Congressional Research Service
Informing the legislative debate since 1914

Joint All-Domain Command and Control: Background and Issues for Congress

Updated July 8, 2021

Congressional Research Service
https://crsreports.congress.gov
R46725

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Joint All-Domain Command and Control: Background and Issues for Congress

SUMMARY

R46725

July 8, 2021

John R. Hoehn
Analyst in Military Capabilities and Programs

The Department of Defense (DOD) is in the process of a once-in-a-generation modernization of its approach to commanding military forces. Senior DOD leaders have stated that the department's existing command and control architecture is insufficient to meet the demands of the 2018 National Defense Strategy (NDS). Joint All-Domain Command and Control (JADC2) is DOD's concept to connect sensors from all of the military services—Air Force, Army, Marine Corps, Navy, and Space Force—into a single network.

DOD points to ride-sharing service Uber as an analogy to describe its desired end state for JADC2. Uber combines two different apps—one for riders and a second for drivers. Using the respective users' positions, the Uber algorithm determines the optimal match based on distance, travel time, and passengers (among other variables). In the case of JADC2, that logic would find the optimal platform to attack a given target, or the unit best able to address an emerging threat. For JADC2 to work effectively, DOD is pursuing two emerging technologies: automation and artificial intelligence, and new communications methods.

Several agencies and organizations within DOD are involved in JADC2-related efforts. The following list highlights selected organizations and projects associated with JADC2 development:

- **DOD Chief Information Officer:** Fifth Generation (5G) Information Communications Technologies.
- **Office of the Secretary of Defense (Research & Engineering):** Fully Networked Command, Control, and Communications (FNC3).
- **Defense Advanced Research Projects Agency:** Mosaic Warfare.
- **Air Force:** Advanced Battle Management System (ABMS).
- **Army:** Project Convergence.
- **Navy:** Project Overmatch.

As DOD develops new methods to command and control military forces, Congress may consider several potential issues:

- How can Congress consider JADC2-related activities in advance of validated requirements or cost estimates?
- How can DOD ensure interoperability among each of the military services' and allies' communications systems?
- How should DOD prioritize competing communications requirements for its future network?
- What role will artificial intelligence play in future command and control decisionmaking systems?
- What potential force structure changes will be necessary to meet JADC2 requirements?
- How should DOD manage JADC2-related efforts?

Contents

Figures

Tables

Appendixes

Contacts

What Is JADC2?[1]

Joint All-Domain Command and Control (JADC2) is the Department of Defense's (DOD's) concept to connect sensors from all of the military services—Air Force, Army, Marine Corps, Navy, and Space Force—into a single network. Traditionally, each of the military services developed its own tactical network, which was incompatible with those of other services (e.g., Army networks were unable to interface with Navy or Air Force networks). With JADC2, DOD envisions creating an "internet of things" network that would connect numerous sensors with weapons systems, using artificial intelligence algorithms to help improve decisionmaking.[2]

DOD officials have argued that future conflicts may require leaders to make decisions within hours, minutes, or potentially seconds, compared with the current multiday process for analyzing the operating environment and issuing commands.[3] The unclassified summary of the National Defense Strategy (NDS) Commission's report states that current C2 systems have "deteriorated" against potential peer competitors.[4] Similarly, the NDS identifies command and control systems as a modernization priority.[5] Congress may be interested in the JADC2 concept because it is being used to develop many high-profile procurement programs, as well as determining how effective and competitive the U.S. military could be against potential adversaries.

Figure 1. Conceptual Vision of JADC2

Source: https://www.monch.com/mpg/news/ew-c4i-channel/7334-saic-and-usaf-partner-for-jadc2.html.

[1] For a summary of JADC2 see CRS In Focus IF11493, *Joint All-Domain Command and Control (JADC2)*, by John R. Hoehn.

[2] Jim Garamone, "Joint All-Domain Command, Control Framework Belongs to Warfighters," *DOD News*, November 30, 2020, at https://www.defense.gov/Explore/News/Article/Article/2427998/joint-all-domain-command-control-framework-belongs-to-warfighters/. For a broader discussion of DOD's efforts for Artificial Intelligence, see CRS Report R45178, *Artificial Intelligence and National Security*, by Kelley M. Sayler.

[3] For example, according to joint operational doctrine, military commanders plan air operations between 72 and 96 hours in advance. See Department of Defense, *Joint Air Operations*, JP 3-30, Washington, DC, July 25, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf.

[4] See Gary Roughead, Eric Edelman, et al., *Providing for the Common Defense, National Defense Strategy Commission, The Assessment and Recommendations of the National Defense Strategy Commission, 2018*, p. 25, https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf.

[5] James Mattis, *Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Department of Defense, January 2018, p. 6, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

JADC2 envisions providing a cloud-like environment for the joint force to share intelligence, surveillance, and reconnaissance data, transmitting across many communications networks, to enable faster decisionmaking (see **Figure 1**).[6] JADC2 intends to help commanders make better decisions by collecting data from numerous sensors, processing the data using artificial intelligence algorithms to identify targets, and then recommending the optimal weapon—both kinetic and nonkinetic (e.g., cyber or electronic weapons)—to engage the target.

DOD points to ride-sharing service Uber as an analogy to describe its desired end-state for JADC2.[7] Uber combines two different apps—one for riders and a second for drivers. Using the respective users' positions, the Uber algorithm determines the optimal match based on distance, travel time, and passengers (among other variables). The application then provides directions for drivers to follow to deliver passengers to their destination. Uber relies on cellular and Wi-Fi networks to transmit data to match riders and provide driving instructions.

Some analysts take a more skeptical approach to JADC2. They raise questions about its technical maturity and affordability, and whether it is possible to field a network that can securely and reliably connect sensors to shooters and support command and control in a lethal, electronic warfare-rich environment.[8] Analysts also ask who would have decisionmaking authority across domains, given that, traditionally, command authorities are delegated within each domain rather than from an overall campaign perspective.[9] Some also question how much a human would be needed for JADC2 to make decisions in real time, and whether it is appropriate to reduce the amount of human involvement in military-related decisions.

What Is Command and Control: Dimensionality of C2 and Implications of Artificial Intelligence

One can view command and control through the context of the five questions: who, what, when, where, and how. Traditionally, Congress has focused on command and control through two different, yet related issues: authorities (the "who") versus technology (the "how"). The first issue that Congress has traditionally focused on reflects the authority a commander has to execute an operation.[10] This line of discussion focuses on the chain of command, reflecting the differences between the military services—charged with organizing, training, and equipping U.S. forces—and the combatant commands, who have the authority to employ forces abroad. This issue can be summarized by the question: "who commands forces?"

The second issue represents the technical aspects that enable commanders to make these decisions and transmit them to the field. Terms like *command, control, communications* (C3), *C3 plus computers* (C4), and *intelligence, surveillance, and reconnaissance* (ISR) enter the discussion.[11] This technical issue of command and control looks at the data (and method of collection) that commanders use to make decisions (i.e., ISR is the data to enable decisionmaking), the processing power to transform data into information, and the systems that enable

[6] Sydney J. Freedberg Jr., "Building JADC2: Data, AI & Warfighter Insight," *Breaking Defense*, January 13, 2021, https://breakingdefense.com/2021/01/building-jadc2-data-ai-warfighter-insight/.

[7] Rachel S. Cohen, "Want to Understand MDC2? Think About Uber, USAF Official Says," *Air Force Magazine*, September 23, 2019, https://www.airforcemag.com/want-to-understand-mdc2-think-about-uber-usaf-official-says/.

[8] Bryan Clark and Dan Patt, "JADC2 May Be Built To Fight The Wrong War," *Breaking Defense*, January 14, 2021, https://breakingdefense.com/2021/01/jadc2-may-be-built-to-fight-the-wrong-war/.

[9] See Department of Defense, *Joint Operations*, JP 3-0, Washington, DC, January 17, 2017, Incorporating Change 1 October 22, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910.

[10] For more information, see CRS In Focus IF10542, *Defense Primer: Commanding U.S. Military Operations*, by Kathleen J. McInnis.

