MIRANDA PRIEBE, DOUGLAS C. LIGOR, BRUCE MCCLINTOCK, MICHAEL SPIRTAS, KAREN SCHWINDT, CAITLIN LEE, ASHLEY L. RHOADES, DEREK EATON, QUENTIN E. HODGSON, BRYAN ROONEY

Multiple Dilemmas

Challenges and Options for All-Domain Command and Control

For more information on this publication, visit www.rand.org/t/RRA381-1

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0628-6

Published by the RAND Corporation, Santa Monica, Calif.

Cover: Jets: Marine Corps Air Station Miramar; Satellite: Getty Images/iStockphoto; Ships: Jarrod A. Schad; Tanks: Spc. Marcus Floyd; Cyber screen: J.M. Eddins Jr.

Cover design: Rick Penn-Kraus

Preface

In order to counter increasingly capable near-peer competitors, the services have been developing new concepts for multidomain operations (MDOs), which aspire to better integrate operations in the air, land, maritime, space, and cyber domains as well as in the electromagnetic spectrum and information environment. The U.S. Air Force asked the RAND Corporation to identify potential changes to command-and-control (C2) doctrine, authorities, and systems to enable MDOs.

The research reported here was commissioned by Major General Charles Corcoran, who was then Director of Air and Space Operations, Strategic Deterrence and Nuclear Integration, U.S. Air Forces in Europe and U.S. Air Forces Africa and conducted within the Strategy and Doctrine Program of RAND Project AIR FORCE as part of a fiscal year 2019 project Multi/All-Domain Command and Control Doctrine, Authorities, and Information Systems.

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Manpower, Personnel, and Training; and Resource Management. The research reported here was prepared under contract FA7014-16-D-1000.

Additional information about PAF is available on our website:
www.rand.org/paf/

This report documents work originally shared with the DAF on September 20, 2019. The draft report, issued on September 27, 2019, was reviewed by formal peer reviewers and DAF subject-matter experts.

Contents

Figures

Tables

Summary

Issue

In order to counter increasingly capable near-peer competitors, the services have been developing new concepts for multidomain operations (MDOs), intended to better integrate operations in the air, land, maritime, space, and cyber domains. The joint force already conducts MDOs today, but current initiatives aim to expand the scope, scale, and speed of such operations. As a result, the joint force is considering how current command-and-control (C2) constructs may need to adapt to enable MDOs. This report identifies potential impediments to MDOs in the current operational C2 construct for joint operations. It then proposes alternative approaches to joint all-domain command and control (JADC2) within a geographic combatant command for further analysis and experimentation.

Approach

Drawing on joint warfighting principles, we proposed five C2 characteristics that could prevent MDO options from being considered, make MDOs too time consuming to plan, or create too much planning uncertainty. We then analyzed current laws, regulations, and joint doctrine and conducted over 150 interviews to identify aspects of the current C2 structure that have these characteristics. To generate alternative C2 constructs to overcome some of these potential impediments to MDOs, we proposed two key questions: (1) Which organizations would conduct multidomain planning within a geographic combatant command (GCC)? (2) How would control of forces be divided within a GCC? We developed four alternative C2 constructs by proposing different answers to these questions.

Conclusions

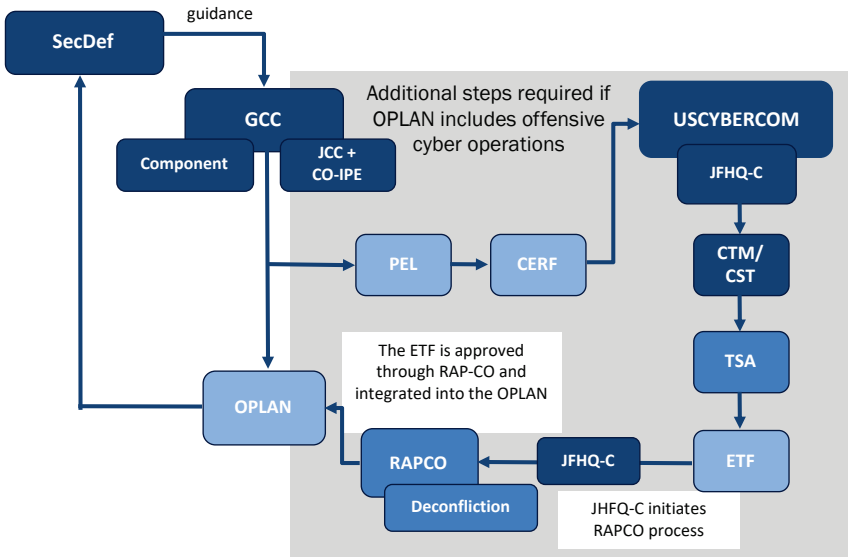
- Specific concepts for MDOs are still emerging, so it is not yet clear which C2 changes are most important or how beneficial such changes would be.
- There are tensions among three emerging C2 concepts for conflict against a near-peer competitor: global integration, the JADC2, and distributed control.
- Operational planning is currently component-centered, creating the risk of insufficient expertise in all domains and a preference for solutions in certain domains.
- MDOs often involve forces controlled by multiple organizations, which increases C2 complexity.
- Single-service initiatives cannot resolve C2 impediments that involve forces from multiple combatant commands or services.
- Reducing the number of steps and approvals for space, cyber, and intelligence operations may facilitate MDOs but reduce efficiency and increase risk.
- MDOs that rely on planning by, approval of, or execution from outside the theater may be particularly vulnerable in a communications-contested environment.

Recommendations

- Specify MDO concepts and thoroughly assess operational costs and benefits to inform JADC2 changes and investments.
- Set priorities among concepts for global integration, the JADC2, and distributed control.
- Experiment with alternative JADC2 constructs to assess effectiveness and trade-offs before making significant C2 changes.
- Review exercises for opportunities to practice approval processes for capabilities controlled outside the GCC.
- Simplify and update authorities related to MDOs.
- Assess trade-offs associated with giving more planners access to information about space and cyber effects.

Figure S.1. Offensive Cyber Request and Approval Process

Planning, executing, and assessing MDOs often require additional steps and approvals because capabilities are controlled by multiple organizations. For example, if the air component wanted to include offensive cyber operations to its suppression of enemy air defense (SEAD) plans, it would need to account for all of the steps in the offensive cyber operations request and review and approval process (RAP) below in addition to typical approvals for air operations plans.



Acronyms:
CERF: cyber effects request form
CMT: cyber mission team
CO-IPE: cyber operations-integrated planning element
CST: cyber support team
ETF: electronic target folder
GCC: geographic combatant command
JCC: joint cyber center
JFHQ-C: joint forces headquarters-cyberspace
OPLAN: operation plan
RAPCO: review and approval process-cyberspace operations
TSA: target system analysis
PEL: priority effects list
USCYBERCOM: U.S. Cyber Command

SOURCES: JP 3-12, 2018, pp. IV-8–IV-10; JP 3-60, 2013, pp. I-8–I-10.

Acknowledgments

We thank Major General Charles Corcoran (then USAFE-AFAFRICA A3/10) and Brigadier General Michael Koscheski (USAFE-AFAFRICA A3/10) for sponsoring the study and for providing helpful feedback throughout the project. Lieutenant Colonel Larissa Ruiz, the project action officer, Lieutenant Colonel Matthew Flynn, and Bob Appleton provided valuable insights as well.

Staff in the following organizations shared their expertise in various aspects of multidomain operations and command and control: Joint Staff, Headquarters USAF, USEUCOM, USAFE-AFAFRICA, USAEUR, USINDOPACOM, PACAF, USARPAC, USNORTHCOM, NORAD, USSTRATCOM, USSPACECOM, AFSPC, Space Security and Defense Program, National Space Defense Center, Air Education and Training Command, Curtis E. LeMay Center for Doctrine and Education, and Air Combat Command.

We also wish to thank Jon Fujiwara, Nathan Chandler, and Ben Boudreaux for contributions to the project and Lee Remi and Laura Poole for formatting the document.

Abbreviations

A2/AD	anti-access, area denial
AADC	area air defense commander
AADP	area air defense plan
AAMDC	Army air and missile defense command
ACC	Air Combat Command
ADAFCO	air defense artillery fire officer
ADOC	all-domain operations center
AFATD	Advanced Field Artillery Tactical Data System
AFB	Air Force base
AMD	air and missile defense
AMRAAM	Advanced Medium-Range Air-to-Air Missile
AOC	air operations center
AOR	area of responsibility
ARFOR	Army forces
ASC	air, space, and cyber
ATACMS	Army Tactical Missile System
ATO	air tasking order
AWACS	Airborne Warning and Control System
BCD	battlefield coordination detachment
BDA	battle damage assessment
C2	command and control
CAL	critical asset list
CAP	combat air patrol
CCDR	combatant commander
CCMD	combatant command
CFSCC	Combined Force Space Component Command

CIA	Central Intelligence Agency
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMA	collection management authority
CMT	cyber mission team
COA	course of action
COCOM	combatant command (command authority)
CO-IPE	cyber operations integrated planning element
COMAFFOR	commander, Air Force forces
CONOP	concept of operations
COP	common operating picture
CPX	command-post exercise
CRC	control and reporting center
CSAF	Chief of Staff, Air Force
CSpOC	Combined Space Operations Center
CTO	cyber tasking order
CTP	common tactical picture
DAADC	deputy area air defense commander
DAL	defended asset list
DCA	defensive counter air
DIRNSA	Director of the National Security Agency
DIRSPACEFOR	director of space forces
DNI	Director of National Intelligence
DoD	Department of Defense
DoDD	Department of Defense directive
DoDI	Department of Defense instruction
DOJ	Department of Justice

EW	electronic warfare
EXORD	execute order
FBI	Federal Bureau of Investigation
FCC	functional combatant command
GCC	geographic combatant command
GMLRS	Guided Multiple-Launch Rocket System
GPS	Global Positioning System
HIMARS	High Mobility Artillery Rocket System
IAD	integrated air defense system
IAMD	integrated air and missile defense
IC	intelligence community
IGL	intelligence gain-loss
IPE	integrated planning element
ISR	intelligence, surveillance, and reconnaissance
J-2	joint directorate for intelligence
J-3	joint directorate for operations
J-5	joint directorate for strategy, plans, and policy
JA	judge advocate
JACCE	joint air component coordination element
JADC2	joint all-domain command and control
JAGIC	joint air-ground integration center
JAOP	joint air operations plan
JCC	joint cyber center
JCS	Joint Chiefs of Staff
JECC	Joint Enabling Capabilities Command
JFACC	joint force air component commander
JF(ASC)ACC	joint force air, space, and cyber component commander
JFHQ-C	joint force headquarters cyberspace

JFLCC	joint force land component commander
JIOC	joint intelligence operating center
JIPCL	joint integrated prioritized collection list
JIPOE	joint intelligence preparation of the operating environment
JIPTL	joint integrated prioritized target list
JOC	joint operations center
JPP	joint planning process
JSTO	joint space tasking order
JTCB	joint targeting coordination board
JTCR	joint targeting cyber request
JTF	joint task force
LNO	liaison officer
LOE	line of effort
MAJCOM	major command
MDB	multidomain battle
MDC2	multidomain command and control
MDO	multidomain operation
MDOC	multidomain operation center
MIP	Military Intelligence Program
NDAA	National Defense Authorization Act
NIP	National Intelligence Program
NSA	National Security Agency
NSPM	national security presidential memorandum
OPCON	operational control
OPLAN	operational plan
OSC	offensive space control
OSD	Office of the Secretary of Defense
PACAF	Pacific Air Forces

PEL	priority effects list
PGM	precision guided munition
PIR	priority intelligence requirement
PRISM	Planning Tool for Resource Integration, Synchronization, and Management
RADC	regional air defense commander
RAP	review and approval process
RAPCO	review and approval process for cyber operations
SA	situational awareness
SADC	sector air defense commander
SAM	surface-to-air missile
SCA	space coordinating authority
SEAD	suppression of enemy air defenses
SecDef	Secretary of Defense
SIGINT	signal intelligence
SME	subject-matter expert
SOF	special operations force
SPINS	special instructions
SPOD	seaport of debarkation
SROE	standing rules of engagement
TACON	tactical control
TBMCS	theater battle management core systems
TFIAMD	task force integrated air and missile defense
THAAD	Terminal High Altitude Area Defense
TRADOC	Training and Doctrine Command
TSOC	theater special operations command
TST	time sensitive target
TTP	tactics, techniques, and procedures
TTX	table-top exercise

UCMJ	Uniform Code of Military Justice
UCP	Unified Command Plan
USAF	U.S. Air Force
USAFE-AFAFRICA	U.S. Air Forces Europe and Air Forces Africa
USCYBERCOM	U.S. Cyber Command
USEUCOM	U.S. European Command
USINDOPACOM	U.S. Indo-Pacific Command
USNORTHCOM	U.S. Northern Command
USSOCOM	U.S. Special Operations Command
USSPACECOM	U.S. Space Command
USSTRATCOM	U.S. Strategic Command
USTRANSCOM	U.S. Transportation Command

1. Introduction

In a 2015 speech, former Deputy Secretary of Defense Robert Work argued that the joint force needed a new approach to defeating Chinese and Russian anti-access, area-denial (A2/AD) capabilities.[1] During operations against Iraq in 1990 and 2003, U.S. forces employed a largely sequential approach, beginning with an air campaign against Iraqi air defense systems, followed by a large ground invasion. But in the context of major combat operations against a near-peer competitor, the United States may not be able to counter sophisticated air defenses primarily through air operations or to gain air superiority before conducting ground or maritime operations. Instead, Work argued that conflict with a near-peer competitor would require "a future where you synchronize cross-domain fires and maneuver in all domains to achieve physical, temporal and positional advantages."[2] In other words, the joint force would need better integrate operations in the air, land, maritime, cyber, and space domains in addition to the electromagnetic spectrum and information environment.[3]

Multidomain operations (MDOs), which employ capabilities in at least two domains, are not an entirely new phenomenon. Land and naval forces have been coordinating operations for thousands of years.[4] Close air support, which uses aircraft to support ground fires and maneuver against adversary ground forces, has been used since World War I.[5] Today, air and missile defense (AMD) is also a multidomain mission area. Still, U.S. military leaders argue that MDOs have been episodic and that operations in different domains have often been deconflicted rather than truly integrated. Moreover, the joint force is grappling with how to integrate space and cyber, which are emerging as more important warfighting domains. The current focus on MDOs aims, therefore, to develop the concepts and capability to continuously integrate across all domains.[6]

Concepts for MDOs are still emerging, so the specific ways that joint operations will change is not yet clear. Still, U.S. Air Force (USAF) has emphasized that changes to command and

---

[1] Sydney J. Freedberg Jr., "DepSecDef Work Offers Dough for Army Multi-Domain Battle," *Breaking Defense*, October 4, 2016b; Sydney J. Freedberg Jr., "Air Force Leading Way to 3rd Offset: Bob Work," *Breaking Defense*, September 21, 2016a.

[2] Jim Garamone, "Work Details Multidomain Battlefield of the Future," Defense.gov, October 4, 2016.

[3] As discussed below, there is not a single authoritative definition of MDO or list of relevant domains. Moreover, the Joint Staff prefers *all-domain operations*, arguing that this term emphasizes the constant interaction of domains. This report uses the term *multidomain operations* because it is still the most widely used and because individual operations may not involve all domains; Jim Garamone, "U.S. Military Must Develop All-Domain Defenses, Mattis, Dunford Say."

[4] Michael Spirtas, "Toward One Understanding of Multiple Domains," *C4ISRNet*, May 1, 2018b.

[5] John Schlight, *Help from Above: Air Force Close Air Support of the Army: 1946–1973*, Washington, D.C.: Air Force History and Museums Program, 2003, p. 18.

[6] Annex 3-99, *Department of the Air Force's Role in Joint All-Domain Operations (JADO)*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, October 8, 2020.

control (C2) will be essential to MDOs in any form. USAF therefore asked the RAND Corporation to identify changes to doctrine, authorities, and systems to enable MDOs. Rather than focusing on integrating only USAF operations in the air, space, and cyber domains, USAF asked RAND to consider integration of any combination of domains in the context of joint operations. In other words, we focus on joint all-domain command and control (JADC2). In order to respond to this request, we began with the following questions:

- What are potential impediments to MDOs in the current C2 construct for a conflict with a near-peer competitor?
- What are alternative approaches to the JADC2 and what trade-offs do they create?
- What key changes to doctrine, authorities, and systems would be required for each alternative JADC2 construct?

In this report we consider general C2 challenges to integrating more than one domain and identify options for the joint force to consider as specific MDO concepts mature. We do not make recommendations for which C2 construct would best enable MDOs for a number of reasons. First, concepts for MDOs are still emerging, so it is not yet clear how much they will improve warfighting effectiveness or which specific C2 changes would enable these concepts. Second, significantly more analysis and experimentation will be needed to assess the benefits and costs associated with changing the current C2 construct. The alternative C2 constructs we present could be used as the basis for additional analysis, including of the costs, personnel, and other requirements of alternative approaches. Finally, the choice of a JADC2 construct will depend not only on what best enables MDOs but on a wider range of considerations. In particular, any C2 changes need to account for other features of conflict with a near-peer competitor including kinetic and nonkinetic attacks on C2 nodes and communication links and a higher pace and wider scope of conflict.[7]

Emerging Concepts for Multidomain Operations

The prospect of MDO is tantalizing, and the U.S. armed forces have taken initial steps toward achieving that promise. However, much work remains to translate broad aspirations for MDO into validated concepts that are likely to significantly improve warfighting effectiveness.

The services have been the centers of development for MDO principles, operational concepts, and organizational requirements. The Army began by focusing on MDOs,[8] while USAF has focused primarily on the C2 implications of MDO, what it initially termed multidomain

[7] For an overview of threats to communications during a high-end conflict, see Miranda Priebe et al., *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation*, Santa Monica, Calif.: RAND Corporation, RR-2959-AF, 2019, pp. 23–27.

[8] U.S. Army, *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1, December 6, 2018, p. 17.

command and control (MDC2).[9] Meanwhile, the Navy and the Marine Corps have argued that their activities have always been multidomain. The services generally agree about the value of MDOs and share some common themes in how they think about it. But there is still no single definition of MDO.[10]

Still, Army and USAF statements on MDOs show some important areas of agreement. The Army and USAF agree that these operations are designed primarily for conflict with near-peers, namely, China and Russia.[11] MDOs involve the integrated use of military forces across domains.[12] For instance, aircraft could acquire and pass targeting information to land-based forces to allow them to destroy enemy ships or ground forces.[13] MDOs could create adversary uncertainty about how the United States may accomplish missions or create multiple operational challenges for U.S. adversaries since U.S. adversaries would have to plan for and adapt their operations to counter each U.S. option.[14] U.S. military leaders often call this creating multiple dilemmas for the adversary.[15] Greater ability to conduct MDOs will also make the United States

---

[9] Here we speak of general trends in the services. Recent USAF Air Combat Command (ACC) and Army Training and Doctrine Command (TRADOC) collaboration on a multidomain approach to suppression of enemy defenses (SEAD) has suggested that USAF is shifting its approach, and the Army has taken steps toward establishing a new fire control center to coordinate fires. Yet the overarching historical priorities have been MDC2 and MDO, respectively. Kevin A. Huyck, "ACC Operationalizing Multi-Domain," Briefing at the USAF Air Combat Command-U.S. Army Training and Doctrine Command Multi-Domain Operations Symposium, Joint Base Langley-Eustis, Va., April 29, 2019; Sydney J. Freedberg Jr., "IBCS: Northrop Delivers New Army Missile Defense Command Post," *Breaking Defense*, May 1, 2019c.

[10] The Army defines MDO as "operations conducted across multiple domains and contested spaces to overcome an adversary's (or enemy's) strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture; employment of multidomain formations; and convergence of capabilities across domains, environments, and functions in time and spaces to achieve operational and tactical objectives" (U.S. Army, 2018, p. GL-7). A USAF initiative on MDC2 defined MDO as the "combination of operations from multiple domains generating offensive and defensive actions, including but beyond those designated as cross-domain support, that create and take advantage of vulnerabilities, and present multiple, simultaneous dilemmas for an adversary at an operations tempo they cannot match" (Chance Saltzman, "Multi-Domain Ops in the 13OXX," Briefing Prepared for 705th Training Squadron, U.S. Air Force, November 13, 2018a).

[11] Jim Garamone, "Air Force, Army Developing Multidomain Doctrine," January 25, 2018; U.S. Army, 2018, p. 6. Although the Marine Corps has not framed its new operating concepts in terms of MDO, the 2016 Marine Corps Operating Concept also shifted focus to conflict with great powers; see Dan Parsons, "Why the US Needs a Marine Corps: Multi-Domain Before It Was Cool," *Rotor & Wing International*, August 3, 2018. The Chief of Naval Operations Adm. John Richardson has as well; see U.S. Navy, *A Design for Maintaining Maritime Superiority*, January 2016.

[12] U.S. Army, 2018, p. C-1; David G. Perkins and James M. Holmes, "Multidomain Battle: Converging Concepts Toward a Joint Solution," *Joint Forces Quarterly*, Vol. 88, January 10, 2018, p. 57.

[13] Kris Osborn, "Cross-Domain Fires: US Military's Master Plan to Win the Wars of the Future," *National Interest*, July 19, 2016; Huyck, 2019.

[14] U.S. Army, 2018, p. 17.

[15] Perkins and Holmes, 2018; Charles Pope, "Goldfein Details Air Force's Move Toward a 'Fully Networked,' Multi-Domain Future," 2019. U.S. Army GEN Robert Brown, commanding general of U.S. Army Pacific, explained: "Anyone would want more options. It allows you to create multiple dilemmas" (Connie Lee, "News from AUSA Global: Army Sharpens Focus on Multi-Domain Warfare," *National DEFENSE*, March 27, 2019).

more resilient by giving U.S. forces greater options. If, for example, the enemy prevents the United States from creating an effect in the air domain, the joint force could employ options for attacking from the maritime domain.[16]

The Navy and Marine Corps have not framed their recent concepts in terms of MDOs because they consider their operations to be inherently multidomain already, but their new concepts share many of the same principles.[17] The Navy's Distributed Maritime Operations seeks to improve integration across the air, subsurface, and surface domains.[18] Similarly, the Marines' concept of Littoral Operations in a Contested Environment describes operations in five dimensions of the littorals: seaward, landward, the airspace above, cyberspace, and the electromagnetic spectrum.[19]

Initially, the Army and USAF viewed MDOs as a way to enable operations within the domains in which they already operate. In this sense, MDOs were initially seen as distinct from joint operations. The Army, in what was known at the time as multidomain battle (MDB), focused on using space, cyberspace, electronic warfare (EW), and information operations to support the ground fight. USAF initially focused on integrating air, space, and cyberspace capabilities in an effort to create windows of superiority in those domains.[20]

Even while the services were focused on improving MDO with their own capabilities, they recognized the need for greater cooperation.[21] For example, the Marine Corps worked in conjunction with the Army on MDB.[22] Further, one of the central elements of the Marines' concept is improved integration with the Navy,[23] and the Marine Corps commandant's latest guidance stresses the need to effectively coordinate across all warfighting domains.[24] Jointly, the Navy and Marine Corps have coordinated on the Expeditionary Advanced Base Operations concept, which entails establishing a persistent presence on maritime terrain using long-range

---

[16] Dave Goldfein, *CSAF Focus Area: Enhancing Multi-Domain Command and Control . . . Tying It All Together*, Washington, D.C.: U.S. Air Force, March 2017.

[17] Sydney J. Freedberg Jr., "All Services Sign On to Data Sharing—But Not to Multi-Domain," *Breaking Defense*, February 8, 2019a; Parsons, 2018.

[18] Bryan Clark and Timothy A. Walton, *Taking Back the Seas: Transforming the U.S. Surface Fleet for Decision-Centric Warfare*, Washington, D.C.: Center for Strategic and Budgetary Assessment, 2019.

[19] U.S. Marine Corps Concepts and Programs, "Littoral Operations in a Contested Environment," n.d.-b.

[20] Perkins and Holmes, 2018, p. 55. Goldfein, 2017.

[21] Indeed, a brief coauthored by TRADOC and ACC stressed that it was vital for the concepts of the services to merge; Perkins and Holmes, 2018.The Army shifted from the term *multidomain battle* to MDO to better align the concept with other services; see Stephen Townsend, "Accelerating Multi-Domain Operations: Evolution of an Idea," West Point, N.Y.: Modern War Institute, July 23, 2018.

[22] Mark Pomerleau, "Marines Take Multi-Domain Battle to the Littorals," *C4ISRNET*, September 21, 2017b.

[23] U.S. Marine Corps Concepts and Programs, n.d.-b.

[24] David H. Berger, *Commandant's Planning Guidance. 38th Commandant of the Marine Corps*, p. 10.

weapon systems against enemy ships and aircraft.[25] The Army's Training and Doctrine Command (TRADOC) and the USAF's Air Combat Command (ACC) have conducted wargames to develop the best C2 structure to compete with a near peer,[26] as well as a follow-on experimentation effort. The Army and USAF are also working together to improve the capability to use target information from aircraft to queue ground fires.[27] More recently, the Army has explicitly included all domains in its MDO constructs, as has USAF.[28]

Consistent with long-standing differences in C2 philosophies, the Army initially had a more decentralized vision for C2 of MDOs than USAF.[29] The Army envisioned empowering forward forces to conduct MDOs within the commander's intent, a principle known as *mission command*, to seize opportunities during fast-moving operations and sustain operations even when communications are disrupted.[30] USAF has historically sought to centralize air power to remain flexible and able to shift priorities rapidly in response to changes in the battlefield.[31] USAF initially applied the same logic to MDOs. For example, USAF discussed the idea of a multidomain tasking order modeled on the air-tasking order to centrally allocate and coordinate multidomain capabilities.[32]

The services have nonetheless identified and coordinated on a number of challenges to the JADC2. Primarily there is worry that the current C2 structure, which is used for episodic synchronization of domains, is not built to handle widespread and continuous multidomain integration.[33] Similarly, the USAF has focused on new technology to enable the JADC2.[34] The Chief of Staff of the Air Force (CSAF) launched a high-priority initiative on MDC2, which led to the establishment of the Doolittle War Games series, designed to identify and test the best C2 structures for MDO.[35] USAF has also developed the combat cloud network for data

---

[25] U.S. Marine Corps Concepts and Programs, "Expeditionary Advanced Base Operations," n.d.-a; Jim Lacey, "The 'Dumbest Concept Ever' Just Might Win Wars," *War on the Rocks*, July 29, 2019.

[26] Kevin Huyck and Mark Odom, *ACC/TRADOC TXX Series: Results and Insights*, October 23, 2018.

[27] Huyck, 2019, p. 6.

[28] U.S. Army, 2018; Air Force Doctrine Annex 3-99, 2020.

[29] On the differences in C2 philosophies between air and ground forces, see James W. Harvard, "Airmen and Mission Command," *Air and Space Power Journal*, March–April 2013.

[30] Chadwick D. Igl et al., "568 Balls in the Air: Planning for the Loss of Space Capabilities," *Joint Force Quarterly*, No. 90, July 3, 2018, p. 27; U.S. Army, 2018, p. 19.

[31] Perkins and Holmes, 2018, p. 56. On the USAF C2 philosophy of centralized control and decentralized execution, see Air Force Core Doctrine Volume I, *Basic Doctrine*, Maxwell Air Force Base, Ala., February 27, 2015.

[32] Goldfein, 2017.

[33] U.S. Army, 2018, p. 20; Eric K. Wesley, interview with the Armor & Mobility, October 2018; Air Force Doctrine Annex 3-99, 2020.

[34] Goldfein, 2017.

[35] Amy McCullough, "USAF Looks to Create New Command and Control Structure," *Air Force Magazine*, June 6, 2018; Grant J. Smith, "Multi-Domain Operations: Everyone's Doing It, Just Not Together," *Over the Horizon*, June 24, 2019.

distribution and information sharing, and has begun to vet C2 systems at the Shadow Operations Center at Nellis Air Force Base (AFB) with live flight tests.[36]

The Army and USAF have both identified a need to train their forces in MDOs from the ground up, including providing technical, intellectual, and doctrinal tools and engaging in joint and combined training to ensure that they can apply these capabilities earlier, in greater capacity, at lower echelons, faster, and with greater agility.[37] As a result, USAF has created a new career field for multidomain planners.[38]

The services thus provide a broad and somewhat varied picture of MDOs. Each service supports MDOs and agrees that its central tenets, include speed, cross-domain fires, and the interoperability and convergence of capabilities.[39] Yet the specifics of MDOs are still being developed and differences in C2 approaches remain even as the services are now working together on the JADC2.[40] Moreover, MDO concepts, once developed, will still need to be compared with alternative options for improving warfighting effectiveness. For example, some defense analysts have argued that investments in more munitions could substantially improve U.S. military outcomes in a conflict with a near peer.[41] Investments in additional munitions and capabilities for MDOs could be made simultaneously, but given limited resources, the joint force will need to assess their relative benefits against a peer competitor.

In this report, we assume that MDO initiatives could result in any combination of three broad changes to U.S. military operations. First, commanders may start to consider more options for achieving their objectives.[42] For example, with more awareness of the strengths and limitations of each domain, a commander would be able to weigh the trade-offs of attacking adversary surface-to-air missiles (SAMs) from the air versus using cyber operations to disable, rather than destroy, them.

---

[36] Aaron Kiser et al., *The Combat Cloud: Enabling Multi-Domain Command and Control Across the Range of Military Operations*, Maxwell Air Force Base, Ala.: Air University, 2017; Rachel S. Cohen, "Multi-Domain Ops Push Turns to Joint Force," *Air Force Magazine*, July 25, 2019b.

[37] U.S. Army, 2018, p. ix.

[38] Airmen will spend the first half of their careers gaining tactical expertise in operational career fields before crossing over to the new 13O career field, where they will specialize in planning and integration across domains. Rachel S. Cohen, "Moving MDC2 from Research to Reality," *Air Force Magazine*, May 2019a; Amy McCullough, "Facing the Unknown in a Multi-Domain Command and Control Environment," *Air Force Magazine*, November 11, 2017.

[39] Air Force Doctrine Annex 3-99, 2020; Wesley, 2018, p. 9.

[40] Theresa Hitchens, "Navy, Air Force Chiefs Agree to Work on All Domain C2," November 12, 2019a.

[41] Michael Spirtas, "Are We Truly Prepared for a War with Russia or China?," *The Hill*, October 5, 2018a; David Johnson, "Cluster Munitions and Rearming for Great Power Competition," *War on the Rocks*, May 9, 2019; Jerry Hendrix, *Filling the Seams in U.S. Long-Range Penetrating Strike*, Washington, D.C.: Center for a New American Security, September 10, 2018.

[42] Goldfein, 2017.

Second, U.S. forces could develop new multidomain tactics. For example, rather than using only the air domain to find and fire on an adversary SAM, U.S. forces could use aircraft to find a SAM and ground fires to destroy it. MDOs of this kind offset the weaknesses of one domain with the strengths of another. In this example, aircraft have the advantage of being able to find and fix targets over a larger area than ground forces. However, aircraft also carry limited munitions, so ground units with deeper magazines may be better situated to fire on the targets. Multidomain tactics could also be used to create windows of superiority within a contested domain. As one Army leader explained, "It is no longer possible to maintain total dominance in all domains all of the time."[43] As a result, operations in one domain may be used to create a window of opportunity in another. For example, a cyber attack on adversary integrated air defense systems (IADs) may open up a window of air superiority in a limited geographic area, allowing U.S. aircraft to safely transit the area to strike a target.

Finally, such initiatives might enable MDO schemes of maneuver. The example above indicates how multiple domains may be used together in a single tactical engagement. If, at the operational level, the ground and air components are operating primarily according to their own schemes of maneuver, then multidomain tactical engagements may only be possible using whatever long-range ground fires happen to be available to support the suppression-of-enemy-air-defenses (SEAD) campaign and located in the right place at the right time. An MDO scheme of maneuver, conversely, would plan for the movement and employment of ground fires specifically to coordinate with air operations in support of the SEAD mission. In other words, an operational commander would plan for how forces in multiple domains are positioned and used over time in order to achieve operational, not just tactical, objectives.

Scope and Assumptions

In this report we focus on operational level C2 for major combat operations against a near-peer competitor. As a first step toward disentangling this complex topic, we limit our discussion to impediments to and options for C2 of joint, rather than coalition, military operations.[44] Although we discuss some national and tactical level C2 issues, our analysis is centered on C2 within a geographic combatant command (GCC) such as U.S. European Command (USEUCOM) or U.S. Indo-Pacific Command (USINDOPACOM).

---

[43] David G. Perkins, "Multi-Domain Battle: The Advent of Twenty-First Century War," *Military Review*, November–December 2017.

[44] MDO may also be employed in other conflict scenarios or during steady-state operations to deter a near-peer competitor. The way the U.S. government conducts such operations and the timelines for planning and executing such operations may be different, so the insights from this report may not directly apply to those situations. Moreover, in any of these contexts, the United States is likely to fight with or coordinate with U.S. allies, as it has done historically. The addition of coalition partners creates additional C2 complexity and likely impediments to MDO. Those topics should therefore be considered in future analysis.

Many other ongoing initiatives are considering new C2 as well as communications technologies that may enable the JADC2.[45] As a complement to these efforts, we focus in this report primarily on changes to operational doctrine and authorities. For the purposes of our analysis, we assume that changes in C2 or communication technologies will not fundamentally overcome C2 impediments in the near term.

Following joint and service assessments of the future operating environment, we assume that conflict with a near-peer competitor may be transregional, meaning it may involve operations in more than one combatant command (CCMD).[46] As a result, national leaders will need to make decisions about how to allocate national resources among CCMDs. As discussed in Chapter 2, we further assume that a near peer would attack U.S. communication and C2 systems to undermine U.S. operations. Long-distance communications between the continental United States and forward forces would likely be the most vulnerable, but local communications among U.S. forces could also be degraded.[47]

We also made a number of assumptions to simplify the analysis of the current C2 construct. First, we assume that the combatant commander (CCDR) would not establish a subordinate joint task force (JTF) and would therefore be the joint force commander for major combat operations against a near-peer competitor.[48] Second, we assume that the CCDR would establish and conduct operations using functional components that integrate operations within each domain (e.g., joint force land component commander [JFLCC]).[49] Third, we assume that the commander of Air Force forces (COMAFFOR) is appointed as the joint force air component commander (JFACC).[50]

Organization of This Report

This report is organized around two analytical tasks: identifying potential C2 impediments to MDOs and generating alternative options for the future. Chapter 2 discusses the methodological approach to identifying potential C2 impediments. Chapter 3 describes potential legal and regulatory impediments to MDOs. Subsequent chapters consider potential C2 impediments to MDOs when planning for a contingency, planning during a contingency, and execution and

[45] Goldfein, 2017.

[46] For a CJCS statement that future conflicts will be transregional, see, for example, Joseph F. Dunford Jr., "Gen. Dunford's Remarks and Q&A at the Center for a New American Security Next Defense Forum," n.d.

[47] Priebe, 2019.

[48] CCDRs sometimes establish JTFs, but this additional complexity does not help us consider aspects of multidomain C2, our focus here.

[49] Although doctrine indicates functional components are optional, the United States has often used them in recent military operations; JP 1, 2017. See also Deployable Training Division, Joint Staff J7, "Insights and Best Practices Focus Paper: Geographic Combatant Commander (GCC) Command and Control Organizational Options," August 2016, p. 6.

[50] Doctrine describes this as standard practice; JP 3-30, 2019; Air Force Doctrine Annex 3-30, 2014.

assessment phases. Chapter 4 describes these challenges using a multidomain scenario for joint suppression of enemy air defenses. Chapters 5 and 6 discuss additional challenges that arise when integrating offensive cyber and space into MDOs. Conversely, Chapter 7 describes the C2 enablers of AMD, a mission area that has traditionally been multidomain. Chapter 8 summarizes the potential C2 impediments to and enablers of MDOs that we identified in the preceding chapters.

The remaining chapters of the report describe alternative approaches to the JADC2 within a geographic CCMD. Chapter 9 presents four alternative JADC2 constructs for the joint force to consider for further analysis and experimentation. Chapter 10 provides a framework for evaluating the trade-offs associated with alternative approaches to the JADC2 and offers a preliminary assessment of the four alternative C2 constructs. We conclude by offering findings and recommendations for the joint force.

2. Potential Command-and-Control Impediments to Multidomain Operations

A C2 construct is the collection of organizations, processes, authorities, roles, and responsibilities that the joint force uses to gain situational awareness (SA) as well as plan, execute, and assess operations.[1] In the chapters that follow, we describe the current C2 construct and identify elements that may impede MDOs. This chapter describes our approach to identifying potential impediments.

We use the phrase *potential C2 impediments to MDOs* throughout this report because our analysis is general in nature and not linked to specific MDO concepts. We also remind the reader that the joint force's ultimate goal is to improve its operational effectiveness. MDOs and the JADC2 may be one way to do that. But since we do not yet know how effective emerging MDO concepts will be, C2 impediments to MDO are not necessarily impediments to effective warfighting. Therefore, although we focus on potential impediments to MDOs throughout this report, we do not necessarily recommend making C2 changes to address all of them. The current C2 construct accounts for many considerations beyond MDO, as well as reflecting lessons from past operations and the model the joint force has employed in training and combat. Decisions about which aspects of the current construct to change should be informed by these broader considerations. This report highlights areas that the joint force may need to reexamine as its MDO concepts mature and C2 changes are considered.

Aspirations for Joint All-Domain Command and Control

Since we cannot identify C2 impediments to MDOs directly, we came at the problem from another direction. We began by looking at USAF's aspirations for a future C2 structure that enables MDOs and, more generally, is suited for conflict with a peer competitor. We then asked which aspects of the current C2 construct may fall short of this vision.

USAF has suggested some general characteristics for a C2 structure that may enable MDOs. First, the joint force needs C2 structures and processes that allow decisions to be made more quickly. Second, sufficient expertise and SA in relevant domains are essential to generating and executing multidomain options. Third, planners and commanders must move beyond service and domain stovepipes and adopt a mindset that emphasizes domain-agnostic

[1] Alkire et al. use the term *C2 concept* instead of *C2 construct*. We use the latter term to avoid confusion with newly proposed concepts for MDO or MDC2; Brien Alkire et al., *Command and Control of Joint Air Operations in the Pacific: Methods for Comparing and Contrasting Alternative Concepts*, Santa Monica, Calif.: RAND Corporation, RR-1865-AF, 2018, p. 2.

solutions.[2] Finally, USAF leaders frequently note the threat to communications in a conflict with a near peer and the need for greater resilience in any future C2 construct.[3]

Although not explicit in discussions of the JADC2, USAF and joint leaders likely want any future C2 construct to ensure unity of effort, or coordination toward a common purpose.[4] Even as C2 structures adapt to enable MDOs, the joint force would likely aim to ensure that this enduring warfighting principle is upheld.

Command-and-Control Characteristics That Could Impede Multidomain Operation

In this section we identify C2 characteristics that may prevent USAF and joint vision for the JADC2 from being realized. In Chapters 3–7, we describe specific manifestations of these characteristics in current C2 doctrine or practice.

More steps and approvals are required to integrate multiple domains. We propose that the USAF vision of faster decisionmaking may not be realized if planning, executing, or assessing multidomain options requires more time or involves more complexity than single-domain alternatives. Therefore, as we reviewed the current C2 construct, we asked whether MDOs require more steps and approvals than single-domain alternatives. For example, it would be a potential impediment to an MDO if planning for SEAD using air and ground forces involves more steps and approvals than SEAD conducted through air operations alone.

Planners have insufficient expertise in or access to information about relevant domains. In order to generate multidomain options, planners need to understand both the capabilities and limitations of operations in all domains. They also need information about what forces are available as well as information on what other activities are taking place in the operating environment. It often takes significant expertise to identify planning considerations for a particular domain and to interpret information about the operating environment to generate SA.[5]

---

[2] Goldfein, 2017; McCullough, 2018, p. 30.

[3] For comments about the need for C2 resilience from the CSAF, see, for example, McCullough, 2018, p. 30. "An Interview with Gen David L. Goldfein Twenty-First Chief of Staff of the US Air Force Conducted 5 January 2017," *Strategic Studies Quarterly*, Vol. 11, No. 1, Spring 2017, pp. 4, 9; Theresa Hitchens, "Gen. Goldfein Launches Air Force Doctrine for Joint All-Domain Ops," *Breaking Defense*, March 18, 2020; Sandra Erwin, "Air Force Chief Goldfein: 'We'll Be Fighting from Space in a Matter of Years,'" *Space News*, February 4, 2018.

[4] *Unity of effort* is defined as "coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization, which is the product of successful unified action" (JP 1, 2017, p. V-1).

[5] Situational awareness (SA) is a critical aspect of C2. JP 5-0 states that SA "encompasses activities such as monitoring the global situation, identifying that an event has occurred, recognizing the event is a problem or a potential problem, reporting the event, and reviewing enduring and emerging warning concerns and the CCMD's running intelligence estimate (based on continuous joint intelligence preparation of the operational environment [JIPOE])" (JP 5-0, 2017, p. II-14).

Insufficient expertise or SA means that planners and decisionmakers do not have ready access to information on capabilities in multiple domains, availability of friendly assets, or adversary operations that could affect the ability to execute MDOs.[6] This does not mean that multidomain planners need access to the highly detailed information that domain experts need to conduct tactical planning or execute operations in their domain. Rather, it means that multidomain planners at the operational level need access to sufficient expertise and information to know what options are available and appropriate in a given situation.

