CSIS BRIEFS

Battle Networks and the Future Force

Part 2: Operational Challenges and Acquisition Opportunities

By Todd Harrison

NOVEMBER 2021

THE ISSUE

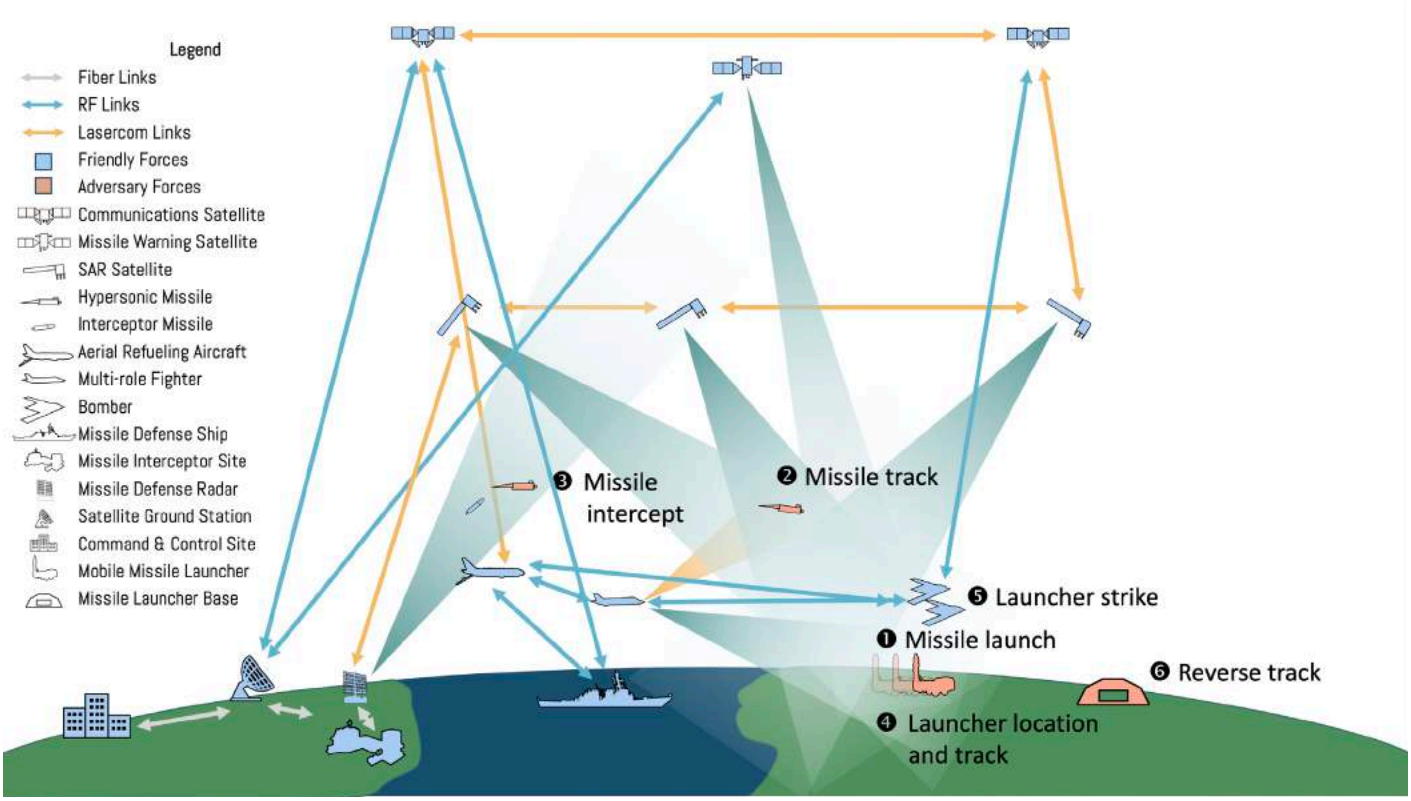
This CSIS brief is the second in a series on the future of battle networks and Joint All-Domain Command and Control (JADC2). This paper examines the operational advantages and adversary threats driving the requirements for greater interoperability and resilience in battle networks. It draws on lessons from previous attempts to improve battle network integration and explores how DoD can properly scope the problem it is trying to solve and organize itself to effectively and efficiently acquire the systems needed to realize its vision for JADC2. This paper recommends that DoD (1) clearly define organizational roles and responsibilities for JADC2 to include the possibility of creating a Joint Program Executive Office, a new independent agency under the Under Secretary of Defense for Research and Engineering (USD/R&E), or a lead combatant command (COCOM) for JADC2; (2) make key top-level architecture decisions, including narrowing the scope of JADC2 to just battle networks, as soon as possible; and (3) expand its typical make/buy analysis to include options for buying services instead of products and including systems that may be commercially owned and operated.

BATTLE NETWORK COMPETITION

Battle networks, and more specifically DoD's vision for JADC2, should ultimately be about enabling better options for commanders, speeding the tempo of decisionmaking, and optimizing effects in the battlespace. Connecting platforms and units across domains and with allies and partners by seamlessly passing surveillance, targeting, damage assessment, and other information from one platform to another improves the accuracy, range, persistence, and speed of effects. These improvements increase in a nonlinear manner as more platforms, sensors, communication paths, and other nodes are added to a battle network, transforming what was traditionally thought of as a force multiplier effect into a force exponent effect. The ultimate objective is to see farther with greater clarity and to act faster with more precision than one's adversary.