[11] For detailed definitions of each of these terms, see Department of Defense, *DOD Dictionary of Military and Associated Terms*, Washington, DC, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

commanders to communicate their decisions to geographically distributed forces. This technical approach to command and control can be summarized as, "how do you command forces?"

Other dynamics of command and control answer other questions: which systems and units are being commanded (what), the temporal aspect (when), and geography (where). Congress has historically expressed interest in each of these questions in the context of specific, rather than general, issues. For example, rather than considering general purpose forces, Congress has focused on issues regarding nuclear forces and authorities associated with special operations.[12] Command and control topics associated with quick response to nuclear and cyber operations,[13] and to a limited extent in terms of electromagnetic spectrum operations,[14] have been other areas where the issue of timeliness has drawn congressional attention.

Regarding the "when," Congress has expressed interest in command and control associated with quick response to nuclear and cyber operations,[15] and to a limited extent in terms of electromagnetic spectrum operations.[16] However, the greatest sensitivity on "when" appears to be more tactically focused (e.g., when to have aircraft on target, when an assault on a building should begin); these decisions are often delegated to commanders. Finally, the geographic component presents unique challenges for commanding U.S. forces; as long as both the executive branch and Congress continue to support a global national security strategy,[17] geographic decisions largely represent tactical issues that are often delegated to individual commanders.

[12] For more information, see CRS In Focus IF10521, *Defense Primer: Command and Control of Nuclear Forces*, by Amy F. Woolf, and CRS Report RS21048, *U.S. Special Operations Forces (SOF): Background and Issues for Congress*, by Andrew Feickert.

[13] For more information, see CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary.

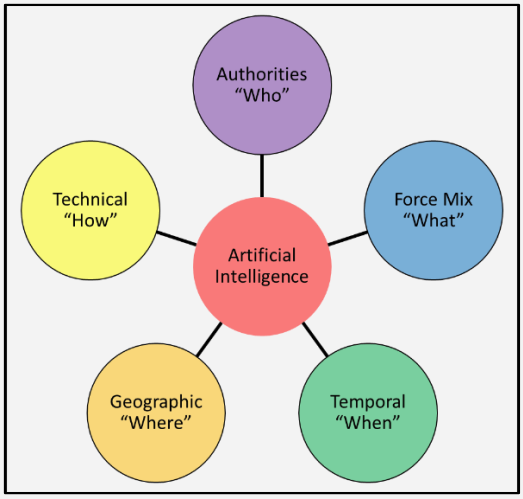
[14] Some analysts argue that spectrum management decisions will require increased speed to maintain communications networks. The presence of adversary electronic jamming, these analysts argue, will require split-second decisions to allow bursts of communications to forces.

[15] For more information, see CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary.

[16] Some analysts argue that spectrum management decisions will require increased speed to maintain communications networks. The presence of adversary electronic jamming, these analysts argue, will require split-second decisions to allow bursts of communications to forces. For example see U.S. Army, "Artificial Intelligence improves Soldiers' electronic warfare user interface," press release, October 8, 2019, https://www.army.mil/article/218705/artificial_intelligence_improves_soldiers_electronic_warfare_user_interface.

[17] For a detailed discussion on this issue, see CRS Report R44891, *U.S. Role in the World: Background and Issues for Congress*, by Ronald O'Rourke.

Figure 2. Dimensionality of Command and Control and Implications of Artificial Intelligence



Source: Congressional Research Service.

Figure 2 depicts how these issues are beginning to intersect through the introduction of artificial intelligence (AI) to optimize results among the various dimensions. As formations increase in complexity—particularly with formations designed for Joint All-Domain Operations—controlling these forces could potentially surpass the ability of human cognition, with algorithms used to help manage these forces. The U.S. military has stated that it intends to keep humans involved throughout the decisionmaking process,[18] but as U.S. forces introduce more artificial intelligence technologies into their decisionmaking apparatus, distinctions among the dimensions begin to blur. For example, the "who" and "how" begin to look similar, particularly as computers or algorithms make recommendations to commanders, who may not understand the information or the process that produced the recommendation.

AI could also affect other aspects of command and control, including the "what," "when," and "where." Combining the "what" and "where" elements can challenge adversaries' ability to find and engage U.S. forces; doing so can also challenge commanders' and their staffs' ability to maintain control of forces without systems helping to manage the complexity. From a "when" perspective, operations requiring quick decisionmaking, particularly electromagnetic spectrum and/or cyber operations, could surpass humans' decisionmaking ability. This raises a significant question of how much commanders can trust AI and how well human operators will need to understand why the AI system recommends a particular action.

Why Change Current C2 Structures?

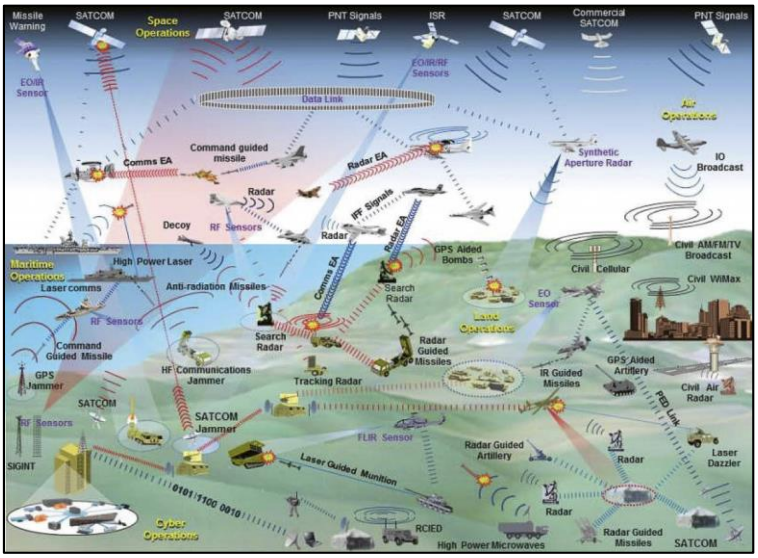
DOD currently performs C2 using separate segments of the battle space—primarily along the identified military domains: air, land, sea, space, and cyberspace. This structure exists because traditional threats came from a single system, like aircraft and tank formations. In response, the military developed highly sophisticated (but costly) sensors to surveille the battle space, providing information to a centralized command center (like an Air Operations Center or Army Command Post). Systems such as the E-3 Advanced Warning and Command System (AWACS) and the E-8 Joint Surveillance Target Attack Radar System (JSTARS) were optimized to provide

[18] Department of Defense, "DOD Adopts 5 Principles of Artificial Intelligence Ethics," press release, February 25, 2020, https://www.defense.gov/Explore/News/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/.

situational awareness to commanders at these centralized outposts, where they could then direct military forces.[19]

The future operating environment articulated by the NDS, the NDS Commission that reviewed it, and other sources describe how potential adversaries have developed sophisticated anti-access/area denial (A2/AD) capabilities (see **Figure 3**).[20] These capabilities include electronic warfare, cyber weapons, long-range missiles, and advanced air defenses.[21] U.S. competitors have pursued A2/AD capabilities as a means of countering traditional U.S. military advantages—such as the ability to project power—and improving their ability to win quick, decisive engagements.[22]

Figure 3. Visualization of A2/AD Environment



Source: https://www.japcc.org/electronic-warfare-the-forgotten-discipline/.

Senior DOD leaders have stated that access to information will be critical in the future operating environment.[23] In addition, these leaders have stated that to challenge potential peer adversaries, a multidomain approach is required (in which U.S. forces would use ground, air, naval, space, and

[19] Concepts like AirLand Battle emerged from this thinking. The theory behind AirLand Battle was that the United States maintained an advantage in long-range reconnaissance and strike capabilities. DOD decided to invest in platforms like AWACS and JSTARS (along with the long-range Army Tactical Missile System [ATACMS]) to engage Soviet tank reinforcements. David E. Johnson, *The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle*, RAND Corporation, PE301, August 2018, https://www.rand.org/pubs/perspectives/PE301.html.

[20] See Gary Roughead, Eric Edelman, et al., *Providing for the Common Defense, National Defense Strategy Commission, The Assessment and Recommendations of the National Defense Strategy Commission, 2018*, https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf.