MDOs increase communications dependence. In a conflict with a near-peer competitor, communications are likely to be contested. Long-distance communications, such as from Europe to the continental United States, are considered most vulnerable since attacks on a smaller number of high-payoff targets such as undersea cables and infrastructure for satellite communications could disrupt or degrade these links. In-theater communications will also be contested, though the larger number of communications links and redundant communications options should make these harder to degrade. C2 nodes, such as large operations centers and headquarters, are also likely to be targets for kinetic and nonkinetic attacks.[7]

USAF leaders aspire to develop a C2 construct that is more resilient to attacks on both long-distance and local communications. Therefore, we propose that an impediment exists when the current C2 construct means that planning, executing, or assessing an MDO relies more heavily on communications than single-domain operations.

A single-domain or service-centric mindset is present. Another potential threat to the USAF vision for the JADC2 is a mindset among planners that prevents them from considering the full range of multidomain options. No component, whether service or functional, is truly single domain in scope, and few missions are the purview of only one service. For example, land component forces employ helicopters and request air support, while the JFACC is concerned about interdicting adversary forces on the ground. Still, functional and service components may have cultural biases or organizational structures that lead them to prioritize missions in some domains over others. These biases could lead planners to overlook or eschew solutions in other domains or to avoid prioritizing support to missions that take place primarily in other domains.

---

[6] For a discussion of the importance of a common operating picture for MDO, see Perkins, 2017, p. 11.

[7] For a brief overview of threats to communications, see Priebe et al., 2019, pp. 23–27. For a discussion of threats to undersea cables, see, for example, Public-Private Analytic Exchange Program, *The Threats to Undersea Communications*, Washington, D.C.: U.S. Department of Homeland Security and Office of the Director of National Intelligence, September 28, 2017; for a discussion of threats to SATCOM, see, for example, Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*, Santa Monica, Calif.: RAND Corporation, RR-392-AF, 2015; for a discussion of threats to airbases and other fixed sites, see Alan J. Vick, Sean M. Zeigler, Julia Brackup, and John Speed Meyers, *Air Base Defense: Rethinking Army and Air Force Roles and Functions*, Santa Monica, Calif.: RAND Corporation, RR-4368-AF, 2020; for a discussion of the contested electromagnetic spectrum, see, for example, Air Force Doctrine Annex 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, July 30, 2019, pp. 1–12.

As a result, any examples of such biases or structures in the current C2 construct would pose potential impediments to MDOs.

Integrating multiple domains increases risks to unity of effort. A final threat to aspirations for the JADC2 is the possibility that integrating multiple domains makes unity of effort more difficult to achieve. Therefore, we look for aspects of the current C2 construct that make it difficult for operations across domains to achieve a common purpose.[8]

Unity of effort, joint doctrine explains, is best enabled by unity of command within the joint force. Unity of command "means all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose."[9] Ultimately, all joint forces conduct operations under the operational chain of command that flows from the president to the Secretary of Defense (SecDef) to CCDRs. However, as we discuss in Chapter 3, branches of this chain of command operate within the same geography and against the same adversaries. Therefore, there is not always unity of command below the national level. As we review the current C2 construct, we point to places where unity of command is not present, since that is the gold standard described in doctrine, while still acknowledging that unity of effort can be achieved through coordination.

Sources of Information

In the chapters that follow, we describe the current C2 construct and identify potential C2 impediments to MDOs. We do this by looking for specific aspects of the current C2 structure that have one of the five characteristics described above. In the next chapter, we discuss potential impediments in the legal and regulatory framework that constrains C2 choices and frames how military leaders approach operational problems. In subsequent chapters we consider potential impediments to MDOs when planning for a contingency. This prewar planning results in an operational plan (OPLAN). Although the steps of the joint planning process (JPP) are the same for planning before and during a crisis, these chapters consider planning during a contingency separately.[10] This is because the pace of planning, type of decisions that need to be made, and other factors change during the two phases. Finally, we discuss potential C2 impediments during execution and assessment.

We use two primary sources of information for our analysis of impediments: current laws, regulations, and doctrine, and interviews with personnel from across the joint force.

[8] For a discussion for unity of command and unity of effort, see JP 1, 2017, p. V-1.

[9] JP 1, 2017, p. V-1.

[10] For a discussion of the JPP, see JP 5-0, 2017, p. iii; JP 3-0, 2018, p. II-6.

Laws, Regulations, and Doctrine

As a starting point for our analysis, we assume that for a near-term conflict with a near-peer competitor, the United States would draw on the C2 approach described in current law, regulations, and joint doctrine. As is detailed in the next chapter, CCDRs are not bound by doctrine and, within the bounds of current law and regulation, can tailor organizations and processes to their operational needs. Still, joint doctrine describes common practices that have been used in the past that individual commanders use as a starting point.

In order to structure our analysis of these documents, we selected a subset of key activities that planners may wish to integrate as they develop specific MDO concepts. We selected activities that might be of interest to an air component planning for traditional tasks such as SEAD, AMD, and interdicting fielded forces. These activities include

- air interdiction
- airborne intelligence, surveillance, and reconnaissance (ISR)
- defensive counter air
- space-based ISR
- offensive space operations
- long-range ground fires
- offensive cyber operations
- air and missile defense fires from the maritime domain.

For some of these activities, we analyzed C2 impediments using multidomain vignettes. First, we used a stylized version of a multidomain approach to SEAD that ACC has been developing.[11] Second, since AMD is a historically multidomain mission, we considered an AMD vignette in order to identify lessons as well as impediments that may still persist in spite of the longer history of MDOs in this mission area. In both cases, we focus on the operational-level organizations and processes that would be required to generate the multidomain tactical engagement. The details of these vignettes are not central to our analysis. Rather, we use the vignettes to illustrate potential impediments to MDOs in a more tangible way.

We do not explore all possible military activities in all domains or combinations of domains. There are likely additional impediments to integrating defensive cyber operations, for example, that have not been captured. However, we found during our review that many potential impediments cut across domains and activities. Therefore, the impediments we identify for integrating the activities described above may also apply more broadly and provide a starting point for analyzing additional activities and combinations of activities.

[11] Huyck, 2019.

Interviews

Although we use current joint doctrine as the primary baseline for our analysis, we also conducted more than 150 interviews across a variety of organizations to gather information from practitioners on C2 practices in exercises, wargames, and real-world operations. Our interviews focused heavily on planning and operations personnel but often included intelligence and legal experts.

We interviewed representatives from four combatant command headquarters (USEUCOM, USINDOPACOM, U.S. Strategic Command [USSTRATCOM], and U.S. Northern Command [USNORTHCOM]) as well as many of their components. We also met with representatives of what would eventually become U.S. Space Command (USSPACECOM). We spent several days at both U.S. Air Forces in Europe and Air Forces Africa (USAFE-AFAFRICA) and Pacific Air Forces (PACAF). We visited U.S. Army Europe and U.S. Army Pacific and also interviewed Navy and Marine Corps officers in joint billets and liaison elements.

In addition, we conducted interviews with key organizations within the Joint Staff and the Air Staff to get their insights and the most current information on discussions regarding the JADC2 and C2 in conflict with a near-peer competitor more generally. We attended the first USAF Doolittle series game on MDC2 and the USAF Air Combat Command (ACC) and Army Training and Doctrine Command (TRADOC) MDO symposium. We also interviewed personnel from the space, cyber, and air operations center and test and evaluation communities to gather a wide range of insights on forthcoming C2 structures and innovations that may mitigate existing challenges.

We used our professional judgment to identify personnel with appropriate backgrounds from the organizations noted above. Most interviews were conducted in person, though we conducted some by phone or video teleconference. The interviews were semistructured, which means that we started with a standard question list but we adjusted the order, followed up with additional questions, and allowed the participants to share additional information as necessary.[12] In addition to the standard questions, we had detailed questions about the current C2 construct, which varied depending on the participant's current or past positions. The interviews were conducted between October 2018 and June 2019. In order to protect the anonymity of interview participants, we do not provide exact interview dates or locations in our citations. Though we sought to gain a wide range of insights from organizations that prepare for the possibility of conflict with a near peer, these interviews represent a small sample of the joint force. Still, interview insights offer an important complement to the structured review of laws, regulations, and doctrine.

[12] For an overview of judgment-based sampling approaches and semistructured interviews, see Margaret C. Harrell and Melissa A. Bradley, *Data Collection Methods: Semi-Structured Interviews and Focus Groups*, Santa Monica, Calif.: RAND Corporation, TR-718-USG, 2009.

3. Potential Legal and Regulatory Impediments to Multidomain Operations

Existing laws, regulations, and doctrine are the starting point for joint operations.[1] These documents create the constraints within which planning takes place, while the structure of these materials and their key principles frame how planners approach problems. Later chapters describe specific aspects of the current C2 construct as outlined in doctrine and how they may impede MDOs. In this chapter, we look at the laws and regulations that shape doctrine. We begin by briefly explaining how laws, regulation, and doctrine relate to one another. Then, we apply the framework we developed in Chapter 2 to laws and regulations.

In brief, the United States plans, prepares for, and fights its conflicts in strict compliance with all requisite laws and regulations that relate to national defense and the conduct of military personnel. By *legal* and *law*, we mean the authorities that are rooted in the U.S. Constitution, treaties to which the United States is a signatory, the Law of War, and federal statutes passed by Congress and signed into law by the president. Regulations are the Executive Branch's (e.g., the president's, SecDef's, services', or Director of National Intelligence's [DNI's]) interpretation and implementation of these laws.[2]

[1] Throughout this report, we use the term *regulatory* or *regulation* to refer to those authorities that derive from the Law of War and other statutory and treaty requirements with which all military personnel must abide. DoD regulations are typically in the form of "Directives," "Instructions," and "Manuals" that are produced by the SecDef, the CJCS, or the services. These are sometimes colloquially referred to as *policy*, but these authoritative documents are more accurately referred to as *regulations*. Although policies also interpret and help to implement laws and regulations, they may be altered or rescinded based on the decisionmaker's discretion, so long as they do not conflict with laws or regulations. Regulations are drafted and approved in accordance with 10 U.S.C. §§ 113 and 121 and are designed to be long-standing bodies of rules. Also, unlike policies, regulations implement legal authorities (laws/statutes, treaties, and so on), such that military personnel may be punished for their violation under the Uniform Code of Military Justice (UCMJ). See Department of Defense, *Department of Defense Law of War Manual*, Washington, D.C., 2015, updated December 2016, sections 18.7, 18.19.3.1.

[2] Military regulations also constitute orders to military personnel, or otherwise impose some duty on personnel to take some action or refrain from taking some action. These regulatory specific acts or omission of acts are (or could be) punishable under Article 92 of the UCMJ. Military regulations can relate to existing laws, or be issued as a result of policy decisions by the president or the SecDef. Military regulations are distinct from other federal regulations issued by other executive branch agencies. Military regulations are issued by DoD or a service component and apply to servicemembers or other personnel under the jurisdiction of DoD. Failure to follow military regulations can result in the prosecution of the offending servicemember or employee under 10 U.S.C. 892 of the UCMJ. Other federal regulations are issued by their respective departments and agencies (DOJ, State Department, Treasury Department, and so on) are not enforceable under the UCMJ; see, generally, 10 U.S.C. 801–964a. Prosecutorial actions under Article 92 refer to prosecutions authorized under 10 U.S.C. 892 ("Failure to obey order or regulation").

Below, we examine the principal laws, such as U.S. Code Title 10 (Armed Forces) and Title 50 (War and National Defense) and primary Department of Defense (DoD) regulations that implement these laws as they apply to MDOs and the JADC2.[3] We examine how these laws and regulations define the roles, duties, and powers of the key actors with respect to MDOs and the JADC2: the president, the SecDef, CCMDs and their components, and the intelligence community (IC). We find that the current legal and regulatory framework creates potential impediments to MDOs. This finding means that, barring changes to the current legal framework, there will be limits to changes that can be made through decisions by CCDRs or their components.

Before we begin, we would note that many discussions of legal, regulatory, and doctrinal matters are influenced by the U.S. armed forces' recent experiences engaging in counterinsurgency and counterterrorism operations. In major combat operations with a near-peer adversary, the existing legal and regulatory proscriptions and restrictions (along with their concomitant liabilities) would still apply. However, the time-consuming consultative processes to interpret and apply them in new circumstances would likely compete with urgent operational needs in a way that many in the U.S. defense community have not experienced firsthand. This will be important for commanders at all levels, along with their staffs, to consider as they prepare for conflict with a near peer and develop MDO concepts.

Laws, Regulations, and Doctrine

In our interviews, interviewees often referred to authorities that tend to add steps to C2 processes and extend for decisionmaking timelines. The term *authorities* obscures a wide range of documents that constrain or shape how the United States carries out military operations. Understanding which authority creates a potential C2 impediment is important because that authority determines which changes a CCMD or component commander can make on its own and which would require changes at a higher level.

The study team developed a definition of the term *authority* by which to categorize and evaluate the various authorities that affect MDOs. *Authority* is *the official right or permission to act, especially on another's behalf, and the power of one person (or organization) to exercise*

[3] Given Title 50's extraordinary breadth, covering issues from espionage (Chapter 4) to export controls (Chapter 58), our study focused on those chapters and sections that concern national and military intelligence, which is most often relevant to issues concerning MDO and MDC2. These are 50 U.S.C. Chapter 44 (National Security), 3021–3093; Chapter 45 (Miscellaneous Intelligence Community Authorities), 3321–3338; Chapter 46 (Central Intelligence Agency), 3506, 3523–3524; and Chapter 47 (National Security Agency), 3501–3524.

control over an area, persons or organizations, assets, or mission sets.[4] For the purposes of this study, we will refer to three principal types of authority:

- legal and command authority,[5] which pertains to the powers granted, created, or delineated/defined by federal statute, executive order (E.O.), or executive directive (e.g., Titles 10, 50; the Law of War; NSPM-13,[6] E.O. 12333, Countering Adversary Use of the Internet execute order [EXORD]), all of which their basis from, and must comply with, the U.S. Constitution[7]
- regulatory authority, which pertains to the powers granted, created, or delineated by DoD, the chairman of the Joint Chiefs of Staff (CJCS), and USAF directives and instructions (e.g., DoD 5100.01, CJCSI 3121.01B)
- doctrine,[8] which pertains to guidance for the employment of U.S. forces toward a common objective and may include tactics, techniques, and procedures (e.g., JP 1, JP 3-12, JP 3-14).

The authorities above are in order of precedence (see Figure 3.1). In other words, legal authorities are paramount and inviolable. The violation of legal authorities can result in prosecution under the Uniform Code of Military Justice (UCMJ) and/or various criminal statutes.[9] Both regulatory and doctrinal authorities must therefore comply with legal authorities both in substance and in their interpretation and implementation. In other words, a JFACC may not apply USAF doctrine or DoD Instructions (DoDIs) in a manner that conflicts with any legal authority. Command authorities are derived from executive issuances but carry the same force of law as a federal statute for purposes of compliance by military personnel. Therefore, for the purposes of this study, we group them together.

---

[4] Adapted from the definition of the term authority in Bryan A. Garner, *Black's Law Dictionary*, 10th ed., St. Paul, Minn.: Thomson West, 2014.

[5] *Command authority* (which is distinct from combatant command authority, or COCOM) refers to the constitutional and federal statutory authority granted military commanders that flows from the president through the SecDef, for example: the 10 U.S.C. 161 authority of the president (by virtue of his powers under Article II of the U.S. Constitution) to create and establish combatant commands (both unified and specified). This authority provides the legal basis for both the president and the SecDef to issue orders to military forces pursuant to the various sections of Titles 10 and 50. Command authority, in this context, enables the four types of command relationships: COCOM, OPCON, TACON, and support, as exercised by CCDRs and their subordinates; Air Force Doctrine Annex 3-30, 2014, p. 13.

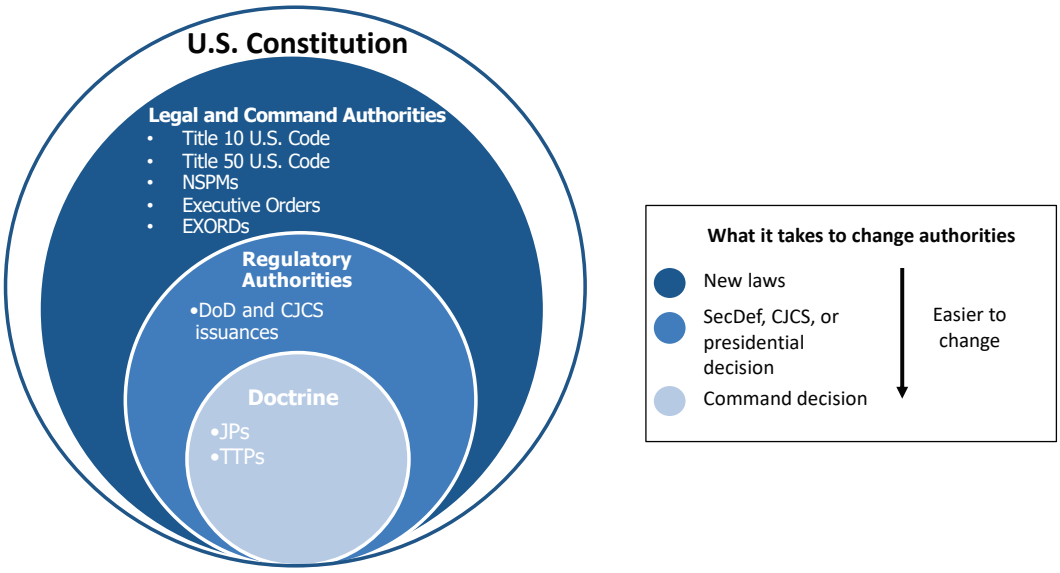
[6] NSPM-13 is a classified document, but some details have been made public by the White House and DoD; see Ellen Nakashima, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *Washington Post*, September 20, 2018. See also interview with Brig. Gen. Alexus Grynkewich in Sydney J. Freedberg Jr., "Trump Eases Cyber Ops, but Safeguards Remain: Joint Staff," *Breaking Defense*, September 17, 2018. References to NSPM-13 within this report are based on these and other similar public reports.

[7] Particularly the president's Article II powers as the commander in chief and Congress's Article I powers to "make rules for the government and regulation of land and naval forces."

[8] Adapted from the definition of *joint doctrine* in Office of the Chairman of the Joint Chiefs of Staff, *DoD Dictionary of Military and Associated Terms*, Washington, D.C.: Joint Staff, June 2020.

[9] DoD, 2016; Headquarters, Department of the Army, *The Battlefield Coordination Detachment*, ATP 3-09.13, July 2015; JP 2-03, 2017.

Figure 3.1. Relationship Among Laws, Regulations, and Doctrine



Additionally, military personnel must comply with regulatory authorities—directives, instructions, and command guidance from both the SecDef and CJCS. They are in essence a form of standing orders that apply to the services and servicemembers. Violations of regulatory authorities can also be prosecuted under the UCMJ, but typically have lesser degrees of punishment associated with them than violations of legal authorities.

Finally, doctrine must comply with both legal and regulatory authorities. Doctrine is not binding on commanders in that violations of these authorities are not punished under the UCMJ as long as they do not violate laws or regulatory authorities. Instead, operational doctrine and tactics, techniques, and procedures (TTPs) are considered to be guidance documents to assist commanders.[10]

Key Elements of the Current Legal Framework

Before discussing potential impediments, we first describe the overarching legal and regulatory authorities that have created and organized CCMDs and how those authorities delineate specific powers that CCMDs have in order to conduct military operations generally. This overarching structure dictates how CCDRs must approach all missions and operations, whether they involve a single domain or all domains. We focus on two aspects of the current legal framework: the division of power among geographic and functional CCMDs and the requirement for adjudication at the national level for transferring authority between the IC and the military.[11]

[10] JP 1 says, for example, "Doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise" (JP 1, 2017, p. ii).

[11] For the term *power*, see DoDD 5100.01, 2010: "Commander of combatant commands; assignment; *powers* and duties" (emphasis added).

Division of Authority Among Combatant Commands

Statutory and executive branch authorities, such as Title 10 and the Unified Command Plan (UCP) have divided military forces and authorities among a mix of GCCs and functional combatant commands (FCCs).[12] GCCs and FCCs have equal statutory authorities under Title 10.[13] The six terrestrial geographic CCDRs have roughly equivalent powers over assigned and attached land, air, and maritime forces within their areas of responsibility (AORs). USSPACECOM, which is also a GCC, has responsibility for on-orbit assets and terrestrial resources and forces that control those assets. The FCC mission sets and jurisdictions, however, are defined by function and not geography. FCCs tend to control capabilities that are high demand and low density, but can also be shifted relatively easily between geographic areas. U.S. Transportation Command (USTRANSCOM) is responsible for strategic mobility (e.g., airlift), U.S. Cyber Command (USCYBERCOM) is responsible for cyber operations, and U.S. Special Operations Command (USSOCOM) is responsible for special operations.[14] Centralized control is intended to allow efficient management and make it easier to reallocate these capabilities when priorities shift. CCMDs typically retain operational control (OPCON) over their assets and forces, even when operating in support of another CCMD and within the geographic CCDR's AOR. USSOCOM is an exception. Geographic CCDRs exercise OPCON over the theater special operations command (TSOC) in their AOR.[15] Although coordination is supposed to occur, the

---

[12] The UCP is a classified executive branch document (i.e., legal authority) approved by the president. It (1) "sets forth basic guidance to all unified combatant commanders"; (2) "establishes their missions, responsibilities, and force structure"; (3) "delineates the general geographic area of responsibility (AOR) for geographic combatant commanders"; and (4) "specifies the functional responsibilities for the functional combatant commanders" (Office of the Chairman of the Joint Chiefs of Staff, 2020, p. 224). The UCP is governed by 10 U.S.C. 161. It is the Executive Branch counterpart to 10 U.S.C. 164. Forces may be assigned to a CCMD either in Title 10 or through the president's direction using the UCP. Dustin Kouba, ed., *Operational Law Handbook*, Charlottesville, Va.: The Judge Advocate General's Legal Center and School, 2018, p. 423.

[13] Both the president and the SecDef issue guidance to further implement the UCP. For example, the Guidance for the Employment of the Force provides direction to CCMDs for operational planning, force management, and so on. These doctrinal-level documents enable the SecDef to communicate strategic priorities from the Quadrennial Defense Review and apply them to operational activities. These documents lack "legal" and "command authority" as defined in this chapter, however, and are subordinate to the UCP. Government Accountability Office, *Warfight Support: An Assessment of DoD Documents Used in Previous Efforts to Rebalance to the Pacific*, Washington, D.C.: Government Accountability Office, GAO-18-192, May 2018, p. 6.

[14] U.S. Transportation Command, "About USTRANSCOM"; U.S. Cyber Command, "Mission and Vision." Until August 29, 2019, STRATCOM was responsible for space forces not assigned to GCCs. On August 29, 2019, those forces transferred to USSPACECOM. Assigned missions included missile warning, satellite operations, space control, and space support. Aaron Mehta, "Space Command to Launch Aug. 29," *Defense News*, August 20, 2019.

[15] Andrew Feickert, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," *Congressional Research Service*, No. R42077, January 3, 2013, 2013, pp. 15, 19. Congressional Research Service, *U.S. Special Forces (SOF): Background and Issues for Congress*, RS21048, March 28, 2019, p. 2; Annex 3-05, 2017, p. 19; JP 3-05, 2014, p. I-3. USSOCOM is also unique in that it is responsible for training forces that have not been assigned to it as a CCMD by the president or the SecDef; Brad Clark et al., *Operational Law Handbook*, 17th ed., Charlottesville, Va.: The Judge Advocate General's Legal Center and School, 2017, p. 62. Air Force Core Doctrine Volume I, 2015, pp. 49, 61.

existing legal structure means that a geographic CCDR does not necessarily control all of the assets that can have effects in his or her AOR. Interviewees also noted that there are cases when a geographic CCDR is not aware of cyber or USTRANSCOM assets that are operating in his or her AOR pursuant to concurrent orders given by the president or the SecDef.

Division of Authority Between the Intelligence Community and Military

Another critical component of today's legal framework is the division of authority between the IC and the military for space, cyber, and dual-use intelligence platforms.[16] By law, in peacetime, many authorities reside with the IC and take place under Title 50 authority.[17] The SecDef may conduct intelligence operations under either Title 50 or Title 10.[18] Intelligence activities therefore involve two chains of command (SecDef and DNI)[19] and two implementing authorities (Titles 10 and 50).[20]

Both chains of command and both sets of authorities employ the same assets in order to accomplish their missions. Therefore, during peacetime, the National Security Agency (NSA) may be directed by the DNI to gather intelligence under the National Intelligence Program (NIP)

---

[16] Andru E. Wall, "Demystifying the Title 10–Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard Law School National Security Journal*, Vol. 3, No. 1, 2011, pp. 89–101.

[17] 50 U.S.C. 3034. Title 10 of the U.S. Code, entitled "Armed Forces," covers general military law, the four services, and the nation's reserve military components. In general, Title 10 covers all DoD activities related to military operations. Thus, when CCDRs are engaged in MDOs and employ their assets and forces in furtherance of military objectives in preparation for, during, or after a conflict, their authority to conduct these actions and employ their assets and forces stems from the various sections within Title 10. Title 50 of the U.S. Code is entitled (more broadly), "War and National Defense." With 58 separate chapters, Title 50 covers a much wider span of topics related to defending the United States and its allies, including areas related espionage, atomic weapons, intelligence, chemical and biological programs, export controls, among numerous others. For the purposes of this report, the material chapters of Title 50 are those related to intelligence operations; 10 U.S.C. Subtitles A through E; 50 U.S.C. Chapter 44 (National Security), Chapter 45 (Miscellaneous Intelligence Community Authorities), Chapter 46 (Central Intelligence Agency), and Chapter 47 (National Security Agency). See also Wall, 2011, p. 87.

[18] DoDD 5100.20, 2010. See also E.O. 12333, which directs the SecDef to "collect (including through clandestine means), analyze, produce, and disseminate information and intelligence [as well as] . . . defense and defense-related intelligence and counterintelligence" (E.O. 12333, United States Intelligence Activities, 46 Fed. Reg. 59941, 1981, code edition dated December 4). If the intelligence operation is in support of, or part of, a military operation, the SecDef's authority stems from Title 10. If he is conducting a peacetime intelligence operation, his authority stems from Title 50, DoDD 5100.20, 2010 (for military intelligence activities), and DoDD 5100.20, 2010 (for national intelligence activities, including peacetime intelligence collection activities).

[19] JP 2-01, 2017, chap. 2.

[20] For example, the National Security Agency (NSA), although part of DoD, is overseen by the DNI for the purpose of executing the National Intelligence Program (NIP). NIP "refers to all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of National Intelligence and the head of the United States department or agency or by the President. Such term does not include programs, projects or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by the United States Armed Forces" (50 U.S.C. 3003[6]). Thus, the DNI exercises his statutory authorities to direct IC assets, as defined in Title 50, pursuant to NIP. See 50 U.S.C. 3034.

authority using a platform assigned to a CCMD.[21] During a contingency, the SecDef (rather than the DNI) could direct NSA to gather intelligence using the same platform via the Military Intelligence Program (MIP).[22] Alternatively, control over those forces could be transferred to a CCDR upon the issuance or initiation of an EXORD, OPLAN, or other implementing order from the president or the SecDef. If disagreements between the IC and the military arise, a myriad of authorities such as DoD 3100.10 (space), NSPM-13 (cyber), and CJCSI 3250.01F (ISR) manage the allocation of these assets.[23] Ultimately, national-level decisions about how to assign forces can affect how and whether a CCDR can use these capabilities during a contingency. These authorities create additional steps and approvals for using some capabilities as part of MDOs, as detailed in the following sections.

Potential Impediments

In this section we describe how the current legal and regulatory framework creates potential C2 impediments to MDOs. As noted above, laws and regulations that potentially impede MDOs are not necessarily bad policy choices given the full range of national considerations, including managing global priorities and highly consequential decisions. Still, we highlight ways that the current legal and regulatory framework may affect MDOs for two reasons. First, impediments to MDOs represent potential trade-offs with status quo arrangements. Second, if we assume the legal and regulatory structure is unlikely to change, then these impediments to MDOs may be a fact of life that revisions to doctrine can do little to change.

Additional Steps and Approvals

When a GCC MDO relies on capabilities controlled by another CCMD or the IC, more steps and processes are required. The additional time and manpower involved in these steps could make it more difficult to conduct this type of MDO at scale during a fast-paced contingency.

GCC requests for other CCMDs or the IC to provide an effect must be adjudicated and may or may not be approved or prioritized. If there is a conflict or dispute at the CCMD level or between a CCDR and an IC member, the request is elevated to the SecDef for adjudication and

[21] JP 2-01, 2017, pp. xii–xv, II-11–II-21.

[22] JP 2-01, 2017, p. II-12. See also, generally, DoDD 5205.12, 2018. Anne Daugherty Miles, *Intelligence Community Programs, Management, and Enduring Issues*, Congressional Research Service, R44681, November 8, 2016, pp. 10–29. NIP and MIP represent two distinct program authorities for conducting intelligence operations for the DNI and the SecDef, respectively. They also are funded through two separate budgeting processes that the DNI and the under secretary of defense for intelligence must coordinate; 10 U.S.C. 137(b)(1) (MIP) and 50 U.S.C. 3038(c) (NIP); Michael E. DeVine, *Defense Prime: Under Secretary of Defense (Intelligence)*, CRS in Focus IF10523, December 19, 2018, p. 2; 50 U.S.C. 3024(c) through (d).

[23] CJCSI 3250.01F, 2019. Not available to the general public. As cited in JP 2-01, 2017.

resolution.[24] Instead of requesting an effect, the CCMD could request control of the capability for a limited period of time. Although functional CCDRs and commanders of USSPACECOM have significant authority over assigned forces, regardless of where they are located geographically,[25] they do not have the authority to transfer control of these forces to another CCMD. As a result, a GCC's request to control a capability that is assigned to another CCMD has to be approved by the president or the SecDef.[26] In either case, the current legal and regulatory framework increases time and uncertainty for planning MDOs that rely on capabilities controlled by other CCMDs or the IC. By granting equal statutory authority over unequal, disparate, and differing missions, forces, and assets, Title 10 and the UCP create both competition and conflict among CCDRs over limited resources. The system of bargaining, negotiation, and adjudication to determine the geographic and functional control therefore creates additional steps and approvals for MDOs that rely on certain types of space, cyber, mobility, and ISR capabilities. If CCMDs cannot work out these issues among themselves, the SecDef has to adjudicate, which adds more steps and time.[27]

Multiple experts we interviewed brought up the steps required to transfer ISR capabilities at the outbreak of war to the GCC as an illustration of the "authorities problem." As noted above, in steady state, an IC organization may be operating an ISR asset within a GCC's AOR.[28] In theory, there could be a standing order from the president or the SecDef transferring this ISR asset to the GCC in the event of a contingency.[29] However, because the delineation of what constitutes

---

[24] DoDD 5100.01, 2010, enclosure 5(1)(c). The CJCS may also be involved in his or her role as global integrator; see 10 U.SC. 153(a). The 2017 NDAA provided for what has become termed the "Global Integrator" role of the chairman, which would also allow him to serve as an adjudicative agent in resource allocation deliberations if instructed by the SecDef; U.S. House of Representatives, "National Defense Authorization Act for Fiscal Year 2017, Conference Report," Washington, D.C.: U.S. Government Printing Office, November 30, 2016, p. 1136.

[25] "Transient forces do not come under the chain of command of the GCC solely by their movement across operational area boundaries, except when the GCC is exercising TACON for the purposes of force protection" (Clark et al., 2017, p. 435). In other words, assets and forces assigned to a different CCDR that operate within another CCDR's AOR remain OPCON to the assigned CCDR unless there are exigent circumstances that would put forces in direct harm. In such a circumstance, the geographic CCDR may exercise TACON for the purpose of defending those forces only. Once the threat is eliminated, TACON (which is inherent in OPCON) returns to the CCDR that is the assignee of the force.

[26] DoDD 5100.01, 2010. 50 U.S.C. 3023. CJCSI 3141.01F, 2019.

[27] DoDD 5100.01, 2010, enclosure 5(1)(c).

[28] Under Title 50, the asset is presumptively under the control of the DNI and/or the Director of the NSA (DIRNSA), particularly if the asset is being used to conduct SIGINT activities; CJCSM 3122.07A, 2013; DoDD 5100.20, 2010.

[29] To facilitate the coordination of ISR assets for use by either the military or the IC in particular, Title 10 mandates that the under secretary of defense for intelligence "shall" develop an ISR integration roadmap in consultation with the DNI; 10 U.S.C. 426(b)(2). This statutory mandate indicates Congress's intent to provide the necessary authorities for both the SecDef and the DNI to manage limited dual-use assets in peacetime (by the DNI) and during military and/or contingency operations (by the SecDef). Additionally, this requirement is coupled with a statutory mandate for the CJCS to inform Congress annually of the ISR requirements (including space-based assets) of CCMDs; see 10 U.S.C. 426(c). In this way, CCDRs are able to provide both the president and Congress with an assessment of their ISR needs and—presumably—whether the management of those resources between the DNI and the SecDef satisfies their operational requirements; see 10 U.S.C. 426(c)(1)(B), requiring a report of the "satisfaction rate of each the combatant commands."

peacetime and wartime could be unclear in an era of gray zone tactics, and because the transition time from peace to war can be seconds, a CCDR may not have control of assets and forces that are within his or her AOR at the outset of a conflict. Instead, the CCDR would need to request control, adding additional time.[30] In a crisis, the SecDef may intervene to adjudicate more rapidly, but gaining control at the outbreak of a contingency still takes additional time.[31] Moreover, the default control of these assets during peacetime can also extend into conflict situations if the IC need is deemed to be a higher priority. As a result, a CCDR may have some uncertainty about whether he or she will have control of these capabilities in the event of war.

All this means that if a GCC has a multidomain option that relies on capabilities controlled by another CCMD or the IC (e.g., space and cyber capabilities), that option will take more time to plan and face greater uncertainty than a single-domain operation or an MDO that employs capabilities under the GCC's control. In this sense, the current legal framework presents a potential C2 impediment to MDOs. However, as noted above, the United States has these arrangements due to other considerations. Coordination mechanisms, although perhaps time and resource consuming, are also intended to ensure that competing equities, interests, and risks are considered before a scarce asset is transferred from one operator to another.

The remainder of this section details the extra steps and approvals that the current legal framework creates. In particular, we examine the review and approval process (RAP) and the deconfliction subprocess of the RAP. Together, the RAP and deconfliction represent one of the best examples of how steps/processes that are mandated by law and regulations affect certain types of MDOs by requiring time, resources, and staff to adjudicate decisions over limited resources.

Review and Approval Process

If a GCC needs a capability controlled by another CCMD or IC organization, a request is made through a mechanism commonly referred to as the RAP.[32] Given the desire to integrate more space and cyber with operations in other domains, such requests are likely to be more frequent and pressing than in the past. Therefore the additional steps involved are worth exploring in detail.

The RAP may be used to request either the assignment or transfer of an asset or force or a particular effect (e.g., cyber fires, space-based jamming, and so on) without assignment, transfer, or placement in support of the asset itself.[33] Depending on the nature of the request, the RAP

[30] Clark et al., 2017, p. 435.

[31] Interviews with JA personnel.

[32] CJCSI 3141.01F, 2019, enclosure B (Plan Preparation, Review, and Approval Process). Detailed discussions of cyber and space, which are not addressed in this report, can be found in CJCSM 3139.01, 2013.

[33] CJCSI 3141.01F, 2019.

requests are transmitted to the national level (SecDef or CJCS) or appropriate CCMD for adjudication.[34] As part of the adjudication, the stakeholders that maintain equities in control of the asset have an opportunity to provide input (an IC community member, for example).

Returning to our ISR example, if a GCC needs intelligence collection using a particular cyber or space-based platform, the relevant CCMD or IC organization will prioritize (or "rack and stack") the request along with others it receives. The CCMD or IC organization, under the direction of the president or the SecDef, would retain control of the space or cyber asset, but would provide the intelligence through a support relationship with the GCC.[35]

Should a GCC require the asset notwithstanding the relevant CCMD's "rack and stack" determination, the decision would be forwarded to the appropriate SecDef or CJCS element for the ultimate determination. GCCs, FCCs, or IC members competing for the ISR asset would have the opportunity to present their case for prioritization. Upon adjudication, the decisionmaking authority would approve, deny, or modify the GCC's RAP request.[36] In the case where another CCMD is the decisionmaking authority and the request is denied, the GCC can ask the SecDef to intervene. This process can involve significant delays. Interviews revealed that in some noncontingency situations, the adjudication process took months.

When planning for a contingency, the GCC may develop concepts that rely on capabilities controlled by an FCC, by USSPACECOM, or by the IC in peacetime. The GCC would have to invest time and energy into creating the most persuasive case possible since he or she is competing for scarce resources. Moreover, because approval may not ultimately be granted, requesting GCCs must factor in this decision uncertainty in terms of the conduct of the operation, future contingencies and/or planning, and the need to have ready alternative options available (e.g., substitute platforms for surveillance/detection, kinetic weapons for fires, and the like). However, if approved, these requests could result in a plan to distribute authorities. Of course, the plan may have to be adapted for an actual contingency. Still, having done a RAP prior to the contingency increases requesting GCC certainty that the attachment of forces or delivery of an effect will be ordered.

Although GCCs can submit requests during the process of planning for a contingency, they may still need to make RAP requests during contingency operations. After first contact, a CCDR may determine that his or her delegated authorities or assigned or attached assets are insufficient. As a result, a CCDR may request additional authorities for a particular asset or effect using the

[34] National-level adjudication may not be necessary in cases where the GCC is requesting a readily available asset. For example, a request for a cyber or space asset may be approved by the respective CCMD in the event that the asset is otherwise available, and any required deconflictions can be resolved between the owning CCMD and the requesting GCC. Alternatively, in a contingency, the requesting GCC may have to proceed to the CJCS, the SecDef, or the president in order to quickly obtain authorization of an asset or effect immediately needed for the fight.

[35] Interviews with JA personnel.

[36] JP 3-14, 2018 (for the SecDef); CJCSI 3141.01F, 2019 (for the CJCS in its advisory capacity to the SecDef).

RAP outlined above. Any amendments or changes to the initial concept of operations (CONOP) after the initiation of hostilities can take time, though it could be minutes/hours in a combat situation (e.g., if the RAP is routed to the SecDef over secure communications for a voice order to be issued) rather than the months it may have taken to complete a RAP request during CONOP planning or steady-state operations. However, in major combat operations against a near-peer competitor, there may be many urgent requests from multiple CCMDs, which could lengthen the RAP timeline as multiple requests have to be adjudicated through the same request chain.

Deconfliction Phase

Deconfliction is a step in the RAP process described above, but bears a separate discussion because interviewees noted it is frequently the most complicated aspect of the RAP. Deconfliction involves identifying the use, capability, availability, and needs (current and future) of the asset or effect vis-à-vis the equities of each stakeholder that is assigned or has made a request for the asset (or effect).[37] *Deconfliction* is defined as resolving the competing and conflicting use or future assignments of a particular asset among DoD, the Department of Justice (DOJ) (and the Federal Bureau of Investigation [FBI] as a subordinate agency of DOJ), and any other members of the IC.[38]

RAP requests are first sent to the responsible CCMD where initial prioritization and deconfliction occurs if the asset in question relates to space, cyber or, conceivably, a USTRANSCOM asset.[39] If the asset is owned or controlled by the DNI, the RAP request will most likely be sent first to the Director of the National Security Agency (DIRNSA).[40] The relevant CCMD or the IC organization must resolve the RAP request by contacting other military or IC entities that have competing equities with regard to the asset in question. For example, a GCC may request collection by a satellite-based ISR asset as part of a contingency operation. However, that asset—in the steady state—is likely already serving a member of the IC, such as the FBI, the Central Intelligence Agency (CIA), or other IC entity. During the process, the IC organization would need to determine if the asset in question may be redirected to support the requesting GCC without negatively affecting the IC entity's (current or future) missions relative to the mission needs of the requesting GCC.

---

[37] CJCSI 3141.01F, 2019, enclosures B through C (discussing deconfliction as part of the in-progress reviews and the Joint Planning and Execution Community review and plan assessment parts of the RAP).

[38] Among others, several regulatory authorities require CCMDs to engage in deconfliction processes in order to assign/attach assets: DoDD 5100.20, 2010, pp. 6–7; DoDD 3600.01, 2013; and similar DoDDs. Additionally, doctrinal authority sources reference the regulatory requirement to deconflict these same types of assets; for example, see JP 3-14, 2018; JP 3-12, 2018.

[39] CJCSI 3141.01F, 2019, enclosures A through C.

[40] DoDI O3115.07, 2010, enclosure 2(2).

Given that both legal and regulatory authorities require the controlling CCMD to obtain information from the IC entity before making a determination for certain requests,[41] a bottleneck of RAP requests could develop, especially during high-intensity combat operations.[42] Alternatively, rather than waiting for a decision, a GCC may opt to deploy his or her own organic assets (perhaps substituting a kinetic solution for a nonkinetic solution) to meet the mission critical need.[43]

Once the other CCMD or IC organization obtains sufficient information, it must then assess and adjudicate the requesting GCC's and the IC entity's competing equities and determine which entity will be assigned the asset. RAP requests or deconflictions that cannot be resolved by CCMD, DIRNSA, or the IC member are forwarded to the SecDef or the president for a final determination.[44] As noted above, some requests go to the president or the SecDef as a matter of course.

There are some potential ways to reduce the number of steps and approvals for these effects and transfers. For example, in the event of hostilities, an EXORD from the president and/or the SecDef could direct the assignment or transfer of a particular cyber, space, or intelligence asset to a GCC, thereby negating the need to engage in the RAP because a GCC already has OPCON pursuant to that order.[45] If the GCC's needs change and EXORD has to be updated, the RAP will restart. Moreover, in practice, transfer of some assets, such as those controlled by CYBERCOM or USSPACECOM, are rarely delegated or distributed further down the chain of command to another CCMD. As a result, the RAP and deconfliction process are frequently triggered.