The hypothetical scenarios below help demonstrate how a battle network can use each of the functional elements discussed in the **first brief in this series** to close the sensor-to-shooter kill chain—or more appropriately, the sensor-to-shooter kill web. The first scenario illustrates the warfighting advantages integrated battle networks can provide. The second scenario shows the other side of the battle network competition—how an adversary can attempt to disrupt and degrade one's battle network. While an adversary may not have (or be successful in using) all the capabilities described to attack a battle network, these attacks can have significant effects even if they are only partially successful. Importantly, many of the steps in the process for both closing and breaking the sensor-to-shooter kill web may occur in parallel as operations unfold, and some processes may take longer and only yield valuable intelligence for future operations.

Figure 1: Example of Future Battle Network Operations



Source: CSIS Aerospace Security Project.

Figure 1 depicts a hypothetical future engagement in which an adversary launches a boost-glide hypersonic missile at U.S. and allied forces. The engagement is divided into six overlapping activities to depict how future battle networks could operate. In this example, a missile launch (1) is detected by a Space-Based Infrared (SBIRS) satellite in geostationary orbit (GEO) and/or by the infrared sensors on F-35s in the area. As the SBIRS satellite and F-35s follow the missile plume to higher altitudes, this data cues infrared and synthetic aperture radar (SAR) satellites in a variety of orbits (some of which could be commercial satellites) to characterize the threat and establish a high-quality track of the missile (2)—including after burnout of its booster stage. This tracking and characterization data is relayed through a variety of means (e.g., through RF and lasercom links, with military and commercial satellites, and among space-based and airborne communications nodes) to crewed and remotely crewed aircraft in the area as well as to sea- and land-based interceptor sites. The battle network acts as a distributed and resilient kill web rather than a serial kill chain to assist operators in deciding which platform is best positioned to fire interceptors (3). The trajectory data is also used to predict the likely impact site and alert forces in the area. While the intercept and other force protection activities are underway, the SAR satellites, F-35s, and other aircraft within range begin a combined response to track the missile launcher's movements on the ground (4). Commanders use this mesh view of the battlespace to determine what combination of strike aircraft, ships and subs with land-attack missiles, and ground units with long-range fires are best suited to destroy the missile launcher depending on where they are located, the weapons they have available, the time of flight to the target, and whether these forces may be needed for other missions (5). In parallel to all of this, analysts aided by artificial intelligence and machine learning (AI/ML) algorithms begin sifting through terabytes of archived surveillance data from space-based and airborne platforms to track the missile launcher's location in reverse from the time it launched its payload (6). The reverse tracking operation follows the missile launcher back in time to determine where it came from and how it operated to better respond to future attacks and, importantly, to refine predictive algorithms to anticipate future attacks before they occur.

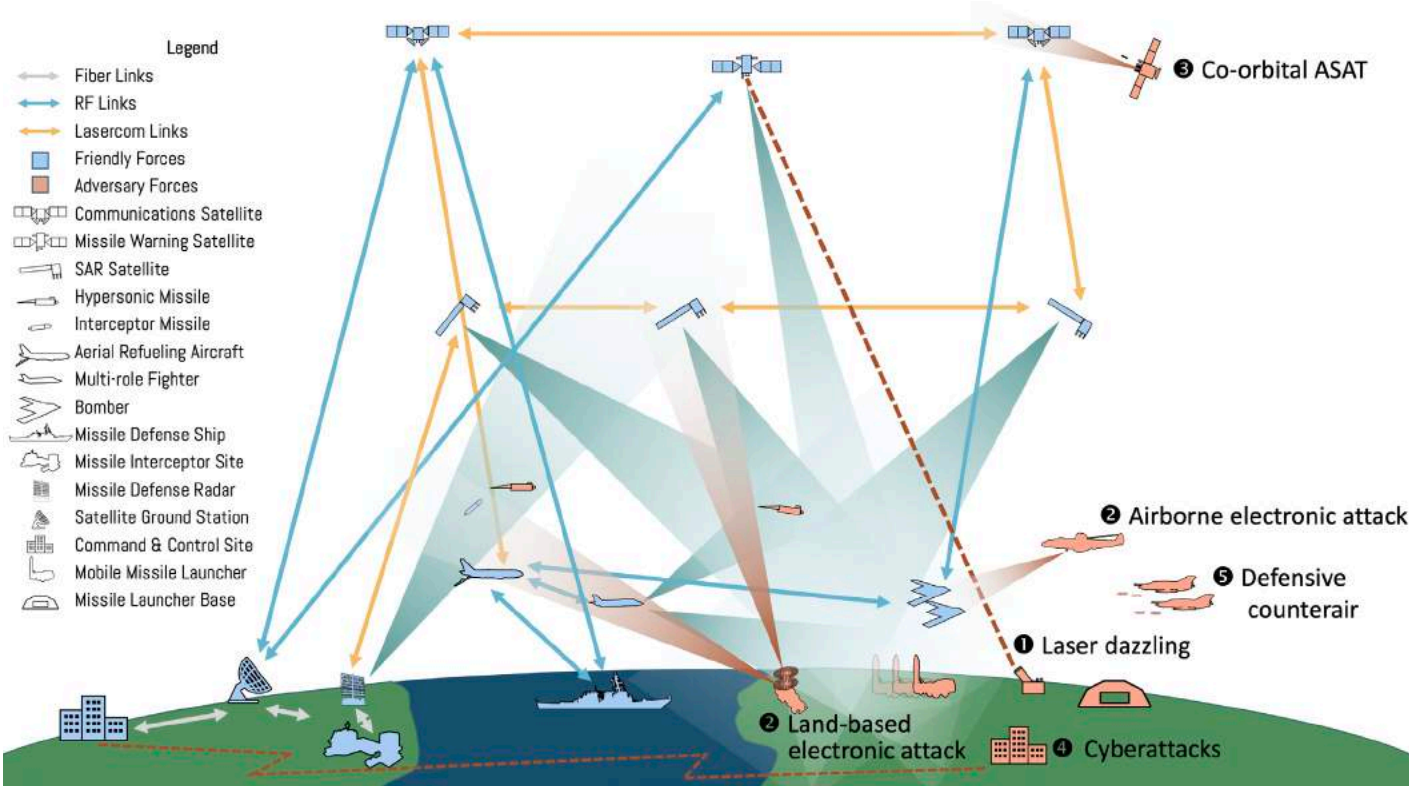
Figure 2 depicts the opposite side of the battle network competition in this hypothetical engagement, showing some of the ways an adversary can use the full spectrum of attacks to delay or prevent detection and to increase the odds its attack will succeed. Even before a missile is launched, an adversary could attempt to disable or degrade the airborne and space-based sensors used for missile defense. For example, a laser could attempt to dazzle the infrared sensors on satellites (1), land and airborne electronic attack systems could attempt to jam or spoof radar and communications systems (2), and co-orbital ASAT weapons could be used to jam or kinetically strike satellites used for missile warning and communications (3). Cyberattacks could also be used to target command and control sites, terrestrial networks, and satellite ground stations to disrupt these networks (4). Defensive counterair aircraft and surface-to-air missiles could threaten aerial refueling aircraft, airborne communications nodes, drones, and strike aircraft (5) to further degrade and disrupt the sensor-to-shooter kill chain.