[21] For more information on these systems, see CRS In Focus IF11118, *Defense Primer: Electronic Warfare*, by John R. Hoehn; CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary; and CRS In Focus IF11353, *Defense Primer: U.S. Precision-Guided Munitions*, by John R. Hoehn.

[22] Jan van Tol, Mark Gunzinger, Andrew F. Krepinevich, et al., *AirSea Battle: A Point-of-Departure Operational Concept*, Center for Strategic and Budgetary Assessments, Washington, DC, May 18, 2010, https://csbaonline.org/research/publications/airsea-battle-concept.

[23] For example, see testimony of Chairman of the Joint Chiefs Gen Joseph Dunford, in U.S. Congress, Senate Committee on Appropriations – Defense Subcommittee, *Department of Defense Budget Hearing*, 115th Cong., 2nd sess., May 9, 2018.

cyber forces to challenge an adversary's targeting calculus).[24] The Joint All-Domain Operations concept thus provides commanders access to information that can enable simultaneous and sequential operations using surprise, and the rapid and continuous integration of capabilities across all domains—thereby gaining physical and psychological advantages and influence and control over the operational environment.

Technological advances since the development of the AirLand Battle concept, which envisioned combining the Air Force and Army's efforts into a single plan to counter the Soviet Union in the 1980s, have enabled DOD to continue developing concepts for joint all-domain operations. Such technological advances include an increased number of methods to engage a target (including electronic and cyber means), the proliferation of relatively low-cost sensors, and increased processing power to transform data from these sensors into information.[25] This increased complexity is designed to offer options for military commanders and complicate adversary decisionmaking. The challenge for maintaining control of all domain operations is that the U.S. military C2 apparatus is not organized to make these types of decisions,[26] and the complexity and speed of the technology being used can exceed the ability of human cognition.

How Has Command and Control Evolved?

The U.S. military's traditional concept for command and control derives from the German military's "auftragstaktik," or mission-type orders.[27] Recognizing that disorder and the "fog of war" are inevitable in military operations, subordinate commanders were entrusted to operate semi-autonomously to achieve their commander's intent (i.e., the overarching goals of a mission) rather than having pre-scripted movements. Information from intelligence sources and reconnaissance took a long time—hours or potentially days—to reach commanders. To maintain control of forces, commanders relied on radio communications and paper correspondence. The limited amount of information available allowed commanders to direct forces across two dimensions—using a single domain responding to adversary actions.

At the height of the Cold War, Soviet forces presented a new problem for military forces: how to counter a numerically superior tank force. To counter this threat, the Army and Air Force proposed a novel approach that combined air and land power by developing new technologies to identify reinforcement locations. This concept was known as AirLand Battle. This three-dimensional approach sought to use advantages in intelligence, surveillance, and reconnaissance to "see deep" to direct firepower on reinforcements (i.e., "strike deep").[28] Deep strikes would complement the ground forces' ability to concentrate firepower at critical places, limiting the adversary's quantitative advantages. To support this vision of using deep strikes to prevent follow-on forces, the U.S. military needed to improve command posts to increase the speed of decisionmaking to direct forces, while still maintaining the tradition of following commander's intent. This need resulted in the development of new systems, like the JSTARS and ATACMS.[29] These systems enabled commanders to gain a quicker understanding of the battle space and to improve the response time to direct fires on enemy forces.

[24] CRS In Focus IF11409, *Defense Primer: Army Multi-Domain Operations (MDO)*, by Andrew Feickert.

[25] For a discussion on the needs to process data for Joint All-Domain Operations, see CRS Report R46389, *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition*, coordinated by John R. Hoehn.

[26] For example, DOD doctrine states that military operations are controlled in each domain. Thus, a land commander, an air commander, and a maritime commander each develops their own operational plan based on of a Combatant Commander's intent. These plans require substantial numbers of personnel, with minimal computer tools, and often require a person communicating via telephone to coordinate effects. See Department of Defense, *Joint Air Operations*, JP 3-30, Washington, DC, July 25, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf.

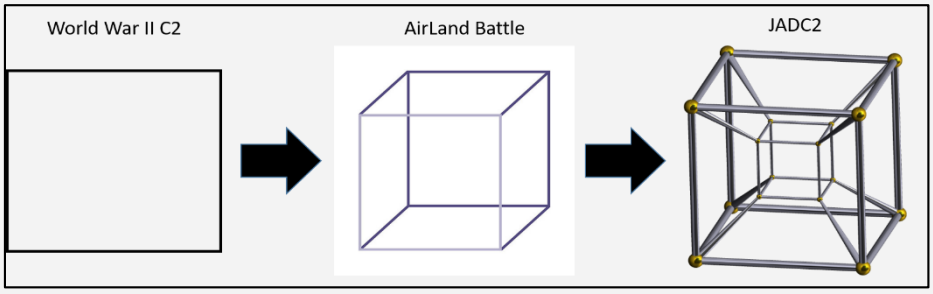
[27] Thomas J. Czerwinski, "Command and Control at the Crossroads," *U.S. Army War College Quarterly: Parameters*, vol. 26, no. 3 (Autumn 1996), pp. 121-132, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1788&context=parameters.

[28] Maj Thomas Gill, "The Air Land Battle - The Right Doctrine For The Next War," *Global Security* (1990), https://www.globalsecurity.org/military/library/report/1990/GTJ.htm.

[29] David E. Johnson, *The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle*, RAND Corporation, PE301, August 2018, https://www.rand.org/pubs/perspectives/PE301.html.

Over the past 20 years, China and Russia have observed the United States' method of war, identifying asymmetric methods to challenge U.S. advantages. China's military modernization, in particular, focuses on preventing the United States from building large amounts of combat power (limiting logistics), increasing risks for high-valued aircraft (tankers, spy planes, command and control aircraft), and increasing its naval footprint (limiting U.S. naval advantages).[30] To counter these new threats, DOD initially proposed the idea of using multidomain operations (which has since transitioned into the term *all-domain operations*). DOD contends that using one or even two dimensions to attack an adversary is insufficient, and that challenging an adversary's targeting calculus thus requires more complex formations (additional dimensions). The increasing complexity, combined with potentially decreasing times to respond to threats from emerging technologies, DOD argues, requires new methods to manage forces.

Figure 4. Changes in Complexity of Command and Control



Source: Congressional Research Service.

JADC2-Enabling Technologies

As DOD develops the JADC2 concept, two types of technologies play an integral role in this approach to command and control military forces: automation and communications.

Automation and Artificial Intelligence

Many senior DOD leaders have articulated that JADC2 is a concept (or perhaps a vision) rather than any specific program. In a January 2021 article, LtGen Michael Groen, director of the Joint Artificial Intelligence Center, stated that "JADC2 is not an IT [information technology] system ... it is a warfighting system…. Historically, you would have a large defense program, and you would spend years refining the requirements, and you would gather big, big bags of money, and then you would go to a defense contractor and spend more years building, testing, and then finally fielding something years and years later."[31] In this article, LtGen Groen described the role of artificial intelligence (AI),[32] and by extension the role of data and data structures, to enable these algorithms to inform commanders. According to LtGen Dennis Crall (director of the Joint Staff's

[30] Jan van Tol, Mark Gunzinger, Andrew F. Krepinevich, et al., *AirSea Battle: A Point-of-Departure Operational Concept*, Center for Strategic and Budgetary Assessments, Washington, DC, May 18, 2010, https://csbaonline.org/research/publications/airsea-battle-concept.

[31] Sydney J Freedberg Jr, "Building JADC2: Data, AI & Warfighter Insight," *Breaking Defense*, January 13, 2021, https://breakingdefense.com/2021/01/building-jadc2-data-ai-warfighter-insight/.