Other changes to reduce the number of steps and approvals needed for using certain cyber, space, and ISR capabilities would require changes to both law and regulation. For example, one way to reduce the number of steps would be to give CCMDs such as CYBERCOM authority to transfer some capabilities to the highest priority CCMD for control. Doing so would require

---

[41] DoDD 5100.20, 2010, pp. 6–7; DoDD 3600.01, 2013; DoDI O3115.07, 2008, enclosure 2; additionally, doctrinal authority sources reference the regulatory requirement to deconflict these same types of assets; for example, see JP 3-14, 2018; JP 3-12, 2018.

[42] Additionally, even if the CCMD in this example is given the asset through the RAP and begins to plan an operation relying on the asset assigned, this does not foreclose the possibility that a more urgent (higher priority) RAP request could be submitted and that it takes precedence over the CCDR's request. This could result in another reallocation, possibly in the middle of the CCDR's planning process, and loss of the asset before it is deployed by the CCDR. It is conceivable that this could occur even after GCC forces have already been repositioned for the operation, potentially wasting time and resources for no benefit. Also, concurrent lines of effort (LOEs) and campaign timelines may be delayed or disrupted by the loss.

[43] See the discussion of the RAP for Cyber Operations (RAPCO) in James E. McGhee, "Liberating Cyber Offense," *Strategic Studies Quarterly*, Winter 2016, pp. 48–49.

[44] In the case of SIGINT assets, for example, the request/deconfliction issue would proceed to the under secretary for intelligence, who is the SecDef's designee to adjudicate or resolve the conflict; DoDI O3115.07, 2008, enclosure 2(1).

[45] Such an order stems directly from the president's or the SecDef's authority to assign or transfer the asset, rather than designate a supporting relationship under Sections 162 and 164 of Title 10.

amending existing legal and regulatory sources that require retention of transfer authority by the president or the SecDef.[46] However, even this change would not remove the RAP/deconfliction impediment. Legal sources such as Title 50 still require IC control of most high-demand assets during peacetime.[47] Even upon gaining control over assets upon the initiation of hostilities, CCDRs would still need to engage in some type of adjudication process with IC members, who also have wartime responsibilities.[48]

Additionally, the delegation or distribution of some of these assets to each CCMD would increase the load on IC points of contact as they contend with communications from up to 11 CCDRs, rather than one or two CCMDs or the SecDef. There would also be other trade-offs, such as making it more difficult to reallocate these capabilities quickly. Notwithstanding the advantage to having these capabilities directly available in an AOR where a contingency has emerged, without a global vantage point, a regionally focused GCC may deny the IC entity or other CCDR use of the asset in a manner that creates unacceptable mission risks, or risks to lives, in other theaters (in both the IC and military context). In other words, optimizing authority over assets for one GCC may result in more C2 impediments for other GCCs, FCCs, or the IC. This is not to say, however, that delegations and/or distributions of authorities over certain cyber, space, and ISR capabilities should not be accorded to CCMDs, particularly where the needs for additional capabilities are identified in the planning process. Rather, the risks associated with such delegations and/or distributions should be carefully delineated and weighed.

Legal Review of Space and Cyber Operations

CCDRs are required to obtain judge advocate (JA) review of "all plans, policies, directives, and rules of engagement issued by the command and its subordinate commands and components."[49] Legal reviews for plans that involve offensive space and cyber operations are longer and more complex due to the potentially broader effects of operations in these domains and disagreements within this newer area of law. Offensive cyber operations begun in one network can have cascading effects in other networks, including on civilian populations or infrastructure. Use of space assets may disrupt or delay communications beyond a geographic command or may increase risk of collision with other space-based assets (both friendly and nonfriendly).[50]

---

[46] Particularly DoDD 5100.01, 2010 (for all domains); NSPM-13 (as publicly reported: Nakashima, 2018; Freedberg, 2018). For more detailed discussions not covered in this report, see CJCSM 3139.01, 2013; CJCSM 3150.07E, 2013; CJCSM 3150.07E, 2013; DoDD 3100.10, 2016.

[47] CJCSM 3122.07A, 2013; DoDD 5100.20, 2010, chapter 47, 3601–3618.

[48] 50 U.S.C. 3024(a)(1)(C).

[49] DoDD 2311.01E, 2006, at 5.11.8.

[50] See Clark et al., 2017, pp. 131–134, at discussion of the "Legal Considerations in Cyberspace Operations." Cyber operations present unique issues because of the nonkinetic, yet potentially devastating, effects of cyber fires. This necessitates a detailed legal analysis of the effect in question to ensure compliance with Article 2(4) of the United Nations Charter (i.e., "threat or use of force" principle) as well as Article 51 (i.e., what constitutes a lawful act in furtherance of the self-defense of an individual nation or collective of nations).

Additionally, some legal and policy documents associated with both space and cyber are also newly issued.[51] Interviews with several JAs indicated that lawyers throughout various CCMDs, the CJCS, the Office of the Secretary of Defense (OSD), and service component headquarters elements often develop different interpretations of newer legal and regulatory authorities. Commanders, their staffs, and JAs must reconcile and apply these new authorities when planning and conducting any operation. For example, if an EXORD provides a CCDR with an offensive cyber capability,[52] there could be disagreements about what responsibilities that a CCDR has to notify other CCMDs or allies with respect to any potential risk to their networks or systems.[53] Thus, MDOs involving new and innovative capabilities or those with greater risk of cascading effects, including offensive space and cyber operations, involve more lengthy legal reviews.

Insufficient Expertise or Access to Information

The numerous authorities pertaining to functions, geographies, command responsibilities, capabilities, and so on could lead to insufficient legal expertise or information needed to plan MDO.

Insufficient Legal Expertise

Given the sheer multitude of authorities, it is difficult for CCDRs, staffs, JAs, and other personnel to develop and maintain expertise within and across domains. As a result, JAs tend to develop subject matter expertise in certain domains (e.g., cyber, space, information operations, intelligence). For example, JAs at USSPACECOM specialize in space law, while JAs at USCYBERCOM specialize in cyber law. These divisions, both intellectual and physical, could make review and approval of MDOs challenging as different groups tend to develop distinct informal processes, procedures, and interpretations of law, regulation, and doctrine.[54] Staffing

---

[51] For example, NSPM-13 was issued by the president in September of 2018 (as reported publicly by Nakashima, 2018; see also interview with Brig. Gen. Alexus Grynkewich in Freedberg, 2018). The requirement to develop a specific space warfighting policy was directed by Congress in August of 2018 pursuant. See John S. McCain National Defenses Act for Fiscal Year 2019, Public Law 115-232, section 1607(a), enacted August 13, 2018. The principle regulation for space operations policy, DoD Directive 3100.10, was issued in 2012, but was amended in 2016 and may require additional amendments given the new requirement of section 1607(a) of the 2019 NDAA noted here.

[52] See, for example, publicly available information regarding the Counter the Enemy's Use of the Internet (CAUI) EXORD: discussion by Gen. (retired) Michael V. Hayden, "The Making of America's Cyberweapons," *Christian Science Monitor*, February 24, 2016.

[53] While the legal clearance process for deploying a kinetic weapon in an ally's AOR may be both quick and simple, additional time for complying with Hague and Geneva requirements may be necessary when a space or cyber weapon is deployed (particularly if the compliance procedures are external to the GCC). See, for example, Geneva Convention of 1949 (various articles); "Hague Regulations" relating to targeting and the "means and methods" of warfare, Hague Convention of 1907 ("Hague IV"), Articles 22–41.

[54] See, generally, Alex A. Kondra and Deborah C. Hunt, "Institutional Processes of Organizational Culture," *Culture and Organization*, Vol. 15, No. 1. Different groups naturally develop different cultures as they adapt to the particular external pressures they face, such as those associated with a particular function (cyber, space) or geographic location (GCC AOR). In turn, the groups can develop different interpretations of experiences, rules, practices, and so on.

resources limit the availability to expand expertise in the relative domains to all CCMDs and levels of command. Thus, although a JFACC may plan for cyber fires, the legal expertise to provide final clearance for such fires may reside in a different CCMD (likely USCYBERCOM) and/or at a different level of command (perhaps CJCS or OSD). This could make it difficult for planners to predict whether a plan will be approved.

Classification of certain programs can compound the challenge of having sufficient legal expertise in all domains. Classification can act as an impediment to knowledge transfer and growth.[55] For example, a GCC planner may request a space or cyber asset as part of an operation. As part of the RAP, another CCMD's staff may determine that the operation may not be technically feasible. Due to the classification of the programs, the owning CCMD may not be able to explain why it denied the request. This may then lead requesting GCC planners and JAs to incorrectly believe that the reason for denial relates to a lack of sufficient requesting GCC authority or prioritization, rather than a lack of existing capability. In this case, the planner and the GCC's JAs would not learn more about how and when cyber capabilities can be used to inform future planning.

Insufficient Situational Awareness

Functional CCDRs and USSPACECOM are not always the supporting CCMD in an operation—they may, for certain operations, be the lead CCMD and may be supported by various GCCs. Hypothetically, the president/SecDef could issue an EXORD to disable a section of Russia's or China's electrical grid, and designate USCYBERCOM as the lead CCMD. In such a case, USCYBERCOM could produce cyber effects within the USEUCOM or USINDOPACOM AORs without providing full information to the relevant GCCs.

Similarly, there may be a covert operation where an IC agency is the lead and military CCMDs are in support. The most famous example of this is the 2011 raid on the Abbottabad compound in Pakistan, where USSOCOM forces located and killed Osama bin Laden. The raid was a covert operation pursuant to Title 50 authorities (50 U.S.C. 3093) and E.O. 12333 1.8I.[56] Because there are circumstances where military personnel may not be authorized to have knowledge of such actions, both as a legal matter and as a matter of maintaining Geneva Convention protections for U.S. military personnel in the event of capture,[57] it is conceivable that IC actions may occur within a GCC's geographic boundaries with no coordination (or

---

[55] Edward L. Bolton Jr., "Cyber and Space—A Way Ahead," *High Frontier*, Vol. 6, No. 4, 2010, pp. 10–11.

[56] Joseph B. Berger III, "Covert Action: Title 10, Title 50, and the Chain of Command," *Joint Force Quarterly*, Vol. 67, October 2012, pp. 32–39.

[57] David A. Deptula, "A New Era for Command and Control of Aerospace Operations," *Air and Space Power Journal*, July–August 2014; Josiah R. Collens Jr. and Bob Krause, *Theater Battle Management Core Systems Engineering Case Study*, Wright-Patterson Air Force Base, Oh.: Center for Systems Engineering at the Air Force Institute of Technology, February 17, 2005; International Committee of the Red Cross, *Geneva Convention Relative to the Treatment of Prisoners of War*, August 12, 1949.

limited coordination at the highest levels of command).[58] In such a case, a GCC's lack of SA regarding the IC action may be a result not of degraded communications, but as a result of legal restrictions themselves.

Another authorities-related impediment that may result in a lack of sufficient SA stems from bifurcated tasking processes for ISR and force application. Certain ISR assets are tasked by the air operations center (AOC) through the Planning Tool for Resource Integration, Synchronization, and Management (PRISM), while the Theater Battle Management Core System (TBMCS) is used to task strike assets such as aircraft.[59] However, some platforms can conduct either type of mission (e.g., F-16s, MQ-9 Reapers).[60] Thus, two separate authorities that dictate tasking procedures and reporting for air-tasking orders would be necessary while exercising control over a single asset.[61] Without a centralized system for tasking and reporting, the CCMD and AOC staff personnel may be strained to maintain SA of multiple assets engaging in multiple ISR and force-projection missions.

Increase in Communication Dependence

As noted above, CCDRs are independent legal agents/actors *and* reliant on each other when an MDO involves capabilities from multiple organizations. Additionally, CCDRs and IC entities are also interdependent and reliant on each other, notwithstanding their differing chains of command, reporting requirements, and mission sets under Title 50. This means that when a GCC MDO relies on capabilities from other CCMDs or the IC, the GCC must be able to communicate to submit RAP requests as described above. If requests are approved, they must also work together to coordinate effects as detailed in later chapters. This means that when a GCC's MDO relies on capabilities from another CCMD or the IC, these operations are also more reliant on long-distance communications links (e.g., SATCOM, undersea cables) compared to operations that rely only on in-theater capabilities under the GCC's control. As discussed in Chapter 2, there is less redundancy of long distance, meaning an adversary may be able to more effectively degrade these links than those in theater. MDOs that rely on approval from or detailed coordination with organizations outside the theater, in turn, may be more difficult to execute and synchronize.

---

[58] This is not to imply that procedures do not exist for the coordination and deconfliction of covert operations under Title 50 and military operations under Title 10. See, for example, Public Law 108-458, Intelligence Reform and Terrorism Prevention Act, sect. 1013, December 17, 2004, which requires the DNI, in consultation with DoD and CIA, to develop such procedures for operations that involve both CIA and DoD.

[59] Deptula, 2014, pp. 12–13; Collens and Krause, 2005, pp. 1–11.

[60] Deptula, 2014, p. 13.

[61] For a discussion of an F-16 performing both ISR and strike missions, see JP 3-30, 2019, p. III-21.

Single-Domain or Service-Centric Mindset

Legal authorities such as Title 10 and Title 50, as well as the regulations that implement their statutory requirements, have created and institutionalized CCMD component-centric processes, cultures, and knowledge centers unto themselves. CCMDs, as well as the CJCS, are statutory and regulatory power centers that each seek to both preserve and enhance their jurisdictions and authorities. This is not to say that they seek to exceed their legal authorities. They do, however, seek to optimize their authorities, particularly if tasked with a mission by the president or the SecDef. Although this is to be expected, doing so results in conflict over scarce resources, particularly space, cyber, and those assets that perform ISR and signal intelligence (SIGINT) functions.

This conflict presented itself clearly in interviews. Those interviewed at FCCs and working on the creation of USSPACECOM explained how centralized processes allow careful prioritization of scarce resources. Representatives of terrestrial GCCs, on the other hand, described the same processes as time consuming and uncertain. Consequently, in the event of a contingency, GCCs may prefer to employ assigned assets rather than employ multidomain options. Ultimately, this may result in the misallocation or underutilization of assets such as space and cyber or any scarce resource that must be shared among CCDRs.

Risks to Unity of Effort

As noted above, doctrine suggests that unity of command is the ideal way for military forces to achieve unity of effort. When that is not possible, such as when other U.S. agencies or allied militaries are pursuing a common purpose, unified actions and coordination mechanisms are intended to promote unity of effort. This section explains that the division of power among CCMDs means that unity of command, the doctrinal ideal for the military branch, is not always present below the national level.

Space and cyber commands have their own legal and regulatory requirements (standing orders, directives, EXORDs, IC missions, or other taskings from the president, the SecDef, or the CJCS). Yet, by their nature, these "global" assets may be physically located or having effects within another CCMD's AOR. Fixing a global asset or effect on a point on the map diminishes, to some degree and at least temporarily, the capability's global characteristics.[62] The principle of unity of command presumes unity over both function and geography.[63] In other words, to exercise complete unity of command, a CCDR would need to have authority over all functions (e.g., space, cyber, transport) within his or her AOR in order to concentrate all effort on all military objectives assigned to that CCMD. However, functional assets, by their nature, cross

[62] As noted in the discussion above, USSOCOM forces are an exception since TSOCs are OPCON to the relevant geographic CCDR.

[63] Air Force Core Doctrine Volume I, 2015, p. 51.

all geographies (and AORs) and are not limited to, or constrained by, any defined area or geography. Because a GCC cannot exercise command beyond his or her assigned geography, and because an FCC cannot exercise command beyond his or her function, unity of command over all five domains (land, air, maritime, space, and cyber) is an impossibility under the current statutory structure of Title 10 and the UCP.

To maintain unity of command within the scope of their legitimate authorities, terrestrial GCCs will necessarily seek to assert their Title 10 authority on all aspects of a conflict within their geography. In contrast, FCCs and USSPACECOM, which are not as bound by geography, will necessarily seek to maintain unity of command by asserting their Title 10 authority over their particular domain or, in the case of USTRANSCOM, across a geographic boundary or domain. At the same time, no CCDR may lawfully encroach on another CCDR's distinct and disparate powers granted to him equally by Congress as a result of the current construction of Title 10 and design of the UCP.[64] Thus, for one CCDR to exercise unity of command, as a principle of war, over all five domains, a statutory violation would likely occur. For all CCDRs to abide by Titles 10 and 50, a violation of the principle of war of unity of command must occur.

As noted above, "unity of command means all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose."[65] There is unity of command over all missions that CCMDs undertake since they are subordinate to the president and the SecDef in the operational chain of command. However, below this level, CCMDs represent separate branches in the operational chain of command. Unity of command below the national level is not present when these branches have authority to create effects against the same adversary or in the same geographic area. In these cases, CCMDs rely on coordination, rather unity of command, to achieve unity of effort.[66] Risks to unity of effort therefore exist where the coordinating mechanisms (the RAP, direct liaison authority, joint staff planning, joint working groups, and so on) fall short, are understaffed, or fail to be exercised.

---

[64] DoDD 5100.01, 2010, enclosure 5(1)(a).

[65] JP 1, 2017, p. V-1.

[66] See discussion of principles of war and additional principles of operations (to include unity of effort), Air Force Core Doctrine Volume I, 2015, pp. 40–51, 61. For authorities that call for such coordination, see, for example, DoDD 3100.10, 2016, enclosure 2(15) empowered the commander of USSTRATCOM to "execute space-related responsibilities in accordance with" the Joint Strategic Capabilities Plan and "conduct space control operations" independent of any other CCDR. This document does instruct CCDRs to integrate space-related activities. The same document instructs CCDRs (as a group) to "integrate" space-related activities when they perform their CCMD functions. However, it may be likely that any lapse or degradation in planning, coordination, or communication could have resulted in commander of USTRATCOM, or—as of August 29, 2019, the commander of USSPACECOM—operating space assets within a particular geographic CCMD without the GCC's knowledge or situational awareness. Similarly, 10 U.S.C. 394 and NSPM-13 (based on publicly available information) authorizes offensive cyber operations, which the SecDef could order the commander of USCYBERCOM to initiate and conduct (by means of an EXORD or fragmentary order during exigent or contingent circumstances) without the concurrent knowledge or situational awareness of any GCC, even if the network in question was located within the GCC's AOR; Nakashima, 2018; Freedberg, 2018.

As we discuss in Chapter 9, new initiatives on global integration aim to improve unity of effort among CCMDs.

Conclusion

In this chapter, we have examined the relationship of law, regulation, and doctrine, and examined the impediments they impose on various C2 functions (see Table 3.1). The division of responsibilities among organizations outlined in Title 10 and Title 50 and primary DoD regulations that implement these laws result in the most significant impediments.

Table 3.1. Potential Impediments to Multidomain Operations in the Current Legal and Regulatory Framework

C2 Characteristics That May Impede MDO	Potential C2 Impediments to MDO	Potential Impact
More processes or approvals required	Space, cyber, ISR/SIGINT, and mobility components of MDO require prioritization by the CCDR or the IC that controls those capabilities.	More time required, planning uncertainty Reluctance to use capabilities provided through support relationships
	The RAP process for certain effects and transferring control of airborne SIGINT, space, and cyber capabilities is adjudicated at the national level with CCDR and IC input.	
	Lack of common legal terminology and interpretation among CCMDs and between the military and the IC can lengthen the RAP and even require adjudication by the SecDef or the president.	
Insufficient expertise in or access to information about relevant domains	CCDRs lack training and experience with space and cyber authorities.	Increases decision risk and strain on JA advisors/trainers
	Planners may be unaware of relevant space and cyber capabilities since classification levels are high.	Underutilization of space and cyber; strain on limited staff with available clearances
	FCCs may not be in the best position to determine which CCMD has seized initiative at particular operational points.	The most important or effective operations not supported by the FCC
	Different authorities for operations and intelligence result in different tasking systems (e.g., PRISM vs. TBMCS).	Strain on staff to operate multiple communication nodes and processes
Increase in communications dependence	MDOs that rely on cyber, space, and intelligence assets require additional reliance on potentially vulnerable long-distance communications to make detailed requests that can compete for limited resources, create issues with coordinating planning, and potentially compromise execution.	Failure to allocate asset if justification insufficiently articulated (despite need) because of communication limitations
Presence of a single-domain or service-centric mindset	Title 10, Title 50, and the various implementing regulations have institutionalized component-centric, CCMD cultures, knowledge, and processes that may tend to lead CCMDs to rely excessively on capabilities they control.	Misallocation of assets and capabilities across the UCP

C2 Characteristics That May Impede MDO	Potential C2 Impediments to MDO	Potential Impact
Increases in risk to unity of effort	Intelligence and DoD organizations, which have two separate chains of command, use the same assets.	Confusion over allocation and mission where assets are jointly used or owned
	Other CCDRs control capabilities that can create effects in the regional GCC's AOR without full coordination.	Possibility for uncoordinated action in AOR

Because critical resources such as space and cyber assets, as well as ISR and SIGINT platforms, are limited and specifically delegated to certain key individuals and commands (the FCC, the GCC, the DNI, and so on), a system of allocation by request and adjudication is necessary to: (1) mitigate and resolve conflicts of needs, (2) balance and respect legally bounded jurisdictions and powers, and (3) ensure completion of a diversity of missions (from geography to function, and from peacetime to wartime). The result is a complex system of authorities to which CCDRs must adhere to when planning and executing MDOs.

This system of authorities has developed and changed over time in order to adapt to complexities as they are encountered and to balance many considerations beyond enabling MDOs.[67] Although authorities may be slower to develop and adapt, and thus may be slower to be issued by Congress, the president, and the SecDef, they are not static, and may be repealed, amended, or superseded to meet changes in the warfighting environment. We address some of these options in Chapter 11. In the next chapter, we will examine in more detail the doctrine and doctrinal principles that were drafted and implemented by the SecDef and the CJCS as a means to further guide commanders on how to fight the nation's conflicts in a manner that adheres to, and complies with, all the various proscriptions and conditions of Titles 10 and 50, the Law of War, treaties, and the various regulations that implement these legal authorities.

[67] For example, in response to rapid technological changes in cyber capabilities, Congress amended Title 10 with regard to the conduct of cyber operations (e.g., sections regarding reporting, cyber testing and ranges, SecDef authorities including clandestine operations, notification requirements, and so on); see 10 U.S.C. 391–396. These amendments only recently began in 2014; see the Public Law 113-291, National Defense Authorization Act of 2015, enacted December 19, 2014, and were even more recently amended in Public Law 115-232, enacted August 13, 2018.

4. Suppression of Enemy Air Defenses: Challenges to Planning and Executing Multidomain Operations

In this chapter and Chapters 5–7, we turn to challenges that arise from current C2 doctrine. As discussed in Chapter 3, doctrine is not binding on commanders, but it does establish principles that both frame how the joint force approaches problems and set the C2 baseline from which commanders deviate. In this chapter, we explore potential doctrinal impediments to a multidomain approach to SEAD that is currently under development.

Recently USAF and the Army have been collaborating on how air, ground, and space sensors can be used to cue long-range precision fires.[1] Both services have also focused on a SEAD mission.[2] ACC is specifically developing multidomain approaches to SEAD, a traditional JFACC task.[3] In this chapter, we explore a multidomain concept for SEAD that integrates air, space, and ground operations. We then use the framework developed in Chapter 3 to identify potential C2 impediments to such a SEAD mission. In doing so, we draw primarily on the C2 structure described in doctrine, though we supplement the discussion with interviews with practitioners.

We found several potential C2 impediments for this multidomain SEAD mission when planning for a contingency, planning during a contingency, and during the execution and assessment phases. SEAD is likely to be a major operational challenge in a conflict with a near-peer adversary. Therefore, CCMDs have an incentive to overcome these impediments either through some of the workarounds described in this chapter or through more significant changes to the current C2 construct. Even with C2 changes, however, the joint force could still face capability and capacity shortfalls.

[1] Clare Heininger, "Army, Air Force Team on Sensor to Shooter Prototype for Multi-Domain Battle," 2018.

[2] Army MDO concepts also emphasize the need to integrate Army capabilities into the joint effort to neutralize an opponent's long-range IADs; U.S. Army, 2018. Support for SEAD operations is not a new concept for the Army. In the opening minutes of Operation Desert Storm, Task Force Normandy, consisting of nine Army AH-64 Apache attack helicopters and three Air Force MH-53 helicopters, attacked two Iraqi early warning radars. The superior navigation systems of the MH-53s allowed them to act as pathfinders for the Army attack helicopters—which destroyed the radars, thus creating a gap in the Iraqi IADS for USAF aircraft on their way to attack Scud missile sites in western Iraq; Eliot A. Cohen, ed., *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness*, Washington, D.C.: Department of the Air Force, 1993, p. 120; Richard P. Hallion, *Storm over Iraq: Air Power and the Gulf War*, Washington, D.C.: Smithsonian Institute Press, 1992, pp.166–167; Frank Schubert and Theresa Krause, *The Whirlwind War*, Washington, D.C.: Center for Military History, 1995, p. 153.

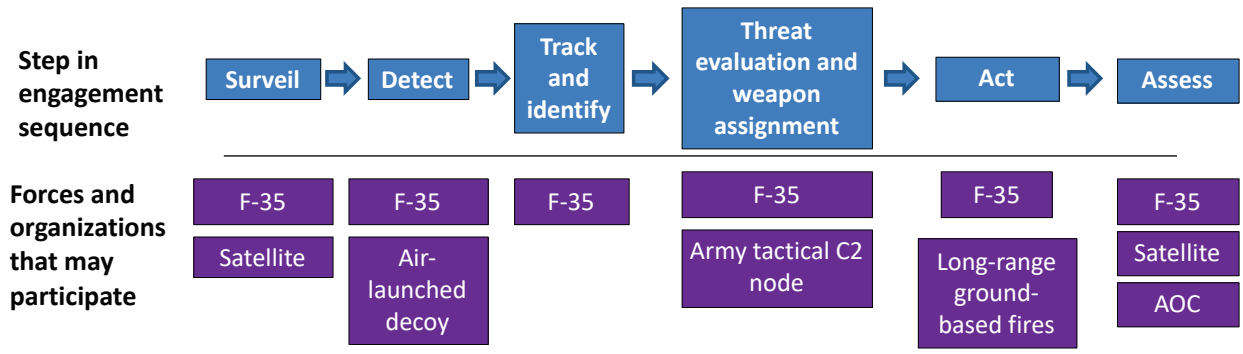
[3] Huyck, 2019.

Multidomain Suppression of Enemy Air Defenses

In recent operations against less capable adversaries, SEAD campaigns were often planned and executed by the air component, sometimes with the support of space-based ISR.[4] However, against a more capable competitor, USAF and the Army are proposing a multidomain approach to SEAD that integrates air, space, and ground operations to detect and destroy SAM batteries.[5] In this section, we expand on the basic outlines of this concept. We then consider the potential C2 impediments to this type of notional multidomain engagement sequence.[6]

ACC argues that the low-observable, multirole F-35 Lightning II Joint Strike fighter could be used as both a sensor and a shooter in a SEAD campaign.[7] Still, air planners will likely want to reduce the amount of time that F-35 aircraft spend in highly contested airspace by leveraging space-based ISR to help locate adversary SAMs.[8] Using long-range precision ground fires would also increase the firepower available to strike targets, offer a redundant capability to strike SAMs if aircraft need to leave the area, and complicate an enemy's defense planning (Figure 4.1).[9]

Figure 4.1. Notional Multidomain Suppression of Enemy Air Defenses Engagement Sequence



[4] In the run-up to Operation Iraqi Freedom, for example, U.S. Central Command's air component conducted a SEAD campaign to finish off Iraqi air defenses, leveraging fourth-generation fighters and satellite imagery. See Suzann Chapman, "The 'War' Before the War," *Air Force Magazine*, February 2004.

[5] A high-priority target such as a double-digit SAM (e.g., SA-20) could be treated as a time-sensitive target (TST). This could potentially limit some of the impediments discussed below, since, for example, the CCDR could compel the ground component to strike SAM. However, there are only a handful of TSTs for each operation, so we focus instead on potential impediments in the more standard targeting process rather than the TST process; JP 3-60, 2013, p. I-9.

[6] We thank RAND colleagues for sharing an earlier version of this multidomain SEAD engagement sequence, which they generated for an ACC-U.S. Army Training and Doctrine Command table-top exercise. As noted above, ACC is developing a similar concept.

[7] Huyck, 2019, p. 4.

[8] JP 2-01.3, 2014.

[9] Huyck, 2019, p. 4; U.S. Army, 2018, p. 33. Long-range ground fires could also be the only option for striking targets if aircraft cannot safely wait for targets over certain areas of enemy airspace.

Prior to conflict, a GCC would likely use intelligence capabilities to locate SAMs and hide sites during the joint intelligence preparation of the operating environment (JIPOE) process. Once conflict begins, the space-based ISR would be used to provide updated—but perhaps not real-time—information on the location of SAM batteries.[10] The space-based ISR, collected historically and in response to emerging requests with the onset of conflict, would help the JFACC build a better understanding of SAM battery movement patterns, likely hide sites, and the scope of the operating area.[11]

We therefore assume that space-based ISR offers information that would help narrow down the search area and that fifth-generation aircraft, acting as both sensors and shooters, would likely play the primary role in positive identification and engagement of a SAM battery. A package consisting of F-35 aircraft might need to use an airborne decoy to stimulate the SAM radar, causing the SAM to reveal its location. Depending on the operating environment, the lead F-35 might decide to engage the target from the air or to request ground fires. The final step would be to assess the effectiveness of the chosen action, whether from the air, space, or other sources of ISR. Incorporating space-based ISR into SEAD planning has been a perennial challenge, and the introduction of ground fires further increases C2 complexity as we describe in the sections that follow.

Planning for a Contingency

When planning for a contingency, the geographic CCDR provides guidance and assigns tasks, but detailed prewar planning takes place within the GCC's components. GCCs have permanent service components and, as discussed in Chapter 1, it is typical to carry out operations through functional components during a contingency. GCCs may also create standing functional components in peacetime to more seamlessly transition from peacetime to wartime.[12] This means planning for a contingency may take place within both service and functional components.[13]

For example, the dual-hatted JFACC and USAF service component commander would typically be given the task of planning the SEAD campaign. To plan a multidomain approach to SEAD like the one described above, the JFACC would need to take steps ahead of the crisis to ensure coordination between the air and ground component, as well as with intelligence

[10] Little has been written in open sources about the success of incorporating real-time space-based ISR into sensor-to-shooter kill chains, but historically it has been a challenge. Barry Watts, *The Military Use of Space: A Diagnostic Assessment*, 2001, p. 14.

[11] Alan J. Vick et al., *Aerospace Operations Against Elusive Ground Targets*, Santa Monica, Calif.: RAND Corporation, MR-1398-AF, 2001, p. 70.

[12] JP 3-30, 2019; Air Force Doctrine Annex 3-30, 2014.

[13] Functional components develop joint but domain-centric plans for the CCDR (i.e., one for air, one for land, and one for sea); JP 3-30, 2019; JP 3-31, 2014; JP 3-32, 2018.

organizations. In this section we discuss three potential impediments in the process of planning for a contingency that make it difficult to develop multidomain contingency plans.

Insufficient Expertise or Access to Information

Even if the components are open to multidomain solutions, they may lack the expertise to generate multidomain options. The majority of component planning staffs typically come from a single service, so they will have expertise in that service's traditional domain or domains, but not all domains. Planning personnel will typically have spent most of their career pursuing service-specific education, training, and assignments, with little time spent in joint assignments. As a result, staff officers may overlook solutions outside of their area of expertise or, even if they have ideas, lack the expertise in how to integrate across domains.[14]

Planners are aware of this possibility, and some reported during interviews that they proactively reach out to experts from other domains within their own component or in other components. Furthermore, interviews suggest that at least some combatant commands are trying to improve integration through more component synchronization meetings throughout the planning process. These practices undoubtedly make it more likely that multidomain options will emerge when planning for a contingency. However, the extent of informal outreach to other components may vary. Moreover, since the experts in some domains reside in other components, their expertise may not be consistently or fully available as component planners generate ways to solve operational challenges.

In the case of our SEAD scenario, air planners would need to recognize that ground fires and space ISR could help with the SEAD mission and reach out to other organizations to get additional experts to aid in the planning process. This would include reaching out to the Army component for expertise in integration of long-range fires. Moreover, the JFACC or USAF component planners would also need expertise in space-based ISR capabilities and would thus need to work with liaisons from the intelligence agencies that sit at the GCC level.[15] However, an important additional consideration is that those with the expertise in space-based ISR may not be able to explain the full range of options to component planning staffs due to classification constraints.

The expertise needed to plan a multidomain SEAD mission resides within a GCC, but not within any one component. Although component planners can potentially get the expertise they need through outreach to other components at the GCC level, the lack of resident expertise in all domains could make it less likely that MDOs will emerge.

---

[14] U.S. Joint Staff Joint Force Development (J7), *Cross-Domain Synergy in Joint Operations*, January 14, 2016, p. 21.

[15] JP 2-03, 2017, pp. xii, xi–xii.

Additional Steps or Approvals

Planning for multidomain engagements, such as this SEAD scenario, will often require more steps to coordinate activities and involve more approvals from decisionmakers. For an air-only approach to SEAD, the air component commander would conduct planning and gain CCDR approval for the proposed plan. Typically, most USAF aircraft are made available for tasking by the JFACC. Subject to the CCDR's priorities, the air component commander can assume that he or she will be able to allocate those aircraft to the SEAD mission once a conflict begins.[16]

However, to integrate ground fires into the multidomain approach described above, more resources—and therefore steps and approvals—would be needed. Ground fires typically remain under the operational control of the Army component to support its scheme of maneuver and are not typically made available for tasking by the JFACC. However, the CCDR can direct the Army to apportion fires from systems such as the Army Tactical Missile System (ATACMS) and Guided Multiple-Launch Rocket System (GMLRS) to support other component priorities. In the future, the CCDR could do the same with longer-range systems that would be most relevant for multidomain SEAD against a near peer.[17] If the CCDR approved the air component's SEAD plan, he or she would establish a support relationship between the air and land components. Under this arrangement, the Army would allocate long-range ground fires based on GCC guidance to SEAD missions.[18] During this process, the CCDR and components would also have to balance the need for the ground fires to support the ground scheme of maneuver.

Additional steps and approvals are also needed for integrating space-based ISR. Many space-based ISR capabilities are global assets controlled by the IC, rather than the GCCs. Tasking those assets therefore requires requesting support and gaining approval from the relevant intelligence organization. As a result, the reliance on space-based ISR could create planning uncertainty and might therefore require branch planning to address the risk of not having space capabilities available. Planners may still use these capabilities, but the additional uncertainty and time may complicate planning and make planners use them less than would otherwise be ideal for the operation.

Single-Domain or Service-Centric Mindset

Components, whether functional or service, tend to focus on their traditional domain or domains rather than all domains. Although components employ liaisons during wartime, interviews suggest that they are not typically present in planning organizations during peacetime

[16] JP 3-30, 2019, p. II-16.

[17] The CCDR can prioritize the allocation or use of joint operating area-wide systems such as the Tomahawk or ATACMS for specific purposes such as SEAD. JP 3-09, 2019, p. I-2.

[18] Doctrine emphasizes that effective fire-support planning and coordination require clear and precise guidance from the GCC. JP 3-09, 2019, pp. II-1, III-1.

(other than in the AOC, which has liaisons that are focused primarily on current operations). With limited "outsider" perspectives coming from experts that focus primarily in other domains, components are at risk of developing single-domain or service bias in their planning. For example, the air component commander oversees planning staff consisting of personnel with experience in the air domain and possibly space and cyber. As the JFACC, the air component command may also conduct some planning through the joint AOC that consists of mostly personnel with experience in the air domain from USAF and other services.

In our SEAD scenario, for example, the air component commander may default first to an air-focused solution because he or she has to produce a joint air operations plan (JAOP), which is inherently focused on air assets. Some degree of ad hoc coordination with other service or functional components is always possible, of course, but given the composition of the staff and the primary tasks a component is assigned, the air component may be predisposed to use capabilities in the air domain. In the event of operational challenges that the air component cannot resolve on its own, it may reach out to other components for support from other domains. The presence of a single domain or service mindset may mean that planners do not conduct domain-agnostic planning, but rather that multidomain solutions arise only when the component's own capabilities are not sufficient.

In sum, existing planning processes may lead to a single-domain mindset among planners, result in insufficient expertise in all domains throughout the planning process, and require additional steps and processes. Combined, these potential impediments could make the most effective multidomain options more time consuming or manpower intensive to plan or make planners reluctant to use them. Flaws in planning for a contingency can also have cascading effects once operations begin. If multidomain options have not been considered and developed when planning for a contingency, it will be more difficult to generate them once a high-intensity conflict begins.

Planning During a Contingency

Once war begins, components draw from contingency plans, but must collect additional intelligence to gain SA on actual conditions, update their plans based on these conditions, and task subordinate forces to carry out specific missions. Planning MDOs during a contingency therefore requires additional detailed planning. As with planning for a contingency, planning during a contingency is component-centric, though there are typically daily events to share information, integrate plans, and set priorities within the GCC. In this section we focus on some additional potential impediments to planning MDOs during a contingency.

Insufficient Expertise or Access to Information

Once a contingency is underway, new problems can emerge that were not entirely envisioned in the contingency-planning phase. Moreover, subordinate units need to be tasked and the timing and tempo of operations established. As a result, experts from each domain may have an important

role to play. As noted above, components tend to be dominated by expertise from one or just a few domains. Often, there are liaisons who can provide advice on their domain's capabilities and limitations.[19] Their relatively smaller number and the way the liaison role is conceived of in doctrine, however, may limit their impact on planning.

Doctrine notes that liaisons represent and are part of their parent organization and are "not full-time planners."[20] Moreover, doctrine emphasizes their advocacy role rather than their role as unbiased subject-matter experts (SMEs) seeking to optimize cross-domain solutions. As described in JP 3-0, "Liaison teams . . . generally represent the interests of the sending commander to the receiving commander, but can greatly promote understanding of commander's intent at both sending and receiving headquarters."[21] For our SEAD scenario, the JFACC would likely look to the battlefield coordination detachment (BCD) to help integrate ground fires.[22] While doctrine does mention the role of the BCD in serving as an advisor to the JFACC, it also emphasizes the BCD's responsibility to focus on the needs of the Army: "The critical role of the BCD is to ensure the exchange of information and to advocate for the Army forces (ARFOR) commander as the liaison element between service components."[23]

In addition to general expertise in how to incorporate ground fires into a SEAD mission, the JFACC would need to know if ground fires are available and capable of striking priority SEAD targets. An AOC does not need a great level of detail about the status of ground units in order to integrate them into a SEAD mission, but it does need to know, for example, that there are ground fires in range of the area where the JFACC plans to search for SAM targets. AOCs do not currently have direct access to such information. The co-located BCD has access to the Army's common operating picture (COP) and could contact the JFLCC for additional information as needed to help the AOC gain SA. However, interviews with AOC personnel suggest that since the BCD has many responsibilities and its personnel are not intended to be full-time planners, the AOC would need to request the information on a case-by-case basis. In other words, since the BCD is not necessarily immersed in the operational challenges that the AOC is trying to solve as a core member of the planning team, the BCD is not likely to proactively identify the need for information and note ways that ground fires could be available for use.

---

[19] JP 3-33, 2018, p. C-1.

[20] JP 3-33, 2018, p. II-25.

[21] JP 3-33, 2018, p. III-10.

[22] Doctrinally, the BCD is a channel for JFACC requests for time-sensitive fires support to the ARFOR's fire cell and is responsible for coordinating, integrating, and synchronizing the ATACMS or GMLRS mission into the targeting process. Headquarters, 2015, pp. 2-4–2-5, B1.

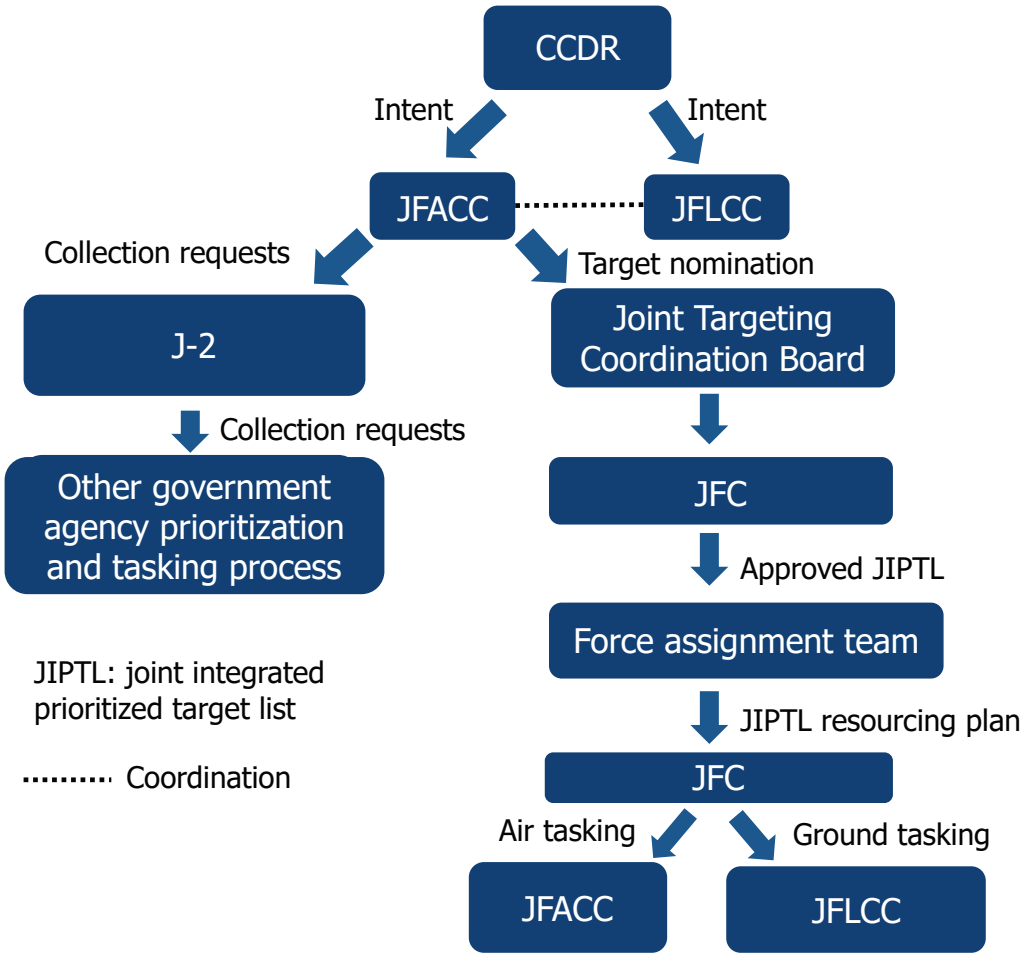
[23] Headquarters, 2015, pp. 1-1, 2-9. Air Force service doctrine does not, however, describe the Air Force's liaison element to the CCDR and other components, the joint air component coordination element (JACCE), as an advocate; Air Force Doctrine Annex 3-30, 2014. Still, others have raised questions about whether airmen are well prepared for JACCE positions; David J. Lyle, *Seeing the Forest from the Sky: Joint Airpower through the Lens of Complex Systems Theory*, Maxwell Air Force Base, Ala.: Air University, 2010, pp. 118–119.

