A CJADC2 Primer: Delivering on the Mission of "Sense, Make Sense, and Act"

A CJADC2 Primer: Delivering on the Mission of "Sense, Make Sense, and Act"

Acting at the Speed of Relevance for Decision Dominance

What is CJADC2, and Why Does it Matter?

In March 2022, the Department of Defense announced the release of its Joint All-Domain Command and Control (JADC2) implementation plan: the final installment following both the JADC2 Strategy and Posture Review (a.k.a. gap analysis). It didn't take long for the initiative's name to expand to include "Combined," making it CJADC2.

In plain language, the CJADC2 mission is to enable decision making at the speed of relevance. It seeks to utilize the ever-increasing, disparate data flows across all domains (Sense), reveal un-intuitive patterns via automated and AI-enabled processes (Make Sense), and deliver the results to the U.S./Coalition warfighter (Act) at unprecedented speed.

Given the nature of the current threat, CJADC2's aim has moved from a warfighting "advantage" to a warfighting "necessity." Driven by the tenets of the Joint Warfighting Concepts (JWC), it is expressed in Service-derived "mission threads," tested in key, Service/Joint exercises, and evaluated by the Joint Requirements Oversight Council (JROC) to translate the successes into requirements.

While the pursuit of objective outcomes is best considered a journey, key elements are being realized at a record pace. "[C]JADC2 will enable the DoD to act at the speed of relevance to improve U.S. national security," said Deputy Secretary of Defense Dr. Kathleen Hicks. "[C]JADC2 is delivering capabilities beginning now, and it will continue to be funded in the coming years."

But while the name "CJADC2" is relatively new, there has been a need for this kind of interoperable, interactive communications flow for decades. Though DoD has the data and systems to create the CJADC2 end state, it has struggled to marry the two. Why hasn't this been its default modus operandi for DoD? Which challenges must DoD overcome to fully realize the CJADC2 vision?

Barriers to Overcome for an Effective CJADC2 Deployment

Acquisitional Challenges

Several challenges to CJADC2's success stem from the structure of the DoD network architecture, the burdensome acquisition process, and the lack of a true vendor-agnostic framework.

1. **Disjointed network architecture** – Companies and programs attempting to solve DoD's technical networking challenges in isolation will not meet CJADC2's needs. If an endpoint solution in one area won't "talk" with an endpoint solution in another area, the DoD cannot achieve an end-to-end mission thread.

2. **Slow and complex acquisition process** – The DoD acquisition process is well known to be very slow and price-driven—two characteristics that do not fit the rapidly changing IT environment. DoD acquisition officers are also risk-averse, which reinforces their reluctance to accept emerging technology solutions.

3. **No vendor-agnostic IT framework** – The largest DoD contractors often propose a holistic solution. These tend to be proprietary offerings that work well only if the customer invests in an entire ecosystem. Meanwhile, solutions based on policy changes, DoD-wide "Standardization," and/or synchronized acquisition are either doomed to fail or won't deliver on relevant time scales.

   Yes, policies should be changed, and acquisition should be modernized. But overly prescriptive Standardization—with a capital "S"—does not have a successful track record of innovating solutions that can complete with adversarial modernization. Instead, the DoD can benefit from small-s "standardization" that sets the frameworks and the discipline of expectations while providing flexibility. This encourages CCJADC2 implementation to focus more on future development while accommodating and accepting what the DoD already has in place.

Organizational Challenges

1. **Siloes** – The military has a long history of identifying its unique needs and purpose-building its own solutions. As a result, DoD developed a case of "not invented here" (NIH) syndrome as the commercial sector began to pursue DoD contract opportunities. This stems from DoD's understandably low tolerance for risk, given its "no-fail" mission requirements. Unfortunately, this has led to a tendency to "reinvent the wheel" when a "wheel" may already exist in the private sector. These internal efforts also tend to take longer, cost more, and lag behind commercial innovation.

   Each service's mission is unique, which only reinforces NIH syndrome. As a result, interoperability among Services is virtually unheard of.

2. **A walled-garden business model** – The DoD can't afford to acquire agile or cutting-edge technologies the same way it acquires complex, long-lead-time items like aircraft. For example, as the Defense-Industrial Complex grew, contractors used the DoD culture to build a business model based on providing large, expensive, closed, proprietary solutions with very long use cycles. For instance, the B-52 bomber was fielded by the U.S. Air Force in 1955—roughly 70 years ago. Boeing built fewer than 750 of them for the Air Force, and about 10% of them are still in use; the company has provided support and upgrades throughout their entire existence. That mindset endures today, even as missions accelerate. With that approach, it will always be late to meet mission needs.

3. **Slow accreditation and certification** – Another challenge to implementing CJADC2 has been accreditation and certification, especially in cybersecurity. Obtaining required approvals dramatically slows the delivery of new systems while the outdated systems they're intended to replace are riddled with data insecurities. Although it's permissible to share developmental/testing toolkits, they are typically bespoke and therefore unshared. And while reciprocity is an authorized action that could reduce fielding timelines, few ever use it, because they either do not know or do not care to know the testing rigor of the sponsor.

Technical Challenges

The organizational challenges are steep, but they're not uncommon for large entities navigating change. The technical challenges facing CJADC2 are also stiff, but not insurmountable (with one caveat). Generally, they fall into one of three categories:

1. **Poorly functioning software**
   - o *Closed systems.* These systems were not designed to be integrated and lack an interface to get data in or out; they need to be assessed individually to determine if/how this can be remedied.