[32] This report uses the terms *artificial intelligence* and *algorithm* relatively interchangeably. Artificial intelligence combines many technologies—primarily databases, processors, and the algorithms themselves. In the context of JADC2, the primary technological advancement of artificial intelligence, however, is its predictive nature, which is derived from the algorithm, or the approach to analyzing the data.

command, control, communications, and computers/cyber chief information officer [JS J6]), artificial intelligence and machine learning are essential to enable JADC2.[33] LtGen Krall stated

> JADC2 is about automating all of it…. It is about taking advantage of that sensor-rich environment—looking at things like data standards; making sure that we can move this information into an area that, again, we can process it properly; bringing on cloud; bringing on artificial intelligence, predictive analytics; and then undergirding this with a network that can handle this, all domains and partners.[34]

Communications

According to DOD, developing JADC2 would require new communications methods. DOD's current communications network has been optimized for operations in the Middle East.[35] As a result, DOD uses satellites as the primary method to communicate with forces abroad. These systems face latency (time delay) issues and are not designed to operate effectively in the presence of electronic warfare.[36] These older architectures rely on satellites in geosynchronous orbits, which orbit approximately 22,200 miles (35,800 kilometers) above the earth. New applications, like AI, will potentially require additional data rates that current communications networks might not be able to support—particularly as DOD increases the number of sensors to provide additional data to improve algorithms. The introduction of autonomous systems, such as the Navy's Large Unmanned Surface and Undersea Vehicles and those resulting from the Army's growing interest in robotic vehicles,[37] could need both secure communications and short latency to maintain control of these systems.

Current JADC2 Efforts

The Joint Staff is the DOD organization responsible for developing the Joint All-Domain Command and Control concept strategy. In addition, there are a number of ongoing studies and efforts connected to the JADC2 concept. Each of the military departments (Army, Navy, Air Force), along with DOD agencies like the Defense Advanced Research Projects Agency (DARPA) and Office of the Undersecretary Secretary of Defense for Research and Engineering (OSD [R&E]), are developing technologies and concepts. The following sections briefly describe selected organizations' efforts.

---

[33] Theresa Hitchens, "Exclusive: J6 Says JADC2 Is A Strategy; Service Posture Reviews Coming," *Breaking Defense*, January 4, 2021, https://breakingdefense.com/2021/01/exclusive-j6-says-jadc2-is-a-strategy-service-posture-reviews-coming/.

[34] Ibid.

[35] U.S. Government Accountability Office, *Defense Satellite Communications: DOD Needs Additional Information to Improve Procurements*, GAO-15-459, July 17, 2015, https://www.gao.gov/assets/680/671484.pdf.

[36] Traditional satellite communications rely on satellites in geosynchronous orbit. Having satellites stay in the same spot in the sky (relative to earth) facilitates communications because the satellite location is known. However, these satellites orbit more than 22,000 miles above earth, increasing the amount of time (latency) for a radio transmission. MAJ Andrew H. Boyd, *Satellite and Ground Communications Systems: Space and Electronic Warfare Threats to the United States Army*, Association of the U.S. Army, November 7, 2017, https://www.ausa.org/publications/satellite-and-ground-communication-systems-space-and-electronic-warfare-threats-united.

[37] For more information, see CRS Report R45757, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress*, by Ronald O'Rourke, and CRS Report R45392, *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*, coordinated by Andrew Feickert.

Joint Staff J6: JADC2 Strategy

The lead DOD organization tasked to develop a JADC2 strategy is the Joint Staff J6 directorate for command, control, communications, and computers/cyber.[38] Originally envisioned to improve the joint force's interoperability (e.g., making sure radio systems can communicate with one another), the JADC2 strategy expanded this focus, developing an information-sharing approach that enables joint operations by providing data for decisionmaking.[39] In addition to developing a strategy, the J6 organizes a JADC2 cross-functional team, through which the services and DOD agencies coordinate their experiments and programs.[40] This aligns with both the DOD Data Strategy and the Deputy Secretary of Defense's efforts of creating a data advantage.[41] The strategy has identified five lines of effort to enable the JADC2 framework:[42]

1. Data enterprise
2. Human enterprise
3. Technical enterprise
4. Nuclear Command, Control, and Communications (NC3)
5. Mission partner information sharing

The Joint Staff J6 states that there will be no single program or line item for JADC2.[43] At a press briefing on June 4, 2021, LtGen Crall stated Secretary of Defense Austin had approved the JADC2 strategy.[44]

OUSD Research and Engineering (R&E): Fully Networked Command, Control, and Communications (FNC3)

According to OUSD R&E "FNC3 identifies, initiates, and coordinates research, development, and risk reduction activities for key enabling technologies [for command, control, and communications]. These activities will encompass distinct but interrelated efforts across the defense enterprise, monitored and synchronized by FNC3 staff in OUSD(R&E)."[45] Dr. Michael Zatman, the Principal Director for FNC3, describes the overall vision of FNC3 consisting of three layers—physical, networking, and application—which provide a tailored approach to developing

[38] Theresa Hitchens, "Exclusive: J6 Says JADC2 Is A Strategy; Service Posture Reviews Coming," *Breaking Defense*, January 4, 2021, https://breakingdefense.com/2021/01/exclusive-j6-says-jadc2-is-a-strategy-service-posture-reviews-coming/.

[39] Theresa Hitchens, "EXCLUSIVE: 'Do-Or-Die' JADC2 Summit To Crunch Common Data Standards," *Breaking Defense*, January 12, 2021, https://breakingdefense.com/2021/01/exclusive-do-or-die-jadc2-summit-to-crunch-common-data-standards/.

[40] Theresa Hitchens, "OSD & Joint Staff Grapple With Joint All-Domain Command," *Breaking Defense*, November 14, 2019, https://breakingdefense.com/2019/11/osd-joint-staff-grapple-with-joint-all-domain-command/.

[41] Department of Defense, *Data Strategy: Unleashing Data to Advance the National* Defense, September 30, 2020, at https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF, and Deputy Secretary of Defense Kathleen Hicks memorandum, *Creating Data Advantage*, May 5, 2021, at https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/DEPUTY-SECRETARY-OF-DEFENSE-MEMORANDUM.PDF.

[42] Telephone conversation between the author and Joint Staff J6, April 30, 2021.

[43] Ibid.

[44] Department of Defense, "Pentagon Press Secretary John F. Kirby Holds a Press Briefing," press release, June 4, 2021, https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2647056/pentagon-press-secretary-john-f-kirby-holds-a-press-briefing/.

[45] OUSD R&E FNC3 Information Paper, April 28, 2021.

command, control and communications systems that aligns with the commercial sector's best practices.[46] Both the physical and networking layers provide the communications infrastructure, which connects a variety of applications. The physical layer represents the radios and transmitters themselves, while the networking layer manages the applications' access to the physical layer by developing DOD-optimized versions of emerging commercial software defined networking techniques such as network slicing.[47] All three layers are designed to increase interoperability and resiliency (i.e., the ability to prevent the network from being jammed or disrupted) and provide the appropriate quality of service for each application.[48] Conceptually, example applications could be nuclear command, control, and communications (NC3); ISR; a fire control mission; and logistics.

According to Dr. Zatman, FNC3 serves as the mid- and long-term technical vision of JADC2,[49] while each of the services (outlined in the following sections) have high-profile efforts focused on developing the near-term acquisition strategies. For example the Department of the Air Force's Advanced Battle Management program is designed to be deployed within the next three years by focusing on mature technologies. OUSD R&E leverages less mature technologies across its portfolio—including technologies developed by DARPA, the Defense Innovation Unit, the Strategic Capabilities Office, the services, and others—to provide the longer term technical means of implementing JADC2.

DOD CIO: 5G Technologies[50]

DOD has proposed that commercial advances in 5G wireless technologies provide the ability to transfer more data (commonly called *data throughput*) and lower latencies.[51] DOD argues that it requires these capabilities to process the increased amount of data from numerous sensors (e.g., satellites, aircraft, ships, ground-based radars), and to process this information at the "edge" (at the same site as the radio receiver). Another aspect of 5G technologies that could enable new command and control concepts is dynamic spectrum sharing. As the electromagnetic spectrum becomes more congested, the federal government has started allowing multiple users to operate on the same frequency band (known as spectrum sharing). The DOD CIO argues that spectrum sharing technology allows for communications systems to transmit and receive data in the

[46] Telephone conversation between the author and Michael Zatman, Principal Director Fully Networked Command, Control, and Communications (FNC3), April 27, 2021. For more information on commercial best practices, see ISO/IEC 7498-1:1994 *Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model*, at https://www.iso.org/standard/20269.html.