Furthermore, since space ISR capabilities are often highly classified, AOC planners do not have direct access to information about the availability of space-based ISR systems or analysis capability. If space-based ISR has already been dedicated to searching for SAMs during the prewar planning, this may not be a significant impediment. But if new needs arise as planning is underway or specific requests need to be made for each operation, it may take time for component planning staffs to find out whether space-based ISR will be available. Planners may not know until a request has been considered and approved by the IC whether the space ISR component of the SEAD operation will be possible.

Additional Steps or Approvals

Integrating space-based ISR and ground fires adds additional steps and approvals during a contingency just as it does during prewar planning. This section details some of the additional planning steps that take place during a contingency to enable multidomain SEAD (Figure 4.2).

Figure 4.2. Planning for Multidomain Suppression of Enemy Air Defenses During a Contingency



SOURCES: JP 2-01, 2017; JP 3-14, 2018; JP 3-60, 2013; Army Technique Publication 3-09.13.
NOTE: Light blue indicates additional steps for planning a multidomain versus a single-domain SEAD mission.

One of the first things the CCDR will do at the beginning of a contingency is request an intelligence update from the joint intelligence directorate (J-2), which is engaged in a continuous JIPOE process to support commanders' intelligence needs.[24] The J-2 likely would have been collecting data on the location of suspected SAM batteries long before the commencement of hostilities. To the extent that new intelligence is needed, the CCDR, who typically retains collection management authority (CMA), might be able to task attached or assigned units to conduct additional collection.[25] For an air-only approach to SEAD, component planners might request a multirole aircraft through the targeting process. Alternatively, if separate airborne ISR were needed, component planners would need to coordinate with the GCC's intelligence division (J-2) to request airborne ISR.

Using space-based ISR to track SAM batteries may involve satellites that are not controlled by the GCC and therefore require additional steps and approvals. The Joint Intelligence Operations Center (JIOC), located in the J-2, would need to work with the relevant on-site intelligence organization liaison to submit a space-based ISR collection requirement to the IC.[26] The intelligence agencies then use internal processes for prioritizing collection requests that are built around the president's National Intelligence Priorities Framework.[27] Because these priorities and processes are not described in open-source publications, it is not possible to analyze them in detail; however, we know that these satellites are low-density/high-demand assets and that CMAs must therefore balance an array of competing collection priorities across the globe.

Thus, the IC might be more likely to validate and prioritize the GCC's collection requirements during a major theater war than during steady-state operations. That said, there could be competing high-priority requests if the conflict is transregional or if multiple conflicts are going on simultaneously. Therefore, JFACC planners would also have to consider that their request may not be prioritized. Moreover, the extra time that may be required to request and have space-based ISR approved could be more problematic once the contingency has started than it would have been during the contingency-planning phase.[28]

---

[24] JP 2-01.3, 2014.

[25] Air Force Doctrine Annex 2-0, 2015. It should be noted here that CMA is broken into two parts: collection requirements management (CRM) and collection operations management (COM). Typically, the GCC delegates the JFACC responsibility for COM although in the case of strategic space assets, the point is moot since those forces are not assigned to the GCC.

[26] JP 2-0, 2013, pp. I-3, I-14; JP 2-01, 2017, p. II-24. As the focal point for intelligence planning and collection management, the JIOC receives direct support from the broader intelligence community, including the National Geospatial Intelligence Agency (NGA) and the National Reconnaissance Office (NRO); JP 2-01, 2017, pp. xxi, II-17; JP 2-03, 2017, p. xiv; JP 2-01, 2017, p. II-24. JP 2-01, 2017, p. III-19.

[27] Director of National Intelligence, *Intelligence Community Directive 204, National Intelligence Priorities Framework*, January 2, 2015.

[28] For one example of how U.S. Central Command acquired its own satellite to avoid this type of planning uncertainty, see Chris Carroll, "CENTCOM's Spy Satellite Set to Beam Images from War Zones," *Stars and Stripes*, July 25, 2011.

Moreover, once a contingency is underway, more detailed planning would also need to take place to integrate ground fires into the SEAD mission. There are a few ways that ground fires might be involved in SEAD, all of which would require additional steps and approvals. If certain long-range ground fires units were dedicated to the SEAD effort, the JFACC would coordinate with the JFLCC, who would plan the ground units' scheme of maneuver to enable fires in the JFACC's priority areas.[29] Alternatively, the long-range ground fires might be primarily part of the JFLCC's scheme of maneuver but made available by the GCC for tasking by the JFACC for a certain period of time. In this case, they could be assigned to targets as part of the joint targeting cycle that the JFACC typically manages for the CCDR.[30] Finally, if the ground fires are not available for tasking by the JFACC, the JFACC may still reach out to the JFLCC in limited circumstances when those fires are needed. However, interviews suggest that, in practice, the AOC does not typically reach out to components for forces that have not been made available for tasking, so it is unlikely that the JFACC would regularly reach out to the Army if units have not been put in support of the JFACC's SEAD effort or made available for joint tasking during periods of availability.

If the GCC has not apportioned the JFLCC fires missions to support the JFACC, and the JFLCC and the JFACC cannot come to an agreement, the JFACC could appeal to the CCDR, who could order the JFLCC to provide the support, but this would be an exception, not the rule. In either case—whether the JFLCC agrees in principle to provide fires in support of the SEAD campaign, or whether the CCDR orders the JFLCC to do so—more steps, and therefore, more time, would be required to plan for the use of those ground fires.

Increase in Communications Dependence

As noted in Chapter 2, U.S. adversaries may attack long-distance communications in a conflict against a near-peer competitor. MDOs that rely on these links for detailed planning, coordination, or receiving intelligence during wartime may therefore be vulnerable to disruption. The approach to SEAD described in this chapter relies on space-based ISR, which must be coordinated with IC organizations in the continental United States. As a result, this approach to SEAD could be more vulnerable to communications disruption than a single-domain approach that relies only on in-theater airborne ISR.

[29] The Army force commander would likely have OPCON of all Army units and would typically be dual-hatted as the JFLCC.

[30] For a detailed discussion of the joint-targeting cycle, see JP 3-60, 2013.

Execution and Assessment

A mobile SAM battery is an "on-call" target, meaning that forces (e.g., aircraft and ground fires) and actions are planned against it, but not for a specific delivery time.[31] As a result, additional steps are needed to ensure the pieces of the multidomain SEAD mission come together in execution. Joint forces would have limited time to engage the SAM battery after the space-based ISR identified its general location, and there are some potential impediments that could arise.

Additional Steps and Approvals

As with the previous phases, there may be additional steps and approvals required to integrate ground fires in execution. The additional steps needed to gain SA from other domains also applies to the assessment process, so we do not repeat those points here.

Data link transmissions can also be a challenge for the JADC2. To allow for cross-domain coordination between air and ground forces to execute the SEAD mission, data systems need to be able to send and receive data, such as targeting coordinates. However, Army personnel have publicly discussed challenges in transmitting data between Link 16, a data link used by a variety of U.S. airborne platforms, and the Advanced Field Artillery Tactical Data System (AFATDs), the data system used by ground weapon systems such as the M142 High Mobility Artillery Rocket System (HIMARS). In particular, different message formats can make it difficult to share information.[32]

There are some ongoing attempts to mitigate these problems, however. In 2019, the Marine Corps demonstrated that an F-35, acting as a sensor, could effectively send targeting coordinates via datalink to a Marine Corps HIMARS.[33]

Until all such challenges to sharing information among the relevant forces involved in MDOs are overcome, sharing data may require additional steps. For example, operators may have to manually transfer information from one system to another or rely on voice communications, which may increase the risk of error.[34] These additional steps are a potential impediment to MDOs since they may be too time consuming in the context of a high-end fight.

In addition, more steps may be required between finding a target and an order for ground fires. In the context of a conflict with a peer competitor, the F-35 flight lead may have target

---

[31] JP 3-60, 2013, p. II-2.

[32] Aaron Sadusky, James Ford, and Arthur Wilas, "Link 16 and AFATDS Interoperability: Addressing the Critical Gap in the Sensor to Shooter Chain," *Redleg Update*, March–April 2019; Joe Russo, "A Lethal Combination: F-35 Joint Strike Fighter and M142 HIMARS Sensor-to-Shooter Integration," *Fires*, November–December 2017, pp. 37–42.

[33] David Cenciotti, "U.S. Marine Corps F-35B Connects to HIMARS for Rocket Shot in a 'Direct Sensor-to-Shooter' Scenario," *The Aviationist*, October 9, 2018.

[34] Heininger, 2018; Sadusky, Ford, and Wilas, 2019; Russo, 2017.

engagement authority.[35] However, if the F-35 does not engage the target itself and instead needs to pass the target to a ground unit, there may be additional steps between locating the target and firing.

In our notional SEAD scenario, the F-35 flight lead would likely pass the targeting information to a tactical C2 node such as a division-level joint air-ground integration center (JAGIC). During the planning phase, the JAGIC would have received the request for SEAD surface fire support from the AOC. The JAGIC would then perform the necessary weaponeering to determine if ground fires were an acceptable option and, if so, coordinate potential attack options. Once a SAM target is located, the F-35 would pass the information to the JAGIC, which would select the appropriate ground attack method and transmit the mission to the appropriate firing unit. This process includes coordinating the necessary airspace control measures.[36] In a highly contested environment, these additional steps for the shooter to be "cleared to target" by a tactical C2 node could take valuable time and lead to a missed opportunity to hit a fleeting target.

Increase in Communications Dependence

For an air-only SEAD operation, an F-35 might locate and fire on the SAM battery, meaning that once the mission is underway, the aircraft in the fighter package have to communicate only among themselves and possibly an airborne C2 node. In our multidomain SEAD scenario, however, more communications links are needed. The fighter package needs information about the SAM location from space-based ISR sources, and then, once the fighter package confirms the SAM location, the aircraft need to be able to pass detailed target information to the ground unit.[37] As discussed in Chapter 2, local communications among forward forces may be more reliable than long-distance communications, but they will still likely be contested by a near peer. To the extent that multidomain options such as this SEAD engagement sequence involve more forces that have to communicate to synchronize their operations, they may be more vulnerable to communications disruptions than single-domain alternatives.

---

[35] In dynamic situations, when the target is not specified on the ATO, the shooter may need to be "cleared to target" from a C2 entity outside the AOC, such as an airborne battle management platform like the Joint Surveillance Target and Attack Radar System due to identification restrictions or other restrictions prior to attack. Sometimes, the AOC may even maintain engagement authority, in which case that authority would need to be passed to aircrews in real time via the theater air control system, and that authority may be contingent on meeting criteria for weapons release. These additional steps are less likely in the context of a conflict with a near-peer adversary. The F-35 flight may have the best situational awareness to make the decision, and other air battle management platforms may be too vulnerable to be used in this role; Air Force Doctrine Annex 3-60, 2019.

[36] Headquarters, Department of the Army, *The Joint Air Ground Integration Center*, ATP 3-91.1, April 17, 2019, pp. A-9–A-11. The JAGIC has responsibility to execute deliberate targets assigned within the division's airspace as well as missions against CCDR-validated time-sensitive targets. Current fires-support doctrine recommends using "events-based triggers" during SEAD operations as this gives greater planning flexibility to fire-support elements and firing units when executing SEAD. JP 3-09, 2019, p. IV-14.

[37] The F-35 has recently demonstrated under exercise conditions that it can transmit targeting information to some Army C2 networks. Sydney J. Freedberg Jr., "F-35 Spots Targets for Army Missile Defenders," *Breaking Defense*, August 6, 2019b.

Conclusion

This chapter has shown that there are a number of potential impediments to developing and optimizing multidomain engagement sequences, such as the notional SEAD engagement sequence discussed throughout (Table 4.1). MDOs may not emerge or be most effective due to a single service or domain mindset, lack of domain expertise, or the extra time and uncertainty associated with bringing together capabilities from other components or organizations. MDOs that bring together more forces, especially those that require detailed coordination with organizations outside the theater, may be more reliant on vulnerable communications links than their single-domain alternatives. In execution, incompatible data standards and additional steps to gain approval for an engagement may also make MDO synchronization difficult.

Table 4.1. Potential Impediments to Multidomain Operations in a Suppression-of-Enemy-Forces Campaign Involving Air, Space, and Ground Forces

C2 Characteristics That May Impede MDO	Potential C2 Impediments to MDO	Potential Impact
More steps or approvals required	Space-based ISR component of MDO requires prioritization, deconfliction, and approval by intelligence agencies.	Planning uncertainty, more manpower intensive, reluctance to use space-based ISR
	Planning to integrate ground fires requires additional steps to coordinate and gain the approval of the JFLCC.	Missed opportunities to use capabilities from other components and domains
	During execution, extra steps are required between the F-35 identifying a target and a ground unit receiving an order to fire.	Time delays that undermine mission effectiveness
	Data standards may not be compatible and thus require additional steps to share targeting information.	Time delays that undermine mission effectiveness
Insufficient expertise in or access to information about relevant domains	Component planning staffs do not have experts from all domains to propose or help plan multidomain options.	Missed opportunities to use capabilities from other components and domains
	Doctrine describes liaisons as advocates for their parent organization rather than full-time planners contributing to multidomain problem-solving.	
	The JFACC may not have direct access to information about forces that are not assigned to air component (e.g., space ISR, ground forces, specifically long-range precision fires).	Planning uncertainty, reluctance to use capabilities from other components and organizations
Increase in communications dependence	During a contingency, MDO that relies on approval, planning, or execution from outside the GCC (e.g., space ISR) may be vulnerable to disruption.	Higher risk of mission failure in a communications-contested environment
	MDO using forces from multiple GCC components may require more reliable in-theater communications links than single-domain options.	
Presence of a single-domain or service-centric mindset	Planning is conducted primarily by service or functional components that are tasked and organized to plan for employing capabilities primarily from a single domain (e.g., air domain for USAF, land for the Army).	Missed opportunities to use capabilities from other components and domains
Increases in risks to unity of effort	Not applicable	Not applicable

5. Integrating Offensive Cyber Operations into Multidomain Operations

Many discussions of MDO note the growing role for cyber operations. In this chapter, we therefore consider potential impediments to integrating offensive cyber operations with operations in other domains. For example, a U.S. adversary may try to prevent a successful U.S. SEAD mission by jamming Global Positioning System (GPS) signals to reduce the accuracy of U.S. or allied precision guided munitions.[1] U.S. planners might therefore wish to employ offensive cyber operations against adversary jamming sites to enable SEAD.

Today, GCC commanders generally do not have the authority or capability to conduct offensive cyber operations like this notional attack on adversary GPS jammers. Rather, U.S. Cyber Command (USCYBERCOM) and its service cyber components develop cyber targets and capabilities and conduct offensive cyber operations for the GCCs through support relationships.[2] This division of responsibility among theater- and national-level authorities and responsibilities affect the way cyber effects are planned and executed as part of an MDO.

Planning for a Contingency

Planning for cyberspace operations follows the same doctrinal process as planning in any other domain. Although the GCCs do not generally have operational control of cyber capabilities, they have cyber SMEs available to help integrate cyber operations into contingency plans. Cyber planners are primarily concentrated at the GCC level rather than in the components. Cyber expertise resides within the GCC's joint cyber center (JCC) and the cyber operations integrated planning element (CO-IPE), USCYBERCOM's forward-deployed planning cells.[3] Each GCC is

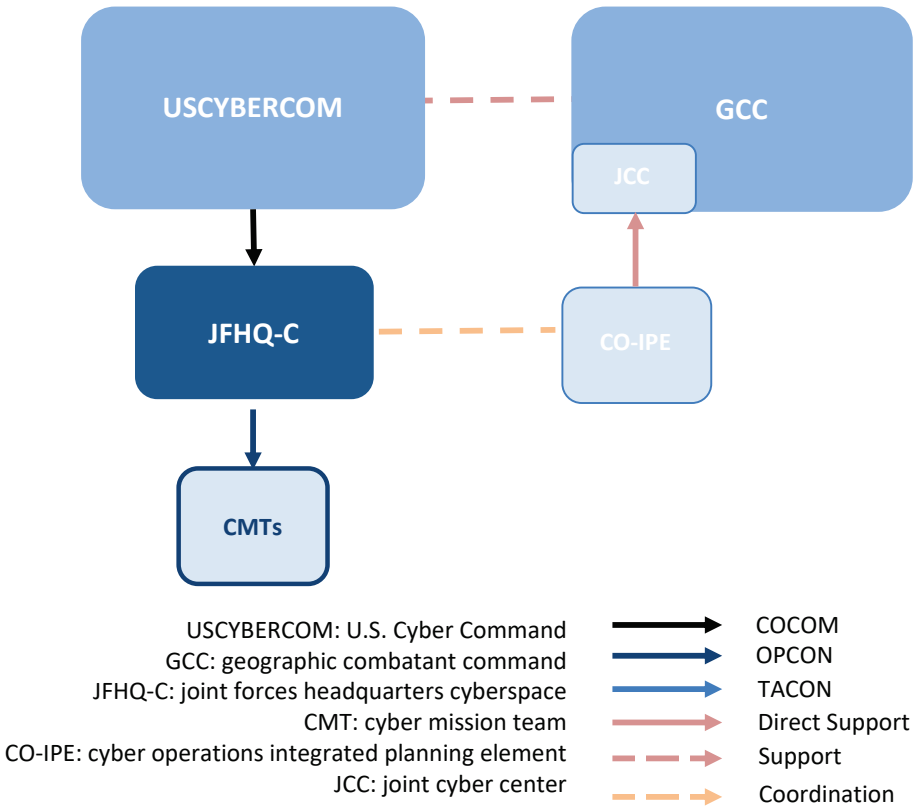
[1] There is considerable open-source information about the various ways to jam GPS and disrupt positioning, navigation, and timing services, which would reduce the accuracy of precision operations or munitions. For a discussion of GPS jamming and examples of Russian use of GPS jamming, see Stan Goff, "Russia Jammed GPS Signals During NATO Military Exercise Involving U.S. Troops," *Inside GNSS*, November 14, 2018; Nathan Strout, "Government Leaders Worry About GPS Spoofing, Hacking," *C4ISRNET*, May 17, 2019; Joe Gould, "Eyeing Russia, Army Fields Jam-Resistant GPS in Europe," *C4ISRNET*, June 6, 2019.

[2] GCCs do have greater control over some defensive cyber authorities and capabilities. According to current doctrine, USCYBERCOM can provide GCC tactical control of offensive cyber forces during a contingency to enable synchronizing cyber effects with those in other domains. However, interviews with the CO-IPE and GCC cyber personnel suggest that CCMDs do not currently anticipate receiving TACON of offensive cyber forces in the event of conflict; JP 3-12, 2018, pp. IV-11–IV-12.

[3] JP 3-12, 2018, pp. III-6, IV-13; Mark Pomerleau, "The 'Real Strength' in Cyber Command's Recent Work," *Fifth Domain*, February 27, 2018a; Mark Pomerleau, "DoD Makes Significant Updates to Cyber Operations Doctrine," *Fifth Domain*, June 22, 2018b.

supported by one of USCYBERCOM's service components (the joint force headquarters–cyberspace [JFHQ-Cs]), which coordinate with the GCC CO-IPEs in refining cyber intelligence requirements, providing input into courses of action (COA) development, integrating cyber effects into CCMD plans and orders, and executing cyberspace operations in direct support of CCDRs.[4] Cyber mission teams (CMTs), the tactical units that conduct offensive cyber operations, are aligned under the JFHQ-Cs in support of the CCMDs (Figure 5.1).[5]

Figure 5.1. Command and Control for Offensive Cyber Operations in Support of Geographic Combatant Command Multidomain Operations



SOURCE: JP 3-12, 2018, pp. IV-13–IV-14.
NOTE: Doctrine envisions the possibility of a GCC having tactical control (TACON) of a mission-tailored force package during a contingency, but interviews suggest this has not been standard practice.

In order for cyber effects to be developed, the GCC's staff or components must identify the need when planning for a contingency. As part of this prewar process, the GCC's JCC, service components, and other GCC staff elements put together a list of domain-specific effects needed

[4] JP 3-12, 2018, pp. I-9, III-6. See also U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," *Joint Force Quarterly*, Vol. 80, No. 1, 2016.

[5] JP 3-12, 2018, p. II-8.

to meet their commander's intent. These lists are combined to create the GCC's priority effects list (PEL).[6] The JCC submits the desired list of cyber effects from the PEL to USCYBERCOM with a cyber effects request form, which formally notifies USCYBERCOM of the GCC's intention to begin planning for the inclusion of these effects in their contingency plan.[7] In the notional example above, planners at USAFE-AFAFRICA or USEUCOM would first have had to identify that a cyber effect would be the most effective way to disrupt an adversary's effort to manipulate data for U.S. precision guided missiles and thereby enable the SEAD mission. Second, they would have had to advocate for and place this desired effect on the GCC PEL to be submitted to USCYBERCOM for prioritization and development.

Once it receives the cyber PEL, USCYBERCOM tasks a CMT to begin developing the prioritized cyber targets. This tasking, however, depends on both the availability of the CMTs to adopt a new mission and CDRUSCYBERCOM's prioritization of the CMTs (e.g., the missions the CMTs are working). As briefly discussed above, there is a divide between national- and theater-level responsibilities, requirements, and authorities, which creates friction between USCYBERCOM and a GCC. Ideally the cyber effect requested by the GCC would be of high enough importance to devote cyber resources to, but this is not necessarily always the case.[8]

Assuming availability and prioritization of resources, the CMT, in coordination with the service cyber component that owns that CMT (in the case of USAFE-AFAFRICA, the JFHQ-C Air Force Cyber [AFCYBER]) begins developing the target, the access, and the capability. Depending on the difficulty of the target and whether or not a new, bespoke capability needs to be developed or if there is an existing cyber capability "on the shelf," this process can take a significant amount of time, potentially years. Additionally, the IC and some international partners are involved in this process to ensure that any access development efforts do not conflict with U.S. or allied intelligence gathering missions (e.g., intelligence gain-loss, or IGL concerns).[9] This fact alone emphasizes the importance of identifying and prioritizing cyber effects early on in the planning process. Once the CMT has developed an access and the cyber capability (or effect), a targeting package, known as an electronic target folder, is assembled.[10] The GCC then needs to submit this package through the review and approval process for cyber

---

[6] Joint Warfighting Center, U.S. Joint Forces Command, *Commander's Handbook for an Effects-Based Approach to Joint Operations*, February 24, 2006.

[7] JP 3-12, 2018, p. IV-6. Hurcules Murray, "Cyber Requirements," briefing delivered at Armed Forces Communications and Electronics Association TechNet: Achieving Force 2025 Rough Signals and Cyber, Augusta, Ga., September 10, 2014, p. 8. See also JP 2-0, 2013, for additional information on information requirements.

[8] Interviews with USEUCOM, for example, revealed that addition to the GCC's PEL has not guaranteed that it will be prioritized by USCYBERCOM.

[9] JP 3-12, 2018, p. IV-10.

[10] JP 3-12, 2018, p. IV-10; Joint Staff J7, "Insights and Best Practices Focus Paper: Integration and Synchronization of Joint Fires," July 2018.

operations (RAPCO).[11] This process takes into consideration risks to tradecraft or intelligence collection (i.e., IGL), potential collateral damage (collateral effects estimates), foreign policy implications (political-military assessments), and other potential interagency concerns.[12] The SecDef ultimately approves these packages.[13] Upon approval, the cyber effect is added into the GCC's OPLAN as a reviewed and approved effect. While the GCC finalizes any outstanding aspects of the contingency plan, the CMT and the JFHQ-C continue to monitor the access and the capability for any changes that may impact the effectiveness of the cyber effect. Once completed, the SecDef reviews and approves the contingency plan, which will be updated regularly until a contingency goes into effect.[14]

Although the process detailed above closely mirrors the joint planning and targeting process in other domains, the planning and targeting timelines for cyber operations are significantly longer than in traditional domains given the need to covertly develop remote or human-enabled access (e.g., through a special operations force [SOF] mission), and complicated cyber tools. As a result, there are limitations to developing MDO before a contingency, and even more so during an ongoing contingency, that result from the current cyber operating environment rather than C2 structures.

The remainder of this section describes prewar planning for cyber operations in more detail as it describes the potential C2 impediments to MDO. We first describe the challenges that result from the current cyber operating environment, then describe challenges resulting from the current U.S. C2 construct.

General Challenges Associated with Cyber Operations

There are some challenges to integrating offensive cyber operations into a multidomain operation that arise from the current state of adversary systems and U.S. cyber capabilities rather than C2 choices. Although our focus is on C2 impediments to MDO, we note these briefly to remind the reader that changes to C2 doctrine and authorities are not sufficient to ensure seamless integration across domains. First, as noted above, the timelines for developing cyber capabilities can be long, taking years in some cases. Unlike kinetic weapons that can be used against a wide range of targets, cyber capabilities are often unique to each target.[15] As a result, it takes significant time and resources to identify targets that are vulnerable to cyber attacks,

---

[11] JP 3-12, 2018, p. IV-8.

[12] Andrew Schoka, "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat," *War on the Rocks*, April 3, 2019. See also JP 3-60, 2013.

[13] The approval process may also require agreement of the DNI pursuant to 50 U.S.C. 3024(f) as both the SecDef and the DNI share jurisdiction over certain IC assets.

[14] JP 3-12, 2018, p. IV-8.

[15] JP 3-12, 2018, p. IV-10. See also JP 3-60, 2013.

develop the access to adversary systems, and build the custom cyber capability for each mission.[16]

A second related limitation is that the efficacy of cyber weapons is difficult to predict, especially over long periods of time. Unlike kinetic weapons, there is not a well-developed approach to testing and assessing the probability that a cyber capability will achieve its objective.[17] Moreover, since cyber capabilities are often only effective against a specific target in a particular configuration, these custom-built capabilities can quickly become obsolete. If either the target or the environment changes in any way, for example through a patch in a regular network update, the capability may no longer be useful and the attacker must re-engineer the exploit, which can be time consuming. Moreover, because networks are interconnected, cyber operations can have unintended cascading effects including on civilian systems.[18]

Planners may need to develop more branch and sequel plans to account for the possibility of cyber effects not working or having cascading effects.[19] Many planners we interviewed explained that planners are reluctant to rely on cyber operations due to the uncertainty surrounding their effects. As one cyber expert at a GCC headquarters explained, GCC planners often see effective cyber operations as "icing on the cake." Another explained that cyber is often thought of as providing a "nuisance effect" on the adversary rather than producing a specific effect. In other words, due to the state of the cyber operating environment, some planners are hesitant to rely on cyber capabilities.

Potential C2 Impediments

On the other hand, some impediments are the direct result of choices the United States has made about laws, regulation, and doctrine as they apply to cyberspace. USCYBERCOM controls and executes most cyber operations because of potentially global effects they can produce and to ensure that limited offensive cyber resources are used against the highest priority targets. Moreover, most cyber effects are coordinated, reviewed, and approved for inclusion in the original OPLAN through the RAPCO process discussed in Chapter 3.[20] Following the declaration of a crisis or contingency, the SecDef or the president can authorize the execution of the approved COAs, including the cyber COAs, in the original contingency plan through an EXORD.[21]

---

[16] JP 3-12, 2018, pp. I-5, IV-10.

[17] Erwin Orye and Olaf M. Maennel, "Recommendations for Enhancing the Results of Cyber Effects," *11th International Conference on Cyber Conflict*, 2019.

[18] JP 3-12, 2018, p. IV-1.

[19] JP 3-12.

[20] JP 3-12, 2018, p. IV-8.

[21] See discussion of EXORDs in JP 5-0, 2017, p. II-32. See also JP 3-12, 2018, p. II-2; Isaac R. Porche III et al., *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, Santa Monica, Calif.: RAND Corporation, RR-1600-A, 2017, p. 53.

Authorities to conduct offensive cyber operations are at a high level because policymakers share concerns over the risk of potential secondary effects of cyber operations on civilian infrastructure, risks to intelligence collection operations, and U.S. relationships with other countries. Public reporting suggests that even with recent changes to cyber authorities in National Security Presidential Memorandum 13 (NSPM-13), the current process of approving and prioritizing cyber operations still requires very extensive coordination and review.[22] This section identifies how these choices can be potential impediments for MDO. Just because they are potential impediments, however, does not mean that the current C2 arrangements are inadvisable. Rather, this section highlights how these choices create trade-offs in terms of planning and generating MDO that include offensive cyber operations.

Insufficient Expertise or Access to Information for Cyber Operations

The first potential C2 impediment to integrating cyber operations with operations in other domains is where cyber planners are located. As discussed above, components are typically the focal point for planning for a contingency within a GCC. However, due to the limited number of cyber personnel in a given GCC AOR, cyber planners are concentrated at the GCC level, not within the GCC's components.[23] Therefore, component planning staffs may lack expertise in the effects cyber operations can produce or how they can be integrated with other capabilities. Without resident cyber expertise in the components, it is less likely that cyber operations will be integrated into component plans from the outset and more likely that cyber effects may be considered later in the process when component plans are reviewed and coordinated by the GCC's joint directorate for strategy, plans, and policy (J-5).[24]

The second potential impediment is that cyber capabilities tend to be highly classified. Interviewees highlighted two important implications related to classification issues. First, planners may not be aware of the range of cyber capabilities that could be used, which makes it less likely that cyber options will be considered if cyber experts are not part of a planning team.[25] Second, the high classification of these effects, and the plans surrounding their development, limits the degree to which they can be integrated into multidomain exercises. Commanders may be reluctant to rely on capabilities in wartime if they do not fully understand and do not have experience with them in peacetime. As one officer we interviewed put it, "You can't C2 what you can't understand."

---

[22] Robert Chesney, "CYBERCOM's Out-of-Network Operations: What Has and Has Not Changed over the Past Year?," *Lawfare*, May 9, 2019.

[23] CO-IPEs are also not yet fully staffed. While envisioned to be small teams with extensive cyber expertise, the CO-IPE construct is still transitioning from the former cyber support element construct, which placed only one cyber planner at GCCs and therefore has not reached full operating capacity; interviews with JCC and USCYBERCOM personnel located at a GCC headquarters.

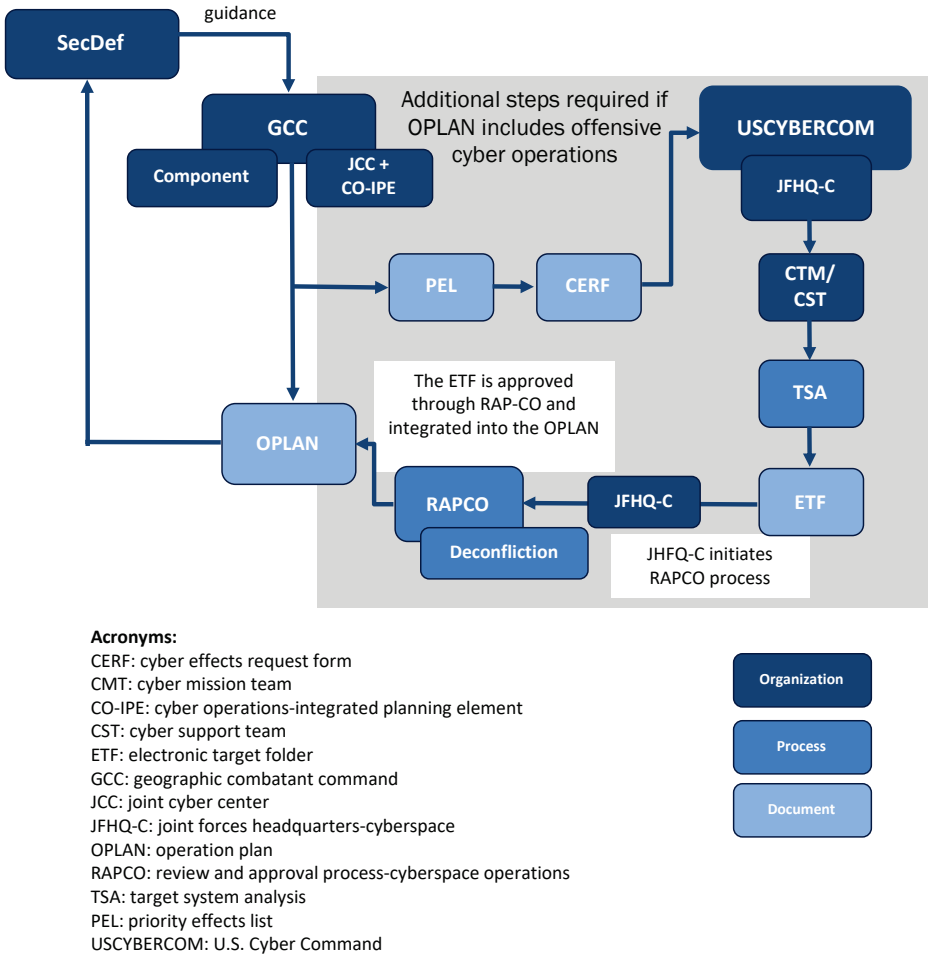
[24] Insights drawn from interviews with the CO-IPE as well as GCC and component planners.

[25] U.S. Joint Staff Joint Force Development (J-7), 2016, p. 21.

More Steps and Approvals Are Required When MDO Includes Offensive Cyber Operations

The third potential impediment resulting from C2 decisions is that planning for cyber operations requires more steps and approvals than for many other types of operations. As discussed above, the authority and capability to conduct offensive cyber operations generally resides outside of the GCC.[26] Figure 5.2 illustrates the extra steps and approvals needed to integrate offensive cyber effects into an OPLAN.

Figure 5.2. Offensive Cyber Request and Approval Process



SOURCES: JP 3-12, 2018, pp. IV-8–IV-10; JP 3-60, 2013, pp. I-8–I-10.

[26] In a narrow range of circumstances, this process could potentially be simpler. In particular, if an offensive cyber operation could be conducted and effects entirely contained within GCC's AOR, then some of these steps may be eliminated. Unfortunately, doctrine does not specify the details of the differences, such as the level of confidence required about the limited scope of a cyber operation or how GCC coordinates such operations with USCYBERCOM and organizations outside of DoD. It is also unclear how often such circumstances arise, given current cyber capabilities.

James McGee, the legal advisor for Special Operations Command North, stated that "this process . . . makes cyber operations, despite their seeming attractiveness, impractical given the extensive planning and approval [process] versus kinetic operations."[27] Many interviewees expressed a similar perspective, with one explaining that "cyber moves at the speed of government processes, not at the speed of cyber." This suggests that it is not just limitations of the cyber domain that makes planners reluctant to employ them as part of MDO. The current C2 construct may add time and create planning uncertainties since the desired effect on a target may not be approved in time for a contingency, if at all.

Lack of Unity of Effort

As discussed in Chapter 3, USCYBERCOM has the authority and capabilities to create effects in the GCC's AOR. In theory, planning for such operations should be coordinated with the GCC. However, senior leaders we interviewed within GCC components noted that such coordination did not take place in past exercises. This means that operations in the cyber domain may not always be well integrated with those in other domains.

Planning During a Contingency

Once a crisis or contingency begins, the GCC assesses whether the approved contingency plan still applies to the emerging crisis. If changes have occurred that affect the cyber portion of a plan, cyber planners can refine or adapt the plan as necessary and gain approval again if required. The GCC then sends the updated contingency plan to the SecDef for review. If he or she approves, the SecDef issues an execute order, which also approves the cyber operations laid out in the plan.[28] A few additional impediments may arise at this stage.

More Steps and Approvals Are Required for Multidomain Options

Once a contingency begins, additional planning takes place for the GCC to approve the execution of cyber effects and synchronize the timing of cyber with other operations. The exact organizations and processes involved varies by the GCC. However, in general terms, cyber and other effects may be considered by different staff elements and working groups before being considered together by the joint targeting coordination board (JTCB) for inclusion on the joint integrated prioritized target list (JIPTL). For example, a CCMD might consider the cyber target through a nonkinetic effects working group before it is considered in a joint targeting working group that reviews both kinetic and nonkinetic targets and produces a draft JIPTL and joint targeting cyber request (JTCR).[29] The elements of the SEAD engagement sequence that rely on

[27] Mark Pomerleau, "Authorities Complicate Use of Cyber Capabilities," *Fifth Domain*, January 9, 2017a.

[28] JP 5-0, 2017, p. VII-2.

[29] JP 3-60, 2013, pp. III-7, C-3.

GCC capabilities would be tasked through air tasking orders (ATOs) and Army orders. The JTCR would inform the JFHQ-C's cyber tasking order (CTO).[30] The information on the ATO and the CTO should match to ensure coordination and synchronization during execution across domains.

If an operation, such as our SEAD with offensive cyber operation, requires a combination of kinetic and nonkinetic effects, representatives from all relevant domains would need to attend each of the working groups to articulate the importance of prioritizing and approving all effects relevant to the operation. Without this involvement, it is possible that only one effect on a target (e.g., only the kinetic strike against the SA-21) could be prioritized and approved.[31]

Insufficient Expertise or Access to Information for Cyber Operations

New ideas for using cyber operations may emerge during a contingency. As noted above, developing cyber access and capabilities can be very time consuming, so unplanned cyber effects may be limited in a short conflict. However, there can be capabilities that are already developed that may prove applicable or a cyber unit may develop new capabilities in the midst of a conflict. In this case, the process for approving cyber operations could proceed as outlined in the previous section. As with prewar planning, during a contingency there may not be expertise in the components to identify opportunities to use cyber effects due to classification, cyber expertise concentration at the GCC level, or limited number of personnel in the CO-IPE. Of course, nonkinetic options may emerge if component planners proactively take targets to nonkinetic working groups or reach out to experts at the GCC or in other components.

Cyber Operations That Rely on Detailed Planning, Approval, or Execution from Outside the GCC May Be More Vulnerable to Disruption

The inclusion of cyber effects also makes planning during a contingency and execution more vulnerable to attacks on long-distance communication links. This vulnerability is the result of the centralization of cyber capabilities and authorities in the current C2 construct.

The primary responsibility for cyberspace attack coordination between USCYBERCOM and the joint force resides with the applicable JFHQ-C and the USCYBERCOM CO-IPEs in coordination with the CCMD CO staff, mainly the JCC. Because USCYBERCOM is the global synchronizer of offensive cyber operations and usually the owner of the attack capabilities, most operations are conducted from their facilities in the continental United States.[32] This geographic separation among the location of execution, location of impact, and location of synchronization (at the GCC), means that planning and executing a cyber effect is reliant on long-distance

[30] JP 3-60, 2013, pp. III-7, C-3; JP 3-12, 2018, p. IV-10.

[31] Joint Staff J7, 2018.

[32] See AFCYBER homepage for information and links to cyber squadrons, such as the 315th Cyberspace Operations Squadron, which is based at Fort Meade. Air Forces Cyber, "315th Cyberspace Operations SQ," November 4, 2016.

communications, which may be contested as discussed in Chapter 2. This increased risk of communications disruptions during a contingency is an additional impediment to the integration of cyber into MDO. If the effect could be achieved through cyber domain operations alone and did require synchronization of operations in other domains as part of MDO, the geographic separation would be less of a challenge.

Presence of a Single-Domain or Service-Centric Mindset

Although there has been some reporting that USCYBERCOM has conducted operations against ISIS and Iran in conjunction with other domains,[33] others have argued that cyber operations remain single-domain focused.[34] The actual extent of integration of USCYBERCOM integration with other domains is difficult to assess. However, continued concerns about a possible disconnect suggests there may still be room for improvement in cultivating a multidomain mindset among the cyber operations community. If the joint force emphasizes MDO during a contingency, USCYBERCOM's forces may need to more deeply integrate with planners from other domains than they have in the past. This could require a shift toward a more multidomain culture.

Execution and Assessment

Integrating cyber operations in the execution and assessment phases also requires additional steps. Multiple organizations and operations centers need to be in contact to make any adjustments to the plan in execution. In an air-only mission, changes to a planned mission might flow from the AOC to the executing unit. However, if cyber operations are part of the mission and some change needed to be made to the timing or tempo of the operation, updates would also have to flow from the AOC to the JCC to the USCYBERCOM joint operations center (JOC) and finally to the CMT.[35]

Assessment also requires multiple steps and organizations. The CMT immediately conducts phase I battle damage assessment (BDA) to confirm that the exploit was delivered against the specified target. Phase II BDA may be conducted by the CMT as well as by organizations within the GCC. They will look for indications that the delivery had the intended immediate effect, such as lights going out in a targeted building. For phase III BDA, the most detailed of the BDA

---

[33] Dan Lamothe, "How the Pentagon's Cyber Offensive Against ISIS Could Shape the Future for Elite U.S. Forces," *Washington Post*, December 16, 2017. The Stuxnet virus, for example, was intended to disrupt the uniquely configured Seimens SCADA system that controlled the centrifuges in Iran's nuclear facility at Natanz, and was reported as having been conducted as part of a broader, multidomain military operation; Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014.