- *Proprietary systems.* These systems have their own interfaces. Their proprietary nature means vendors often will not share documentation on the standards they use. This makes it difficult to fuse and integrate data.

- *Unintuitive and poorly designed human-system interfaces (HSI).* These make data entry cumbersome and error-prone; data visualization is confusing and non-intuitive, if available at all. These can be addressed with better-designed UI, automation, and AI/ML.

- *Lack of cybersecurity engineering resources.* Solutions must fit the requirements of Zero Trust architecture, but this requires making scarce engineering resources more available. This is important as networks and systems become connected, because a more connected environment expands the threat surface and potentially enables adversaries to migrate from one system to another.

- *Long capability delivery cycles.* These have been the norm when DoD upgrades system capabilities; CJADC2 must be agile to succeed and remain relevant, so it's essential to integrate DevSecOps capabilities into engineering to allow frequent iterations.

- *Non-networked systems.* These are less common than before, but DoD still has many systems and sensors that were not built to be network-enabled. One important caveat: some can be retrofitted to become network-capable, but in extreme cases, others cannot. These will need to be re-thought and redeveloped within a short timeframe.

2. Fragile networks

- *Segmented networks.* There are sensors, systems, applications, and people spread across multiple networks—both local and global—that either don't connect or require cross-domain solutions. This prevents data from getting where it needs to go. DoD can address this with the aforementioned cross-domain solutions, but it requires careful planning to minimize the number of nexus points required.

- *Challenging environments at the tactical edge.* Many networks are susceptible to both normal operation demands and actions by adversaries; CJADC2 solutions in this area must be equally robust and flexible. Development and testing must start with the tactical edge and work backwards.

3. Ineffective/inefficient data management

- *Too much data* is the blessing and curse of the information age. Challenges include identifying where data is located, which data to use, garnering permission to use it, addressing multiple classification issues. Solutions are emerging in the private sector, particularly through the use of ML and AI.

- *Data movement* is more than just whether there is a link from the sender to the intended recipients; it also encompasses attributes such as security, latency, resiliency, and throughput. Networked endpoints that are mobile and even communicate on the move (COTM) create additional constraints and limitations. While both unclassified and classified networks are an endemic challenge, operating secure networks can be significantly riskier in a highly contested cyber environment.

Additionally, we can expect the tactical edge to be immensely challenging with a peer/near-peer adversary who will work to degrade our freedom of movement in the electro-magnetic/digital spectrum.

The Sigma Defense Approach to CJADC2

Sigma Defense's philosophy for solving CJADC2 creates a unique framework aligning with our customers' challenges and priorities. We understand CJADC2's scope and how important it is to maximizing the potential of military operations. To create the connective tissue among land, sea, air, and space assets and their data, we focus our vision on DevSecOps—allowing us to integrate information rapidly, accurately, and securely from all spheres.

To enact our CJADC2 vision, Sigma Defense is vendor-agnostic—encompassing open source, open standards, open data, and more. We take an open-ecosystem approach and focus on partnerships with government and industry to deliver solutions. We are committed to enabling additional mission capabilities using the systems the customer already has in place. This increases the value of the investment that DoD has already made. This is both fiscally responsible and takes advantage of what is already deployed, translating to increased speed to capability.

Specifically, Sigma Defense is turning to a comprehensive Modular Open Systems Approach (MOSA) vendor-agnostic integrated solution built on our proven and accredited (USN/USMC ATO) DevSecOps framework. This delivers an agile solution for edge multi-INT sensor data ingestion, processing, management, AI/ML analytics, COP/CIP, and data queuing for potential semi-autonomous/autonomous effects. In this way, whether cached offline or collected online, these MOSA solutions powered by the Sigma Defense DevSecOps framework create a domain that enables the DoD to manage integrated solution sets.

We approach solutions holistically by identifying end-to-end mission threads (think Joint Warfighting Concepts) and synchronizing investments to address the key problems in all technical areas. This means making incremental progress in multiple technical domains that, together, deliver new capacity for warfighter success—enabling DoD to move at the speed of relevance.

We can achieve this because we've identified what to do and where to do it to the CJADC2 matrix. Following this process means that individual technical advancements are evolutionary—but the unlocked capability is revolutionary. The underlying technologies are well proven and do not require unproven technologies to be added to the mix. This delivers real capability with far less risk.

Significantly, Sigma Defense's gateway provides the ability to run a developmental environment that allows multiple users, even partnered forces, to collaborate. These applications allow the individual user to share, distribute, and host the ecosystem. The architecture allows the end user to create a VM or container tailored to ensure everyone is connected to enriched sensor data at the edge or across all domains. Technical integration allows for C2 capabilities for CI/CD and rapid dissemination information to all forces. Critical to the flow of data is inherent software for sensor data encryption that integrates accredited Cross Domain Solutions (CDS) to transmit sensitive data between boundaries, enclaves, and federated environments. This ultimately provides an unprecedented real-time information advantage and enables information dominance over all adversaries.

Ultimately, CJADC2 is about invoking the power of the Mission Partner Environment; it could easily be called "Combined Joint All-Domain Command and Control," or CJADC2. In a special report in National Defense, Cynthia Cook, director of the Defense-Industrial Initiatives Group and a senior fellow at the Center for Strategic and International Studies, observed that including allies under the CJADC2 umbrella will require identifying "triggers for sharing data, triggers for sharing data at different levels of

-time