[47] OUSD R&E FNC3 Information Paper, April 28, 2021. For more information on network splicing see Peter Rost et al., "Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks," *IEEE Communications Magazine*, May 2017. Rost et al. define network splicing "as a concept for running multiple logical networks as independent business operations on a common physical infrastructure." For DOD this represents being able to segment the network for different applications.

[48] Quality of service refers to measures affecting a network's performance. This includes metrics like packet loss, bit rate, throughput, transmission delay, and availability. For more information see International Telecommunication Union (ITU) "Series E: Overall Network Operation, Telephone Service, Service Operation, and Human Factors," September 2008, at https://www.itu.int/rec/T-REC-E.800-200809-I/en.

[49] Telephone conversation between the author and Michael Zatman, Principal Director Fully Networked Command, Control, and Communications (FNC3), April 27, 2021.

[50] For an overview of DOD 5G initiatives, see CRS In Focus IF11251, *National Security Implications of Fifth Generation (5G) Mobile Technologies*, by John R. Hoehn and Kelley M. Sayler.

[51] CRS Report R45485, *Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress*, by Jill C. Gallagher and Michael E. DeVine.

presence of interference. In September 2020, DOD CIO issued a request for information to industry, on how to approach dynamic spectrum sharing. On January 21, 2021, 67 responses to the request for information had been posted.[52]

DARPA: Mosaic Warfare

Mosaic Warfare represents a series of DARPA-sponsored projects designed to use AI to combine systems and networks not traditionally designed to interoperate. Conceptually (see **Figure 5**), these projects would be able to take raw intelligence collected from a satellite and turn that data into targetable information passed to a "shooter"—in this case, a cyber-weapon, electronic jammer, missile, aircraft, or any other weapon that might be able to affect the desired target.[53] A second aspect of this approach uses AI-generated software to enable different radios to communicate with each other within an hour.[54] A third aspect is a project devoted to airspace de-confliction. Rather than relying on a number of specialized personnel to manually identify the location and status of air assets, for example, DARPA software automatically tracks this information and relays it to commanders.[55] As analysts Bryan Clark and Dan Patt of the Hudson Institute explain, Mosaic Warfare "seek[s] to impose multiple overlapping dilemmas on enemy forces that disrupt their operations and thus prevent them from reaching their objectives in time."[56]

[52] "Defense Spectrum Sharing Request for Information," Defense Information System Agency, updated January 21, 2021, https://beta.sam.gov/opp/8f3f0321da074e75a588c8833265791d/view.

[53] Telephone conversation between the author and Timothy Grayson, Director, Strategic Technology Office, November 20, 2020.

[54] Currently, the only way for radio protocols not designed to communicate with one another to do so is to use a radio gateway. This new method would replace physical infrastructure with software. Sydney J. Freedberg Jr, "DARPA AI Builds New Networks On The Fly," October 28, 2020, https://breakingdefense.com/2020/10/darpa-builds-ai-to-reorganize-machines-humans-on-the-fly/.

[55] Sydney J. Freedberg Jr, "DARPA AI Builds New Networks On The Fly," October 28, 2020, https://breakingdefense.com/2020/10/darpa-builds-ai-to-reorganize-machines-humans-on-the-fly/.

[56] Bryan Clark and Dan Patt, "JADC2 May Be Built To Fight The Wrong War," *Breaking Defense*, January 14, 2021, https://breakingdefense.com/2021/01/jadc2-may-be-built-to-fight-the-wrong-war/.

Figure 5. DARPA's Vision of Mosaic Warfare

Source: https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare.

Department of the Air Force: Advanced Battle Management System (ABMS)[57]

The Advanced Battle Management System was originally envisioned to replace the E-8 Joint Surveillance and Target Attack Radar System (JSTARS).[58] The Air Force transitioned the ABMS program in 2019 from developing things—like aircraft or radars—to a "Digital Network Environment that connects warfighting capabilities across all domain, and every echelon, to achieve global decision advantage."[59] In other words, the Air Force pivoted from building a platform to support commanders and decisionmaking (like the E-8 JSTARS) to building a secure, "cloud-like" environment that provides commanders with near real-time data using AI and predictive analysis. According to the Air Force, the ABMS program will develop capabilities along six product lines: sensor integration, data, secure processing, connectivity, applications, and effects integration.

The Air Force has held three "on-ramps" (a term the Air Force uses to describe a demonstration) to demonstrate its approach to ABMS.[60] The first on-ramp, held in December 2019, demonstrated the service's ability to transmit data from secure communications used by F-22s to Army and Navy systems. The second on-ramp enabled an Army howitzer to shoot down a surrogate cruise missile. In addition, the Air Force provided this "cloud-like" Zero Trust tablet—a security feature

[57] For more information on ABMS, see CRS In Focus IF11866, *Advanced Battle Management System (ABMS)*, by John R. Hoehn.

[58] The E-8 JSTARS was developed in the 1980s to counter Soviet tank threats, particularly the so-called second echelon (i.e., Soviet reinforcements). This aircraft uses a synthetic aperture (with radar operators onboard) to identify potential targets. Operators onboard the aircraft then direct U.S. and allied aircraft to engage these targets.

[59] "Department of the Air Force Requirements Decision Memorandum for the Advance Battle Management System Strategic Requirements Document," Department of the Air Force, DAFRDM 09-20-02, signed October 14, 2020, by General John W. Raymond, U.S. Space Force, and General Charles Q. Brown, U.S. Air Force.

[60] U.S. Air Force, "ABMS Fact Sheet," press release, November 6, 2020.

where no sensitive data are stored on a device—to U.S. Northern Command to assist in its response to the COVID pandemic during the spring of 2020.

In November 2020, the Department of the Air Force identified the Chief Architect Office in charge of evaluating architecture on-ramps and integrating enterprise digital architecture. At the same time, the Air Force identified the Department of the Air Force Rapid Capabilities Office as the ABMS Integrating Program Executive Office. The Rapid Capabilities Office focuses on quickly delivering programs to the field, and its involvement may be seen as moving ABMS from experimentation to system development.

Department of the Army: Project Convergence[61]

According to the Army, "Project Convergence is the Army's new campaign of learning organized around a continuous, structured series of demonstrations and experiments" designed to meet the challenges posed by JADC2.[62] Project Convergence comprises five components:

1. ensuring the Army has the right people and talent;
2. linking current Army modernization efforts with Army Futures Command cross-functional teams aligned to the six Army modernization priorities;[63]
3. having the right command and control to meet increasingly fast-paced threats;
4. using AI to analyze and categorize information and transmitted across the Army network; and
5. testing capabilities in the "most unforgiving terrain."

Project Convergence 2020 utilized approximately 750 soldiers, civilians, and contractors across three military installations, culminating in two live capstone demonstrations at Yuma Proving Ground, AZ.[64] During this exercise, the Army demonstrated several technologies, including artificial intelligence, autonomy, and robotics, to test new methods to command and control geographically dispersed forces.[65] The Army plans to integrate Air Force and Navy systems as part of Project Convergence 2021, and intends to incorporate foreign militaries in Project Convergence 2022.[66] The Army has requested a total of $106.8 million for Project Convergence activities in FY2022.[67] This breaks down to $33.7 million requested for Operations and Maintenance, Army appropriations, and $73.1 million for Research, Development, Test and Evaluation, Army appropriations.[68]

[61] For more information see CRS In Focus IF11654, *The Army's Project Convergence*, by Andrew Feickert.

[62] Army Futures Command Information Paper on Project Convergence 2020 provided to CRS on October 15, 2020.

[63] For more information on Army modernization priorities see CRS Report R46216, *The Army's Modernization Strategy: Congressional Oversight Considerations*, by Andrew Feickert and Brendan W. McGarry.

[64] Army Futures Command Information Paper on Project Convergence 2020 provided to CRS on October 15, 2020.

[65] Jen Judson, "Inside Project Convergence: How the US Army is preparing for war in the next decade," *Defense News*, September 10, 2020, https://www.defensenews.com/smr/defense-news-conference/2020/09/10/army-conducting-digital-louisiana-maneuvers-in-arizona-desert/.