[34] David E. Sanger and Eric Schmitt, "U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS," *New York Times*, June 12, 2017.

[35] JP 3-12, 2018, p. IV-14; Air Forces Cyber, 2016.

phases, the geographic CCDRs staff might look at the overall effectiveness of the operation in supporting mission objectives.[36]

Conclusion

There are numerous potential impediments to the integration of cyber effects when planning for a contingency, some resulting from the unique nature of cyberspace and others from the current C2 construct (Table 5.1). Due to classification of cyber operations and concentration of

Table 5.1. Potential Impediments to Integrating Offensive Cyber Operations into Multidomain Operations

C2 Characteristics That May Impede MDO	Potential C2 Impediments to MDO	Potential Impact
More steps or approvals required	Offensive cyber components of MDO require coordination with multiple agencies, effects-based review processes, and approvals outside the GCC.	Planning uncertainty since desired effects may not be approved; manpower-intensive planning and approval process
	In execution, changes to offensive cyber operations plans must be coordinated through multiple organizations at the GCC and USCYBERCOM.	Risks to synchronization
Insufficient expertise in or access to information about relevant domains	Cyber planners are typically at the GCC level rather than the component level where most planning takes place, so cyber operations may not be integrated until later, when the contingency plan is largely developed.	Missed opportunities to use cyber effects
	Cyber capabilities are often highly classified, so commanders and planners may not have exposure to or comfort with the capabilities.	
	GCC planners may not have information on the availability of U.S. cyber mission teams to conduct offensive cyber operations.	Planning uncertainty
Increase in communications dependence	During a contingency, MDOs with elements that rely on approval, planning, or execution from outside the geographic CCDR's AOR (e.g., offensive cyber operations) are vulnerable to disruption.	Reduced warfighting effectiveness
Single-domain or service-centric mindset	Cyber operations may be treated as independent rather than fully integrated with GCC MDO.	The FCC and the GCC working cross-purposes
Lack of unity of effort	USCYBERCOM can create cyber effects without coordinating with the relevant geographic CCDR.	The FCC and the GCC working at cross-purposes

[36] Preparing for the assessment phase, however, begins long before execution during the planning process, when staff decide what to measure and how to measure it. Interviewees at USEUCOM noted that the cyber BDA process was an area of concern.

cyber experts at the GCC level, interviews suggest that it can be difficult for planners, especially at the service component level, to plan for and request cyber effects when they are not aware of how cyber can support their mission. Currently, component planners work around this problem by reaching out to experts at the GCC or relying on limited expertise within the component. However, the existing C2 construct means that some opportunities to use cyber operations may be missed.

Because CCDRs do not generally have organic offensive cyber capabilities to use in support of their operations, GCCs must request support from USCYBERCOM. This planning, request, and approval process for cyber effects can require more steps and time, potentially impacting integration. The additional steps to coordinate in execution may also create risks to synchronization.

Finally, the reliance on long-distance communications for many cyber operations is an additional consideration. Planners may need to balance the operational benefits of using offensive cyber against the risk that the communications degradation described in Chapter 2 could affect planning, approval, or synchronization of these effects.

6. Integrating Offensive Space Control Operations into Multidomain Operations

Space operations can contribute to MDOs in many ways, including by providing intelligence as discussed above, satellite communications, GPS, and position, navigation, and timing information to military forces. Offensive space control (OSC), for example in support of a joint SEAD mission, is an additional role for space operations discussed in joint doctrine.[1] This chapter describes and assesses the C2 processes involved in planning, executing, and assessing MDOs that include OSC operations. Based on our review of these processes, we identified seven potential C2 impediments for integrating such space operations into MDOs.[2]

Planning for a Contingency

In the late 2010s, USSTRATCOM was tasked with planning and executing military space operations—a process that also includes "prioritizing, deconflicting, integrating, and synchronizing" space operations with other ongoing joint operations.[3] On August 29, 2019, USSPACECOM took over responsibilities for planning and executing military space operations.[4] Therefore, for MDOs that include space operations, the GCC space planners must work with USSPACECOM while planning for a contingency.[5] The process of integrating space operations into GCC war plans has a number of potential impediments.[6]

---

[1] JP 3-01, 2017, p. III-21. On offensive space control more generally, see JP 3-14, 2018, p. II-2.

[2] During most of the period of research for this report (October 1, 2018–September 30, 2019) DoD was in the midst of standing up USSPACECOM and was still internally discussing how to organize the new CCMD and how exactly to conduct C2. This chapter describes the process covered in published doctrine and also references proposals discussed in interviews with personnel familiar with the transition from USSTRATCOM to USSPACECOM. USSPACECOM stood up on August 29, 2019.

[3] JP 3-14, 2018, p. III-1. In some cases, a GCC may have OPCON or TACON of space capabilities for a specific operation; JP 3-14, 2018, p. III-7.

[4] Previously, USSTRATCOM's Joint Force Space Component Command conducted the operational mission that is now under USSPACECOM. The transition of personnel from USSTRATCOM headquarters to USSPACECOM is anticipated to take two years to complete. Theresa Hitchens, "STRATCOM Move to Space Command: 2 Years, 100s of People," *Breaking Defense*, August 6, 2019, 2019b.

[5] JP 3-14, 2018, p. IV-2.

[6] There are also potential impediments to integrating space operations that are not the result of C2 issues. For example, space operations planning can be constrained by physical properties and factors beyond the control of planners, such as orbital dynamics, terrestrial and space weather, and limits of current capabilities. Additionally, interviewees noted that many space capabilities have not been combat tested, so it is difficult to know how they will work in practice. JP 3-14, 2018, p. xii.

Insufficient Expertise or Access to Information

As discussed in previous chapters, the bulk of GCC planning for a contingency takes place within the service components. Space experts who contribute to planning for a contingency are present in component staffs.[7] However, interviews with the CCMD and component staff suggest that most space planning expertise is concentrated within the GCC staff and the USSPACECOM integrated planning element (IPE). Although USAF has historically had a greater focus on space and may therefore have more personnel with space experience in its components, interviews suggest that USAF service components have still struggled to integrate some types of space operations into contingency plans.[8]

Moreover, space operations are often highly classified, which means that there are even fewer experts who have a full awareness of space capabilities and their availability. The limited expertise within the components combined with limited information on space capabilities due to classification could result in missing opportunities to use OSC operations where they could have potentially been helpful. Conversely, there are indications that some planners incorrectly believe, perhaps from exercise experience, that space assets are more capable than they truly are.[9]

Planners at the GCC level have both expertise and clearances to integrate space appropriately into contingency plans. However, the number of experts within the GCCs is small, which can limit their impact. Moreover, these experts may not be well integrated with component planning staffs, who do the bulk of planning for a contingency. As a result, space experts at the GCC level may be able to propose ways to integrate space operations only late in the process of planning for a contingency, when the core concepts are already largely developed. As a result, interviewees reported that space operations are sometimes tacked onto plans rather than fully integrated into them.

Additional Steps and Approvals

Due to the legal framework described in Chapter 3, integrating space operations into contingency plans requires additional steps and approvals. GCCs must nominate requests to USSPACECOM, which has its own prioritization and coordination processes. USSPACECOM, like USSTRATCOM, considers requests from all CCMDs as well as other national priorities as it allocates limited space resources. Furthermore, DoD space planners must coordinate with

---

[7] JP 3-14, 2018, p. III-5. Interviews with component planning staffs also indicate that they informally draw on knowledge of space experts from throughout their component to the extent possible.

[8] The research for this report was conducted prior to the creation of the U.S. Space Force. Part of the mandate for the new service is to increase the military effectiveness of the Joint Force and to develop a cadre of space professionals. It is possible that the Space Force will eventually generate and deploy additional personnel to help plan for contingencies, but such a development would take years to come to fruition; Donald J. Trump, "Establishment of the United States Space Force, Space Policy Directive-4," Washington, D.C.: Office of the President, February 19, 2019, pp. 2–4.

[9] These insights are drawn from project interviews.

non-DoD organizations involved in space-related operations to deconflict any plans and ensure unity of effort.[10] While space planners must account for some operational considerations that are similar to those for terrestrial operations, such as space and terrestrial weather, space planners must also take into consideration space-specific laws and relevant policies, including the National Space Policy and DoD Space Policy.[11] As a result, space planning can take more time between request and execution; one interview subject compared it with planning a B-2 mission rather than a fighter mission. When integrating OSC with operations that employ capabilities OPCON to the CCDR, an MDO depends on prioritization and approval in both GCC and USSPACEOM processes. These factors contribute to planning uncertainty and extended timelines for OSC operations, which, in turn, could cause planners to avoid relying on OSC operations or to have to develop additional branch plans in case space operations are not available during the contingency.

Finally, as discussed in Chapter 3, the complexity and age of current legal authorities can make legal reviews of space operations more time consuming especially if differences of interpretation exist among CCMDs.

Planning During a Contingency

Timelines for planning and approving OSC operations can be long, so it is not always possible to quickly integrate space operations during wartime. Still, once a contingency begins, additional planning and coordination may be required and additional requests may emerge. For example, the JFACC may want to use space jamming in support of a SEAD mission, as suggested in doctrine.[12] The JFACC is typically a GCC's space coordinating authority (SCA). In this role, the JFACC vets targets for space operations and coordinates all requests for space support from throughout the command with the help of the director of space forces (DIRSPACEFOR).[13] As Figure 6.1 shows, once a prioritized list is approved by the CCDR, the JFACC forwards these requests to USSPACECOM's Combined Force Space Component Commander (CFSCC).[14]

[10] JP 3-14, 2018, p. IV-1.

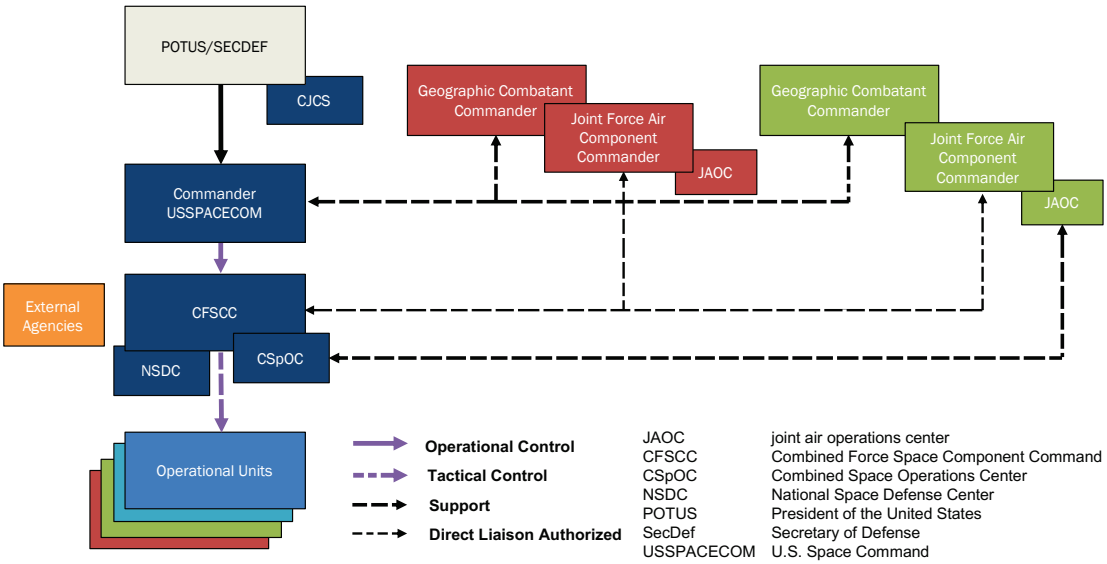
[11] JP 3-14, 2018, p. IV-2.

[12] JP 3-14, 2018, pp. IV-5–6.

[13] The COMAFFOR is typically SCA because the Air Force has a preponderance of space forces and achieving space superiority is one of its core competencies; JP 3-14, 2018, pp. III-3, III-7.

[14] JP 3-14, 2018, pp. III-2, III-7. As of August 29, 2019, STRATCOM's JFSCC described in joint doctrine was renamed the Combined Force Space Component Command and was a subordinate command to the newly formed USSPACECOM. Joint Force Space Component Command Public Affairs, "Combined Space Operations Center Established at Vandenberg AFB," Vandenberg, Va.: U.S. Strategic Command, July 19, 2018.

Figure 6.1. Command Relationships for Global and Multiple-Theater Operations



SOURCE: Adapted from Air Force Doctrine Annex 3-14, 2018, p. 17.
NOTE: Organizational changes since 2018 are discussed in Chiles (2019) and Trump (2019).

As with planning for a contingency, USSPACECOM has processes in place to prioritize and approve specific space support requests during a contingency.[15] Based on the CFSCC's guidance and intent regarding prioritization and apportionment, the Combined Space Operations Center (CSpOC) creates the joint space tasking order (JSTO). Special instructions (SPINS) provide additional information on how to synchronize space operations with other aspects of a GCC's MDO. During a crisis or combat operations, the 30-day JSTO planning and production cycle may be condensed to sync with the supported GCC's much shorter air-tasking order cycle.[16]

Some of the potential impediments for planning during a contingency mirror those of the prewar planning phase. There may not be enough space experts available within the components to identify opportunities to use OSC operations, and classification may prevent planners from knowing their range of options. The additional time required for these processes and uncertainty surrounding prioritization and approval may prove more problematic by increasing the risk to the mission or leading planners to eschew reliance on space operations.

In addition to these challenges, planning during a contingency must consider the risk of contested communications described in Chapter 2. Contested long-distance communications could potentially affect even single-domain operations, but it could pose a greater impediment

[15] Air Force Doctrine Annex 3-14, 2018, p. 17. The Joint Space Operations Center referred to in JP 3-14 is now the Combined Space Operations Center (CSpOC), renamed thus to reflect the integration of U.S. allies; JP 3-14, 2018, pp. xi, III-2; JP 3-60, 2013, p. III-18; Air Force Doctrine Annex 3-14, 2018, p. 17. Joint Force Space Component Command Public Affairs, 2018.

[16] JP 3-60, 2013, p. IV-6.

for integrating OSC operations that require planning, approval, or execution by organizations out of the geographic CCDR's AOR into MDOs. If extensive planning and synchronization are not required while the contingency is underway, then this may not be a problem. However, if planning of a specific mission relies on information or detailed coordination with space operators or decisionmakers outside of the geographic CCDR's AOR, then MDOs that include OSC may be more vulnerable to disruption than those that rely on in-theater capabilities.

Execution and Assessment

In contrast to cyber operations where the AOC has to work through cyber organizations at the GCC level, the JFACC's AOC has the direct liaison authority with the CSpOC, as shown in Figure 6.1. This means that the two operations centers can directly coordinate to synchronize in execution and to share information for assessment.[17] Measures of performance and effectiveness would have been developed during the planning phase. In the example where space operations are being conducted in support of a SEAD mission, the JFACC would be the supported commanders and would therefore establish the measures of effectiveness for the overall MDO.[18] If space were being integrated with other domains, such as an air strike as in our example, there would be only one additional step to coordinate with the CSpOC on execution and assessment. More significantly, however, as with planning during a contingency, the need to coordinate over long distances means that there is a greater risk of communications disruption during the execution and assessment phase.

Moreover, in the execution phase, current doctrine reflects a single-domain mindset in its guidance on execution in a contested environment. Joint space doctrine says that space operations must be "executed in such a way as to ensure security and defense of prioritized assets."[19] In many cases, this is likely the right guidance given that space capabilities are scarce, costly, and time consuming to replace. However, in a major combat operation against a near-peer competitor, there could conceivably be a high-stakes MDO that relies critically on space capabilities. In such a case, national priorities may warrant some additional risk to a space capability given the importance of the GCC's mission. In this sense, current space doctrine encourages a focus on space survival considerations, potentially to the detriment of the GCC's MDO and mission.

Conclusion

Space operations—particularly offensive ones—are inherently complex and present many challenges when they are incorporated into an MDO (Table 6.1). In particular, there appears to

[17] JP 3-14, 2018, p. IV-2.

[18] JP 3-60, 2013, p. IV-8.

[19] JP 3-14, 2018, p. IV-1.

be a lack of expertise in and awareness of most space capabilities at both the GCC level and the component level. While the air component may have more personnel aware of space capabilities, the gaps in knowledge appear to exist everywhere for highly classified space capabilities. As a result, planners within a GCC do not always have awareness of the availability of space-based assets that may help their mission both in general and in a particular theater or timeframe. As with cyber, planning processes, authorities, and prioritization for offensive space operations tend to be more complicated and require additional steps and approvals. Together, these impediments could result in missed opportunities to use space capabilities, planning uncertainty, and a reluctance to use space assets. In a contested communications environment, threats to long-distance communications could increase the risk of mission failure for MDOs that rely on approval or execution from the continental United States.[20]

Table 6.1. Potential Impediments to Integrating Offensive Space Control into Multidomain Operations

C2 Characteristics That May Impede MDO	Potential C2 Impediments to MDO	Potential Impact
More processes or approvals required	Including space operations in MDO requires coordination with, prioritization by, and approval of organizations with authorities within and beyond DoD.	Planning uncertainty, more manpower intensive, reluctance to use space-based assets
	The Joint Space Tasking Order Process happens on a different cycle than the Air Tasking Order and other GCC processes, so planning timelines may not be compatible during a contingency.	Time delays that undermine mission effectiveness
Insufficient expertise in or access to information about relevant domains	There are a limited number of space operations personnel and space experts, and they are typically concentrated at the GCC level rather than in the components that conduct the bulk of planning for a contingency.	Missed opportunities to use space assets, excessive optimism about space operations; space tacked onto plans at the end rather than integrated from the start of planning for a contingency
	Space capabilities are often highly classified, so planners from other domains—or even some space planners who are not cleared at the highest levels or deemed to have a "need to know"—may not have exposure to or familiarity with select capabilities.	
	GCC planners do not have access to information on the availability of space assets or other space activities.	
Increase in communications dependence	During a contingency, MDO that rely on approval, planning, or execution from outside the CCDR's AOR (e.g., offensive space control operations) are vulnerable to disruption.	Higher risk of mission failure in a communications-contested environment
Single-domain or service-centric mindset and lack of unity of effort	Doctrine describes prioritizing force protection of space assets without consideration for risk to mission in other domains.	Risk to national priorities

[20] We note this risk due to the threats to long-distance communications introduced in Chapter 2.

7. Air and Missile Defense: Command-and-Control Enablers of Multidomain Operations

Air and missile defense (AMD) is already a joint and multidomain mission.[1] Fighter aircraft, SAMs (both terrestrial and maritime), antiaircraft artillery, and airborne and ground-based sensors and C2 systems are all involved in AMD.[2] Furthermore, at the theater level, the AMD mission has its own unique planning process that results in an area air defense plan (AADP). The area air defense commander (AADC) leads this process of integrating all air-, maritime-, and land-based air defense capabilities and deciding who has the delegable engagement authority for air defense operations.[3] The doctrinal C2 structure for AMD may therefore provide insights into how to organize for other multidomain missions or highlight potential impediments to adopting and implementing such an approach. In this chapter, we explore a notional multidomain vignette and describe aspects of the C2 structure that enable multidomain AMD.

We find that the doctrinal C2 concept for AMD, particularly as described in JP 3-01, has fewer C2 impediments to MDOs than other mission areas. However, it is important to note that theory and implementation often diverge. Doctrine and C2 processes cannot be effectively employed unless their principles are understood and practiced, adequate communications and data systems exist to support C2 and a common operating picture, personnel are trained in the

[1] Air and missile defense is defined as "direct (active and passive) defensive actions taken to destroy, nullify, or reduce the effectiveness of hostile air and ballistic missile threats against friendly forces and assets." AMD is a primary component of defensive counter air operations, which are "all defensive measures designed to neutralize or destroy enemy forces attempting to penetrate or attack friendly airspace." JP 3-01, 2017, pp. GL-7, GL-10. Multidomain and joint discussions have also been present in earlier versions of doctrine. See, for example, Headquarters, FM 3-01.7, *Air Defense Artillery Brigade Operations*, Washington, D.C.: Department of the Army, October 2000, pp. 2-14, 4-16. During Operation Desert Storm (ODS) Army Patriot units received information from USAF Airborne Warning and Control System (AWACS) through the CRC and information about Scud missile launches from defense support program satellites. However, during ODS a number of work-arounds had to be found to allow USAF and the Army to share data via their incompatible communications systems. Schubert and Krause, 1995, pp. 245–246; Sam LaGrone, "Successful F-35, SM-6 Live Fire Test Points to Expansion in Networked Naval Warfare," *USNI News*, September 13, 2016.

[2] Joint contributions to this effort currently include Army Patriot and Avenger SAM systems, the Terminal High Altitude Area Defense (THAAD) system, and Sentinel and AN/TPY-2 radars; Air Force fighter aircraft assigned to defensive counter air (DCA) operations, airborne early warning (AEW) systems such as the E-3 AWACS, and ground-based sensors such as the AN/TPS-75 air search radar; Navy SM-3 and SM-6 equipped Aegis cruisers and destroyers, fighter aircraft assigned to DCA, AEW systems such as the E-2 Hawkeye; and Marine Corps DCA fighters and surveillance radars. This section does not discuss nonkinetic defenses. Some of these systems would be largely passive in nature (hardening, camouflage and obscurants, and decoys and deception) and would likely have limited C2 implications.

[3] Air Force Doctrine Annex 3-01, 2016, p. 14.

appropriate procedures, and sufficient forces are available for the execution of an MDO.[4] Although there are exercises on the elements of AMD, Army and USAF units rarely conduct joint training exercises involving complex AMD situations. Moreover, the joint force has not had experience with conducting AMD in complex, high-intensity operational environments against a near-peer threat. Therefore, although we interviewed some members of the AMD community, this chapter should primarily be read as an assessment of C2 enablers for AMD as described in doctrine rather than practice.

Moreover, it is important to remember that adequate C2 doctrine, practice, and systems are only a component of successful AMD operations. The joint force has not been confronted by an adversary with a sophisticated offensive air and missile capability for decades. Success against such a complicated and sophisticated threat will likely require new defensive concepts and significantly greater resources aligned with the AMD mission.[5]

Notional Multidomain Air-and-Missile-Defense Scenario

In this vignette, we consider cruise missile defense of a seaport of debarkation (SPOD) through which equipment and supplies will arrive at the outset of the contingency. In order to clearly demonstrate doctrinal C2 arrangements during an AMD mission, this scenario focuses on a single tactical engagement taking place within a complex and stressing operational environment.[6]

Due to its importance during the early phase of a contingency, we assume SPOD is well defended. In this notional vignette, a U.S. Navy Task Force Integrated Air and Missile Defense

[4] Bryan A. Card, "Preparing Air Missile Defense, Joint Force Against Near-Peer Threat," *Fires*, July–August 2018, pp. 33–34, 35; Michael Schwartz, "Leader Development: The Air Defense Artillery Transformation's Biggest Challenge," *Fires*, March–April 2017, p. 17. The services do, however, conduct a number of exercises that practice portions of the AMD network. Exercise Astral Knight 2019, for example, was designed to have the Army Air and Missile Defense Command (AAMDC) focus on AMD of key terrain and the 10th AAMDC deploy personnel to a number of airbases, a port, and onboard an Aegis destroyer. U.S. Central Command conducts the Joint Air Defense Exercise, which includes Army, Navy, Air Force, and partner air-defense assets. In addition, USEUCOM has conducted two Spartan Shield training exercises that include Army Patriot missile batteries, Air Force control and reporting centers, and Army air-defense artillery fire-coordination officers. U.S. Army Europe, "Summer 2019 Series of Exercises," 2019; U.S. Air Force Central Command, "Joint Air Defense Exercise Sharpens Skills, Strengthens Partnerships," February 22, 2019; Cole Keller, "AF, Navy Conduct Joint Air Defense Exercise," November 1, 2016; Robert Durr, "Joint Forces Team Up for Spartan Shield," September 13, 2018; Devin M. Rumbaugh, "WPC Executes Milestone Air Force-Army Integration Exercise," April 25, 2018.

[5] These resources could include increased ground-based defensive systems (including short-range air defense systems), but it could also require more and better sensors, better passive defenses (dispersal, hardening, obscurants, dazzling, camouflage, decoys/deception), ground- and air-based jamming, and more airborne platforms capable of intercepting cruise missiles.

[6] In the event of a conflict with a near peer, a critical port could be attacked along multiple vectors and by multiple systems, including cruise missiles, ballistic missiles, attack aircraft, and armed unmanned aerial systems. In addition, it is probable that a number of important assets would be under attack at the same time as the port. Such a complex attack would stress U.S. defensive assets and C2 systems. There could also be defensive capacity and capability issues in protecting a facility from potentially dozens of cruise missiles.

(TF IAMD), USAF defensive counter air (DCA) combat air patrol (CAP), and U.S. Army Patriot batteries defend SPOD.[7] TF IAMD is also the regional air defense commander (RADC) for the maritime area, with the authority to engage incoming missiles. After having been warned by space and airborne sensors that potential cruise missiles are heading toward SPOD, TF IAMD detects the cruise missiles with its Aegis radar system and identifies them as hostile. In order to preserve the Aegis destroyer's limited supply of SM-6 SAMs for potential later engagements, TF IAMD, as the RADC, cues the fighters to engage the cruise missiles with their Advanced Medium-Range Air-to-Air Missiles (AMRAAMs).[8] If, after the engagement, the RADC determines that not all cruise missiles have been destroyed, depending upon the potential engagement geometry and requirements, it will either engage them with its organic SM-6 missiles or direct the Patriot missiles defending SPOD to engage them on their terminal approach to the defended target.

Planning for a Contingency

When planning for a contingency, the CCDR creates a critical asset list (CAL), which is a prioritized list of assets or areas that need to be protected from air and missile threats during each phase of the operation (Figure 7.1).[9] CAL is forwarded to the AADC, who then allocates available AMD capabilities among the assets on CAL to create the defended asset list (DAL).[10] In our vignette, the port is on both CAL and the DAL because closure of the port would delay the start of the CCDR's operations, thus providing the adversary with additional time to reinforce its defenses and increasing the potential cost of the operation.

Experts from all domains contribute to the development of the DAL and the AADP. The latter is the primary joint planning document for AMD, and it prescribes the integration of active AMD, passive AMD, and C2 systems to provide a comprehensive defensive system. It is the means by which the AADC implements theater priorities, authorities, procedures, tasks, and

---

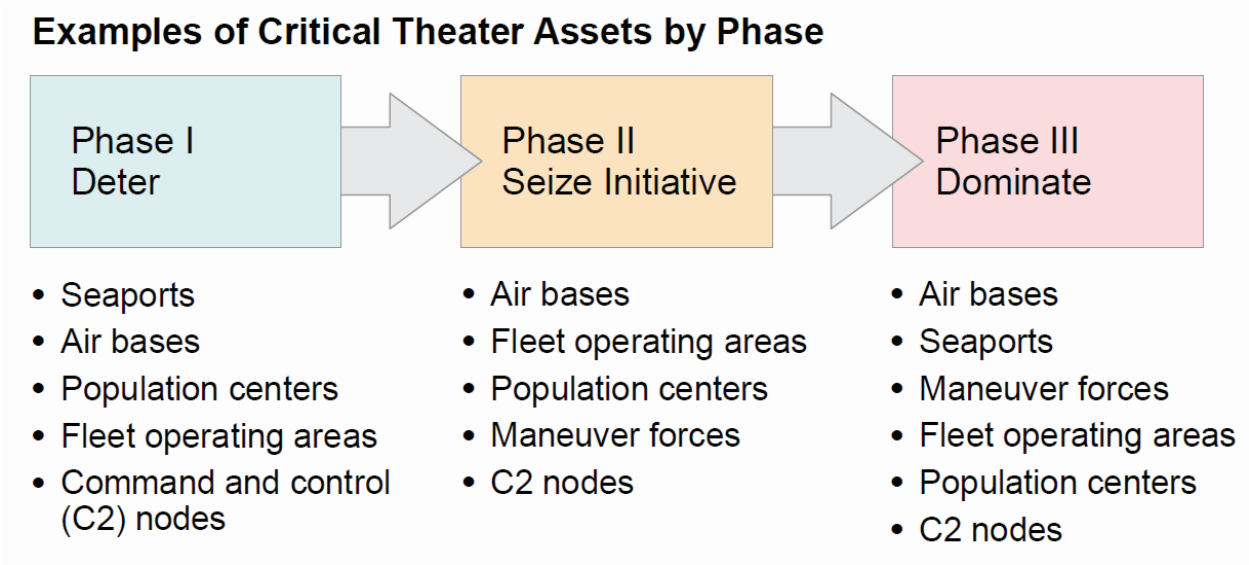
[7] Key area defense systems against enemy cruise missiles are the SM-2, SM-6, and Patriot surface-to-air missiles and the Advanced Medium-Range Air-to-Air Missile (AMRAAM). Department of Defense, *Missile Defense Review*, 2019, p. 53.

[8] The Aegis combat system currently has the capability to hit targets beyond its radar horizon using the cooperative engagement capability (CEC) of the E-2 Hawkeye. Field experiments have demonstrated that the F-35 has a similar capability resident in its Multifunction Advanced Data Link. This experiment was part of the Navy's Naval Integrated Fire Control-Counter Air (NIFC-CA) concept. NIFC-CA currently utilizes cooperative engagement capability and Link-16 and hopes to incorporate other sensors including the F/A-18. LaGrone, 2016.

[9] CAL is developed by the CCDR's plans directorate with input from the components and is based on the level of protection required to support the tasks and missions assigned by the CCDR. The assets on CAL are prioritized based on three primary factors: criticality, vulnerability, and threat. Criticality is the degree to which an asset is essential to accomplishing the mission. Vulnerability is based on the susceptibility of the asset to surveillance, attack, or damage and its ability to recover if damaged. Threat is the assessment of the probability that the asset will be attacked by the adversary. Each asset is evaluated against these criteria, which are weighted based on the CCDR's intent, CONOPs, and center of gravity concerns.

[10] JP 3-01, 2017, pp. III-15, III-18; Headquarters, 2015, pp. 3–6.

Figure 7.1. Example of a Combatant Commander Critical Asset List by Phase



SOURCE: JP 3-01, 2018, p. III-16.
NOTE: Assets such as those listed above may be on both CAL and the DAL. However, given limited capabilities, these assets could still be vulnerable attack.

actions approved by the CCDR.[11] The AADC is generally the COMAFFOR/JFACC, since USAF provides the bulk of theater AMD C2 capabilities to plan, coordinate, and execute DCA operations as well as the majority of the airborne assets that can conduct DCA operations. The deputy area air defense commander (DAADC) is a senior officer from a different service with significant AMD capabilities in theater, typically the commander of the theater Army air and missile defense command (AAMDC).[12] Other joint force components and the CCDR staff also participate in planning through the combatant command's AMD working groups.[13] Finally,

[11] JP 3-01, 2017, p. V-1.

[12] JP 3-01, 2017, pp. II-10-11, II-12; Air Force Doctrine Annex 3-01, 2016, p. 14. With its Patriot and THAAD systems, the Army possesses all of the U.S. military's ground-based theater-level ADA systems. Headquarters, 2015, pp. 2-3–2-4. The AAMDC commander is also normally designated as the theater Army AMD coordinator (TAAMDCOORD). TAAMDCOORD assists in developing Army DCA inputs for the joint air operations plan and participates in the AADC's DCA planning. This triple-hatted arrangement is intended to ensure both that the Army's AMD requirements are integrated into the joint counter air campaign and that Army AMD forces are properly deployed to support the joint area air defense plan; JP 3-01, 2017, pp. II-4, II-22; Air Force Doctrine Annex 3-01, 2016, pp. 3-13.

[13] JP 3-01, 2017, pp. II-7, II-11, II-12, V-1, V-18, V-20; Headquarters, 2015, pp. 2–4. For example, the AADP for Operation Iraqi Freedom was written prior to the commencement of operations at a working conference. Attendees included the commanding general of the 32nd AAMD and key members of his staff, all the ADA brigade and battalion commanders, the CRC squadron commander, and representatives from Aegis, Cobra Judy, combined air operations center, tactical air operations center, and AWACS. 32nd Army Air and Missile Defense Command, *Operation Iraqi Freedom: Theater Air and Missile Defense History*, Fort Bliss, Tex.: 32nd AAMDC, September 2003, p. ix.

liaisons from the service components within the AOC (e.g., the BCD, naval and amphibious liaison element, Marine liaison element, and special operations liaison element) also provide specific weapon system and mission expertise for the development of the AADP.[14]

The doctrine for planning multidomain AMD operations appears to be fairly robust. There is an established procedure for developing an AADP based on the CCDR's protection requirements. Because this plan is developed by personnel from the services and the CCDR's staff who have the requisite domain knowledge, multidomain plans, such as the one for defending SPOD described in our notional vignette, could emerge when planning for a contingency. Furthermore, the two key leaders engaged in developing the AADP, the AADC and the DAADC, are generally "dual-hatted" and have OPCON or TACON over their service forces. This arrangement reduces the number of steps required to gain approval for plans, which should also reduce planning time and uncertainty.

Planning During a Contingency

In the event of a contingency, the AADC executes the AADP using the forces and capabilities that the CCDR apportions to the AMD mission.[15] The JFACC/AADC is then responsible for allocating and tasking available forces to protect assets on the DAL.[16] It is the responsibility of the CCDR to define the command relationships between the AADC and the component commanders. In practice this means that the JFACC/COMAFFOR/AADC will normally exercise OPCON over USAF forces and TACON over other services' air assets made available for joint tasking. This means, for example, that if Navy and Marine Corps sorties are made available to the JFACC/AADC for DCA, they can be employed where the JFACC deems it to be most appropriate to protect assets on the DAL. The available sorties will vary daily based on how the CCDR and the JFACC decide to allocate aircraft among DCA, OCA, and other missions.[17] The AADC receives direct support from surface-based AMD forces, although the AAMDC is often TACON to the AADC to ensure coordination of effort. Direct support means that the surface-based forces allocated to theater AMD are required to support the AADC and are authorized to respond directly to the AADC's request for support. Such a relationship thus improves the potential speed of response and reduces the number of steps in execution.[18] The JFACC/AADC's relationship with Army-based AMD forces is further reinforced by the fact that

[14] Within the AOC, the AADP is produced by the C2 plans team of the combat plans division. JP 3-01, 2017, pp. II-10, II-11. Air Force Instruction 13-1, 2012, pp. 29, 31, 33.

[15] JP 3-01, 2017, pp. II-4, V-3.

[16] JP 3-01, 2017, p. II-9.

[17] JP 3-01, 2017, p. II-9; JP 3-30, 2019, p. II-6.

[18] JP 3-01, 2017, p. II-9; JP 3-31, 2014, pp. 2–11. For the Army, direct support enables the supported unit to assign the position or an area of operations and to set the priorities for the supporting unit. An Army ADA unit that is in direct support of the AADC will focus on the AMD requirements of the AADC. Headquarters, 2015, pp. 1–13; Headquarters, Department of the Army, *FM 3-0 Operations*, October 2017b, p. A-21.

the DAADC has OPCON over Army assets dedicated to theater AMD missions. Integration of Navy AMD assets under the AADC would normally be done by designating an appropriate maritime commander as an RADC/sector air defense commander (SADC). This maritime commander would have TACON over his or her assigned Navy AMD assets.[19]

In addition to adjusting the allocation of forces over the course of the campaign, the AADC may have to adjust the AADP, CAL, and the DAL. These are all living documents that change as a joint campaign unfolds and as the CCDR's protection needs to be changed.[20] For example, the AOC will propose modifications to the AADP in response to both expected and unexpected changes in the adversary's capabilities and to the preplanned changes in CAL as a result of phase transitions.[21] As with before a contingency, the AADC has experts from all domains available in the AOC to assist with updating these lists and determining which multidomain combination of forces is appropriate for defending each asset on the DAL.

As with planning for a contingency, the doctrinal basis for planning during a contingency appears to minimize C2 impediments to MDOs. The one potential impediment is that naval surface AMD assets appear to be less well integrated with the AADC than are Army surface AMD assets. This may be a function of the way that domains are doctrinally defined and operationalized. The land and air domains are largely geographically congruent. Conversely, there will often be a geographically separate maritime area of operations, which can extend into the littoral regions.[22] These maritime areas will generally be provided congruent air defense areas and sectors for which JFMCC will have primary responsibility for providing the operational and C2 capabilities.[23] While these forces fall under the AADC and the AADP, the Navy generally lacks a presence similar to that of AAMDC in the AOC.[24] The practical effects of this weaker integration are unclear given the normal delegation of execution authority to RADCs and SADCs.[25]

---

[19] JP 3-01, 2017, p. II-7.

[20] The DAL is updated throughout the campaign by a DAADC-chaired working group that includes CCMD staff and component representatives. Assessments and recommended changes to the DAL are presented to the AADC for concurrence and then forwarded to the CCDR for approval. JP 3-01, 2017, pp. III-15–III-19.

[21] JP 3-01, 2017, pp. III-15–III-19; Air Force Doctrine Annex 3-30, 2014, p. 103.

[22] The maritime domain is doctrinally defined as the "oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals." The air domain, conversely, is doctrinally defined as the "atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible." There is thus some doctrinal confusion over which domain controls the airspace over the ocean and the littorals. JP 1-02, 2019, pp. 12, 146.

[23] JP 3-01, 2017, p. II-7.

[24] Doctrine states that the JFMCC's integrated air and missile defense (IAMD) cell is the primary conduit for planning and execution coordination with the AOC and AAMDC and that it assists in coordination between naval forces designated as an RADC to achieve integration into the AADP. JP 3-01, 2017, pp. II-7, II-23.

[25] In addition, integration with U.S. Army AMD forces would be reinforced by the positioning of an ADAFCO on the ship serving as the RADC/SADC. JP 3-32, 2018, pp. IV-9–IV-10.

Execution and Assessment

Doctrinally, the execution of the AADP involves multidomain battle management with engagement authority being delegated to RADCs/SADCs who directly control joint air defense capabilities and rely on joint sensors for SA.

The AADC has the command authority to deconflict and control engagements and to exercise real-time battle management.[26] In large operations, the AADC and the CCDR normally divide the operational area into separate air defense regions or even smaller sectors, each of which has an RADC or an SADC who can be given execution authority for DCA operations within that region. That means that the RADC/SADC generally has the authority to directly order an AMD asset to engage with or destroy an air or missile threat.[27] Any service component air control or air defense organizations with the necessary SA and communications links to higher, parallel, and subordinate organizations can operate as an RADC/SADC.[28] These organizations include USAF air operations centers and control and reporting centers (CRCs),[29] Navy aircraft carriers, amphibious assault ships, cruisers, and destroyers, and Marine Corps tactical air operations centers.[30]

Regardless of service, the RADC or SADC can task fighter aircraft to respond to the detection of a hostile, potentially hostile, or unknown airborne target.[31] Army ground-based

---

[26] JP 3-01, 2017, p. II-3.

[27] JP 3-01, 2017, pp. xiii, xix, II-11, II-11–II-13, V-2. Headquarters, Department of the Army, *Air Defense Artillery Brigade Techniques* ATP 3-01.7, March 16, 2016, pp. 3–9. There are three primary forms of authority associated with DCA operations that the CCDR normally delegates to the AADC, which is in turn authorized to delegate to lower tactical echelons: ID authority, commit authority, and engage authority. ID authority is the authority to assign an identity classification to an unknown target. Commit authority is a battle management tool that enables the possessor to authorize assets to prepare for engagement with a contact; this can include positioning DCA fighters to intercept or directing an ADA unit to track and target a contact. Engagement authority is the authority to order the engagement or destruction of an air or missile threat; JP 3-01, 2017, pp. III-13, III-14.

[28] JP 3-01, 2017, p. II-13.

[29] A CRC is a deployable Air Force airspace control and surveillance radar facility directly subordinate to the AOC. It is a ground component of Air Force's theater air control system. The CRC is assigned an airspace control sector by the AOC and manages and directs the activities of all deployed Air Force surface radars within that sector. The CRC communicates up to the AOC, down to subordinate units, and laterally to other units engaged in AMD to ensure that defensive assets are employed in mutually supporting roles within the CRC's assigned sector. Air Force Doctrine Annex 3-01, 2016, pp. 18–19. The CRC's TPS-75 radars can provide 360-degree coverage out to about 240 nautical miles and a real-time radar airspace picture. Data from the radars passed through the CRC's operations module for processing and action. 552nd Air Control Wing, "Control and Reporting Center (CRC)," December 6, 2016.

[30] JP 3-01, 2017, pp. II-5, II-6.

[31] JP 3-01, 2017, pp. II-21,V-13,V-24. Each C2 node has a fire control coordination/watch officer assigned by the RADC/SADC. This position can be manned by component liaison officers, upper-tier coordination officers, air defense artillery fire officers (ADAFCOs), or a combination of such personnel depending upon AMD defense design. The fire control/coordination watch officer position is manned continuously and is responsible for passing updated firing orders and guidance from the AADC/RADC/SADC to the firing units. These officers also provide advice on the potential tactical impact of weapon system degradation and changes in firing orders, rule of engagement, and defense design. JP 3-01, 2017, pp. II-13–II-14, V-14.

missiles units assigned to the theater ADM mission remain under the command of AAMDC but have their area of operations and mission priorities set by the RADC/SADC.[32] As a result, an Army air defense artillery fire officer (ADAFCO) is embedded with the RADC/SADC to enable him or her to exercise engagement control over subordinate air defense units.[33] With the combination of delegated authorities, particularly engagement authority and its direct link to Army air defense artillery units through the co-located ADAFCO, RADC, or SADC can task all forces regardless of domain or service. Further multidomain coordination is possible in execution since all counter air forces are subject to rules of engagement, airspace control, weapons control measures, and fire control measures established by the JFACC.[34]

Unlike in other mission areas, execution of AMD is facilitated by a common tactical picture (CTP)[35] at the RADC/SADC level and a COP at higher echelons.[36] It fuses information from sensors that can include satellites, surface-based radars, and airborne C2 aircraft such as the AWACS or the E-2 Hawkeye.[37] The CTP is possible because of tactical data links (TDLs) and joint data networks (JDNs) that allow for the sharing of the information between service systems and RADCs/SADCs.[38] The CTP provides RADCs/SADCs with the information they need to

---

[32] This is due to the direct support relationship that is established with the RADC/SADC. For the Army, direct support is a significant support relationship as it enables the supported unit to assign the position or an area of operations and to set the priorities for the supporting unit. An Army ADA unit that is in direct support of the AADC will focus on the AMD requirements of the AADC. Headquarters, 2016, pp. 1–3; Headquarters, 2017b, p. A-21.

