GENERAL DYNAMICS
Information Technology

1 April 2022

The MPE and JADC2

GDITs Vision and Commitment to the Warfighter

For more information, please reach out to Eric Tapp eric.tapp@gdit.com

Mission Partner Environment

Today, our national defense is intrinsically tied to our ability to effectively partner with our allies. As the newly released Joint All-Domain Command and Control (JADC2) strategy notes, the “ideal mission partner system integration is realized when data from each partner’s C2 systems can be accessed, viewed, and acted upon by every other partner.” We are not at the beginning of our MPE journey, but there is a great deal of work that needs to be done before the vision is realized.

The United States and our Allies have seen the benefits of partners and coalitions coming together to advance combined national interests and security efforts. While information-sharing during peacetime is important, timely sharing during a conflict can enable so much more because the strengths each partner brings to the fight can be more effectively leveraged.

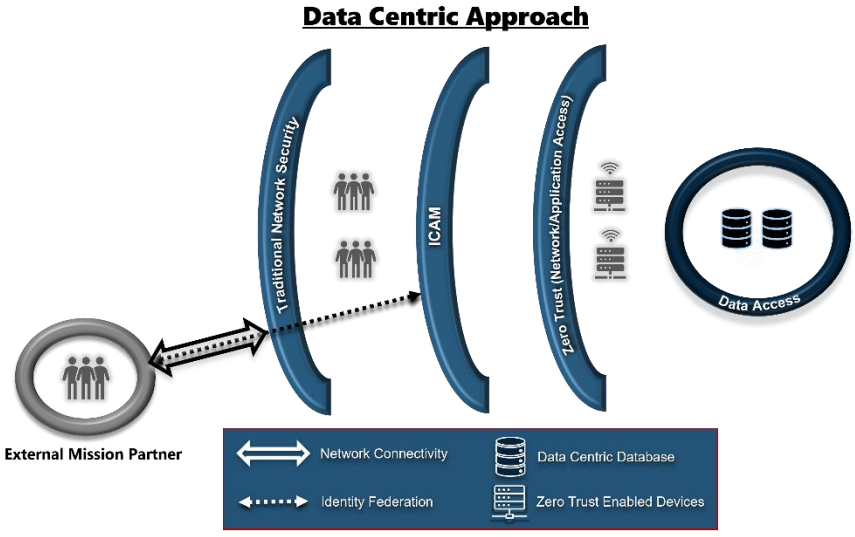
> The Joint Force Commander continuously strives to establish and maintain a common understanding of the operational environment through shared situational awareness with mission partners… integration is realized when data from each partner's C2 systems can be accessed, viewed, and acted upon by every other approved partner… JADC2 system interoperability is foundational for conducting combined and partnered operations with speed, precision, relevance, and security.
>
> LOE 5: MODERNIZE MISSION PARTNER INFORMATION SHARING - JADC2 STRATEGY

Future MPE

In the future, the MPE must be seamless and enable the Warfighter to sense, make sense, and act at the speed of operations. Disparate data types and formats at varying levels of releasability, streaming from different sensors and environments, present significant challenges. These challenges exist across the Combatant Commands, our Mission Partners and even the individual defense Services themselves.

The future of the MPE is a data-centric, zero trust based, transport agnostic architecture that provides maximum interoperability and flexibility to the Warfighter and coalition partners. These technologies allow us to develop environments with the ability to federate and control access to data based on identity, regardless of the user’s location or enclave.

With the advancements in coalition interoperability and information sharing, we can now envision a future where the MPE moves beyond just information sharing



and becomes the warfighting network. As the Services, Combatant Commands and the Department continue to align their vision and efforts, we grow closer to a time where Warfighters can conduct training and pre-deployment coordination with Mission Partners on the same network that they will conduct operations on. The goal is for Warfighters, at home or in theater, US or Coalition, to have access to the right information at the right time at the speed the mission requires.

Path to End State

We also know that the path forward will require interim solutions to achieve the desired end state. Right now, we have a vast collection of different MPE networks all meeting different needs. BICES, Combatant Command MPE networks, SABRE, CENTRIX, et al. We employ the TNE now to tie those environments together, but that capability comes a huge cost to Warfighter effectiveness. The future of the MPE and BICES lies beyond the TNE but how do we get there?