[66] CRS In Focus IF11654, *The Army's Project Convergence*, by Andrew Feickert.

[67] Email correspondence between the author and Army Futures Command, June 3, 2021.

[68] $43.7 million of the RDT&E request is allocated for All Domain Convergence Applied Research (Program Element 0602181A) and All Domain Convergence Advanced Technology (Program Element 0603041A). Email correspondence between the author and Army Futures Command, July 7, 2021.

Department of the Navy: Project Overmatch

Project Overmatch is the Navy's effort to create a "Naval Operational Architecture" to link ships to Army and Air Force assets. On October 1, 2020, Admiral Gilday, the Chief of Naval Operations, tasked a 2-star admiral to lead the Navy's Project Overmatch effort.[69] In his memorandum, Admiral Gilday directed that Project Overmatch take an engineering and development approach similar to the Navy's effort to develop nuclear power and the AEGIS system. The primary goal is "to enable a Navy that swarms the sea, delivering synchronized lethal and nonlethal effects from near-and-far, every axis, and every domain. Specifically, you [RADM Small] are to develop the networks, infrastructure, data architecture tools, and analytics." In a parallel effort, Admiral Gilday tasked Vice Admiral Kilby, the Deputy Chief of Naval Operations for Warfighting Requirements and Capabilities, to develop a plan to incorporate unmanned systems, including ships and aircraft,[70] into the naval operational architecture.[71] According to press statements, the Navy intends to reach initial operating capabilities (i.e., being capable to field the initial systems) in 2023.[72] The Navy requested funding for Project Overmatch in three classified program elements in FY2022.[73]

At the AFCEA West Conference 2021 in June 2021, Admiral Gilday discussed Project Overmatch's current efforts. At the event, Gilday stated that Project Overmatch had completed three spiral development cycles since the program's inception in October 2020.[74] Gilday further explained "[w]e're actually experimenting in a way that allows us to essentially pass any data on any network to the warfighter…. It's a software-defined communication system that allows us to essentially unpack all of our networks in a way we never have before."[75] According to news coverage, Gilday stated that he anticipated scaling Project Overmatch testing to a carrier strike group either in late 2022 or early 2023.[76]

Potential Issues for Congress

The following sections discuss potential issues for Congress, including requirements and cost estimates, interoperability challenges, balancing communications capabilities, the role of AI in decisionmaking, and potential force structure changes needed to implement JADC2.

[69] Memorandum from Admiral Gilday to Read Admiral Douglas Small, *Project Overmatch*, October 1, 2020.

[70] For more information on the Navy's approach to unmanned ships, see CRS Report R45757, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress*, by Ronald O'Rourke.

[71] Memorandum from Admiral Michael Gilday to Vice Admiral James Kilby, "A Novel Force," October 1, 2020.

[72] Jason Sherman, "Navy eyes 2023 for initial delivery of Project Overmatch capability to fleet," *Inside Defense*, January 29, 2021, https://insidedefense.com/daily-news/navy-eyes-2023-initial-delivery-project-overmatch-capability-fleet.

[73] Mark Pomerleau, "Classified Navy JADC2 budget plan has a few spending hints," *C4ISRNet*, June 15, 2021, https://www.c4isrnet.com/c2-comms/2021/06/15/part-4-classified-navy-jadc2-budget-plan-has-a-few-spending-hints/.

[74] Aidan Quigley, "Gilday: Project Overmatch progressing well toward strike group testing," *Inside Defense*, June 30, 2021, https://insidedefense.com/insider/gilday-project-overmatch-progressing-well-toward-strike-group-testing.

[75] Ibid.

[76] Adian Quigley, "Gilday: Project Overmatch progressing well toward strike group testing," *Inside Defense*, June 30, 2021, https://insidedefense.com/insider/gilday-project-overmatch-progressing-well-toward-strike-group-testing.

Requirements and Cost Estimates

DOD has requested funding for JADC2-related efforts for several fiscal years, in particular during the concept's early stages of development. DOD is actively developing a JADC2 strategy, which is expected to be released by the spring of 2021.[77] Some in Congress have expressed concern that DOD has not provided cost estimates or validated requirements in the manner that a traditional acquisition program might.[78] As a result, the armed services committees and the appropriations committees have reduced the requested funding for these efforts, especially for ABMS and 5G research and development.[79] The FY2021 National Defense Authorization Act (NDAA) required DOD to produce requirements for JADC2 by April 2021.[80]

Interoperability Challenges

As DOD envisions using JADC2 to command forces in multiple domains simultaneously, the need to connect different types of forces increases. DOD owns and operates many communications systems, each using different radio frequencies, standards, and datalinks.[81] These systems are often unable to "talk" with each other and therefore require a gateway to "translate" from one radio protocol to another. The inclusion of allies and partners increases interoperability challenges. Former Undersecretary of Defense Michael Griffin, in his March 2020 testimony to the House Armed Services Subcommittee on Intelligence, Emerging Threats, and Capabilities, identified this issue as justification to continue pursuing the OSD R&E efforts for FNC3.[82]

The challenge of enabling DOD to share information from different services and units could be solved by three approaches to interoperability:

- **Procure gateways.** Communications gateways (perhaps more aptly called "translators") can receive multiple protocols, security levels, et cetera, and rebroadcast this information to the rest of the force.[83] The ABMS program has developed such gateways (see **Figure 6**) to enable communications.[84] This approach allows for information sharing, potentially reducing the cost of development because the gateway can be a subsystem of an aircraft/ship/ground system, potentially capable of being fielded relatively quickly. The challenge with this approach is that such gateways may not be using the most advanced, and therefore protected, waveforms to rebroadcast to the force.

[77] Theresa Hitchens, "CJCS Gen. Milley Reviews JADC2 Strategy While Industry Jostles For Position," February 24, 2021, https://breakingdefense.com/2021/02/cjcs-gen-milley-reviews-jadc2-strategy-while-industry-jostles-for-position/.

[78] P.L. 116-283 §157.

[79] P.L. 116-283.

[80] P.L. 116-283 §157.

[81] For more discussion on this issue, see CRS Report R46564, *Overview of Department of Defense Use of the Electromagnetic Spectrum*, by John R. Hoehn, Jill C. Gallagher, and Kelley M. Sayler.

[82] Testimony of Undersecretary of Defense Michael Griffin, in U.S. Congress, House Armed Services Subcommittee for Intelligence, Emerging Threats, and Capabilities, *FY2020 Science and Technology Posture Hearing*, 116th Cong., 2nd sess., March 11, 2020, https://www.congress.gov/116/meeting/house/110655/witnesses/HHRG-116-AS26-Wstate-GriffinM-20200311.pdf.

[83] This capability is best demonstrated by the U.S. Air Force's Battlefield Airborne Communications Node (BACN).

[84] U.S. Air Force, "ABMS Fact Sheet," press release, November 6, 2020.

Figure 6. E-11 Battlefield Airborne Communications Node (BACN)

Source: https://www.janes.com/amp/usaf-to-buy-more-bacn/ZnIJK3dHVU9mZ28xajRJVkc5dVI5VFp1cVMwPQ2.

- **Procure new communications equipment.** This approach uses a "top-down" approach (i.e., where either OSD or the Joint Staff identifies the solution and then requires the military services to adopt it). Using a similar model to the Joint Tactical Radio System (JTRS) development,[85] this option would purchase a new communications architecture focusing on interoperability. For example, the FNC3 effort appears to use this approach. Although this approach could ensure that the joint force develops communications systems that can share information seamlessly, and potentially in a secure fashion, it could require large investments and might encounter schedule delays. Another possible disadvantage of this approach is that as systems are fielded, they may not be as effective against adversary technologies.
- **Develop software to create networks.** A third approach is to use software that enables users to create customized networks. DARPA's Mosaic Warfare and some aspects of the ABMS program are examples of this approach.[86] More modular than other interoperability solutions, this approach enables units and systems tailored to a specific operation to communicate with one another. A primary risk to this approach is the technical immaturity, specifically advances in software, used to create these networks. Another risk concerns the amount and classification of information shared with different systems certified for different levels of classification (e.g., Secret Releasable, Secret Nonreleasable, Top Secret).