As these examples illustrate, U.S. and allied forces must be able to protect their battle networks from attack while they simultaneously go on the offensive to disrupt the operations and battle networks of adversary forces. The systems that are best suited to operate in a contested battle network environment include platforms that are stealthy or can operate effectively outside (or above) the range of adversary defenses; methods of communication that are difficult to detect, intercept, and disrupt; distributed and diversified sensors and communication nodes (i.e., web or mesh networks rather than serial data links); and sensor fusion systems that automatically aggregate and pass data among platforms. The last characteristic is particularly important because operators are increasingly overloaded with tasks and require higher levels of automation in the way sensors are operated and data is transmitted. Where possible, the tasking of sensors should be automated or remotely controlled by others in the network to reduce the workload on platform operators and ensure the highest priority missions receive the data they need.

ROLE OF ARTIFICIAL INTELLIGENCE

This competition among battle networks, while not new, is an increasingly important component of modern warfare, and it is a competition that will largely be fought

Figure 2: Example of Future Counter Battle Network Operations



Source: CSIS Aerospace Security Project.

directly among machines in rapidly evolving ways. Much attention has been paid in recent years to how AI/ML can enhance warfighting capabilities, but robust and resilient battle networks are the underlying enabler that makes these enhanced capabilities possible—specifically the **communications** and **data processing** elements of battle networks. AI/ML algorithms depend on having timely access to large volumes of sensor data and the ability to communicate data products and analysis among decisionmakers and operators. Robust and resilient battle networks using AI/ML algorithms can speed decisionmaking and automate processes to enable algorithmic warfare at the tactical and operational level. In peacetime competition, these same networks and algorithms can greatly improve indications and warnings to prevent an adversary from avoiding detection and ultimately enhance deterrence.

Using algorithms to enhance indications and warnings is analogous in some ways to the way algorithms are already used for detecting and tracking the spread of diseases. For example, the AI system known as BlueDot was **able to detect the emergence of the Covid-19** virus in December 2019, before many global health agencies were aware. The system mines data from a variety of sources, such as statements from official health agencies, social media, livestock health reports, and airline ticketing data. BlueDot uses this information to locate outbreaks and predict how they will spread. It had similar success in 2016 when it predicted the spread of the Zika virus to Florida six months before it occurred. The key to the algorithm's success, however, is not that it takes the human out of the loop. Rather, it uses algorithms to find the "needles in the haystack" and present them to experts for analysis.

The potential advantages of algorithmic warfare are not unique to the United States. Other nations can use the same methods and capabilities to enhance the situational awareness and decision speed of their own forces. This will inevitably lead to peacetime competition in which algorithms are fighting one another through overlapping and competing battle networks. This algorithmic competition is similar in some respects to the **high-frequency trading systems** used in financial markets today. These systems use algorithms to process large volumes of data in real time, ranging from economic analysis and business financial reports to social media and news feeds. Trading algorithms use this information to make decisions in fractions of a second, competing against other investors across multiple markets simultaneously. In some cases, stock prices can be driven significantly higher or lower in short periods of time as one trading firm's algorithms battle against the algorithms of others.