[33] Headquarters, 2016, pp. 3-8, 3-9; Headquarters, Department of the Army, *ADRP 3-09 Fires*, February 8, 2013, pp. 2-9, 2-10; Headquarters, 2016, pp. B-1–B-2.

[34] JP 3-01, 2017, p. II-3; JP 3-32, 2018, p. IV-6.

[35] A common tactical picture is an "accurate and complete display of relevant tactical data that integrates tactical information from the multitactical data link network, ground network, intelligence network, and sensor networks." A common operating picture is a "single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness." Office of the Chairman of the Joint Chiefs of Staff, 2020, p. 43.

[36] Joint capability to provide an AMD CTP is evolving and will likely improve over time. The U.S. Army is developing an integrated AMD battle command system (IBCS), which will provide networked internal connectivity for all Army AMD radars, weapon systems, and command posts. In addition, it is planned that this system will also connect Air Force, Marine Corps, and Navy systems. Recent field experiments have shown that the F-35 is capable of integrating with IBCS and transmitting targeting data. Tests conducted by the Navy have demonstrated that the F-35B can use its Multifunction Advanced Data Link to integrate with the Aegis combat system and guide an SM-6 missile to a target that could not be directly seen by the Aegis radar. Freedberg, 2019b; LaGrone, 2016; Sean Gallagher, "Marine Corps F-35B Scores a Kill (Sort of)—with a Navy-Launched Missile," *arsTechnica*, September 14, 2016. Doctrinally, the information flow supporting this CTP/COP needs to be complete, reliable, secure, and near real time. Each C2 node thus requires rapid communication links and procedures, data fusion and decisionmaking nodes, warning and cueing systems, links to dedicated weapon systems, and interoperability. JP 3-01, 2017, pp. II-11, II-20–II-21. The operational efficacy of this network is critical for the smooth function of IADs. Creating an ideal single integrated information architecture that smoothly links service and national data is technically challenging. Craig Corey, "The Air Force's Misconception of Integrated Air and Missile Defense," *Air and Space Power Journal*, Vol. 31, January 2017.

[37] JP 3-01, 2017, p. V-4.

[38] JP 3-01, 2017, p. II-13.

engage a target.[39] The CTP/COP also helps to manage seams between RADCs. For example, since ports can be threatened from both their seaward and landward sides, doctrine highlights the need for complete integration between the afloat RADC and land-based RADC.[40] This is achieved in part through the shared CTP.[41]

The doctrinal C2 structure that delegates engagement authority to RADCs/SADCs is an important component of enabling multidomain AMD operations. The RADC has access to a CTP fed by multidomain sensors and the authority to direct the AMD assets under its control to engage adversary air and missile threats.

Conclusion

Doctrinally, there appears to be a well-established C2 system for planning and executing multidomain AMD operations using capabilities that have traditionally been involved in this mission (Table 7.1). This system integrates operations in these traditional domains under a single

Table 7.1. Enablers of Multidomain Air and Missile Defense

C2 Characteristics That May Enable MDO	Potential C2 Enablers to MDO	Potential Impact
MDO do not require more steps and processes.	Personnel with appropriate authority are present at operational and tactical C2 nodes, limiting the number of steps to approve plans and to execute.	Less planning uncertainty; enables rapid execution
Expertise and access to information on relevant domains is available.	Personnel with expertise and appropriate rank contribute to AMD planning.	Multidomain expertise available to generate multidomain plans
	Doctrine calls for all C2 nodes to have a common operational or tactical picture with information from all domains.	Planning and execution nodes have information to determine the most appropriate domain to employ
Operating across domains does not increase communications dependence.	Tactical planning and execution authority for AMD operations from all domains is delegated to regional and sector air defense commands.	Potential to speed up decisions and enable execution of theater-wide complex operations
Multidomain mindset	Doctrine emphasizes that this is a multidomain and joint mission area.	Planners consider multidomain options from the outset

[39] JP 3-01, 2017, pp. V-2, V-23.

[40] JP 3-01, 2017, p. II-13.

[41] JP 3-01, 2017, p. II-13. The CTP is the responsibility of the CCDR's joint networks operation officer who is supported by the JFACC's component joint networks operations officer equivalent. The JFACC is also generally responsible for the joint multitactical data link network, which is the primary data source supporting the generation of the CTP. Each RADC/SADC has an interface control officer who is responsible for TDL continuity and who coordinates with the theater's joint interface control officer (JICO) the planning and execution of TDL links across the theater. JP 3-01, 2017, pp. II-10, II-24–II-25.

commander who can both develop plans for these forces and decide how to use them. However, as noted in previous chapters, integration of offensive cyber or space, which have not traditionally been part of AMD, would require additional steps and processes. Since the United States has not conducted AMD against a near-peer competitor in recent decades, we were unable to assess the potential C2 impediments to multidomain AMD in practice. Still, the doctrinal C2 approach is useful to study because it offers a different model from C2 of other mission areas.

There are several facets of doctrinal AMD operations that could be applicable to other mission areas. The first is that AMD operations have a distinct and integrated planning process at the CCDR level, which results in the CCDR-approved AADP. This process allows for the integration of multidomain capabilities into theater-wide AMD operations and helps synchronized service and component AMD efforts. The second is that execution of AMD operations is decentralized to multidomain C2 nodes that have direct links to AMD sensors and to the tactical units that conduct AMD operations. Finally, and supporting the previous point, service and component representatives with the required knowledge and command authority are embedded in all C2 nodes throughout the AMD network.

The integrated nature of AMD may be facilitated by the fact that each service already has some forces dedicated primarily to the AMD mission. The sole function of Army Air Defense Artillery units is to conduct AMD, primarily at the theater level. The Navy often conducts AMD in its own defense and has weapon systems on its multimission cruisers and destroyers dedicated to area AMD. Similarly, USAF's CRC's primary function is to support air defense operations. In addition, AMD is an enduring and theater-wide mission that will be required on a continual basis as long as the adversary poses an air and missile threat. Other potential multidomain mission sets may not have dedicated capabilities. Rather, these capabilities may be flexibly applied across mission areas. In addition, their requirements may be more transient in nature or focused on relatively narrow periods of time.[42] This may be a significant impediment to creating specialized C2 arrangements similar to those that AMD has.

[42] SEAD, for instance, may require MDO operations only during narrow windows of time when aircraft or strike packages are penetrating through an adversary's IADs.

8. Summary of Findings on Potential Command-and-Control Impediments to Multidomain Operations

Conflict against a near-peer competitor would likely present many challenges for joint operations. We focus in this report specifically on potential impediments to integrating across domains while employing the current C2 construct in a high-end fight. The preceding chapters have therefore detailed potential impediments to MDOs in the current C2 construct as described in joint doctrine. This chapter summarizes the key potential C2 impediments to MDOs that emerged from our analysis. We refer to these as *potential impediments to MDOs* since we cannot assess the extent to which each affects the viability of MDOs or joint warfighting effectiveness.

As noted above, there are some important caveats to these findings. First, these findings may not be comprehensive, since *our analysis did not consider the full range of activities across domains, all possible combinations of activities, or the additional complexities of the JADC2 in a multinational coalition*. Second, although we conducted over 150 interviews to better understand current practice, *our analysis focuses on current doctrine*. There may be ad hoc work-arounds or experimental solutions that can mitigate some of the impediments we identify below. These, however, may not be widely used or develop into formal practices without time and support from leaders. Finally, *although each of the findings below points to a potential impediment to MDO, that does not mean that this aspect of the current C2 construct is necessarily, on net, a poor C2 choice.* C2 structures must balance many considerations beyond enabling MDOs, as discussed in subsequent chapters. In spite of these caveats, many of the same themes emerged across domains and in interviews with different organizations, reinforcing that the findings highlighted here are an important starting point as the joint force begins to examine how it could change C2 structures to facilitate more effective MDOs.

Component-centric planning may make identifying multidomain options more difficult. As discussed in previous chapters, service and functional components conduct the bulk of operational planning under the guidance of the GCC. The GCC's J-5 integrates component plans, and components interact informally to coordinate across domains. In some cases, this interaction may be sufficient to identify multidomain options. However, service and functional components do not currently, on their own, strive for truly domain-agnostic problem-solving and planning. These organizations are organized around employing capabilities from a single domain or subset of domains. This means that each organization may have a shortfall in expertise in other domains and therefore have a natural predisposition toward solutions in its traditional domain. Without the appropriate expertise and mindset, planners may not think of multidomain options. In other cases, multidomain options may be considered, but planners may not fully understand the capabilities and limitations of other domains. It may take additional time to confer with experts in other organizations to determine whether and how such options could be developed. This is

time that may not be available in a conflict with a near-peer adversary over a large area. The potential impediments associated with component-centered planning for a contingency may be particularly consequential since options that are not developed and exercised in peacetime may be difficult to plan and execute in wartime.

The planning process for AMD, as envisioned in doctrine, is an important exception within the current C2 construct. Doctrinally, that process includes experts from all domains and starts from the premise that solutions should be multidomain.

MDOs make C2 more complex. MDOs that rely on capabilities from multiple GCC components or CCMDs may require more steps and approvals than single-domain operations conducted by a single organization. For example, using ground fires as part of a SEAD campaign requires coordination between and agreement from both the JFACC and the JFLCC. The JFLCC would either need to agree to a multidomain scheme of maneuver that ensures ground fires are available to assist with the SEAD campaign or designate whatever ground fires happen to be available each day for tasking by the JFACC. If the components do not reach an agreement, this type of multidomain approach would require CCDR adjudication. In some cases, the components may agree, minimizing the effects of these extra steps. But in other cases, the need to gain additional approvals could create uncertainty for planners and make them more likely to rely on capabilities their component already controls.

Moreover, GCC MDOs that employ space, cyber, intelligence, and mobility forces typically controlled by an FCC or by USSPACECOM or the IC require additional steps and approvals. For mobility forces, this may mean coordination with an FCC for support or requests to the national command authority to attach the capabilities to a GCC. For space, cyber, and intelligence capabilities, there may be additional review and approval processes that include deconfliction with all interested parties. These traditional arrangements prioritize efficient management of limited resources, weighing intelligence gain and loss considerations and keeping consequential decisions at a high level. However, at the same time, the current structure and processes make it more time consuming and manpower intensive to integrate these capabilities into a terrestrial GCC's MDO. Moreover, uncertainty surrounding approval for certain effects and availability of different capabilities may create planning uncertainty, thereby necessitating more branch planning or leading planners to avoid using these capabilities.

Legal framework for space and cyber operations can lead to conflicting interpretations among CCMDs. In addition to requiring more steps and approvals, incorporating space and cyber operations can sometimes be challenging due to conflicting interpretations among CCMDs. Interviews suggested this is due, in part, to a legal framework that has not been fully developed and, in some cases, is behind the state of technologies in those domains. Reconciling these interpretations is left to individual CCMDs, their staffs, and their JAs. Differing or conflicting interpretations as a result of dated authorities have to be resolved when operations or contingencies are planned or executed, and that takes time.

Classification is a potential barrier to space and cyber integration. Personnel we interviewed from CCMDs and their components as well as in the space and cyber communities frequently pointed out that classification is a barrier to integration of space and cyber operations into plans. If planners are not aware of all available capabilities in the domains, they will not be considered. And even if options are known, commanders may not feel comfortable relying on capabilities they do not fully understand or have limited practical experience in using, as in exercises or wargames.

MDOs may increase dependence on vulnerable communications systems. Integrating across domains may address some of the operational challenges that a near peer may present for U.S. forces, such as highly capable IADS. However, near peers can also contest communications. In this environment, MDOs that rely on detailed coordination or synchronization among more units or platforms than single-domain alternatives could be more vulnerable to disruption. That does not mean that an MDO is not possible in a communications-contested conflict. In fact, having redundant options may be advisable under these conditions. Still, concepts for MDOs and the JADC2 will need to balance the gains in warfighting effectiveness from integrating multiple domains with a potentially greater risk of communications disruptions.

CCMDs may perceive a lack of unity of effort. Under the existing legal framework and the UCP, at least some GCC MDOs will require coordination with FCCs or USSPACECOM for mobility, space, and cyber operations. During a high-end contingency with a near peer, CCMDs will need a shared understanding of each other's plans and priorities to achieve unity of effort. In spite of recent efforts to improve coordination among CCMDs, interviews suggest that there may still be work to do in this area. Regional GCC interviews revealed a perception, if not a reality, that GCC priorities are not always appropriately reflected in the allocation of global resources and that FCC operations are not always coordinated with the GCCs. Conversely, interviews with CCMDs and components responsible for global capabilities suggest that terrestrial GCCs sometimes fail to understand that resources are scarce and their priorities may simply not be national priorities. It is not clear from our research how substantial the unity of effort problem is or whether this perception is held at the highest levels of leadership. However, the perception alone could be an impediment to terrestrial GCC-planned MDOs if it makes the GCC component planners reluctant to consider multidomain options using capabilities controlled by an FCC or by USSPACECOM or the IC.

9. Alternative Joint All-Domain Command-and-Control Constructs

Because MDO concepts are still emerging, it is not yet clear how much they will improve warfighting effectiveness. This makes it difficult to evaluate how much cost and risk the joint force should bear to optimize its C2 structures for conducting MDOs. Moreover, without a sense of what types of MDOs are most beneficial, it is difficult to know which C2 changes are most important. As a result, we do not recommend specific changes to GCC C2 structures to enable MDOs. Instead, this chapter proposes four alternative C2 concepts for the joint force to consider as MDO concepts and their benefits become clearer.

In developing alternative JADC2 constructs it is important to first consider other C2 challenges the joint force would face in conflict with a near-peer competitor. Since this report focuses on the JADC2, we do not address these challenges in detail. Rather, we describe our basic assumptions about how the United States may handle these challenges before providing our JADC2 alternatives.

Other Command-and-Control Challenges in a Conflict with a Near-Peer Adversary

Joint and service documents anticipate that conflict with a near-peer competitor will present two additional C2 challenges: it will be transregional, and it will take place in a communications-contested environment. Joint and service organizations are developing new C2 concepts to address these challenges, but to date, these concepts are evolving largely in parallel with each other and with the JADC2.

Global Integration for Transregional Conflict

Joint documents contend that a conflict with a near-peer competitor may be transregional, meaning that it may cross combatant command (CCMD) boundaries.[1] For example, an adversary may launch an attack on countries near its periphery, conduct cyberattacks on the U.S. homeland, harass U.S. forces in a third region, or contest U.S. space communications. The joint force has therefore been developing concepts for managing priorities, synchronizing effects, and following a coherent global strategy in peacetime and wartime.

Beginning in 2015, in response to Senator John McCain's hearings on potential reforms of military authorities and structures, Chairman of the Joint Chiefs of Staff General Joseph Dunford began calling for an expanded joint staff that could monitor events globally to inform decisions

[1] Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, March 16, 2018.

on the allocation of resources across combatant commands.[2] In 2017, the National Defense Authorization Act for Fiscal Year 2017 (NDAA 2017) codified "the Chairman's responsibility to provide advice to the president and the SecDef on ongoing military operations and to provide advice to the SecDef on the allocation and transfer of forces among COCOMs [combatant commands]."[3] The CJCS and the SecDef began using the term *global integrator* to describe the chairman's role.

As part of the joint initiative on global integration, the joint staff and CCMDs are examining new staff organizations and processes for transregional conflict. There have been exercises and wargames designed to test C2 structures, identify gaps and seams among CCMDs, and inform strategic assessments and resource allocation.[4] That the SecDef, the CJCS, and CCDRs have personally participated indicates the priority they place on global integration initiatives.[5] In spite of these practical steps toward global integration, it is not yet clear exactly how C2 processes and organizations will change to facilitate global integration.

Distributed Control for a Communications-Contested Environment

Given the threat to U.S. communications (e.g., adversary attacks on undersea cables or satellites), the services have been developing concepts to sustain operations even when communications are degraded.[6] Concepts for distributed control therefore aim to give forward forces the authority and capability to make decisions based on the intent of higher headquarters. PACAF in particular has been developing a concept and taken steps to empower wings to act as distributed control nodes, but there is still much work to be done.[7]

Integrating Command-and-Control Concepts for Conflict with a Near-Peer Competitor

Global integration, the JADC2, and distributed control can potentially coexist, but there are inherent tensions among them. For example, if more authorities and forces are held at the

---

[2] Dunford, n.d.; Colin Clark, "CJCS Gen. Dunford Proposes 'Staff,' to Handle Transnational Threats," *Breaking Defense*, December 14, 2015; Colin Clark, "CJCS Dunford Calls for Strategic Shifts; 'At Peace or at War Is Insufficient,'" *Breaking Defense*, September 21, 2016.

[3] U.S. House of Representatives, 2016.

[4] Francis J. H. Park, *Chairman's Vision of Global Integration*, U.S. Army, May 24, 2018, p. 6.

[5] Others have urged caution and counseled drawing lessons from past efforts to reorganize the military to deal with global threats, such as General George Marshall's post–World War II proposal for a "Unified Department of the Armed Forces." Paula Thornhill and Mara Karlin, "The Chairman the Pentagon Needs," *War on the Rocks*, January 5, 2018.

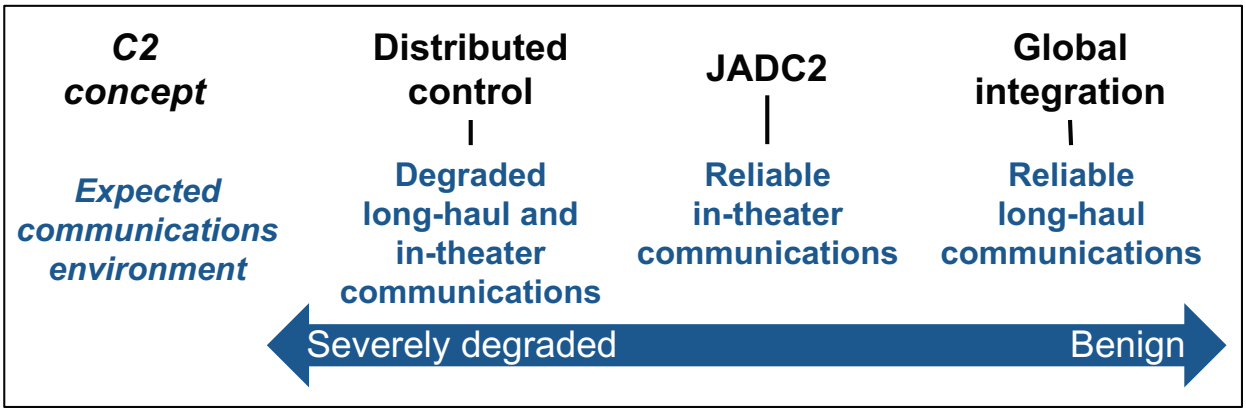
[6] Examples of "degraded" communications could include communications that are denied or delayed as well as those whose information cannot be authenticated. For an example of a C2 concept for a communications-contested environment, see T. J. O'Shaughnessy and Matthew Strohmeyer, *Multi-Domain Command and Control: Ensuring Offensive Initiative at the Theater AOC and below in a Contested Environment*, Joint Base Pearl Harbor–Hickam, Hi.: Pacific Air Forces, Strategic Thinking White Papers, 2018.

[7] For a more detailed discussion of distributed control, see Priebe et al., 2019.

national level to facilitate global integration, then it is more difficult to give forward forces control over those capabilities during communications disruptions or to empower CCMDs to quickly plan for and execute an MDO. Similarly, giving geographic CCMDs more operational or tactical control of forces that can act globally (e.g., cyber mission teams) may make multidomain integration easier, but also makes it more difficult to synchronize effects globally or reallocate these forces as global priorities shift. Optimizing a C2 structure to address any one of the three C2 challenges may, therefore, create trade-offs for managing the other two C2 challenges. The joint force will need to decide how to set priorities to manage these trade-offs as the United States develops an overarching and adaptable C2 structure for a high-end conflict.

One of the most important factors for determining the relative priority among these concepts may be the expected communications environment during a conflict. As shown in Figure 9.1, concepts for global integration assume that long-distance communications between CCMDs and the continental United States will be reliable. Concepts for the JADC2 tend to assume that in-theater communications are reliable, allowing operational-level commanders to plan MDOs and to direct forward forces. Conversely, concepts for distributed control assume that long-distance communications may be degraded, thereby necessitating more local control. The expected communications environment can therefore guide prioritization of C2 concepts: If more benign, then concepts for global integration and the JADC2 are viable, and concepts for distributed control are less important; however, if, during a high-end fight, communications are heavily contested, then optimizing the C2 structure for distributed control may be the highest priority.

Figure 9.1. Command-and-Control Concepts and Assumptions About the Communications Environment



Assumptions About Global Integration and Distributed Control

For the purposes of this study, we assume that some level of global integration remains a priority for the joint force going forward. The exact decisions that national leaders make about global integration are not critical for our purposes. Instead, we make the broad assumption that

capabilities that can have global effects, such as cyber, space, and mobility forces, will remain largely under the control of currently designated CCDRs. Terrestrial GCCs would continue to rely on a support relationship with global CCMDs to execute MDOs with these capabilities. We do not assume any dramatic changes to the current UCP, though we do assume that some space and cyber capabilities may be attached or assigned to terrestrial GCCs in future conflicts.[8] For example, in future conflicts, the SecDef may attach or assign cyber forces to the GCC due to the high pace of operations or the risk of communications contestation. For similar reasons, a terrestrial GCC may also control some counterspace systems in theater.[9]

We also assume that our alternative C2 constructs must account for distributed control in a contested communications environment. Therefore, each of our alternative C2 constructs considers broadly how MDOs might continue when communications between forward forces and higher headquarters are severely degraded. Given our focus on operational-level C2, we do not detail these arrangements. Rather, we provide a preliminary assessment of how alternative C2 constructs would affect the broad outlines of distributed control arrangements.

We also assume that any future C2 arrangement needs to account for the possibility of a kinetic attack on headquarters and other C2 nodes. Therefore, any future C2 arrangement may include distributed rather than large headquarters.

Generating Alternative Command-and-Control Concepts

Two fundamental features of the current C2 construct appeared to drive many of the potential impediments to MDOs. First, component-centered planning creates the risk of insufficient expertise in all domains and a preference for solutions in certain domains versus all domains. Second, control of multidomain capabilities is often divided among components, which is one reason that an MDO can involve more steps and processes. Changes to these two elements of the current C2 structure therefore seem valuable to explore.

In order to generate alternative C2 constructs, we asked two questions: Which organization within the GCC conducts multidomain planning? Who controls capabilities across domains? In order to generate more detailed alternatives for the joint force to consider, we focused on four alternatives that range from small changes to the status quo to more fundamental changes. We then consider how these alternatives might handle the key responsibilities of C2 organizations at the operational level—planning, monitoring, and assessing operations—and the extent to which they could overcome the potential impediments we describe above.

---

[8] In today's legal framework, assigning these assets to theater would require a presidential or SecDef order; 10 U.S.C. 162(a) and 164(c)(1); 50 U.S.C. 3023.

[9] For a general discussion of such systems, see Defense Intelligence Agency, *Challenges to Security in Space*, January 2019; National Air and Space Intelligence Center, *Competing in Space*, Wright-Patterson Air Force Base, Oh., December 2018, pp. 20–21.

In developing these alternatives, we focused on options that retained multidomain planning primarily at the operational level—at the CCDR or component level. The first two alternative C2 constructs—incremental change and the air, space, and cyber component—entail evolutionary changes from the current C2 construct. They largely retain component-centered planning and domain-centric functional components. The second two alternatives—the CCDR-centric and line-of-effort (LOE) component construct—would be more significant departures from the current C2 construct.

We did not consider options creating smaller, forward joint task forces, akin to USSOCOM's use of smaller JTFs. While empowering forward forces to operate more independently from operational-level organizations could be an additional way to bring together domains, it is a change that may be even further afield than the alternatives discussed below. The approach we use in this report could, however, be used to develop and explore additional alternatives such as this.

The four alternatives we describe below are ideal types. We focus on ideal types in order to more clearly show the range of options and the trade-offs associated with different approaches. In reality, there may be hybrid approaches and elements from different constructs that a geographic CCDR could mix and match to enable an MDO. For example, the CCDR could direct that planning for a contingency be conducted by the CCDR's J-5 rather than in components to maximize all-domain expertise and coordination. During contingency operations the same CCDR could plan and execute operations using a components plan in a way that is only incrementally different from today. Similarly, the CCDR could retain the component-centered C2 construct, but supplement it with some mission-focused components for one or two operational challenges that require deeper levels of multidomain integration. As we discuss in the sections below, the joint force will need to engage in more experimentation and analysis to determine the right approach for different operating environments.

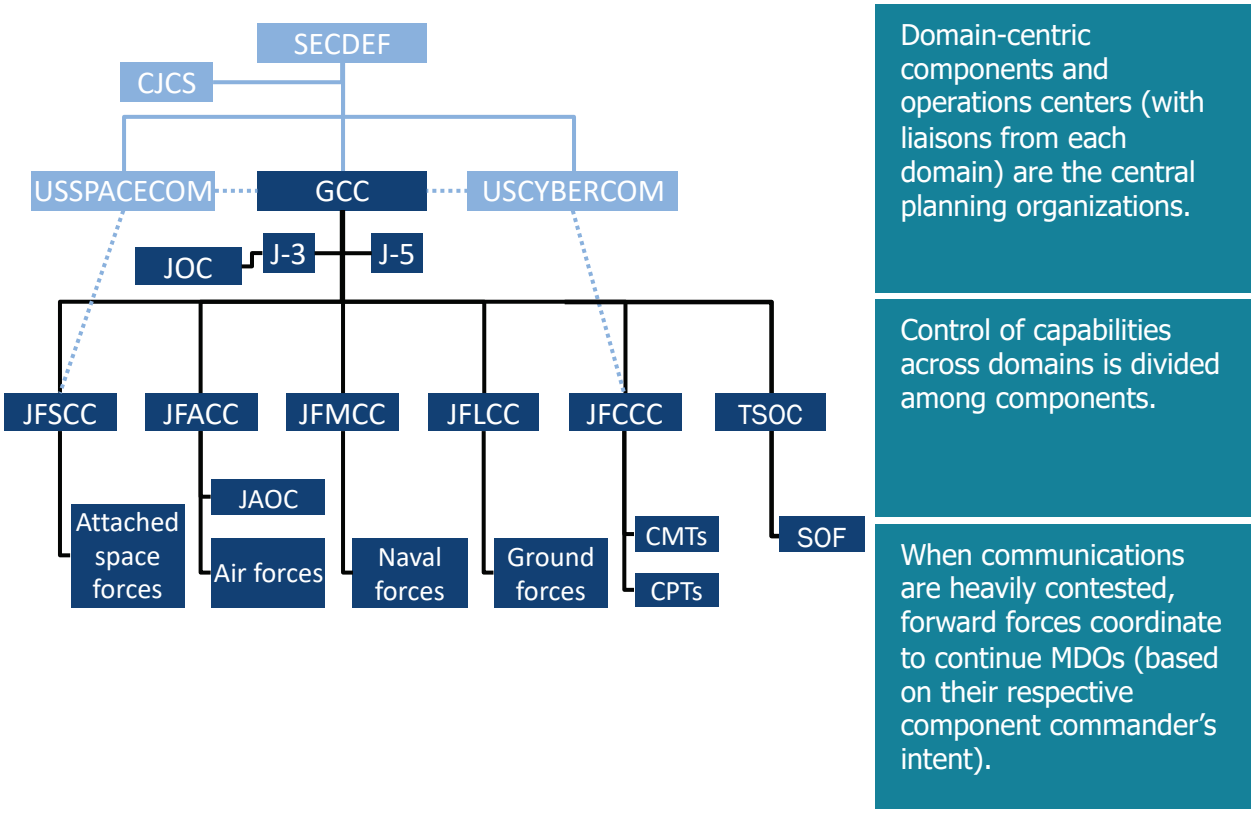
Incremental-Change Joint All-Domain Command-and-Control Construct

The incremental-change JADC2 construct incorporates minimal changes to today's domain-based baseline approach. Its primary goal is to generate more multidomain options during the planning process by addressing the "lack of sufficient expertise" category of impediments. First, in peacetime, the incremental-change C2 concept would have planners from every domain in every component's planning directorate, which is not necessarily the case today. This could come from changes in service component staffing or through the exchange of liaisons from other components. In wartime, expert planners from every domain would also need to be in every operations center. Second, the CCDR would promote a culture where liaisons are not primarily advocates for their parent organization, but instead act as expert planners within the other components' multidomain planning teams.[10]

[10] As noted above, in some cases doctrine emphasizes the advocacy role. Revisions to doctrine could therefore help with this cultural change as well.

Given the expanded role of space and cyber capabilities in future conflicts, the CCDR could also create space and cyber components with control of any space and cyber forces attached or assigned to the GCC (Figure 9.2). These components would also be responsible for coordination with USSPACECOM and USCYBERCOM for additional space and cyber support. We assume a relatively small amount of space and cyber capabilities are allocated to the theater. This implies that the space and cyber components would be smaller than traditional service or functional components and more like a TSOC or USTRANSCOM Joint Enabling Capabilities Command.

Figure 9.2. Incremental-Change Command-and-Control Construct



NOTE: This figure is illustrative and does not include all relevant organizations such as service components.

The main advantage of this construct is that it builds on the existing baseline approach, so the organizational and cultural change is less significant. This approach also contributes to CCMD and component resilience by retaining operations centers with experts from each domain who can fill in if other centers are attacked during a contingency. That said, the much larger number of liaison officers (LNOs) would require a larger staff size for each operations center.

The following sections describe some of the changes to doctrine and authorities that would be required to implement the incremental-change JADC2 construct.

Reorganization

In this model, the GCC would still conduct planning and operations through domain-centric components and operations centers. However, the CCDR would ensure that there were expert planners from each domain involved throughout the process. Existing liaison elements that focus on current operations such as the joint air component coordination element (JACCE) and the BCD are consistent with this approach. The incremental change would call for similar liaison elements to be in place in component planning directorates to enable multidomain planning during peacetime.

To ensure that each component has expert planners from other domains, the CCDR would likely need to engage the services and service component commands. This model would ask either for the services to assign more personnel to enable the establishment of peacetime liaison elements or for service components to give up expert personnel for these positions at a time when staffs are already stretched thin. Alternatively, the CCDR could pursue an agreement with the services and components to create liaison elements using service billets. In either case, the CCMD would be asking the service to ensure that personnel assigned to new joint or liaison positions have the appropriate planning skills and expertise.

Geographic CCDRs would also need to distribute space and cyber IPEs among the components, which they do not currently have the authority to do. Therefore, to have space and cyber planners involved in each component's planning process, USCYBERCOM and USSPACECOM would have to agree, and more trained personnel would be needed. Interviews suggest that the shortage of expert cyber and space planners has made USCYBERCOM and USSTRATCOM (the predecessor to USSPACECOM for space operations) hesitant to agree to such requests in the past. It remains to be seen how much staffing USSPACECOM will have and whether or not it will remain hesitant as well.

Another key change would involve the introduction of space and cyber components within a GCC, which would require new doctrine and additional personnel. Doctrine would need to be developed to support theater-level space- and cyber-component commands and to specify their relationships with USCYBERCOM and USSPACECOM.

Situational Awareness for Planning, Execution, and Assessment

Since every functional component would be doing multidomain planning and assessment, each operations center or command staff would have an increased demand for data and information on friendly forces and adversary forces across all the domains. The level of specificity may not need to be too detailed for every domain (e.g., the commander in the air component will need to know ground force disposition and status, but not details on supplies). Still, each component may have priority information requirements in more domains than in the past. This could, in turn, lead to higher demands on each domain's operations center or intelligence organization as well as a GCC J-2's allocation process.

Common data and reporting standards across services would enable the incremental-change concept. Moreover, services would need to develop interoperable systems that can display different levels of detail to different users. A potential impediment to this change is therefore that the services may not agree on the standards and systems. Moreover, USSPACECOM and USCYBERCOM may be reluctant to share information with a larger number of operations centers.

Planning

As noted above, planning for a contingency in this construct would resemble current planning efforts, with each component planning for assigned tasks based on GCC guidance and with additional liaisons from other components. As the expert planners from their domains, these liaisons would be deeply involved in crafting component plans. As components approach their assigned planning tasks, liaisons would provide ideas on how operations in other domains could integrate with or offer alternatives to the component's primary domain. In addition to proposing ideas that may not have otherwise been considered, liaisons could provide guidance on limitations to those options and facilitate dialogue with their owning command.

Past experience shows that empowered LNOs can enhance the planning process.[11] However, on a planning staff dominated by planners from the component's traditional domain(s), LNOs' impact may be limited.[12] The commander and his or her senior staff would have to set the tone for employing and empowering LNOs in an integrated planning fashion, rather than perpetuating distinctions between a "core" planning staff and LNOs. Otherwise, the most likely drawback to this approach is that the planning would still remain relatively domain-centered.

Components would continue to rely on support relationships to coordinate MDOs that involve forces from other components, so this C2 construct would not likely do much to reduce the number of steps and processes in planning.

Direction of Forces

The direction of forces in the incremental-change alternative is likely to remain largely the same as in the current approach: operations centers from each relevant component (e.g., the AOC, maritime operations center) would need to be involved to make changes to planned operations, such as multidomain time-sensitive targeting (TST). When communications are degraded, operational units would adjust to changing circumstances following the intent of their component commander. The longer these nodes remain isolated from their headquarters, the

[11] Joint Staff J7 Deployable Training Division, "Insights and Best Practices Focus Paper: Design and Planning," Suffolk, Va., July 2013, p. 20.

[12] JP 3-31, 2014, p. II-8.

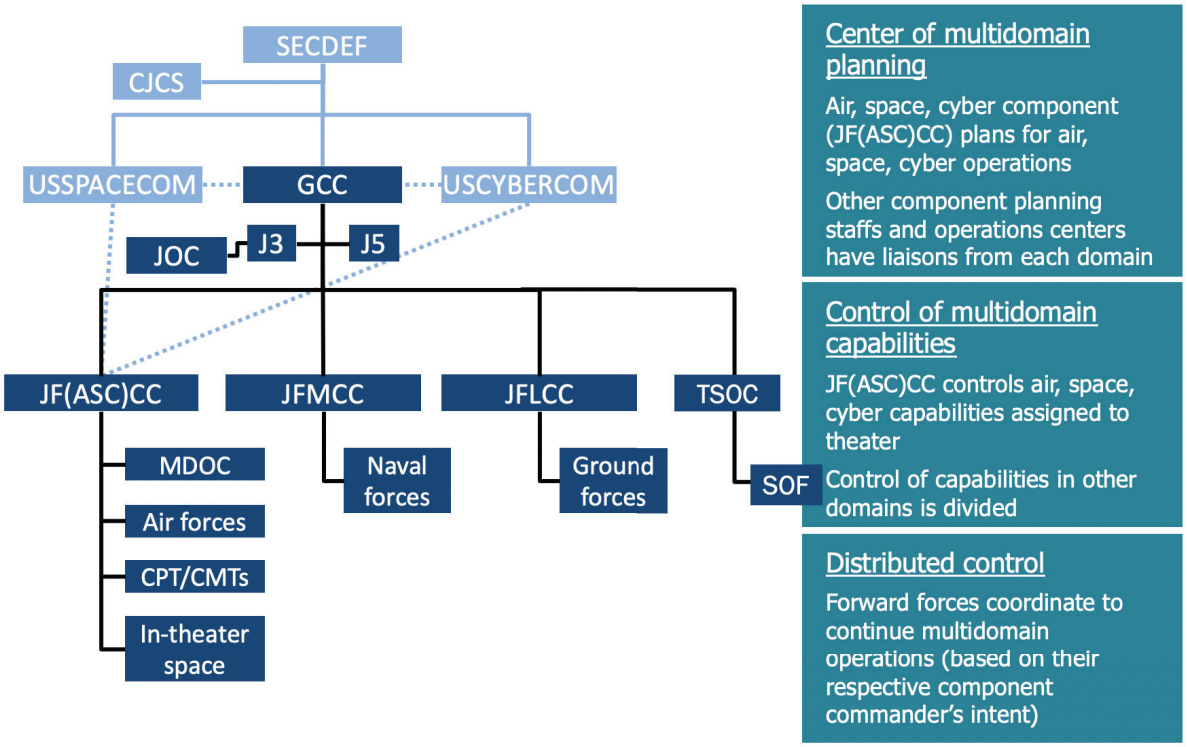
more difficult it will be to execute an MDO effectively since forces from different domains would be following the intent of different commanders.

Alternative Command-and-Control Construct: Air, Space, and Cyber Component

The next alternative maintains some of the traditional domain-based component planning and operations approach, but it combines forces from three domains—air, space, and cyber—in one component. Instead of having an air component led by a JFACC, this alternative would feature an air, space, and cyber (ASC) component led by a joint force air, space, and cyber component Commander (JF(ASC)CC). The land and maritime components would remain essentially the same, but would incorporate additional liaisons in a way that would be similar to the incremental alternative. In theory, any of the components could have more of these capabilities combined, but we focus here on the expansion of the air component as an example since it has been discussed as an option within USAF.

The JF(ASC)CC would have operational control over all air, space, and cyber forces assigned or attached to a GCC and direct liaison authority with USSPACECOM, USCYBERCOM, and USTRANSCOM for coordinating their support to GCC MDOs (Figure 9.3). Cyber and

Figure 9.3. Air, Space, and Cyber–Component Command-and-Control Construct



NOTE: This figure is illustrative and does not include all relevant organizations such as service components.

space planners who currently reside at the GCC level would become part of the JF(ASC)CC component. Given the broader mandate, the JF(ASC)CC would expand the current AOC to become a Multidomain Operations Center (MDOC).

The main advantage of this construct is that it would place control or coordination of air, space, and cyber capabilities under one commander, thus likely reducing the number of steps and approvals required for an MDO using capabilities in these domains. Some coordination with USCYBERCOM and USSPACECOM would still be necessary for some space and cyber operations. However, the number of steps would likely be reduced since intra-GCC planning for these domains would take place within a single organization. Arguably, the air component is well situated to take greater responsibility for the space and cyber domains since the JFACC already has SCA and includes cyber operations on its ATO.

Combining these domains would, however, still present challenges given the different timelines, authorities, and considerations for space and cyber. Moreover, it is not clear that MDOs that combine air, space, and cyber are more important to combat outcomes than integration of other domains. The benefits may therefore be limited to integration of air, space, and cyber, as plans and processes involving land and maritime forces would remain the same as they are today.

Reorganization

CCDRs have the necessary authority to create an ASC component, though some coordination with other organizations would be needed to move some personnel. Since some joint billets (e.g., JCC personnel) would move to the ASC component, the CCDR may treat it as a standing joint functional component with the USAF component commander dual-hatted as the JF(ASC)CC. Compared to the incremental-change C2 construct, the ASC-component construct tries to address the space and cyber personnel limitation by centralizing space and cyber planning within one component. As with the incremental-change JADC2 construct, USSPACECOM and USCYBERCOM would need to agree to have their IPEs placed at the component, rather than CCMD, level.

A geographic CCDR could decide to locate JCC staff and space planners within an MDOC to support the JF(ASC)CC.[13] This type of change would also require approval from both USSPACECOM and USCYBERCOM to place the preponderance of their LNOs at the MDOC rather than at the AOC. USSPACECOM and USCYBERCOM may be more willing to send their liaison elements to the new air, space, and cyber (ASC) component rather than dividing up these small elements.

[13] Moving joint organizations in this way is not unprecedented. USEUCOM, for example, has delegated joint target coordination authority to the JFACC and placed its joint target effects cell within the AOC; Steven Schaar, "Joint Targeting Effects Cell Update," unpublished briefing slides, January 24, 2019.

Situational Awareness for Planning, Execution, and Assessment

In the current AOC, the predominance of effort and focus is on the air domain, with space and cyberspace playing important but secondary roles. The AOC has nonkinetic effects planners and some information about space and cyber operations, but far more air-domain experts and greater SA of the air domain.

In this JADC2 construct, an ASC commander would control in-theater space and cyber capabilities. In order to produce an integrated tasking order that tasks these forces and assesses their effects, the MDOC would need much greater SA in the space and cyber domains than the AOC has today. Although ASC would not have operational control over all space and cyberspace assets contributing to the mission, it would likely still need access to relevant information from outside the theater on these two domains.

Planning

In the ASC-component construct, components would continue to plan under GCC guidance. The key changes would be that the ASC component would have more expert space and cyber planners and that the GCC's space and cyber planners, the CO-IPE, and space IPE would sit with ASC's planning staff. During a contingency, ASC would manage targeting for the GCC. The key difference in targeting, compared with the incremental model, is that ASC would have all attached and assigned space and cyber capabilities available for joint tasking.

The main advantage of this construct is that it would place a range of different types of air, space, and cyber experts under one command center, likely reducing the number of steps and approvals for operations in those domains. Today, a JFACC is typically designated by the GCC as an SCA with the responsibility to request and integrate theater-specific space operations and capabilities.[14] A similar arrangement could allow a JFACC to coordinate with USCYBERCOM for cyber operations.