DOD and Congress may select one or more of these approaches. One particular approach may offer short-term benefits while DOD pursues a longer-term approach to solve the interoperability challenge.

[85] JTRS was a radio program intended to replace all of the radio systems used by the Department of Defense. For more information, see the **Appendix**.

[86] U.S. Air Force, "ABMS Fact Sheet," press release, November 6, 2020, and Sydney J. Freedberg Jr, "DARPA AI Builds New Networks On The Fly," October 28, 2020, https://breakingdefense.com/2020/10/darpa-builds-ai-to-reorganize-machines-humans-on-the-fly/.

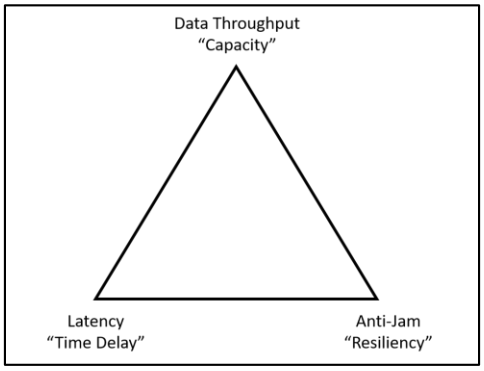
Balancing Communications Capabilities in a Degraded Environment

DOD's approach to developing communications networks to meet JADC2 requirements incorporates three competing capabilities:

- data throughput (i.e., the rate at which data can be transported),
- latency (i.e., the time delay in receiving a message/data), and
- resiliency (the ability to maintain a communications signal in the event of disruption by natural or intentional sources).[87]

The rise of new technologies for military operations, such as artificial intelligence, tactical datalinks (like Link 16 and Multifunction Advanced Data Link [MADL]), and adversary electronic warfare capabilities, presents distinct challenges in balancing these capabilities for future communications systems like 5G and FNC3. AI and information operations could potentially require substantial data to enable predictive analytics and give commanders an accurate picture of the battle space. Datalinks, which share data with all available users, do not necessarily require high data rates; however, datalinks do need low latency to ensure that sensors can prove "target-level data," particularly for fast-moving systems like cruise missiles and aircraft. Finally, the proliferation of electronic jammers requires resilience (or anti-jam properties) to maintain communications while being actively jammed. **Figure 7** illustrates how these three competing requirements must be balanced to develop a new waveform (regardless if the waveform is designed for civilian or military applications).[88] Radio signals are able to offer each capability; however, prioritizing one requirement means that the other two requirements may suffer, potentially creating a dilemma for policymakers in terms of which capabilities to prioritize in acquisition.

Figure 7. Balancing Communications Requirements



Source: Congressional Research Service.

[87] For example, see Department of Homeland Security, "First Responder Electronic Jamming Exercise," press release, 2017, https://www.dhs.gov/science-and-technology/first-responder-electronic-jamming-exercise#:~:text=DHS%20S%26T%20works%20to%20combat,jamming%20threats%20and%20reporting%20channels; Youness Arjoune and Saleh Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," Las Vegas, NV, January 8, 2020, https://ieeexplore.ieee.org/document/9031175; and Hossein Pirayesh and Huacheng Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," January 1, 2021, https://arxiv.org/abs/2101.00292.

[88] Waveforms are defined as software applications that determine the total functionality of the radio from the user's perspective.

As DOD modernizes its communications systems, it may consider technology features and limitations to select requirements that advance mission goals while protecting the security of its networks. For example, technologies like 5G can offer high data capacity and low latency, but it is unclear how these signals may be affected by adversary jamming. FNC3, on the other hand, appears to be designed to provide resiliency with high data rates; however, because it relies on satellites, latency will increase.

Role of Artificial Intelligence in Decisionmaking[89]

AI represents a potentially critical component to enabling JADC2. As AI is introduced into military decisionmaking, several potential issues arise. First, to what degree should artificial intelligence play in decisionmaking? At what appropriate level is human judgement required when using lethal weapons?[90]

Second, how does DOD ensure the security of the data being used for AI algorithms to assist decisionmaking? Although DOD has focused on the data structures,[91] it has not discussed how it plans to ensure data validity and security for JADC2 specifically. Erroneous data could cause commanders to select options that compromise mission objectives (such as algorithms recommending targets that might waste high-value munitions). Relatedly, how does DOD intend to secure these data in cloud environments to prevent adversaries from manipulating them? Are these security plans sufficient to prevent adversary manipulation?

Potential Force Structure Changes

Because JADC2 potentially requires different types of forces and weapons systems, each of the military services may look to change how it trains, organizes, and equips its forces. For example, the Marine Corps, in its force redesign, announced that it would eliminate units it determines are not aligned with National Defense Strategy guidance, and would reinvest the funding into other programs that better fit the future operating environment.[92] Similarly, the Navy's Project Overmatch looks to potentially change the number and types of ships the service fields.

The balance of capabilities that reside in the active and reserve components is another aspect of force structure changes. For instance, the Army historically has decided to transfer logistics capabilities from the active component to the reserve components.[93] Thus, if the United States were to go to war, the Army would presumably need to activate reserve forces to enable operations. As DOD and military services prepare to meet the challenges presented by JADC2, how would these organizations choose to balance capabilities and force structures between active and reserve components?

[89] For a broader discussion of artificial intelligence and its role in national security, see CRS Report R45178, *Artificial Intelligence and National Security*, by Kelley M. Sayler.

[90] Department of Defense, "DOD Adopts 5 Principles of Artificial Intelligence Ethics," press release, February 25, 2020, https://www.defense.gov/Explore/News/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/.

[91] Theresa Hitchens, "OSD, Joint Staff Double Down On DoD-Wide Data Standards," *Breaking Defense*, February 10, 2021, https://breakingdefense.com/2021/02/exclusive-jadc2-data-summits-will-drive-dod-standards-requirements/.

[92] CRS Insight IN11281, *New U.S. Marine Corps Force Design Initiatives*, by Andrew Feickert.

[93] CRS Report R43808, *Army Active Component (AC)/Reserve Component (RC) Force Mix: Considerations and Options for Congress*, by Andrew Feickert and Lawrence Kapp.

Management of JADC2 Efforts

The Joint Staff J6 is the lead coordinator for DOD's JADC2 efforts, with each of the services and a number of DOD agencies performing various activities. Some in Congress, in the past, have expressed an interest in creating DOD-wide program offices (such as the F-35 Joint Program Office) to centralize management of large-scale efforts.[94] It appears that DOD research and development efforts will increase over time, and that, as a result, managing these efforts may become more challenging. Congress may, in the future, seek to identify or create an organization charged with program management, development of network architecture, and financial management.

[94] For more information on the background of the F-35 program, see CRS Report RL30563, *F-35 Joint Strike Fighter (JSF) Program*, by Jeremiah Gertler. For an example of a joint communications program intended to achieve similar results to JADC2, see the **Appendix**.

Appendix. Historical Example of Joint Interoperability: Joint Tactical Radio System[95]

The Joint Tactical Radio System (JTRS) was a communications program intended to improve communications interoperability by fielding radios across all of the military services. The program was started in the mid-1990s and was ultimately canceled in 2011 by former Under Secretary of Defense for Acquisition, Technology, and Logistics Frank Kendall.[96] In his justification notification, Under Secretary Kendall noted that "the technical challenges of mobile ad hoc networks and scalability were not well understood due to the immaturity of technology at the time … it is unlikely that products resulting from the JTRS GMR [Ground Mobile Radio] development program affordably meet Service requirements." Over the course of the 15-year development effort, DOD spent approximately $15 billion, requiring an additional $13 billion at termination.[97]

The JTRS program was intended to replace the 25 to 30 families of radio systems used by the military—many of which could not communicate with each other—with software-based radios that could operate across much of the radio frequency spectrum.[98] JTRS was envisioned to enable the services to operate together, along with selected allied nations, in a "seamless" manner via wireless voice, video, and data communications through all levels of command, including direct access to near real-time information from airborne and battlefield sensors.[99] Described as a "software-defined radio," JTRS would have functioned more like a computer than a conventional radio; for example, it would have been upgraded and modified to operate with other communications systems by the addition of software, as opposed to redesigning hardware—a more costly and time-consuming process. DOD asserted that in "many cases, a single JTRS radio with multiple waveforms can replace many separate radios, simplifying maintenance" and that because JTRS is "software programmable, they will also provide a longer functional life," with both features offering potential long-term cost savings.[100] The JTRS program was originally broken into five "clusters," with each cluster having a particular service "lead" (see **Table A-1**) and a Joint Program Office managing the overall architecture.