A telling example of the potential consequences of not being prepared for the dynamics involved in competing algorithms is the "**flash crash**" that occurred on May 6, 2010. On that afternoon, the Dow Jones Industrial Average plunged by more than 9 percent in less than five minutes—the fastest decline in its history. This precipitated sharp drops in other stock exchanges. But as the trading continued, the Dow rebounded to near its original level within 15 minutes. While the factors that triggered the momentary crash continue to be debated, the dynamics observed that day were the result of competing algorithms at work in the markets responding to one another and to human traders.

In the military domain, the battle network competition can potentially have additional consequences that should be considered when developing operational concepts and testing algorithms and decisionmaking processes. For example, blinding an opponent's intelligence, surveillance, and reconnaissance (ISR) or severing command and control links among its forces during a crisis could increase the odds of miscalculation and escalation if adversary forces begin acting without accurate information. Moreover, without adequate situational awareness, an opponent may not be able to detect signs of de-escalation or could confuse benign or defensive actions with offensive or escalatory behavior.

OPERATIONAL CHALLENGES

As battle networks grow to encompass more capabilities, their complexity, effectiveness, and vulnerabilities will increase as well. Several operational factors should be considered when designing the battle networks of the future, including adversary threats, the resilience of networks to interference and attacks, and the interoperability of networks across the military services and with allies and partners.

THREATS

In his book, ***Kill Chain: Defending America in the Future of High-Tech Warfare***, Chris Brose provides a vivid account of how adversaries are exploiting vulnerabilities in battle networks to gain devastating advantage. He describes how in the 2014 seizure of Crimea, Russia's "Little Green Men" used electronic attacks to jam the control links to Ukrainian drones, prevent fuses on bombs from arming

properly, and target Ukrainian forces whenever they used radios to communicate. In one disturbing incident, the Russian forces called the mother of a particular Ukrainian commander they were trying to locate and told her that he had been badly injured. When the mother called her son's mobile phone, they quickly detected the signal, located him, and killed him with rocket fire.

The many operational advantages battle networks provide make them a natural target for attack. For example, both Russia and China have made significant advances in building and testing a suite of **kinetic and non-kinetic anti-satellite (ASAT) weapons** designed to disrupt U.S. and allied battle networks that depend upon or transit through space. Many of these ASAT weapons are designed to have reversible effects, such as jamming or spoofing satellite communications (SATCOM) and Global Positioning System (GPS) signals, and may be difficult to detect or could be publicly deniable. Forms of attack against battle networks that are difficult to attribute in a timely manner or can be ambiguous in terms of intent are ideal for use in gray zone activities. They can be used to confuse U.S. and allied indications and warnings or conceal low-level aggression and malicious activities. In situations like this, the best defense is **not necessarily a good offense**. Rather, battle network resilience gives senior leaders better options and more decision space.

RESILIENCE

Resilience can involve many forms of risk avoidance, management, and mitigation to allow networks to respond to and quickly recover from disruptions. Resilience assumes that disruptions and attacks will occur as part of both peacetime and wartime operations, and systems must be designed to accommodate this reality. Resilience can be enhanced by improving passive defenses, such as using **laser communications** (lasercom) or **forms of radio frequency (RF) communications** that are difficult for an adversary to detect, intercept, and disrupt. Likewise, having redundant nodes and paths in the network, such as multiple types of sensors that can identify and track a target and multiple communication paths to relay this information, improves both resilience and performance. Dispersion and diversification improve resilience by limiting single-point vulnerabilities in the network and greatly increasing how many targets (and domains) an adversary must attack to be successful. Resilience can also be enhanced by incorporating more active defenses into the systems that comprise a battle network. For example, aircraft acting as forward sensors can be armed with air-to-air missiles or electronic attack systems to protect themselves and other aircraft operating in a battle network.

One of the ways battle networks can be made more resilient and capable is by linking distributed sensors across multiple domains and orbits using diverse methods to collect information, such as infrared, optical, and radar. Distribution and diversification can be achieved, in part, by using existing assets for multiple roles and missions simultaneously, rather than keeping them focused on just one mission. For example, aircraft intended primarily for strike or counterair missions may also have significant ISR capabilities. From an altitude of 40,000 feet, airborne platforms can see a distance of roughly 240 miles on the surface, limited by the curvature of the Earth. Once a target missile or aircraft rises above the horizon, the distance at which aircraft can detect them increases even more and is ultimately limited by the resolution of the sensors. The infrared sensors used on the F-35, for example, have been able to **detect and track a rocket launch** at a distance of more than 800 miles.

Graceful degradation of capabilities under attack is also a key element of resilience. Graceful degradation in battle networks means using a mesh architecture and designing systems so that they dynamically break into smaller subnetworks as necessary and automatically connect to alternative networks as opportunities arise. AI/ML systems can be used to detect anomalies and network attacks that humans might otherwise miss and reconfigure networks as necessary. Alternative networks can include commercial systems used to provide additional surge capacity or to augment capabilities that have been degraded.