USAF argues that of all the services it is uniquely strategically minded and that it is thus the best suited to exploit the strategic effects of cyber operations, but this is an untested assumption.[15]

The most likely disadvantage of this approach to planning is that it could lead to COAs that do not integrate land and maritime operations sufficiently due to ASC's focus on air, space, and cyber. The absence of a large land and maritime element and the additional steps and approvals required for operations across these domains could lead ASC-component planners to discount MDOs that include the land and maritime domains. Similarly, the land and maritime domains

[14] JP 3-14, 2018, pp. xi, II-10, II-11, III-1, III-6–III-7.

[15] The Air Force defines *airpower* as "the ability to project military power or influence through the control and exploitation of air, space, and cyberspace to achieve strategic, operational, or tactical objectives" (Air Force Core Doctrine Volume I, 2015, pp. 25, 28, 29, 31).

may find it more difficult to gain support from the air, space, and cyber forces that are already working so closely together and are intellectually inclined to favor use of space and cyber forces in support of "strategic" objectives over more operationally oriented objectives that could directly support land and maritime operations.[16] Ultimately, an ASC component could cultivate a multidomain mindset, rather than an all-domain one.

Direction of Forces

Direction of forces in the ASC-component alternative faces similar challenges as it does in the incremental-change C2 construct. Direction and coordination of attached air, space, and cyber forces would be managed through an integrated tasking order modeled on the ATO. The integrated tasking cycle could provide some flexibility by laying out secondary targets and missions, but it will be limited according to the ability of ASC staff to plan for them. To provide synchronization and direction of forward, air, space, and cyber forces would require developing battle management nodes that are able to communicate with all three types of forces. The challenges associated with synchronizing with other components' forces would remain the same as in the incremental-change alternative.

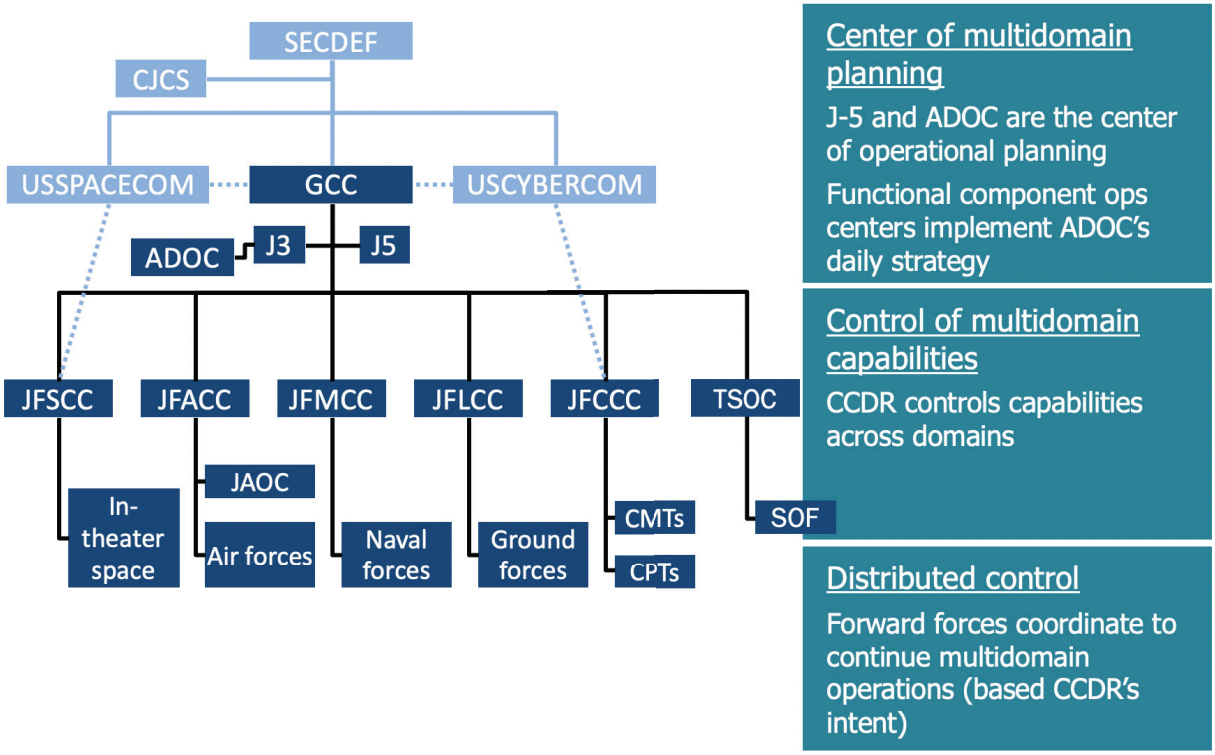
As with the incremental-change JADC2 construct, forward forces would continue MDOs to the extent possible during communications disruptions, with each unit following its respective component commander's intent. However, the gains from having air, space, and cyber forces following a single commander's intent may be marginal in this model as authority to use these capabilities may not be delegated to forward forces.

Combatant Commander–Centric Joint All-Domain Command-and-Control Construct

The next alternative concentrates operational planning at the CCMD level rather than at the component level. This alternative seeks to enable domain-agnostic planning by concentrating experts from all domains in an organization that has a joint, all-domain culture. This alternative also aims to reduce the number of steps and approvals by ensuring that the level of command responsible for planning has the authority to approve most MDOs. As with the incremental-change C2 construct, the CCDR-centric alternative would create new space and cyber components (Figure 9.4). Functional components would implement the CCDR's daily strategy via their own operations centers and would manage tasks such as airspace control.

[16] The Army, for instance, envisions using offensive cyber operations in support of brigade combat team-level operations; Headquarters, Department of the Army, "Cyberspace and Electronic Warfare Operations," *Field Manual*, Vol. 3, No. 12, 2017a, pp. 3-6–3-7, 3-12.

Figure 9.4. Combatant Commander–Centric Command-and-Control Construct



NOTE: This figure is illustrative and does not include all relevant organizations such as service components.

Reorganization

In this construct, the GCC headquarters staff would be significantly larger and would include expert planners from each domain approaching problems as a multidomain team, thereby providing a CCDR enough expertise to develop multidomain plans for all mission areas from the outset. In order to prevent a larger CCMD staff at an all-domain operations center (ADOC) from becoming a single point of failure, its staff may be distributed to multiple operation locations.

Today, USCYBERCOM already provides expert planners to the GCC level, and USSPACECOM has also recently started sending IPEs to some CCMDs. Therefore, the bigger impact would be to the traditional domains and the effective placement of experts capable of conducting more detailed planning at the GCC level. Moving planners to the GCC level would result in a significant reduction in the component planning staff or at least a recurring detail of component planners to the CCDR. For example, many of the planners who currently reside in USAFE-AFAFRICA's planning directorate would work from USEUCOM as air-domain planning experts within a multidomain planning staff. The components and the CCDR could decide if the planners are actually assigned to the CCDR or detailed there for extended tours of duty while remaining aligned from a manpower perspective to their component billets. This change would likely require significant negotiation between CCDRs and the services and, if

new joint billets were created, use of the Joint Manpower Validation process.[17] As with the incremental-change JADC2 construct, this model would also involve the creation of new space and cyber components.

Situational Awareness for Planning, Execution, and Assessment

In the CCDR-centric alternative, the demand for developing and maintaining detailed SA shifts up to the GCC level. Because the GCC staff is engaged more heavily in planning and assessing operations, the CCDR requires more detailed SA across all domains. The ADOC would need to draw on information from both within theater and across all domains, and from USSPACECOM and USCYBERCOM for space and cyberspace, respectively. The ADOC would need to develop this capability while continuing to offer the CCDR a less detailed picture to facilitate his or her decisionmaking. The risk of information overload at the CCMD would likely increase.

Planning

Traditionally, CCDRs, supported by the staff, gain an understanding of the operational environment, define the problem, and develop an operational approach. CCDRs then communicate their operational approach to their staff, subordinates, supporting commands, agencies, and multinational/nongovernmental entities as required in their initial planning guidance so that their approach can be translated into executable plans.[18] In the CCDR-centric C2 construct, a CCDR's planning staff would conduct the COA development process and more of the detailed operational planning than it does today.

The component planning staffs could still support planning for a contingency by conducting some of the detailed analysis to support operational plans, but their efforts would be in support of a CCDR's planning staff rather than an independent step that then requires CCDR staff to merge plans. To implement this construct, doctrine would need to clearly delineate which planning functions (and at what level of detail) would be centered in a GCC's joint directorate for operations (J-3) and J-5 and which would remain the responsibility of components.

In theory, this C2 construct would enable MDOs by ensuring experts from all domains work together to solve planning problems. It may also reduce the number of processes and steps because it would remove the iterative approach used to integrate component-specific planning today. The ADOC could conduct multidomain targeting, which would also reduce the number of steps and approvals for coordinating multidomain engagement sequences. The ADOC would likely play a direct role in production of a JIPTL and assigning forces. As a result, a GCC's ADOC would require robust staff cells for each relevant domain to produce more detailed plans

[17] CJCSI 1001.01B, October 7, 2014.

[18] JP 5-0, 2017, p. V-2.

on a more compressed planning cycle and a mechanism for coordinating and integrating their more detailed planning processes and products.

Given the amount of planning currently conducted at the component level and below, concentrating planning at the GCC level could be quite challenging. The potential pay-off, however, could be domain-agnostic planning and more efficient allocation of capabilities to achieve a CCDR's objectives. A potential downside is that this approach would reduce the degree to which the components could independently plan and execute operations, which, in turn, would reduce C2 resiliency. This approach may also tend to undercut efforts to prepare forward forces for distributed control by making tactical units more dependent on centralized planning processes.

Direction of Forces

The CCDR-centric C2 construct starts from a position of developing integrated multidomain plans. These plans convey a commander's intent to subordinate units. The synchronization of effects starts in the planning phase, but an MDO requires execution of operations in each domain often with precise timing to ensure that effects in one domain support the effects in another. To do this, the ADOC would need to be able to communicate with all-domain battle management nodes with the capabilities to communicate with multidomain forces.

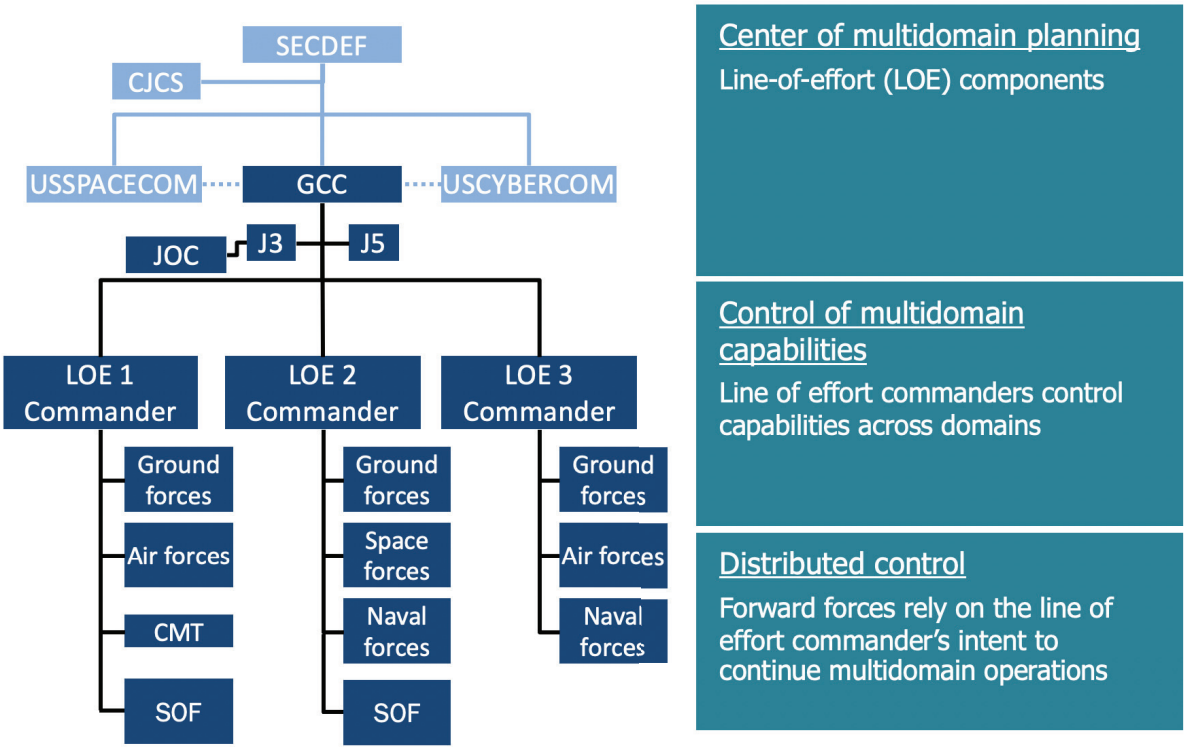
During periods of severe degradation, forward forces would continue an MDO based on the commander's intent from a single CCDR. This could potentially enable better coordination than the previous two models, which filter a CCDR's intent through functional component commanders.

Line-of-Effort Joint All-Domain Command-and-Control Construct

The final alternative for consideration organizes components around LOEs instead of domains. Instead of using functional components, the CCDR would designate a few key missions and assign a commander and forces to each (Figure 9.5). For example, there could be a component for degrading and destroying IADs and ensuring access in the theater, another for stopping invading ground forces, and another for stopping an amphibious force. Each LOE may not have forces from all domains due to limited resources, but each would likely have forces from multiple domains to achieve its assigned mission. In the LOE-component JADC2 construct, the seams between different components are based on different objectives or missions, rather than domains. This is a major change from the domain-based organizations usually seen in U.S. military operations, but one that is inspired by the unique C2 construct for AMD. Moreover, military officers across the joint force are familiar with the concept of LOEs, which are often discussed in operational art and planning.[19]

[19] JP 5-0, 2017.

Figure 9.5. Line-of-Effort-Component Command-and-Control Construct



NOTE: This figure is illustrative and does not include all relevant organizations such as service components.

The GCC level would retain coordination with other CCMDs for space, cyber, and SOF capabilities. The service components would likely be designated leads for different LOEs in addition to some of their traditional responsibilities. The USAF component, for example, would still provide overall airspace management and area air defense coordination.

As in the CCDR-centric concept, a single commander would be able to conduct multidomain planning and make decisions to execute an MDO. At the same time, though, the LOE-component construct would use operational-level components to give CCDRs a more reasonable span of control. A key disadvantage to this alternative is that it decentralizes control of forces from the same domain, thereby making it more difficult to redistribute forces among LOEs.

Reorganization

Creating LOEs rather than functional components would be within the scope of power granted to a CCDR by 10 U.S.C. 164.[20] While current doctrine does not proscribe an

[20] CCMDs have created LOE-focused C2 structures in operations, such as the Multi-National Security Transition Command-Iraq. Moreover, doctrine notes that JTFs can be formed on a functional basis to accomplish missions or to address security challenges that cross AOR boundaries or multiple noncontiguous areas. JP 3-0, 2017, 2018, pp. IV-5–IV-6.

LOE-centric C2 approach, it also does not provide much guidance as to how it could be put into practice. Doctrine would need to be updated to provide guidance on what missions are most appropriate for LOE-centered C2 organizations, how a GCC might choose which and how many LOEs to create, how to organize the internal structure of an LOE-centered C2 organization, how to allocate and balance resources among the LOEs, and how such C2 organizations would interact with each other or with service components.

The GCC would need to delineate the supported and supporting relationships among various LOE components to ensure they were executing their mutually interdependent operations in a coordinated and mutually supportive way. The GCC would also need to provide a mechanism for adjudicating among the competing objectives and requirement demands of the various components.

This approach, however, would require much more than a few new doctrinal publications. It would require a cultural change in how a GCC organizes the joint force to plan and conduct operations. GCCs would also need to regularly organize and train along these lines in order to be effective in combat, and would require the service components to cede some responsibility for operational-level organization and training to LOE-focused components. If the GCCs were not organized along LOEs during peacetime, procedures would need to be in place to transition to such a structure as necessary during a contingency as well as to provide the personnel required to fill out the necessary LOE-oriented joint operating centers.

Situational Awareness for Planning, Execution, and Assessment

As with today's components, each LOE component would have its own operations center which would help its commander gain SA. In order to plan, execute, and assess multidomain operations, these operations center would need information on multiple domains. The LOE commander would have OPCON of some ISR assets, but the CCMD J-2 would still need to prioritize LOE component requests for national-level capabilities. Where the CCDR-centric construct centralizes these functions, the LOE-component construct would have multiple operations centers attempting to gain SA in the same domains. As a result, there would likely be some amount of duplication in systems and larger staff sizes. This could be both a strength and a weakness of the LOE-component construct. On the one hand, having multiple operations centers would be more resource intensive, but the duplication could also be a source of resiliency in a conflict with a near-peer competitor that would likely see both kinetic and nonkinetic attacks on headquarters.

Planning

When planning for a contingency, a GCC J-5, with guidance from its CCDR, would work to develop an operational-level view of key missions in the potential conflict and would plan to assign forces along LOEs in order to carry out these missions. The CCDR would set clear priorities among lines and would also set conditions under which forces from one LOE could be used to assist another line.

Planning for a contingency could take place within a GCC, with planning teams within J-5 organized around LOEs. Alternatively, a GCC could make service component commanders dual-hatted as LOE commanders and have them conduct prewar planning for their LOE. In doing so, the GCC would need to ensure that each component's planning staff was significantly expanded to include expert planners from the domains that LOE-component commanders would likely employ.

During a contingency, each LOE-component staff and operations center would conduct planning for the assigned mission area. Each LOE commander would decide how to allocate his or her assigned forces as conflict unfolded and would oversee multidomain targeting. The LOE components would only have to submit requests for support from other CCMDs (e.g., USCYBERCOM, USSPACECOM) or GCC components.

A CCDR would, of course, have the authority to move forces among LOE components over the course of a campaign, but would probably try to minimize the changes for reasons discussed in more detail in Chapter 10. As a result, the planning processes envisioned in the LOE-component alternative may have less efficiency and flexibility than the CCDR-centric C2 construct.

Direction of Forces

In an LOE-component C2 construct, the direction of forces apportioned to a particular LOE is likely to function similarly to the CCDR-centered model, but on a smaller scale. Each LOE component's operations center and multidomain battle management nodes would monitor execution. Like the others, this C2 construct would face challenges to directing forces in a communications-contested environment.

The LOE construct would have the advantage of smaller sets of forces working with one another over time, which could help ease coordination and communication when it is not possible to interact with higher command. Smaller, more focused teams could be more resilient in the face of communications disruptions than other organizational alternatives.

Comparison of Alternative Joint All-Domain Command-and-Control Constructs

This section summarizes the similarities and differences in how the four JADC2 constructs approach key C2 functions of gaining SA, planning, and directing forces.

Situational Awareness

All four JADC2 constructs would need new investments to enable SA. MDO concepts will likely require investments that include data links, software or software applications, visualization

tools, and communications networks, to name just a few.[21] Some of these initiatives may be useful regardless of the JADC2 construct. However, as Table 9.1 shows, the constructs have different implications for the number of operations centers that need SA in all domains.

Table 9.1. Situational Awareness Approaches in Alternative Command-and-Control Constructs

C2 Construct	Approach	Trade-Offs	How to Make the Change	Potential Challenges to Change
Incremental change	All functional component operations centers have capability to gain sufficient SA in all domains to generate multidomain options.	More users of information in each domain may overwhelm information providers; sensitive information may be accessible to more users.	Services invest in common data and reporting standards and invest in systems that provide tailored information; global CCMDs provide more information to GCC component operations centers.	Services may not agree on standards and systems; global CCMDs may be reluctant to share information with so many operations centers.
ASC component	In addition to changes noted for the incremental-change construct, the ASC component has detailed information on air, space, and cyberspace to plan, execute, and assess MDO in three domains.	Information needed for detailed planning and execution with land and maritime domains still requires coordination among multiple components.	Services invest in common data and reporting standards; USAF develops systems to integrate and present data for the air, space, and cyber domains at multiple classification levels.	Land and maritime components may seek greater integration of cyber and space into their components.
CCDR-centered	Terrestrial GCC headquarters integrates multidomain data and information into a multidomain COP.	Construct relies on accurate, timely information flows from components to the CCDR in communications-contested environment.	Establish manpower validation for increased staffing of a CCDR with requisite clearances and skills; implement systems to integrate and process data and information.	CCMD may not receive enough joint billets to manage detailed COP.
LOE components	Each LOE component has the capability to gain SA to plan and execute MDO.	Demand for information to originators from multiple LOE components increases.	Implement systems to integrate data and information at multiple LOE headquarters; develop training and exercises during competition phase to prepare for gaining SA in LOE operations centers.	Service components may be reluctant to organize around LOEs.

[21] For ongoing initiatives, see, for example, Kessel Run's work on software development for the AOC; Mark Pomerleau, "How the Air Force's New Software Team Is Proving Its Worth," *C4ISRNET*, January 14, 2019. The shadow AOC can also be a test bed to demonstrate the potential value of new command systems through experimentation and exercises. James Drew, "USAF Standing Up Shadow Ops Center at Nellis AFB," *Aerospace Daily*, November 17, 2017.

Planning

The four alternatives place responsibility for multidomain planning in different organizations (Table 9.2). The incremental-change and ASC-component constructs aim to overcome impediments to multidomain planning by ensuring that expertise from all domains is available to generate multidomain options. The CCDR-centric and LOE-component constructs go further by conducting planning in organizations designed to be multidomain rather than organized around a functional component. Moreover, these constructs aim to reduce the number of steps and approvals associated with an MDO by ensuring that the same organization that plans also controls forces in multiple domains and can approve planned operations.

Table 9.2. Planning for a Contingency in Alternative Command-and-Control Constructs

C2 Construct	Approach	Trade-Offs	How to Make the Change	Potential Challenges to Change
Incremental change	Include expert planners from every domain in each component planning staff.	Manpower intensive	Seek CCDR decision and agreement from services, components, USCYBERCOM, and USSPACECOM.	Insufficient expert planners available; reluctance by USCYBERCOM and USSPACECOM to distribute IPE staff to components.
ASC component	Integrate air, space, and cyberspace planning functions.	Prioritizes space and cyber integration with air operations but not land and maritime.	Move GCC space and cyber planners to ASC component; gain support from USCYBERCOM and USSPACECOM to move IPEs to the component level.	Objections by land and maritime components to integration of space and cyber with air; ASC staffing not resources to degree needed.
CCDR-centric	Expand GCC J-5 to create an all-domain planning staff capable of conducting detailed operational planning.	Requires significantly more planning capacity at the GCC level than currently exists; trade-offs in staff between GCC and components.	Validate manpower and systems requirements for the GCC.	Desire by services to retain planning staff at component levels; may not achieve; requires new planning systems at joint level.
LOE components	Implement multidomain planning based on pre-identified LOEs for large-scale contingency operations.	Trade off with current component-level planning for theater campaign and partnership capacity building.	Assign LOE lead to service components; validate any additional manpower and system requirements.	Reluctance of service components to take on LOE-focused approach.

Directing Forces

The direction of forces would differ in the C2 constructs (Table 9.3). As with planning, the most significant changes come with the CCDR- and LOE-component C2 constructs. Directing forces from a CCMD-level ADOC would mean a dramatic change in focus for that echelon from

strategic and broad operational concerns to operational details. Directing forces in multiple domains from an LOE-component operations center would also be a significant shift from today's practice, in which operations centers focus primarily on a single domain.

Each of the four approaches we examined in this chapter has the potential to improve C2 for planning and executing MDOs. CCDRs have significant authority already to organize and direct their command's approach to preparing for and operating in contingencies, but there are areas as we have described above where doctrine or authorities are just the beginning of the story. Manpower, training, exercises, and new systems would be needed to implement these changes. Whether one of these alternatives carries greater promise for achieving the vision of MDOs is the subject of the next chapter.

Table 9.3. Direction of Forces in Alternative Command-and-Control Constructs

C2 Construct	Approach	Trade-Offs	How to Make the Change	Potential Challenges to Change
Incremental change	Component operations centers retain primary direction of forces, role; the CCDR intervenes as needed.	Requires accurate and timely SA and operations assessment to inform changes to execution from the CCDR.	No changes to authorities or doctrine are likely to be needed.	None
ASC component	ASC provides direction of attached and assigned air, space, and cyber forces through ASC battle management nodes. Other components use traditional tactical C2 structures.	Focuses only on synchronization of space and cyber with air.	USSPACECOM and USCYBERCOM delegate TACON to ASC.	Global CCMDs' wish to retain OPCON/TACON of space and cyber forces.
CCDR-centric	All-domain battle management nodes synchronize execution of operations; the CCDR intervenes as needed.	Complicates maintaining synchronization of effects across domains in communications-contested environment.	Deploy all-domain battle management nodes to ensure synchronization of effects.	Ensuring sufficient robust communications to battle management nodes and to national assets.
LOE components	LOE battle-management nodes synchronize multidomain effects and support transfer of TACON for time-sensitive targets.	Creates risk of uncoordinated action with other LOEs.	Deploy all-domain battle management nodes to ensure synchronization of effects.	Ensuring sufficient robust communications to battle management nodes and to national assets.

10. A Framework for Assessing Alternative Joint All-Domain Command-and-Control Concepts

The joint force's focus on the JADC2 indicates a belief that improved integration across domains will substantially improve operational performance. There are, however, challenges in predicting the impact of a C2 construct on combat outcomes. Combat outcomes are determined by many factors, including political decisions, operational concepts, military leadership, the performance of operators, planners, supporting forces, military systems, and how the adversary acts and responds.[1] Even the best C2 construct will face the enduring problems of fog and friction. In spite of these challenges, additional experimentation with and analysis of alternative C2 structures could help military leaders better assess which C2 structure is likely to be most effective in wartime and to weigh other costs and benefits.

In this chapter, we propose seven criteria that the joint force may wish to consider as it evaluates alternatives.[2] We propose asking whether each construct will allow the joint force to conduct cross-domain planning, monitor how operations unfold in different domains, and evaluate operational effectiveness; whether a commander has too many direct reports or responsibility for too many missions; how difficult it is for peacetime staff to create wartime operations centers; whether a commander can redistribute forces within the area of operation; how well a command construct handles communications degradation or disruption; how well the command construct leverages existing organizations and processes; and how difficult it would be to implement the command construct.

Comparing alternative C2 structures will require rigorous assessment of each of these dimensions through exercises and additional analysis. This chapter provides initial thoughts about how the four alternative C2 constructs compare as a starting point for more in-depth assessment in the future.

[1] For example, see the discussion of the importance of the commander's personality and style on outcomes in Deployable Training Division, 2016.

[2] Our list focuses on areas where our proposed MDC2 alternatives appear to differ. The joint force could also consider more general criteria for evaluating C2 structures. For example, past RAND research has proposed evaluating on the versatility of the C2 structure for multiple types of contingencies; Alkire et al., 2018. For other general criteria for GCC C2 structures, see Deployable Training Division, 2016.

Facilitates Planning, Execution, and Assessment of Multidomain Operations

The first criterion we consider is how well a C2 construct impacts the joint force's ability to conduct an MDO. If we think that increasing collaboration across domains will improve military outcomes, then we should build a C2 construct that facilitates these operations. Does the construct allow the joint force to conduct cross-domain planning, monitor how operations unfold in different domains, and evaluate operational effectiveness? To determine whether a C2 construct meets this criterion, we ask how each C2 construct addresses the impediments identified above, such as lack of expertise in and SA in multiple domains and greater numbers of steps and approvals for MDOs.

Of the four alternatives, the incremental-change construct would likely perform the worst on this criterion. Adding additional liaisons would help improve information sharing among components and may make more planning expertise available for generating multidomain options. However, the overall C2 structure would still be organized around domains, and functional components would likely be staffed primarily by personnel from that domain. A relatively smaller number of liaisons from other domains is unlikely to fundamentally change how domain-based components plan, monitor, and assess operations.[3] As a result, each component may continue to have more of a single rather than multidomain mindset. Moreover, the incremental model would not reduce the number of steps and approvals for MDOs compared with single-domain operations, notwithstanding the fact that increased (and, perhaps, more routinized) liaison communications may help complete some steps in RAPs slightly faster.

The air, space, and cyber–component construct would offer some improvements to multidomain integration. Planning air, space, and cyber operations would likely involve fewer steps than in the past since a JF(ASC)CC would have the authority to decide how to apply assigned and attached air, space, and cyber capabilities based on his or her CCDR's intent. A JF(ASC)CC would also have direct liaison authority with USSPACECOM and USCYBERCOM. However, the focus on integration of only three domains may prevent the joint force from fully realizing all-domain integration.

The CCDR-centric construct would likely be the best of the four at all-domain integration, as it brings together all five domains under one organization that can both plan and approve MDOs. With experts from all domains and systems to monitor them, the ADOC would be able to plan for truly MDOs, oversee them, and assess their performance. Since planning and decisionmaking would all take place in one organization, the processing of request, review, and approval steps

[3] LNOs can provide information and expertise about their domain, but without having the ability to move or assign forces, their influence on operations is rather limited. For a discussion of the limitations of the JACCE in operations, see James C. Cooper, *The Joint Air Component Coordination Element: Middleman, or an Effective Airpower Broker?*, Newport, R.I.: Naval War College, May 4, 2012.

for most kinds of operations across domains would be facilitated. A CCDR-centric construct may also be more likely to foster an all-domain mindset than a construct built around functional components.

Similarly, in the LOE construct each LOE component would have expertise in and SA of each of the domains. An LOE commander would also have the authority to approve multidomain plans using forces under his or her control. However, unlike the CCDR-centric construct, each LOE commander may not have forces from all domains. As a result, additional steps and processes might be needed in the LOE construct to gain support or have forces redistributed from another LOE. LOEs would also have to work through the GCC level to coordinate support for space, cyber, and other capabilities outside the GCC.

Has Reasonable Span of Control for Operational Commanders

Having too many direct reports or responsibility for a large number of diverse missions can detract from a commander's ability to make good decisions.[4] Similarly, having a large headquarters can create inertia and communication challenges and thus decrease operational effectiveness.[5] As a result, changes to C2 structures that create excessive span of control for CCDRs or component commanders could undermine effectiveness.

All four of our alternatives increase the span of control of either the CCDR or one of the component commanders, as every one brings more space and cyber capabilities and thus the need to plan, monitor, and assess their use. The incremental alternative would not create as much of a change in span of control, because the presence of additional liaisons from other domains would not likely have a large impact on GCC-level or component-level commands.

For the air, space, and cyber construct, a JF(ASC)CC would experience a significant increase in his or her span of control due to the additional in-theater space and cyber forces, growth in MDOC staff, and added responsibility for coordinating with USCYBERCOM. A CCDR's span of control would decrease to some extent as cyber and space staff functions move to the ASC component. Other component commanders would not have any change in their spans of control.

The CCDR-centric construct, which fared well on the first criteria, scores worse on span of control. Today, the CCDR provides guidance on and monitors operations in all domains, but has component commanders who have responsibility for operational planning, execution, and assessment. In the CCDR-centric model, the CCDR, his or her staff, and the ADOC would take on all of these functions for all domains. The CCDR would therefore have a greater span of

[4] Alkire et al., 2018, pp. 17–18; JP 3-30, 2019, p. II-1. Interestingly, the term *span of control* is not defined in the Joint dictionary. Span of control can also be affected by qualitative factors such as similarity in subordinates' functions; William G. Pierce, *Span of Control and the Operational Commander: Is It More Than Just a Number?*, Leavenworth, Ka.: School of Advanced Military Studies, September 12, 1994.

[5] Deployable Training Division, 2016.

control than in any of our constructs, which could be problematic given the CCDR's existing responsibilities.

The LOE-component construct's implications for the CCDR and component commander span of control is indeterminate in the abstract. This construct could potentially increase or decrease the CCDR's span of control, depending on the number of LOEs compared with the number of components today. That said, LOEs would take over some operational planning tasks from the CCDR. For example, each LOE would have its own targeting and collection management processes, so an LOE commander rather than the CCDR would be responsible for approving the JIPTL and the joint integrated prioritized collection list. As with the CCDR level, the number of subordinate units in each component LOE would depend on the number of LOEs. At the same time, though, organizing around LOEs could also focus each component on a narrower range of objectives than today's functional components have to consider.

Minimizes Organizational Transition from Peacetime to Wartime

In the event of an escalating crisis with a near-peer competitor, a GCC may have to rapidly transition from steady-state operations to a contingency.[6] For all of the alternative C2 constructs, staffing of all operations centers would likely expand in the event of a contingency.[7] There are, however, differences in the *type* of change a staff would experience in the four alternatives. Changes in roles and assignments create discontinuities that require staff adjustment that can slow processes, sow confusion, and decrease operational effectiveness. Therefore, all things being equal, a lesser organizational change between peace and war is preferable.

The number of cross-component liaisons would expand in the incremental-change JADC2 construct, but the transition from peacetime to wartime would otherwise look very similar to the baseline. Likewise, we assume that the air, space, and cyber component would be a standing organization prior to a contingency and that it would also need to augment staff, but it would not experience additional disruption as the MDOC moves to conflict.[8] If, however, the air, space, and cyber was not standing prior to conflict, then the transition would be more significant as space and cyber planners and liaisons moved from the GCC level to the ASC component for the duration of the contingency.

---

[6] There are concerns that building and/or augmenting C2 organizations once a contingency arises is detrimental to operational effectiveness. For example, in the early 2000s there was a drive to create standing JTFs to reduce or eliminate the need to create headquarters staff during a crisis. For example, see Charles A. Flynn, *Standing Joint Task Force Headquarters: Creating Opportunities from Chaos*, Norfolk, Va.: Joint Advanced Warfighting School, May 15, 2006. This is consistent with the joint staff C2 consideration of responsiveness; Deployable Training Division, 2016.

[7] Interviews suggest that AOC staff are already stretched by the workload for steady-state operations, so the high pace of contingency operations would require a significant number of augmentees.

[8] Of course, this would depend on the number of augmentees. The more augmentees, the greater the disruption as they are integrated into the MDOC.

Similarly, the CCDR-centric alternative is also likely to transition well from peacetime to wartime if an ADOC were set up prior to hostilities. However, having a standing ADOC would require service components to either cede billets to the CCDR level or to rotate personnel periodically to the ADOC. If the services did not support a larger number of joint billets or rotations in peacetime, then building up CCDR staff and the ADOC for a contingency would be a more significant transition.

In contrast to the first three constructs, the LOE-centered approach could face a considerable transition as it moves from peace to war, assuming no change from today's peacetime structures. If a CCDR has to wait until a crisis breaks out to determine which LOEs he or she wants to organize around, there might be little continuity between peacetime staffs and wartime staffs. One way to mitigate this transition challenge would be to engage LOE components in large-scale exercises. In this construct, contingency plans for conflict with a near-peer competitor would delineate LOEs and the forces likely to be assigned to each of them. These plans would have to be adapted to the specific contingency that emerges, but peacetime relationships and exercises could offer a way to make a wartime transition less dramatic, especially for LOEs that would be relevant in multiple possible contingencies.

Allows Redistribution of Forces Within the Geographic Combatant Command as Priorities Change

To capitalize on opportunities and to change course as priorities shift, the joint force needs to be able to redistribute forces geographically and against different missions and tasks.[9] Constructs that ease redistribution are therefore preferable to those that hinder or impede operational agility. Centralized control tends to make redistribution simpler, which is why USAF generally makes its forces available for joint tasking and prefers to task all of its forces within a theater through a single ATO. Reallocating forces to new missions in the current construct can be undertaken by changing the CCDR's guidance on allocation in the joint targeting process. Redistribution is more difficult in the ground and maritime domains due to fundamental differences in these domains as well as to C2 choices.[10] In the ground and maritime domains, component commanders generally use their forces for their components' assigned tasks. A CCDR can establish support relationships with other components and can intervene if these are not upheld, but will likely do this only by exception due to limited SA and other limits on staff and time. The

[9] Joint doctrine discusses how forces are assigned, apportioned, and allocated. In each case, commanders are setting goals and designating forces to meet them. To cover all three of these activities, we use the term *redistribution*. See JP 5-0, 2017, p. III-10. For an air-based application of these terms, see JP 3-30, 2019, pp. III-19–III-26.

[10] Not all forces can be equally allocated. For example, it is easier to retask aircraft from one geographic area to another (conduct SEAD in location B instead of location A) than it is to retask ground forces, which move more slowly.

incremental-change and ASC-component JADC2 constructs would preserve the ability to reallocate centrally controlled air forces as well as fungible cyber and space capabilities.

The real difference in the ease of distribution emerges between the CCDR-centric and LOE-component JADC2 constructs. We would expect the CCDR-centric construct to be the best of the four alternative JADC2 constructs on this dimension. Since the CCDR would not be operating through components, but would retain control of forces in all domains, his or her ADOC would be able to redistribute the forces the CCDR controls across the entire area of operations and against different operational needs, constrained only by the flexibility of these forces and operational conditions.[11]

In the LOE-component construct, forces would be assigned to components rather than centrally controlled, and these components would be empowered to use these forces to accomplish assigned missions. The CCDR would therefore have a smaller staff and less focus on operational planning compared with the CCDR-centric construct. Just as the CCDR may be reluctant to frequently intervene in how component commanders use assigned force in the baseline and incremental C2 constructs, the CCDR may be reluctant to move forces among LOEs.

Enables Unity of Effort During Communications Disruptions

Command centers need to be able to avoid or, if that is not possible, mitigate the impact of disruptions in communications during an operation. Lower echelons and fielded forces will likely prepare for communications disruptions by establishing procedures to meet a commander's intent without direct oversight. In any of the C2 constructs, commanders may decide to use a C2 philosophy of mission command, providing forward forces with clear understanding of commander's intent and giving them greater autonomy to determine how to carry out the mission. Doing so even when communications are reliable could not only help to manage fast-paced and complex operations, but also prepare forward units to take over when communications are severely degraded. Even if not used throughout the conflict, some form of distributed control would be necessary if communications are severely degraded.[12]

That said, all of the C2 concepts would face challenges in distributing control for space and cyber operations. If communications with higher headquarters are degraded, long-distance communications with space and cyber assets from outside the GCC may also be degraded. Still, if technology made it possible, a presidential or SecDef order could potentially allow some space and cyber authorities to devolve to forward forces during severe communications disruptions.

[11] The baseline conditions and requirements associated with requesting non-GCC organic assets and obtaining the necessary review and approval of the request would still apply, however.

[12] Mission command has traditionally been associated with ground and maritime forces. For a discussion of mission command and its applicability to air operations, see Harvard, 2013; Priebe et al., 2019.

However, given centralized control of these capabilities today, such a change is by no means assured.

Beyond space and cyber, each of the constructs has different implications for how forward forces receive their commander's intent and how well they may be able to carry out MDOs when communications are degraded for significant periods. In the incremental alternative, lower command echelons and fielded forces would follow their domain-based commander's intent. Although component commanders are all operating under the broad guidance of the CCDR in the incremental C2 concept, each component commander would translate this into more specific guidance for subordinate units. As a result, forward forces from different domains may receive different variations from higher headquarters. The longer the period of degraded communications with higher headquarters, the more difficult it may be for forward units from different domains to coordinate and agree on how to continue an MDO. As a result, unity of effort may be undermined.

The ASC-component concept could potentially improve unity of effort among the air, space, and cyber domains, if authorities were pushed forward pursuant to national-level approvals. In that case, air, space, and cyber forces attached or assigned to a GCC would be following JF(ASC)CC's intent. To the extent that local communications allowed coordination, these forces could be able to achieve unity of effort since they would be following a single commander's intent.

The CCDR-centric alternative, which features the ability to plan across all domains, offers a better chance for forces from all domains to establish working relationships that might endure through degraded or disrupted communications. A CCDR-centric operation would allow lower-level C2 organizations and fielded forces more direct access to the CCDR and staff and could increase the extent to which they understand the CCDR's intent. Moreover, all forward forces would be operating under the same commander's intent.

The LOE construct would have the advantage of smaller sets of forces working with one another over time, which could help ease coordination and communication when it is not possible to interact with higher command. Smaller, more focused teams could be more resilient in the face of communications disruptions than other organizational alternatives.

Leverages Existing Organizations and Processes

The perfect C2 construct, if there were one, would be useless if it was not possible to create and sustain it. Building around established organizations eases transition to a new C2 construct by increasing the likelihood of having experienced personnel as well as tested and refined processes. The incremental-change and ASC-component alternatives use many existing organizations and processes and therefore are easiest to implement.

The CCDR-centric construct would require much more significant change. The JOC, which would be the basis of the ADOC, does not currently undertake the kind of detailed operational planning that the CCDR-centric construct envisions. Establishing an ADOC at the combatant command level would therefore require creating a host of new and untested practices and would bring together staff in new ways.

The most discontinuity would be evident in the LOE-component alternative, the most novel of the constructs. LOE operations centers may build on existing C2 nodes, such as an AOC. Still, turning these into all-domain operations centers would require significant investments in systems and processes capable of gaining multidomain SA and conducting multidomain planning. Depending on the number of LOEs, this could be more costly and require more personnel than the other constructs.

Can Gain Joint Support

Implementing new C2 constructs will entail a range of challenges, including changes to authorities, increasing costs, disruption to established processes, personnel shortages, and cultural biases. Here we highlight a specific implementation challenge: building support for change. C2 constructs that move resources away from the services or change how they organize, train, and equip responsibilities, for example, may provoke greater resistance.

In the incremental-change model, the services would need to provide more personnel for liaisons to each component command, but this would not dramatically increase costs, change C2 processes, or alter the role of the services.[13] In contrast, the air, space, and cyber alternative may generate more resistance. The other services may resist giving USAF the enhanced authority over, and operational responsibility for, space and cyber planning due to resource implications. Moreover, the other services may worry that the historical focus on air operations may bias how these capabilities are used. The Army's concept for multidomain task forces envisions organic space and cyber capabilities, which could be incompatible with this C2 construct.

