner environments to bring data together from disparate systems is hardly new. Efforts to exchange cross-domain military data date back decades to programs like the Combined Enterprise Regional Information Exchange System (CENTRIXS), U.S. Battlefield Information Collection and Exploitation Systems (BICES), and Combatant Command MPE networks.

What’s changing is the need to collapse and improve the speed and effectiveness of an expanding array of networks to share information securely with coalition partners.

“There’s going to be no action in the future where we’re operating alone,” commented Maj. Gen. Robin Anderton-Brown, U.K. Strategic Command capability director, in response to the SABRE MPE program. “And the importance of sharing information is only going to get more acute.”

The Defense Department has made strides in that direction by developing the Secret and Below Releasable Environment (SABRE). But clearly, more fundamental efforts need to be made to establish technical standards to clarify a path to advanced automation but secure data-sharing practices.

Eric Tapp, a 21-year veteran of the U.S. Army, is among those who’ve demonstrated how that vision for data interoperability has been gaining momentum. Before retiring from the military in 2022, Tapp led a team at USCENTCOM tasked with developing, testing and implementing a data-centric mission partner environment.

“The approach we took was to start from a user perspective — kind of the opposite direction where a lot of IT systems are developed from,” said Tapp, now the MPE lead at GDIT. Tapp’s team at USCENTCOM took a bottom-up approach using open-source standards, starting with basic documents, he explained in a recent interview. The goal was to identify the necessary handoff protocols and controls to share information with any foreign partner the DOD might have to engage with in the future.

“The [MPEs are] not just about connecting major Departments and Ministries of Defense, but connecting British and American F-35s and connecting warfighter to warfighter.”

Eric Tapp
GDIT MPE Lead
“We came up with subsets of ICAM — identity, credentialing, and access management — and a data tagging and management strategy to solve for the most basic things, allowing a user to markup data so that it could then go into the system and be shared appropriately,” he said. Eventually, they developed an application capable of factoring in a user’s country affiliation, clearance status and other information that permitted access to data appropriate to that user’s clearance, effectively enabling the collapse of those networks, which is still in progress, he said.

THE EXPANDING ROLE OF MPEs
Since joining GDIT a year and a half ago, Tapp has seen the need for MPEs take on mounting importance.

“Every combatant command, every service will eventually have to deal with this,” he said. “It is now not just about connecting major Departments and Ministries of Defense but connecting British and American F-35s and connecting warfighter to warfighter.”

“MPEs are moving from this massive point-to-point connection on a standalone network to the point where eventually all warfighters working in NATO or working in a coalition environment will be able to communicate effectively and share data,” he explained. “It will mean handling unclassified data all the way up to secret data. And it will mean [sharing information] in austere, disconnected environments, as well as inside of a big data center.”

What’s missing, contends Tapp, “is the operational art and the art of deployment.” At one level, it’s about greater standardization. But at a more practical level, it requires working with experts who “understand the operational art in weaving all this together.” And, he added, it will be critical that policy keep up with advances in the technology.

THE PATH TO MODERN MPEs
Tapp maintains that the task of developing effective MPEs that function across coalition partner domains requires a combination of development experience with military IT and communication systems and technical expertise around three core disciplines:

MPEs must be data-centric – By implementing established data tagging standards, such as the Intelligence Community Trusted Data Format (IC-TDF), and proven data wrapping mechanisms, it is readily feasible to encrypt and protect data while leaving metadata readable and actionable by different parties. That also requires comprehensive ICAM systems and Attribute Based Access Control (ABAC). However, with the proper setup, coalition partners can employ policy-based access control decisions that function at lightning speeds.

MPEs must leverage Zero Trust – By establishing zero trust security practices, employing micro-segmentation strategies, and designing systems to work with robust ICAM platforms, coalition partners can automate the fluid movement of data from one legacy system to another and into the hands of warfighters at the network edge.

MPEs must be transport agnostic – By embracing modern communications capabilities — that maximize available bandwidth, provide for automated, fail-over and offer dynamic routing across Wi-Fi, 5G, low, medium and geostationary SATCOM — coalition partners will be able to ensure information reaches warfighters in austere and disconnected environments.

GDIT has been helping the DOD modernize enterprise IT systems over the past five decades, but when it comes to developing MPEs, “I think we’re at an inflection point,” Tapp said. “What happens after the inflection point is a rapid evolution of capabilities and a rapid evolution of the number of users, types of data, velocity of data, usability of data, and exchange of data.”

When it comes to interacting with coalition partners, he stressed, “Ultimately, it’s not just the DOD that we’re talking about. It’s the entirety of the U.S. government.

Learn more about Mission Partner Environments and how GDIT is helping the U.S. Defense Department improve situational awareness and decision-making.