The GPS constellation of satellites is an example of a system that degrades gracefully. The Space Force typically **operates 30 to 32 satellites** in the constellation, even though only 24 are needed to provide global, continuous coverage. If some satellites are disrupted, the "extra" satellites in the constellation minimize the effects on users. And if the constellation drops below 24 satellites, their orbits can be modified to ensure continuous coverage of priority areas and direct coverage gaps to times and locations that are lower priorities. Moreover, GPS receivers that can use other space-based navigation systems, such as Europe's Galileo, Russia's GLONASS, or Japan's QZSS (to name a few), can continue to operate without disruption even if the entire GPS constellation fails. **Most commercial GPS chips** sold today (in phones

or other devices) use multiple constellations and are not dependent on GPS alone.

INTEROPERABILITY

The ability to share data across platforms, domains, military services, and allied nations is fundamental to the concept of JADC2. This vision of dynamic interoperability requires coordination on multiple levels: data standards, communications protocols and waveforms, multilevel security standards, and—perhaps most importantly—policy agreements with allies and partners that allow for real-time data sharing and access. Interoperability is not a binary variable—there are degrees of interoperability among systems and networks, and the right level of interoperability depends on the advantage provided and the costs involved.

A **May 2021 memo** from Deputy Defense Secretary Hicks outlines five "DoD data decrees" aimed at improving the Department's ability to share data and create data interfaces that are more automated and platform-independent. While this policy memo is broader than battle networks, it specifically cites its application to Joint All Domain Operations. It calls on the DoD chief data officer to issue policy and guidance to implement these decrees and work with the Joint Staff "to scale existing capabilities that have proven themselves in the battlespace and in real-world operations, simulations, experiments, and demonstrations."

DATA-CENTRIC VERSUS NET-CENTRIC

PRIOR EFFORTS

The current concept for data sharing and interoperability as applied to battle networks is reminiscent of the network-centric warfare concept of more than two decades ago. While the two initiatives are not identical—the current effort appears to be more focused on data sharing than connecting networks—their ultimate aims have many similarities. The **2001 Quadrennial Defense Review (QDR)** noted that "new information and communications technologies hold promise for networking highly distributed joint and combined forces and for ensuring that such forces have better situational awareness—both about friendly forces as well as those of adversaries—than in the past." The QDR was informed in part by Joint Vision 2020 and its concept of **network-centric warfare,** which it described as a way to achieve "asymmetric information advantage" by making data more readily available and usable. Underpinning network-centric warfare was the **Global Information Grid (GIG)**, which was scoped to include the entire information technology infrastructure of DoD, including government-owned and leased software and hardware across all missions (strategic, operational, tactical, and business).

To implement this vision nearly 20 years ago, DoD reshaped organizations, issued new policies and requirements, and redirected many acquisition programs already in progress. For example, in May 2003, Defense Secretary Rumsfeld redesignated the assistant secretary of defense (ASD) for command, control, communications, and intelligence (C3I) to be the ASD for network and information integration (NII). ASD/NII subsequently issued a number of policies that, for example, directed all DoD radio acquisition programs to adhere to the standards in the Software Communications Architecture (SCA) and to build only software-programmable radios with waveforms that could be ported across systems. The Joint Staff went a step further by issuing a set of **Net-Ready Key Performance Parameters (NR-KPPs)** to levee requirements across programs at all acquisition category (ACAT) levels.

LESSONS LEARNED

Despite the steps taken in the early 2000s to put DoD on a path to greater data sharing and interoperability across the joint force, the objectives of Joint Vision 2020 remained elusive when 2020 arrived. While a myriad of factors contributed to the slow pace of progress, several lessons stand out as providing valuable insights for current efforts.

- **Overly ambitious acquisition programs:** Many of the flagship acquisition programs intended to enable the new net-centric way of operating—programs such as the Army's Future Combat System (FCS), the Air Force's Transformational SATCOM (TSAT), the Navy's DDG-1000 destroyer, and the Joint Tactical Radio System (JTRS)—attempted to "leap ahead" and **skip a generation of technology**. Instead of leveraging advances in proven commercial technology or scaling back program objectives, too often these programs attempted to proceed with key technologies that were immature. Each of the programs listed above were ultimately canceled or curtailed, negating many of the efforts and funding that had been invested in net-centric warfare.
- **Assigning responsibility without authority:** ASD/NII was intended to be a focal point within the office of the secretary of defense (OSD) for net-centric transformation, but the office proved ineffective in practice and was eventually **eliminated,** along with

its counterpart office in the Joint Staff (J6), as part of efficiency initiatives within OSD. While it was given significant responsibilities for oversight and it pursued these with vigor, ASD/NII did not have the necessary authority to enforce its decisions. It could issue policies and weigh in during acquisition milestone reviews, but the military services retained the ultimate authority—budget authority—over program plans and schedules.