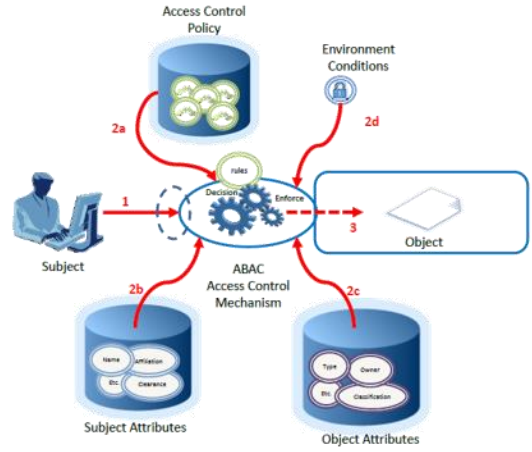


Figure 2: Basic ABAC Scenario

Data Centric

A data centric approach is the most viable way to achieve the seamless capability the Warfighter needs to fight and win. By refocusing our security efforts on the thing that truly matters on any network, the data, we can streamline the users access to it. Through the implementation of Attribute Based Access Control (ABAC), following NIST 800-162, we can ensure the right person, gets the right data, at the right time to make critical, time sensitive decisions. Matching tagged data to a user's individual identity attributes allows us to employ policy-based access control decisions at lightning speeds. The Intelligence Community Trusted Data Format (IC-TDF) as one example of a tagging standard that enables this type of data protection by wrapping the data object with metadata. This wrapping mechanism also allows for advanced protections such as object encryption while leaving metadata readable and actionable by access control policies. Ultimately, the important factor is that a tagging standard is selected, and the contents of the tag are made known. By governing the content of the tags, we can ensure that access control policies are applied appropriately. Through the implementation of comprehensive Identity, Credentialing, and Access Management (ICAM) systems, following NIST 800-63 (and more specifically -63C), we can form the basis of trust that allows us to federate with any other system with like capabilities, enabling internal decisions to be made based on trusted remote sources with the most up-to-date credential information.

Zero Trust

Zero Trust is the framework that will enable these data-centric capabilities to the edge and allow us to incorporate legacy, non-data aware applications during transition. As we can see from current event, mobility remains one of the most critical factors in warfare. Identity based access to the edge is critical to the Warfighter maintaining dominance. By employing principals such as micro-segmentation, a key element of the network security pillar of zero trust, we can implement ABAC down to the network segment level. Using this

technique, we can employ legacy, non-data aware, systems while new, data aware systems are being developed. It also provides an avenue to incorporate less technologically capable partners going forward. One key element to remember is that any solution has to integrate into existing operational networks as we move forward. Green field implementation is really only feasible at limited scale. Industry and the department must work together to iterate on solutions that extend into the operational and tactical realm in order to find the best solution for the Warfighter.

Transport Agnostic

Warfighter access must be transport agnostic to survive and win the future conflicts. Static PACE plans are antiquated stopgaps that must be replaced with maximized use of available bandwidth, automated fail-over and dynamic routing. WIFI, 5G, low/medium/geo-stationary SATCOM, and SDWAN are all critical technologies to ensure ubiquitous access to data and applications.

JADC2 Overlaps

Overall, the Joint All Domain Command and Control (JADC2) initiative is closely aligned with the MPE vision. The goal of JADC2 is to empower Joint Force Commanders to effectively command across all warfighting domains through the employment of innovative technologies to enable faster decision-making. JADC2 problems and MPE problems are inherently similar. Where MPE seeks to solve for sharing amongst different countries and at differing releasabilities, JADC2 seeks to do the same but between different security domains and technological separations. Each of the Services have numerous mission command systems that are specifically designed to support their associated warfighting functions. Each of them performs those functions across multiple security enclaves. Invariably, there are pieces of information on these separate enclaves that contribute to the whole picture needed for commanders to make the best decisions. Unifying that information is the crux of the problem. Both for JADC2 and MPE. Going forward, by ensuring we are sharing lessons learned and technologies amongst all JADC2 LOEs, we will make exponentially greater progress and achieve a more unified, national warfighting information system than through each effort alone.

Program Consideration

One additional consideration as we navigate the transitional period is the importance of a shared end state and the adoptions of an open standards-based approach. A shared end state is critical to ensuring that the multitude of parallel efforts all have common goals in mind. Each effort needs only make slight changes to their current azimuth to ensure we all reach that common endpoint. By incorporating open standards, systems and applications developed in parallel, even with little to no collaboration, will be able to achieve the level of interoperability needed to form a fully data-centric, zero trust, federated ecosystem.

Final Thoughts

At GDIT, our focus is to innovate around interoperability. The DoD employs hundreds of mission command applications and ensuring they can interoperate with each other and with mission partners is critical. We are working on the MPE to understand where those shortfalls are and to effect change, helping to ensure the US, and our partners, can collaboratively counter peer and near-peer adversaries.

Without question, the MPE and JADC2 initiatives are vitally important DoD efforts focused on fostering collaboration and communication. GDIT is proud to do our part to support these initiatives via our MPE work and are committed to its continued success.