[95] This section is derived from CRS Report RL33161, *The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS): Issues for Congress*, by Andrew Feickert.

[96] Memorandum from Undersecretary of Defense Frank Kendell to Representative Howard P. "Buck" McKeon, *JTRS Cancellation Notification*, October 13, 2011, https://www.govexec.com/pdfs/101411bb1.pdf.

[97] Bob Brewin, "Pentagon shutters Joint Tactical Radio System program office," *Nextgov*, August 1, 2012, https://www.nextgov.com/it-modernization/2012/08/pentagon-shutters-joint-tactical-radio-system-program-office/57173/.

[98] Peter A. Buxbaum, "Jitters Over JTRS," *Armed Forces Journal*, July 2005, p. 31.

[99] U.S. Government Accountability Office (GAO), Report to the Chairman, Committee on Appropriations, House of Representatives, "Defense Acquisitions: Resolving Developmental Risks in the Army's Networked Communications Capabilities is Key to Fielding Future Force," GAO-05-669, June 2005, p. 9. Peter A. Buxbaum, "Jitters Over JTRS," *Armed Forces Journal*, July 2005, pp. 31-33.

[100] DOD pamphlet on JTRS published by the JTRS Joint Program Office, undated.

Table A-1. JTRS Clusters

Cluster	One	Two	Three	Four	Five
Description	Ground vehicle and helicopter radios	Hand-held radios	Fixed-site and maritime radios	High-performance aircraft (fixed wing) radios	Handheld, dismounted, and Small Form Factor[a] radios
Service Lead	U.S. Army	U.S. Special Operations Command (USSOCOM)	U.S. Navy	U.S. Air Force	U.S. Army

Source: Reproduced from CRS Report RL33161, *The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS): Issues for Congress*, by Andrew Feickert.

Note: Form factor radios are essentially miniaturized radios that soldiers would carry, as well as radios for weight- and power-constrained platforms.

As discussed below, JTRS experienced a number of difficulties during development. These issues may be relevant for future JADC2 development.

Size and Weight Constraints and Limited Range

According to a 2005 Government Accountability Office (GAO) report

> To realize the full capabilities of the Wideband Networking Waveform,[101] including transmission range, the Cluster One radio requires significant amounts of memory and processing power, which add to the size, weight, and power consumption of the radio. The added size and weight are the results of efforts to ensure the electronic parts in the radio are not overheated by the electricity needed to power the additional memory and processing. Thus far, the program has not been able to develop radios that meet size, weight, and power requirements, and the current projected transmission range is only three kilometers—well short of the 10-kilometer range required for the Wideband Networking Waveform.... The Cluster One radio's size, weight, and peak power consumption exceeds helicopter platform requirements by as much as 80 percent.[102]

The inability to meet these fundamental design and performance standards raised concerns that Cluster One may not have been able to accommodate additional waveforms as intended (the plan was for Cluster One to have four to eight stored waveforms) and that it may be too bulky or heavy to fit into the stringently weight- and size-constrained Future Combat System (FCS) Manned Ground Vehicles (MGVs),[103] as well as the Army's helicopter fleet. Some observers were concerned that to meet these physical requirements, the Army would significantly "dumb down"

[101] The Wideband Networking Waveform is described as the core of the JTRS networking capability and is intended to operate across a wide range of the radio frequency spectrum, from 2 megahertz (MHZ) to 2 gigahertz (GHz), and would provide increased routing and networking capability—as much as a hundred times more than existing communications systems.

[102] U.S. Government Accountability Office (GAO), Report to the Chairman, Committee on Appropriations, House of Representatives, "Defense Acquisitions: Resolving Developmental Risks in the Army's Networked Communications Capabilities is Key to Fielding Future Force," GAO-05-669, June 2005, p. 15.

[103] FCS Manned Ground Vehicles (MGVs) are envisioned as a family of eight different combat vehicles—with some having more than one variation—based on a common platform and designed to be transported by U.S. Air Force transport aircraft and deployed directly into combat with little or no post-flight reconfiguration. MGVs would be equipped with various passive and active protection systems and sensors that the Army hopes will offer them the same survivability as the current heavy armor force.

Cluster One performance specifications.[104] According to the Army, however, it made progress in terms of reducing Cluster One's weight and size and in increasing its transmission range; however, incorporating all of the desired waveforms into Cluster One proved to be difficult.[105] Cluster Five radios also reportedly experienced similar size, weight, and power difficulties; these difficulties were more pronounced because some Cluster Five versions were supposed to weigh no more than 1 pound.[106]

Security

Security for JTRS emerged as a significant developmental difficulty. According to one expert, one of the program's biggest problems was security, "namely encryption, as JTRS encryption is software-based and is, therefore, vulnerable to hacking."[107] Computer security experts generally agree that software used for any purpose is vulnerable, as no current form of computer security offers absolute security or information assurance. According to GAO, JTRS required applications to operate at multiple levels of security; in order to meet this requirement, developers had to account not only for traditional radio security measures but also for computer and network security measures.[108] In addition, National Security Agency (NSA)[109] security concerns about JTRS interface with radio systems of U.S. allies posed developmental challenges.[110]

Interoperability with Legacy Radio Systems

Some analysts expressed concerns that the goal of making JTRS "backward compatible" with legacy radios may have been technologically infeasible.[111] Reportedly, early program attempts at cross-banding[112] to synchronize incompatible legacy radio signals proved to be too complex. Current Army efforts are focusing on using the Wideband Networking Waveform to link with legacy radio frequencies.[113] One report suggested that while the Wideband Networking Waveform could receive signals from legacy radios, legacy radios cannot receive signals from JTRS. To rectify this situation, the Army considered using 19 different waveforms to facilitate JTRS

[104] Sandra I. Erwin, "Military Sets Less Ambitious Goals for New Tactical Radio," *National Defense*, National Defense Industrial Association (NDIA), Washington, DC, August 2005.

[105] Meeting between CRS and the Army Staff's G-8 (Force Development) Section's Directorate of Integration FCS Office, September 15, 2005.

[106] U.S. Government Accountability Office (GAO), Report to the Chairman, Committee on Appropriations, House of Representatives, "Defense Acquisitions: Resolving Developmental Risks in the Army's Networked Communications Capabilities is Key to Fielding Future Force," GAO-05-669, June 2005, p. 19.

[107] Buxbaum, p. 32.

[108] Buxbaum, p. 32.

[109] The National Security Agency is the U.S. government's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and produce foreign signals intelligence information.

[110] Buxbaum, p. 32.

[111] Sandra I. Erwin, "Military Sets Less Ambitious Goals for New Tactical Radio," *National Defense*, National Defense Industrial Association (NDIA), Washington, DC, August 2005.

[112] Cross-banding is a technique of receiving a number of incompatible frequencies and then retransmitting them on previously designated channels, thereby allowing communications systems operating on different bands to communicate with one another.

[113] Sandra I. Erwin, "Military Sets Less Ambitious Goals for New Tactical Radio," *National Defense*, National Defense Industrial Association (NDIA), Washington, DC, August 2005.

transmissions to legacy systems.[114] Incorporating this number of different waveforms into a JTRS radio would have significantly increased memory and processing power requirements which, in turn, would have increased JTRS size, weight, and power requirements.

Author Information

John R. Hoehn
Analyst in Military Capabilities and Programs

Disclaimer

[114] Jen DiMascio, "JTRS Cluster One to Play Role, Execs Say: Exercise to Test Mettle of Early FCS Technologies Will Begin this Year," *Inside the Army*, vol. 17, no. 25, June 27, 2005, p. 7.