- **Issuing requirements and policies prematurely:** ASD/NII and the Joint Staff also fell into the trap of moving too quickly to implement policies and requirements without providing enough technical detail for effective implementation. Both the JTRS/SCA policy and the NR-KPPs created significant uncertainty and instability as acquisition programs struggled to understand how they could be implemented in existing programs at various stages of development. The **2003 JTRS/SCA policy**, for example, required all radios (including those operating at much higher frequencies and data rates) to be software programmable and SCA compliant. The problem was that the JTRS compliance guidelines (as they existed at that time) **were not intended** for the higher data rates and higher frequencies used for some applications, such as wideband and protected satellite communications. While it is important for policymakers to act quickly to rein in divergent programs, it is difficult for program managers and engineers to meet requirements that are ill-defined or ill-conceived.
- **Expanding the scope beyond battle networks:** Perhaps the most important lesson to learn from this earlier attempt at improving network and data interoperability is to scope the problem more appropriately. There are many advantages to be gained from greater interoperability and accessibility of data across all DoD networks used for strategic, operational, tactical, and business missions. But scoping the problem to include everything—as was the case with the GIG—is a recipe for dysfunction. Data sharing across backend business systems is a fundamentally different challenge than interoperability among battle networks, and the two should not be part of the same effort.

KEY DECISIONS AND RECOMMENDATIONS

Experience from the 2000s suggests that the organizational structure and acquisition strategy for JADC2 are likely to be determining factors in how much progress is made. In the coming months, DoD will need to make several key decisions that will have major implications for how JADC2 proceeds and its prospects for success. Time is of the essence because each of the military services and several defense-wide agencies are pressing ahead with JADC2-related programs of their own without a plan for how these efforts will converge or deconflict.

ORGANIZATIONAL ROLES AND AUTHORITIES

DoD needs to define the responsibilities and authorities of different organizations in the JADC2 development and implementation process—who is in charge of what, and how the various organizations involved will work together. Many different organizational models are possible, and as **CSIS's Morgan Dwyer previously noted,** DoD has tried many models in the past without much success. Below are a few examples of how DoD could assign roles and authorities for JADC2 development, and many hybrid approaches are possible that incorporate one of more of the organizational structures discussed below.

JPEO: DoD could create a Joint Program Executive Office (JPEO) to centralize the management of JADC2 development and procurement. This is similar to the approach tried for the JTRS program in the 2000s, which had **many shortcomings**. A lesson learned from the F-35 joint program office is that each of the services may benefit from establishing their own integration offices to liaison with the program office and ensure their requirements are properly represented. A joint program office can also make it easier to interface with allies and partners during development by providing a single point of contact for technical and programmatic issues, and it gives senior leaders in DoD and Congress a specific focal point (the person serving as the joint program executive officer) for accountability. However, the Department should be mindful not to create a major acquisition program (or set of interdependent programs) that is simultaneously too big to fail and **too big to succeed**.

Independent Agency: The Department could create a new independent agency under USD/R&E for JADC2 with its own acquisition authority and budget, similar to the Missile Defense Agency (MDA) and the Space Development Agency (SDA). Alternatively, it could expand the role of the Defense Information Systems Agency (DISA) to include JADC2, although this would go well beyond the agency's core capabilities and could come at the expense of efforts to modernize and support defense-wide IT systems. An independent agency could manage multiple ongoing programs and make trades across investments within its portfolio as prototyping and experimentation

begin to yield results. Like the JPEO model, an independent agency provides a focal point for interfacing with allies and partners, and it gives Congress and senior DoD leaders a specific person to hold accountable for results. One of the risks with using an independent agency is that it creates the possibility of redundancies and conflicts with the services' existing JADC2-related programs if they are not completely transferred to the new agency. There is also no guarantee that whatever the agency develops will be adopted and used by the services—a variation on the so-called valley of death. To be effective, an independent agency would require close coordination with service-led platform and munitions programs, strong support and a sustained commitment from top OSD leadership, and top-level decisions that are enforced by OSD through the annual program review process.

Lead Military Service: A different approach would be to designate a lead military service for JADC2 and direct the other services, agencies, and COCOMs to work with the lead service to ensure it develops the capabilities they need. This approach goes against the cultural instincts and the institutional incentives of the services, and the past seven decades since the Key West Agreement are replete with examples of where this approach has not worked well (e.g., close air support, missile defense). For the lead service approach to be effective, OSD and Joint Staff leaders would need to be consistent and disciplined during the Planning, Programming, Budgeting, and Execution (PPBE) and Joint Requirements Oversight Council (JROC) processes to ensure (1) that the lead service is fully responsive to the requirements of the other services, (2) that the lead service fully funds these efforts in each year's budget, and (3) that the other services do not begin alternative programs or procure incompatible systems on their own. In short, it would likely be a constant struggle to make this work.

Lead Functional Command: Another approach would be to designate a lead COCOM for JADC2 and provide it with independent acquisition authority in the model of Special Operations Command. This could be a new functional command created specifically for command and control, or this function could be assigned to an existing COCOM, such as Strategic Command, Space Command, Cyber Command, or Northern Command. Like the JPEO and independent agency models, designating a lead COCOM provides a focal point for interfacing with allies and partners and makes a senior commander accountable to DoD and Congress for delivering results. A challenge with this approach is preventing redundancies and conflicts with the military services if some of their JADC2-related efforts are not transferred to the command. A COCOM would arguably be more in tune with warfighter requirements to make cross-portfolio trades among programs than an independent agency, and if it retained operational authority for global command and control, it could also ease the transition of capabilities it develops into operational forces. A risk (and potential benefit) of this approach is that COCOMs typically have a relatively near-term focus on what the warfighter needs now and over the next couple of years. That could speed early development efforts to get new capabilities fielded sooner, but it could also hamper long-term strategic planning and the development of more complex capabilities.

Decentralized Development: The default approach if a deliberate decision is not otherwise made is to continue with decentralized development of JADC2 systems and components across the services and agencies with oversight by OSD and the Joint Staff. Responsibility could again be assigned to an ASD, and both the ASD and Joint Staff could issue policies, strategies, and KPPs that attempt to guide and coordinate the services' independent efforts—as was the case with ASD/NII and J6 for net-centric warfare in the early 2000s. The services would retain independent control of JADC2-related program schedules and budgets, which would likely proceed at different paces, depending on the other budgetary priorities within each service. But cross-program and cross-service interoperability becomes increasingly difficult if some programs are proceeding through development into procurement well before other programs. A likely outcome from this approach is that the services would each develop a new generation of stove-piped command and control systems that are highly capable within their respective domains. Cross-service and cross-domain interoperability would be a secondary priority—or worse, an unfunded requirement.

TOP-LEVEL JADC2 ARCHITECTURE

DoD also needs to make several key decisions about the overall architecture it envisions for JADC2 and how it will be implemented. These architectural decisions are interconnected with the organizational models discussed in the previous section because some architectures are better suited for development under certain organizational structures.

Scope: One of the most consequential architectural decisions is the scope of what is considered part of

JADC2—what types of systems, data, networks, and missions will be part of the architecture. OSD's **data strategy** and the **Joint Staff's JADC2 strategy** appear to be taking a broad, enterprise-wide approach to scoping JADC2. This approach was tried in the 1990s and 2000s with DoD's concepts for the GIG and net-centricity. The challenge is that the more the scope expands, the more divergent the mission requirements become and the more difficult it is to make meaningful progress. When drawing the lines around what is included in JADC2 and what is not, DoD should be mindful that not all interoperability is worth the price, and one-size-fits-all approaches to data standards, security, and communications protocols are often suboptimal at best and unworkable at worst. For example, do the data systems that process and manage medical records and spare parts inventories need to be interoperable with missile defense systems and tactical fighter networks? If not, then why make them part of the same effort and subject to the same policies?

The key to solving big problems is to break them into smaller, more manageable problems. The scope of JADC2 should be carefully narrowed to only the **five functional elements** that comprise battle networks: sensors, communications, data processing, decisionmaking, and effects. While there are many other information systems that these functional elements rely upon for support, the Department risks traversing down a slippery slope if it begins to include supporting systems within the scope of JADC2. Likewise, attempting to define the scope of JADC2 by the level of missions supported (strategic, operational, and tactical) leaves too much to interpretation because many of the systems and components that make up battle networks can be used for multiple missions. Importantly, DoD should acknowledge the increasingly important role commercial systems play in its battle networks—for sensing, communications, and data processing in particular—and include these systems in its architecture.

Common Operating System: A key architectural decision for JADC2 is whether to mandate the use of a common operating system or allow different parts of the battle network to run separate operating systems. Dissimilar operating systems within and across networks have been the traditional approach, and the main advantage is that it allows systems to be optimized for the functions they perform and the specific hardware they use. Technologies like **DARPA's System-of-systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES)** can be used to automatically generate "middleware" that integrates dissimilar systems into a battle network. However, this means that applications written for one operating system will not be natively interoperable with other systems and will require some level of preparation time and development work to make them interoperable. A common operating system creates the possibility of a truly open ecosystem for software development, which can reduce barriers to entry for small companies, encourage innovation, increase software reusability, and prevent **vendor lock**. The downside of creating a common operating system for JADC2 is that it would be difficult to develop one operating system capable of meeting the diverse and often yet-to-be-define requirements of users, and whatever is developed will not be fully optimized for any specific mission or hardware configuration.

Interfaces: The JADC2 architecture should also identify and define key interfaces both internally and externally. Interfaces are a critical part of defining the scope of the system, and DoD should carefully articulate the interfaces to the data systems and networks that support battle networks but are not directly part of the battle networks (delineating what is external to the architecture and therefore outside the scope of JADC2). External interfaces would include things like maintenance and inventory management systems, training systems, and personnel management systems. Interfaces are more than just technical specifications; they also include the policies and processes that govern how the interfaces will be used and by whom. The JADC2 architecture should also define the internal interfaces necessary for allies and partners to be part of U.S. battle networks and share data in real time, including the policies and agreements across nations to enable this connectivity both in peacetime competition and in conflict. Similar internal interfaces are needed to enable DoD to leverage and integrate commercial capabilities into battle networks to augment government systems.

MAKE/BUY/BORROW DECISIONS

In a traditional acquisition approach, one of the first analyses conducted is whether warfighter requirements can best be met by (1) upgrading or repurposing something that already exists, (2) buying something that has already been developed (i.e., off the shelf), or (3) developing a new material solution. While this framework still applies, given the rapid advancement of commercial technology in areas that have considerable overlap with military battle networks, the range of options should be expanded.

The first option (upgrading or repurposing) can mean adding new sensors and payloads to existing platforms or adjusting operational concepts to use existing platforms in different ways. For example, the military has added strike capabilities to ISR platforms, used strike platforms for ISR, and is planning to use aerial refueling aircraft as communication and data processing hubs. The third option (a new start development) should usually be considered as a last resort to meet truly military-unique requirements that cannot be met otherwise. New developments do not necessarily mean hardware programs—they could include applications (such as AI systems) that sit on top of the network to process and exploit information in new ways.

The second option, buying capabilities off the shelf, needs to be expanded and reimagined to fully leverage the capabilities resident in the private sector, including both traditional and non-traditional defense contractors. Buying something "off the shelf" can be done in many ways. The military can buy something as an off-the-shelf product and operate it using government personnel, what is known as government owned and government operated (GOGO). In some cases, the military can access similar capabilities by buying something as a service instead of a product, where the capability is commercially owned and commercially operated (COCO). In other cases, the military can lease a capability from a commercial firm and operate it using government personnel, what is known as commercially owned and government operated (COGO).

While the traditional approach to off the shelf is GOGO, the COCO and COGO approaches offer several potential advantages. First, COCO and COGO leverage private capital for the large, upfront expenses involved in developing and acquiring systems. It also allows the military to continually adjust how much of something it uses and only pay for what it needs rather than being saddled with a fixed number of assets at all times. It also gives the government flexibility to switch between capabilities quickly as technology improves and warfighter demands evolve, and this in turn gives contractors an incentive to invest their own capital in continuing to improve capabilities to better anticipate and meet the military's needs and win more task orders. Importantly, the COCO and COGO approaches give contractors a direct financial stake in reducing operation and sustainment costs, which often comprise the **majority of a system's total lifecycle cost**.

To be sure, commercial approaches are not appropriate in all situations. For example, the COCO and COGO approaches would not be suitable for missions where the operators and platforms may be put at grave risk (such as in a combat zone) or where the operators may be required to perform uniquely military functions (such as directing fires or carrying out strikes). And neither COCO nor COGO would be viable for capabilities that private firms cannot legally or financially develop on their own. The JADC2 acquisition strategy should, however, make a deliberate effort to decide what it needs to buy as a product versus a service and what needs to be government versus commercially operated.

CONCLUSION

Battle networks and the competition among them are an increasingly important component of military power. In a highly "informationized" warfighting environment, U.S. and allied forces must be able to protect their battle networks from attack while simultaneously attacking the battle networks of adversary forces. AI/ML algorithms running within highly integrated battle networks can be used to improve indications and warnings, speed decisionmaking, and enable an exponential increase in operational efficiency and effectiveness.

The resilience and interoperability of battle networks are closely connected because one enables the other. Resilience can be enhanced by passive and active defenses; and interoperability across services, domains, and nations enhances resilience by providing more opportunities for diversification and distribution of capabilities. But this does not mean that everything needs to be interoperable. The right level of interoperability among systems depends on the advantage provided and the costs involved.

This paper finds that current efforts to improve interoperability and data sharing across DoD—what has become known as JADC2—are similar to the "transformation" and "net-centric" initiatives of the late 1990s and early 2000s. DoD should heed the lessons from these initiatives when charting a path forward for JADC2. In particular, it should avoid (1) starting overly ambitious acquisition programs that attempt to "leap ahead" in technology, (2) assigning responsibility for JADC2 strategy and oversight to organizations that do not have budget authority over programs, (3) issuing policies and requirements without sufficient technical maturity, and (4) expanding the scope of JADC2 beyond battle networks.

DoD is at a pivotal point in JADC2 development where it needs to make several key decisions that will have long-term effects on how successful this attempt at creating a more networked and interoperable force will be. First,

it needs to define organizational responsibilities and authorities for JADC2 development and implementation. Several organizational models are available, such as consolidating programs into a JPEO for JADC2, creating a new independent agency for JADC2 development under USD/R&E, designating a lead service for JADC2, and designating or creating a COCOM for JADC2 development and operations. The default approach if no decision is made is to continue with decentralized development of JADC2 systems across the military services and agencies with oversight by OSD and the Joint Staff.

DoD also needs to make several important decisions about the JADC2 architecture and acquisition strategy. The most important architectural decision is the scope of what is considered part of JADC2, and the Department should learn from past efforts (like the GIG) and not expand the scope of JADC2 to include more than just battle networks. It needs to define key internal and external interfaces in the system, which also helps define the scope. DoD also needs to decide whether the military wants to use a common operating system for JADC2 and how that operating system will be developed and managed. Importantly, the JADC2 acquisition strategy needs to include processes for determining what it can buy as a product versus a service and what can be government versus commercially operated.

The many questions that remain unanswered for JADC2 are not merely academic or hypothetical. Billions of dollars are already being invested in programs, activities, and capabilities that are intended to form the battle networks of the future, and the ability of the U.S. military to maintain its qualitative advantage is at stake. The vision and ideas behind JADC2 are not new—they have been decades in the making, and the lessons drawn from past organizational and acquisition missteps should serve as a guide for how to proceed. It is not a question of if DoD will eventually achieve its vision for JADC2 but rather how long it will take to get it right. ■

Todd Harrison *is the director of Defense Budget Analysis and director of the Aerospace Security Project at the Center for Strategic and International Studies in Washington, D.C.*

This brief is made possible by support from General Atomics, Lockheed Martin, and general support to CSIS.

CSIS BRIEFS are produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s). *© 2021 by the Center for Strategic and International Studies. All rights reserved.*

Cover Photo: Petty Officer 3rd Class Marianne Guemo U.S. Northern Command