The CCDR-centric approach would likely face resistance from all of the services. This construct would require a significant shift of personnel from service to joint billets or extended periods of temporary duty for component personnel at CCDR headquarters, new planning practices, and even new facilities, systems, and communications equipment for CCDRs. Such a shift would represent a major cultural change in the joint force C2s operations, as it represents a move from service- and domain-based components to an increasingly centralized C2 operation. As we mentioned above, some of the personnel shifts could be temporary, but even with mitigations like this, there would be a shift of resources and power from the services to joint organizations.

Organizing around LOEs could also meet resistance from the services. Preparing personnel to lead and work in LOEs instead of domain-based components would require significant changes in leader development, training, and service culture. Today, warfighting takes place in a joint context, but below the GCC or JTF level, organizations are largely based on a single service. For example, the AOC is augmented with staff from other services to become a joint

[13] Adding LNOs will require that they be validated by the Joint Manpower Validation process and that the services accommodate this in their program objective memorandums; CJCSI 1001.01B, 2014.

AOC to conduct joint air operations. However, the core of the air component and the AOC still remains USAF. In the LOE-component construct, some LOEs may still be dominated by a single service. However, others may be truly joint. In order to prepare more personnel for joint and multidomain planning and leadership positions, the services may need to spend more time on joint training and education and less time on service-specific programs.

Conclusion

The analysis in this chapter highlights some of the potential trade-offs associated with alternative C2 constructs (see Figure 10.1). We would remind readers of this report that our

Figure 10.1. Preliminary Assessment of Trade-Offs Associated with Alternative Joint All-Domain Command-and-Control Constructs

NOTE: This figure provides a notional depiction of how we might assess the different command constructs across our criteria. Green suggests a high performance on the criteria, orange a moderate performance, and red a poor performance. The colors reflect a preliminary assessment. To conduct a more rigorous assessment, we would need to observe structured command-post exercises, and real-world operations, as well as other data and methods.

assessment is preliminary and needs to be augmented with observations from experiments, exercises, modeling, and, ultimately, actual use in combat operations. As this type of analysis goes forward, it is important to remember that each of the seven criteria in our framework are not equal. As a result, this framework should be used only as a starting point for joint force discussions about the trade-offs associated with alternative approaches to the JADC2.

Different expectations about the nature of future military operations could impact perceptions of which construct is best. For example, if one assumes that the joint force will gain a great deal from enhancing its ability to work across domains, it might make sense to turn to the CCDR alternative, which places C2 of all domains in the same place. The gains from becoming "more multidomain" would need to outweigh the disruption entailed in departing from current C2 constructs. If one assumes that the gains from working across domains are low, then it might make more sense to focus on the incremental alternative, which adds a limited ability to work across domains, but would not entail significant costs or disruption to the C2 enterprise. If one judges that there are significant gains to be realized from linking air, space, and cyber, but not ground and maritime operations, the ASC alternative would be more attractive.

Aspirations for the JADC2 are high, but resources are finite. Each of the alternatives we discuss calls for increased planning, monitoring, and assessment capabilities and would likely require additional personnel both in peacetime and during a contingency. With resource constraints looming large over the joint community, it is unclear where these resources are likely to come from. To progress, the joint force would do well to experiment, exercise, and implement change over time. Experimentation and analysis will help build greater understanding about the costs and benefits of different C2 structures and about their impact on operational performance. To realize the potential of MDOs, the joint force will need to undertake a long-term program that includes intermittent assessment of gains and risks to operational effectiveness.

11. Conclusion

The services and the joint force are developing new concepts for MDOs with the aim of improving warfighting effectiveness in military operations against a near-peer adversary. More work remains to be done before we know what types of MDO concepts and C2 changes may help achieve that goal. In this report we have offered an assessment of some of the potential C2 impediments to multidomain integration generally, as summarized in Chapter 8. We do not recommend specific doctrinal or authorities changes to facilitate the JADC2 since MDO concepts are still emerging and more experimentation and analysis are needed. Moreover, we do not consider the additional complexities of the JADC2 in a multinational coalition. However, in Chapter 9 we have presented options for changes to the overarching C2 construct as well as specific changes to doctrine and authorities, and we have presented a framework for evaluating these options in Chapter 10. This chapter summarizes our findings on the future of the JADC2 and recommends next steps as USAF and the joint community continue to develop MDO and JADC2 concepts.

Findings

Specific MDO concepts are still emerging, so their impact on warfighting effectiveness and implications for the JADC2 are not yet clear. While armed forces have long integrated operations in multiple domains, new applications of MDOs are in their infancy. The joint force is just beginning to sketch out tactical-level applications, such as using air-based F-35s as sensors to cue ground-based GMLRs. ACC and TRADOC are experimenting with tactical-level links that make these operations possible. As more such concepts are developed, it may become clearer what types of C2 changes are most needed to enable them. There are those who argue that implementing MDOs will result in a significant increase in joint force effectiveness. If these claims bear out, then it may be worth making significant changes and accepting some additional risks to adjust C2 structures to facilitate the JADC2. However, if the benefits are more marginal, then making major changes to the C2 structures that the joint force has used in combat may not be worth the significant risk.

Emerging C2 concepts for conflict against a near-peer competitor are in tension. As discussed in Chapter 9, the joint force faces multiple C2 challenges in a conflict with a near-peer competitor. Any comprehensive C2 construct will need to account for the possibility of transregional conflict, contested communications, and the need to plan and execute MDOs. The desire to retain some authorities outside the GCCs to manage priorities globally and keep consequential decisions at the strategic level may, in some cases, be in tension with the

need to integrate more quickly across domains or delegate authorities to forward forces during communications disruptions.

Some potential C2 impediments to MDOs result from the current legal and regulatory framework and thus cannot be resolved through changes to doctrine. U.S. forces must comply with a large and complex regime of legal and regulatory authorities that dictate how they conduct themselves both in peace and in war. As discussed in detail in Chapter 3, many of these authorities are potential impediments to GCC MDOs. Given this current legal and regulatory framework, it is not possible to overcome all potential C2 impediments to MDOs through CCDR decisionmaking, changes to doctrine, or new communications systems. Such changes will not overcome statutory and regulatory requirements to submit requests and approvals for nonorganic assets or capabilities, deconflict requests with IC partners, or clear certain types of operations that have a global, civilian, or diplomatic effect with either the SecDef or the president. Removing some of the additional steps and processes to facilitate MDOs would likely require substantive changes to both Titles 10 and 50 or a significant reassignment/redistribution of assigned forces and powers among the 11 existing CCMDs. The former would require new legislation to pass both houses of Congress and be signed into law by the president. The latter would require alterations to the UCP, which, although within the authority of the president, may also be difficult to obtain. As discussed in the next finding, there may also be significant downsides to such changes.

Reducing the number of steps and approvals for MDOs may require accepting less efficiency and more risk. Integration of more domains often increases the number of steps and approvals to plan and execute a mission. Within a GCC, an MDO that involves forces from multiple components requires approval from multiple commanders and could even require CCDR intervention to adjudicate disputes. An alternative approach, such as the LOE-component C2 construct, which gives a single operational planner forces from multiple domains, may reduce the number of steps and approvals. However, it could also make it more difficult to reallocate forces and efficiently manage forces in a single domain.

For space and cyber operations, additional steps and approvals are due, in part, to decisions to centralize allocation of scarce resources efficiently across global priorities or to make potentially consequential decisions at a high level. Giving GCCs control of more space and cyber forces and authorities to execute them would reduce the number of steps and approvals. But it would also make it harder to reallocate forces, and it would thereby reduce efficiency. Moreover, a geographic CCDR's decisions about offensive space and cyber operations may be driven by theater considerations, yet have broader impacts. For example, a cyber operation could affect allied civilian populations, while a space operation could undermine a national intelligence operation. Providing geographic CCDRs rules of engagement and clear guidance on national goals as well as maintaining some requirements for coordination in certain circumstances could manage these risks. Still, pushing control of capabilities to lower echelons would have trade-offs that need to be weighed against the operational benefits in a conflict with a near peer.

The additional steps for some space and cyber operations would be required for single-domain operations. However, the challenge is amplified with MDOs, which require taking all of the steps associated with each domain that is part of the operation and ultimately synchronizing effects of operations controlled by multiple organizations.

Single-service or GCC-component JADC2 initiatives may have only limited impact. Throughout this report, we have discussed joint C2 structures because we started from the assumption that all-domain may best enhance warfighting effectiveness. In reality, we do not yet know which combinations of activities across domains will have the greatest impact. Improving integration across domains within a single GCC component is undoubtedly easier than across components or even CCMDs. And such changes can likely address some potential C2 impediments to MDOs. Still, it is not obvious which component MDO concepts will be the most operationally important. To the extent that effective operational concepts require capabilities controlled by multiple components or CCMDs, improving integration will require JADC2 concepts and systems that cross these boundaries as well. For such operations, it will take cooperation among multiple organizations to reduce the number of steps and approvals, ensure expertise and information are available to planners, and minimize dependence on potentially vulnerable communications.

Multidomain planning is currently constrained by the availability of expert planners. One reason for concentrating space and cyber expertise at the GCC level is that there have not been sufficient qualified and experienced personnel available to distribute planners to the component level. More broadly, staffing shortfalls were frequently mentioned during CCMD, component, and liaison interviews. Without planning expertise in relevant domains, multidomain options may not emerge. To some extent, requirements for multidomain planners and planning would likely compete with single-domain efforts. There could be competition between multidomain billets, on the one hand, and single-domain billets in single-domain-focused components and other service-focused roles. Services have tended to focus on developing expertise in one domain, which has led to considerable advances, but potentially at the cost of better integration. On a related note, there could be tension between breadth—having people focus on a variety of domains—and depth—having people focus on one particular domain.

Recommendations

Specify MDO concepts and assess the benefits for warfighting effectiveness. MDOs can be more complex than operations that are limited to one domain, which, as we have detailed, can make them more time consuming to plan and more vulnerable to communications disruptions. To better understand the trade-offs associated with new MDO and JADC2 concepts, we recommend that USAF encourage MDO advocates to be as specific as possible and address some unanswered questions: What operational problems can USAF or joint forces solve that cannot be solved using existing practices? How much will it cost, in terms of budgets, time, and

possibly even risk, to pursue a particular MDO concept? Decisionmakers across the military will need a better basis upon which to decide how to move forward on MDOs and the JADC2, and this will require a degree of specificity that is rare in official writing on the subject. As specific concepts for MDOs emerge, the joint force will be able to better evaluate what benefits those concepts provide, what kind of C2 changes are most important to enable them, and what costs and risks such C2 changes may bring.

Set priorities among global integration, the JADC2, and distributed control. An overarching C2 construct for conflict against a near-peer competitor needs to address all three C2 challenges. Joint and service initiatives on global integration, the JADC2, and distributed control need to remain in dialogue to identify potential trade-offs among these concepts as they mature. The relative priority among these concepts will likely depend on the contingency. For example, expectation of communications contestation in a conflict with a near-peer competitor may demand pushing control of more forces forward.

In order to develop a comprehensive C2 construct for conflict against a near peer, national leaders, CCDRs, and component commanders will need to discuss the operating environment and its implications for managing these C2 challenges. They will have to weigh which C2 practices will be viable and most important in that context. Moreover, leaders at all levels will need to discuss which types of authorities they are willing to delegate to lower levels when communications are degraded.

Continue to build shared understanding among CCMDs. Inherent differences between FCCs and GCCs will place limits on achieving shared understanding, but to the extent that various combatant commands can take steps to better understand each other's priorities and operational design, they can better approach unity of effort. With a better understanding of GCCs and even GCC-component concepts, other CCMDs—particularly those that control global assets—may better understand the trade-offs associated with approving and prioritizing other GCC requests. Similarly, FCC- and USSPACECOM-planned operations may be better coordinated with terrestrial GCC plans and vice versa. JCS initiatives on global integration already aim to address seams between CCMDs and achieve unity of effort. Continuing to prioritize collaboration when planning for a contingency may help to overcome the perception or reality of a lack of unity of effort.

The JCS may also wish to consider whether there are additional opportunities for promoting dialogue among CCMDs. In addition, it may be beneficial for CCDRs to study and familiarize themselves with the processes and procedures (e.g., the RAP, RAPCO, and so on) that the "other" CCDRs must initiate and complete before an asset can be allocated, transferred, or provided in support. For example, by gaining awareness and understanding of the "rack and stack" or IC deconfliction process an FCC is required to perform (by statute and regulation), a GCC may be able to make more informed decisions when planning for and during a contingency.

Experiment with alternative JADC2 structures. USAF has conducted several TTXs to examine the JADC2. TTXs are a useful way to explore new ideas, but USAF and its joint

partners will need to move beyond TTXs to examine and assess the costs and benefits to changes to command organizations. To build on TTXs, we recommend that USAF use command-post exercises (CPXs), perhaps at the Shadow AOC at Nellis AFB. The Doolittle wargame series is beginning to explore issues, but to this date USAF has yet to stage a full CPX. USAF could use CPXs, ideally commanding fielded forces working in different domains, to learn how it might develop an integrated tasking order and how it might develop links to operational- and tactical-level commands focused on operations in other domains.

To learn more about how to plan across domains, USAF component commands associated with GCCs might develop new contingency plans in new ways, perhaps by collaborating with teams of planners from other domain-based components. Realistic experiments and planning efforts can give USAF and its joint partners a better understanding of the potential benefits and drawbacks of working across domains. These can also help build understanding of the systems and processes necessary to make the JADC2 work.

Prioritize consideration of new approaches to multidomain planning. We found that component-centered planning creates potential impediments to MDOs, such as lack of expertise or a single-service or -domain mindset. In previous chapters we presented alternative approaches that the joint force could adopt to overcome these impediments. The joint force could take a number of approaches such as adding more liaisons within components, bringing planning up to the GCC level, creating an air, space, and cyber component, or organizing planning around LOEs. While we do not recommend one of these approaches over another, we do recommend that if the joint force wants to prioritize MDOs, that it prioritize adjustments to planning processes. Current initiatives focused on data standards, communications technologies, and artificial intelligence all have an important role to play in the JADC2. However, if planning teams do not generate multidomain options, then these innovations may not be used to their greatest effect in a contingency.

Give OPCON or TACON of global forces to terrestrial GCCs (and GCC forces to global CCMDs) for limited periods during steady-state operations. Giving GCCs and FCCs OPCON or TACON of forces that typically belong to the other during peacetime (consistent with SecDef approval) could offer insights into options for wartime C2 structures. The transfer of control could be for limited periods of time and with sufficient conditions to return the asset to centralized FCC or GCC control should the need arise. Interviewees noted that terrestrial GCCs lack familiarity with many space and cyber assets because they are never assigned the assets in a manner that provides them OPCON or TACON over the asset. As a result, GCCs seek organic alternatives to solve operational mission problems rather than exercising the RAP to obtain the asset. So, for example, by experimenting with terrestrial GCC control of these capabilities during steady-state operations, the joint force can explore the risks of such arrangements, and both FCCs and GCCs may become more comfortable with the release (by the other CCDR) and control/use (by the terrestrial GCC) of the asset. Similarly, allowing FCCs and USSPACECOM to exercise control over terrestrial GCC assets (as opposed to simply being in support if the FCC

or USSPACECOM is the lead CCMD) would enable FCCs and USSPACECOM to gain corresponding knowledge and understanding of the terrestrial GCC's organic assets. Such exercises and operations may build trust among CCMDs such that they are open to wartime transfers when necessary due to communications contestation or to enable faster decisionmaking.

Simplify and update authorities related to MDOs. Currently, there is no single authority or compendium of authorities that addresses C2 for MDOs. Authorities that relate to MDO assets, functions, capabilities, processes, and procedures are covered in hundreds of different statutes and CJCS and DoD issuances, as well as doctrinal documents.[1] It seems likely that some forms of MDOs will need to be in compliance with more authorities than single-domain alternatives. Therefore, commanders and JAs alike may need some tools to understand and review the larger number of relevant authorities. The creation of an authoritative, DoD-wide electronic library for all authorities relevant to MDOs would be a helpful first step.

DoD may also want to consider a comprehensive review of all 1,700 (approximate) regulations for the purposes of updating and/or consolidation.[2] It was outside the scope of this study to assess the degree to which redundancies may exist in these regulations. However, the greater the number of regulations (and authorities, generally), the more burdensome compliance becomes at all levels of command.

Additionally, many existing regulations are well over a decade old and may therefore lack material value given the demands of not only MDOs, but of developments in joint operations more generally. For example, the current standing rules of engagement (SROE) for the use of force, CJCSI 3121.01B, was issued on June 5, 2005 (with some amendments made on June 18, 2008). This is a crucial document for CCDRs as they plan for and conduct operations, including in the rapidly changing space and cyber domains. SMEs whom we interviewed reported that this fact seriously diminished the value of the SROE and has led to confusion across CCMDs as staffs and JAs in various commands develop their own interpretations of how the SROE relates to more recently issued authorities. Updating this document could therefore reduce the time required for planning and executing certain MDOs.

Build GCC staff experience with space and cyber authorities and approval processes. If a geographic CCDR or component commanders anticipates employing space and cyber

---

[1] For example, to conduct MDOs involving cyber, planners would need to ensure compliance with, and perhaps even directly reference, authorities such as DoDD 5100.01, 2010 (for general authority of the CCDR); DoDD 5100.20, 2010 (if coordination with DIRNSA is necessary); DoDD 5205.12, 2018 (if involving the collection of military intelligence); DoDD 3600.01, 2013 (if involving information operations); DoDI O3115.07, 2010 (if involving SIGINT). For general rules of engagement, see CJCSI 3121.01B, 2005; CJCSI 3250.01F, 2019, not available to the general public; CJCSI 3150.07E, 2013; CJCSM 5140.01A, June 26, 2015.

[2] There are approximately 350 CJCS regulations and approximately 1,316 DoD regulations (see, generally, Joint Chiefs of Staff, *Current List of CJCS Guides, Instructions, Manual, and Notices*, June 20, 2019); Executive Services Directorate, "DoD Directives Division," n.d.

capabilities more often, then it may be helpful for more of the staff to have exposure to the relevant authorities and approval processes. Here we describe several possible approaches.

- Increase involvement of JAs in planning. JA staff are the experts regarding the interpretation of authorities. If involved early on in CONOP development and operational planning, JAs may be able to spot complex issues regarding CCDR statutory powers, RAP requirements (or likely RAP requirements), and issues that may arise regarding Title 50 and IC deconfliction. By identifying these issue early in planning, JAs can develop solutions that could avoid authorities impediments when operations are initiated. JAs can also help planners understand what is possible, which may make them more willing to consider space and cyber integration even if more steps and approvals are required. USAFE-AFAFRICA has reportedly had success with early integration of JAs in CONOP development.
- Review exercises for additional opportunities to practice approval processes. Interviews with SMEs indicated that during nearly all wargames and exercises, the processes and procedures related to assigning, obtaining, delegating, or otherwise determining which command has authorities over assets and forces is often "white carded" rather than exercised. For example, if a contingency operation is being wargamed, it is typical to assume that cyber or space effects will be approved through the RAP. The result, as reported by interviewees, is that planners sometimes have unrealistic expectations about how quickly or efficiently this process occurs once an actual operation is initiated.

  The recent globally integrated exercise, which included SecDef and CJCS participation in approval processes, is an important exception that the joint force can build on. There are likely more opportunities to include approval processes within existing exercises. This would require the staff and personnel responsible for the RAP to participate in the wargame and exercise every step of the authorities process before the wargame can continue. Alternatively, CCMDs may decide to create wargames devoted entirely to the process of identifying, delegating and/or distributing, and approving authorities for various types of operations (planned and contingency). In either case, practicing these approval steps may make planners faster and more effective at communicating their operational equities. Over time, the inclusion of authorities processes in wargaming will also build institutional knowledge about what is possible with regard to obtaining certain authorities within and across CCMDs.
- Develop authorities training programs. There are wide differences in understanding and knowledge of the concept of authorities. As noted above, the term itself is not defined within DoD. Some individuals are unaware or unsure of the tiered precedential weight of the various authorities (as described in Chapter 3). This often leads to confusion, or even a misplaced blame, as to what is causing a delay or failure in obtaining an asset for an operation. In some cases, interviewees reported that operators blamed a delay or denial of a request for an asset on "authorities" when, in fact, the actual asset (or capability desired of the asset) did not actually exist or was simply not available. A training module for commanders and staff on authorities (perhaps taught by JAs teamed with operational planners) may help them gain better understanding of the actual constraints of authorities as opposed to the constraints imposed by procedures that implement the authorities, or constraints related to the assets and forces that are the subjects of different authorities.

Look for opportunities to streamline space and cyber approval processes. If GCCs begin using space and cyber operations more often as part of MDOs, then there may be value in finding ways to streamline the existing RAP.

- Develop RAP templates. RAP requests are essential tools for CCDRs to navigate complex authorities issues in order to gain the assets, forces, or effects they need. GCCs may wish to develop RAP templates that facilitate their unique operational needs during MDOs. RAPs that are approved and denied should be reviewed (perhaps even reviewed as part of after-action reviews for exercises and wargames and for actual operations) so that the CCDR and his or her staff can learn what elements of a RAP have been successful or unsuccessful.
- Automate RAP and deconfliction processes and procedures. To the extent possible, it may be beneficial to automate the RAP and the deconfliction mechanism to create a more dynamic approval process. Interviewees reported that many of these processes and procedures are completed by paper, fax, and voice phone calls. An online system (on a classified network) may streamline the RAP.

Analyze trade-offs associated with giving more staff access to information on space and cyber capabilities. Classification of space and cyber capabilities is widely seen as an impediment to MDOs. If a CCDR needs to plan for a highly classified capability, the staff on both ends of the RAP or deconfliction will need the appropriate clearance level. Many interviewees indicated that the RAP and deconfliction processes are often delayed because there are limited staff members with the required level of clearance. Although it is difficult and resource intensive to qualify staff for higher-level clearances, it may be worth the investment where delay issues related to access currently exist. Reviewing the classification levels of information about space and cyber effects to see if some can be lowered is another approach. It may be possible to reduce classification levels on information about effects without revealing more sensitive details.

However, space and cyber capabilities are highly classified for many reasons, including that adversary awareness of them could allow them to develop countermeasures. Hence, changes to classification or access to improve integration will necessarily create trade-offs. Whether sharing more information about these capabilities is, on net, beneficial depends crucially on how much closer integrations of space and cyber operations with operations in other domains would improve warfighting effectiveness. Development of and experimentation with specific operational concepts for integrating space and cyber may help to determine the benefits that can be gained from deeper integration.

Prepare personnel to serve in multidomain command, planning, and liaison positions throughout professional military education. Having qualified and properly trained personnel serving in planning and liaison positions is an important component of more effectively implementing MDO operations. USAF has already acknowledged this with its new multidomain planning career field. Beyond this change, a larger number of commanders and planners will likely need to be educated as to the kinds of cross-component support available to them in

making planning and operational decisions. This will help ensure that they integrate and embed available multidomain planners and experts into their planning processes.

Final Thoughts

The joint force is taking many steps to prepare for the possibility of conflict with a near-peer competitor. Ultimately, the goal for the joint force is to increase warfighting effectiveness. As with any new initiative, there is a risk that MDO initiatives may lose sight of this ultimate goal and make integration of domains an end in itself. To avoid this trap, JADC2 initiatives will need to stay focused on C2 changes that enable clearly defined MDO concepts and account for the trade-offs associated with such changes.

References

"315 Cyberspace Operations Squadron (ACC)," July 31, 2015. As of October 8, 2020: https://www.afhra.af.mil/About-Us/Fact-Sheets/Display/Article/862193/315-cyberspace-operations-squadron-afspc/

32nd Army Air and Missile Defense Command, *Operation Iraqi Freedom: Theater Air and Missile Defense History*, Fort Bliss, Tex.: 32nd AAMDC, September 2003.

552nd Air Control Wing, "Control and Reporting Center (CRC)," webpage, December 6, 2016. As of June 4, 2020: https://www.552acw.acc.af.mil/Library/Fact-Sheets/Display/Article/430827/control-and-reporting-center-crc/

Air Force Core Doctrine Volume I, *Basic Doctrine*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, February 27, 2015. As of October 8, 2020: https://www.doctrine.af.mil/Portals/61/documents/Volume_1/Volume-1-Basic-Doctrine.pdf

Air Force Doctrine Annex 2-0, *Global Integrated ISR Operations*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, January 29, 2015. As of October 8, 2020: https://www.doctrine.af.mil/Doctrine-Annexes/Annex-2-0-Global-Integrated-ISR-Ops/

Air Force Doctrine Annex 3-01, *Counterair Operations*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, February 1, 2016. As of August 1, 2019: https://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-01-Counterair-Ops/

Air Force Doctrine Annex 3-05, *Special Operations*, Washington, D.C.: Headquarters U.S. Air Force, February 9, 2017.

Air Force Doctrine Annex 3-14, *Counterspace Operations*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, August 27, 2018. As of August 1, 2019: https://www.doctrine.af.mil/Portals/61/documents/Annex_3-14/Annex-3-14-Counterspace-Ops.pdf

Air Force Doctrine Annex 3-30, *Command and Control*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, November 7, 2014. As of August 1, 2019: https://www.doctrine.af.mil/Portals/61/documents/Annex_3-30/3-30-Annex-COMMAND-CONTROL.pdf

Air Force Doctrine Annex 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, July 30, 2019, pp. 1–12. As of October 20, 2020: https://www.doctrine.af.mil/Portals/61/documents/Annex_3-51/3-51-D01-EW-EMSO-Introduction.pdf

Air Force Doctrine Annex 3-60, *Dynamic Targeting Engagement Authority*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, March 15, 2019. As of August 1, 2019: https://www.doctrine.af.mil/Portals/61/documents/Annex_3-60/3-60-D16-Target-Dynamic.pdf

Air Force Doctrine Annex 3-99, *Department of the Air Force's Role in Joint All-Domain Operations (JADO)*, Maxwell Air Force Base, Ala.: Curtis E. LeMay Center for Doctrine Development and Education, October 8, 2020. As of October 20, 2020: https://www.doctrine.af.mil/Portals/61/documents/Annex_3-99/Annex%203-99%20DAF%20role%20in%20JADO.pdf

Air Force Instruction 13-1, *Operational Procedures-Air Operations Center (AOC)*, Washington, D.C.: Department of the Air Force, November 2, 2011, Incorporating Change 1 on May 18, 2012. As of August 1, 2019: https://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi13-1aocv3/afi13-1aocv3.pdf

Alkire, Brien, Sherrill Lingel, Caroline Baxter, Christopher M. Carson, Christine Chen, David Gordon, Lawrence M. Hanser, Lance Menthe, and Daniel M. Romano, *Command and Control of Joint Air Operations in the Pacific: Methods for Comparing and Contrasting Alternative Concepts*, Santa Monica, Calif.: RAND Corporation, RR-1865-AF, 2018. As of June 4, 2020: https://www.rand.org/pubs/research_reports/RR1865.html

"An Interview with Gen David L. Goldfein Twenty-First Chief of Staff of the US Air Force Conducted 5 January 2017," *Strategic Studies Quarterly*, Vol. 11, No. 1, Spring 2017, pp. 4–13. As of October 20, 2020: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Goldfein.pdf

Army Doctrine Reference Publication 3-09, *Fires*, Washington, D.C.: Headquarters, Department of the Army, February 8, 2013.

Army Technique Publication 3-09.13, *The Battlefield Coordination Detachment*, Washington, D.C.: Headquarters Department of the Army, July 24, 2015. As of September 11, 2020: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp3_09x13.pdf

Army Technique Publication 3-91.1, *The Joint Air Ground Integration Center*, Washington, D.C.: Headquarters, Department of the Army, April 17, 2019.

ATP 3-01.7, *Air Defense Artillery Brigade Techniques*, Washington, D.C.: Headquarters, Department of the Army, March 16, 2016. As of August 1, 2019: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp3_01x7.pdf

Berger, David H., *Commandant's Planning Guidance. 38th Commandant of the Marine Corps*, Washington, D.C.: Marine Corps, 2019. As of October 8, 2020: https://www.marines.mil/Portals/1/Publications/Commandant's%20Planning%20Guidance_2019.pdf?ver=2019-07-17-090732-937

Berger, Joseph B., III, "Covert Action: Title 10, Title 50, and the Chain of Command," *Joint Force Quarterly*, Vol. 67, October 2012, pp. 32–39.

Bolton, Edward L., Jr., "Cyber and Space—A Way Ahead," *High Frontier*, Vol. 6, No. 4, 2010, pp. 8–11. As of August 1, 2019: https://www.afspc.af.mil/Portals/3/documents/HF/AFD-101019-079.pdf

"Capabilities Integration Across Domains," *Armor & Mobility*, October 2018. As of October 8, 2020: https://tacticaldefensemedia.com/capabilities-integration-across-domains/

Card, Bryan A., "Preparing Air Missile Defense, Joint Force Against Near-Peer Threat," *Fires*, July–August 2018, pp. 32–35. As of August 1, 2019: https://sill-www.army.mil/firesbulletin/archives/2018/jul-aug/articles/18-4_July-Aug_11_Card.pdf

Carroll, Chris, "CENTCOM's Spy Satellite Set to Beam Images from War Zones," *Stars and Stripes*, July 25, 2011. As of August 1, 2019: https://www.stripes.com/news/centcom-s-spy-satellite-set-to-beam-images-from-war-zones-1.150088

Cenciotti, David, "U.S. Marine Corps F-35B Connects to HIMARS for Rocket Shot in a 'Direct Sensor-to-Shooter' Scenario," *The Aviationist*, October 9, 2018. As of August 1, 2019: https://theaviationist.com/2018/10/09/u-s-marine-corps-f-35b-connects-to-himars-for-rocket-shot-in-a-direct-sensor-to-shooter-scenario/

Chairman of the Joint Chiefs of Staff Instruction 1001.01B, *Joint Manpower and Personnel Program*, Washington, D.C.: Joint Chiefs of Staff, October 7, 2014. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Library/Instructions/1001_01.pdf

Chairman of the Joint Chiefs of Staff Instruction 3121.01B, *Standing Rules of Engagement/ Standing Rules for the Use of Force for U.S. Forces*, Washington, D.C.: Joint Chiefs of Staff, June 13, 2005, not available to the general public.

Chairman of the Joint Chiefs of Staff Instruction 3141.01F, *Management and Review of Campaign and Contingency Plans*, Washington, D.C.: Joint Chiefs of Staff, January 31, 2019.

Chairman of the Joint Chiefs of Staff Instruction 3122.07A, *Integrated Joint Special Technical Operations Supplement to Joint Operations Planning and Execution System (JOPES)*, Volume I, *Planning Policies, and Procedures*, Washington, D.C.: Joint Chiefs of Staff, October 22, 2013, not available to the general public.

Chairman of the Joint Chiefs of Staff Instruction 3139.01, *Review and Approval Process for Cyberspace Operations*, Washington, D.C.: Joint Chiefs of Staff, October 22, 2013, not available to the general public.

Chairman of the Joint Chiefs of Staff Instruction 3150.07E, *Joint Reporting Structure for Cyberspace Operations Status*, Washington, D.C.: Joint Chiefs of Staff, November 8, 2013.

Chairman of the Joint Chiefs of Staff Instruction 3250.01F, *Policy Guidance for Intelligence, Surveillance, and Reconnaissance and Sensitive Reconnaissance Operations*, Washington, D.C.: Joint Chiefs of Staff, August 7, 2019, not available to the general public.

Chairman of the Joint Chiefs of Staff Instruction 5140.01A, *Military Targeting Committee Governance and Management*, Washington, D.C.: Joint Chiefs of Staff, June 26, 2015.

Chapman, Suzann, "The 'War' Before the War," *Air Force Magazine*, February 2004. As of August 1, 2019: https://www.airforcemag.com/PDF/MagazineArchive/Documents/2004/February%202004/0204war.pdf

Chesney, Robert, "CYBERCOM's Out-of-Network Operations: What Has and Has Not Changed Over the Past Year?," *Lawfare*, May 9, 2019. As of August 1, 2019: https://www.lawfareblog.com/cybercoms-out-network-operations-what-has-and-has-not-changed-over-past-year

CJCSI—*See* Chairman of the Joint Chiefs of Staff Instruction.

CJCSM—*See* Chairman of the Joint Chiefs of Staff Manual.

Clark, Brad, Mike Harry, Eric Hettinga, David LaBalle, Patrick O'Brien, Matt Aiesi, Sandy Branom, Moises Castillo, Tim Cronin, John Doyle, Rich Gallagher, John Goodell, Dave Jones, Ryan Kerwin, Rachel Mangas, Jason Nef, Tripp Otto, Jess Rankin, Emily Roman, Jim Sleesman, Jeremy Snellen, Corey Thomas, Alan Wehbé, Edward Westfall, Jonathan Stevens, Jan Bartels, Doug Dribben, and Allison Polcheck, *Operational Law Handbook*, 17th ed., Charlottesville, Va.: The Judge Advocate General's Legal Center and School, 2017.

Clark, Bryan, and Timothy A. Walton, *Taking Back the Seas: Transforming the U.S. Surface Fleet for Decision-Centric Warfare*, Washington, D.C.: Center for Strategic and Budgetary Assessment, 2019. As of November 17, 2020: https://csbaonline.org/uploads/documents/CSBA8192_(Taking_Back_the_Seas)_WEB.pdf

Clark, Colin, "CJCS Gen. Dunford Proposes 'Staff' to Handle Transnational Threats," *Breaking Defense*, December 14, 2015. As of August 1, 2019: https://breakingdefense.com/2015/12/cjcs-gen-dunford-proposes-staff-to-handle-transnational-threats/

———, "CJCS Dunford Calls for Strategic Shifts; 'At Peace or at War Is Insufficient,'" *Breaking Defense*, September 21, 2016. As of August 1, 2019: https://breakingdefense.com/2016/09/cjcs-dunford-calls-for-strategic-shifts-at-peace-or-at-war-is-insufficient/

Cohen, Eliot A., ed., *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness*, Washington, D.C.: Department of the Air Force, 1993.

Cohen, Rachel S., "Moving MDC2 from Research to Reality," *Air Force Magazine*, April 15, 2019a. As of October 8, 2020: https://www.airforcemag.com/article/moving-mdc2-from-research-to-reality/

———, "Multi-Domain Ops Push Turns to Joint Force," *Air Force Magazine*, July 25, 2019b. As of October 8, 2020: http://www.airforcemag.com/Features/Pages/2019/July%202019/Multi-Domain-Ops-Push-Turns-to-Joint-Force.aspx

Collens, Josiah R., Jr., and Bob Krause, *Theater Battle Management Core Systems Engineering Case Study*, Wright-Patterson Air Force Base, Oh.: Center for Systems Engineering at the Air Force Institute of Technology, February 17, 2005. As of August 1, 2019: https://apps.dtic.mil/dtic/tr/fulltext/u2/a572204.pdf

Congressional Research Service, *U.S. Special Forces (SOF): Background and Issues for Congress*, Washington, D.C.: Congressional Research Service, RS21048, March 28, 2019.

Cooper, James C., *The Joint Air Component Coordination Element: Middleman, or an Effective Airpower Broker?*, Newport, R.I.: Naval War College, May 4, 2012. As of August 1, 2019: https://apps.dtic.mil/dtic/tr/fulltext/u2/a563894.pdf

Corey, Craig, "The Air Force's Misconception of Integrated Air and Missile Defense," *Air and Space Power Journal*, Vol. 31, January 2017, pp. 81–90. As of August 1, 2019: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-31_Issue-4/V-Corey.pdf

Defense Intelligence Agency, *Challenges to Security in Space*, Washington, D.C.: Defense Intelligence Agency, January 2019. As of August 1, 2019: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

Department of Defense Directive 2311.01E, *DoD Law of War Program*, Washington, D.C.: U.S. Department of Defense, 2006.

Department of Defense Directive 3100.10, *Space Policy*, Washington, D.C.: U.S. Department of Defense, November 4, 2016. As of August 1, 2019: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/310010.pdf?ver=2019-02-04-130744-620

Department of Defense Instruction 03115.07, *Signals Intelligence (SIGINT)*, amended November 19, 2010, Washington, D.C.: U.S. Department of Defense, September 15, 2008, not available to the general public.

Department of Defense Directive 3600.01, *Information Operations (IO)*, Washington, D.C.: U.S. Department of Defense, May 2, 2013. As of August 1, 2019: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf?ver=2019-08-12-094732-187

Department of Defense Directive 5100.01, *Functions of the Department of Defense and Its Major Components*, Washington, D.C.: U.S. Department of Defense, 2010.

Department of Defense Directive 5100.20, *National Security Agency/Central Security Service (NSA/CSS)*, Washington, D.C.: U.S. Department of Defense, January 26, 2010. As of August 1, 2019: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510020p.pdf

Department of Defense Directive 5205.12, *Military Intelligence Program (MIP)*, amended at Change 1, Washington, D.C.: U.S. Department of Defense, May 10, 2018. As of August 1, 2019: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520512p.pdf?ver=2018-05-10-083514-693

Deployable Training Division, Joint Staff J7, "Insights and Best Practices Focus Paper: Geographic Combatant Commander (GCC) Command and Control Organizational Options," August 2016. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/gcc_organ_options_fp.pdf

Deptula, David A., "A New Era for Command and Control of Aerospace Operations," *Air and Space Power Journal*, July–August 2014, pp. 5–16. As of August 1, 2019: https://apps.dtic.mil/dtic/tr/fulltext/u2/a604518.pdf

DeVine, Michael E., *Defense Prime: Under Secretary of Defense (Intelligence)*, CRS in Focus, Washington, D.C.: Congressional Research Service, IF10523, December 19, 2018.

Director of National Intelligence, *Intelligence Community Directive 204, National Intelligence Priorities Framework*, January 2, 2015. As of August 1, 2019: https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf

DoDD—*See* Department of Defense Directive.

DoDI—*See* Department of Defense Instruction.

Drew, James, "USAF Standing Up Shadow Ops Center at Nellis AFB," *Aerospace Daily*, November 17, 2017. As of August 1, 2019: https://aviationweek.com/awindefense/usaf-standing-shadow-ops-center-nellis-afb

Dunford, Joseph F., Jr, "Gen. Dunford's Remarks and Q&A at the Center for a New American Security Next Defense Forum," n.d. As of August 1, 2019: https://www.jcs.mil/Media/Speeches/Article/636952/gen-dunfords-remarks-and-qa-at-the-center-for-a-new-american-security-next-defe/

Durr, Robert, "Joint Forces Team Up for Spartan Shield," September 13, 2018. As of August 1, 2019: https://www.army.mil/article/211075/joint_forces_team_up_for_spartan_shield

Erwin, Sandra, "Air Force Chief Goldfein: 'We'll Be Fighting from Space in a Matter of Years,'" *Space News*, February 4, 2018. As of October 20, 2020: https://breakingdefense.com/2020/03/gen-goldfein-launches-air-force-doctrine-for-joint-all-domain-ops/

Executive Order 12333, *United States Intelligence Activities*, 46 Fed. Reg. 59941, 1981, code edition dated December 4.

Executive Services Directorate, *DoD Directives Division*, n.d. As of August 1, 2019: https://www.esd.whs.mil/DD/

Feickert, Andrew, "The Unified Command Plan and Combatant Commands: Background and Issues for Congress," Washington, D.C.: Congressional Research Service, No. R42077, January 3, 2013, pp. 15–19.

Field Manual 3-0, *Operations*, Washington, D.C.: Headquarters, Department of the Army, October 2017. As of August 1, 2019: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN6687_FM%203-0%20C1%20Inc%20FINAL%20WEB.pdf

Field Manual 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, D.C.: Headquarters, Department of the Army, April 2017. As of October 8, 2020: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf

Flynn, Charles A., *Standing Joint Task Force Headquarters: Creating Opportunities from Chaos*, Norfolk, Va.: Joint Advanced Warfighting School, May 15, 2006. As of August 1, 2019: https://apps.dtic.mil/dtic/tr/fulltext/u2/a451266.pdf

Freedberg, Sydney J., Jr., "Air Force Leading Way to 3rd Offset: Bob Work," *Breaking Defense*, September 21, 2016a. As of August 1, 2019: https://breakingdefense.com/2016/09/air-force-ops-centers-lead-way-to-3rd-offset-bob-work/

———, "DepSecDef Work Offers Dough for Army Multi-Domain Battle," *Breaking Defense*, October 4, 2016b. As of August 1, 2019: https://breakingdefense.com/2016/10/depsecdef-work-offers-dough-for-army-multi-domain-battle/

———, "Trump Eases Cyber Ops, but Safeguards Remain: Joint Staff," *Breaking Defense*, September 17, 2018. As of August 1, 2019: https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/

———, "All Services Sign On to Data Sharing—But Not to Multi-Domain," *Breaking Defense*, February 8, 2019a. As of August 1, 2019: https://breakingdefense.com/2019/02/all-services-sign-on-to-data-sharing-but-not-to-multi-domain/

———, "F-35 Spots Targets for Army Missile Defenders," *Breaking Defense*, August 6, 2019b. As of August 1, 2019: https://breakingdefense.com/2019/08/f-35-spots-targets-for-army-missile-defenders/

———, "IBCS: Northrop Delivers New Army Missile Defense Command Post," *Breaking Defense*, May 1, 2019c. As of August 1, 2019: https://breakingdefense.com/2019/05/ibcs-northrop-delivers-new-missile-defense-command-post-to-army/

Gallagher, Sean, "Marine Corps F-35B Scores a Kill (Sort of)—with a Navy-Launched Missile," *arsTechnica*, September 14, 2016. As of August 1, 2019: https://arstechnica.com/information-technology/2016/09/marine-corps-f-35b-scores-a-kill-sort-of-with-a-navy-launched-missile/

Garamone, Jim, "Work Details Multidomain Battlefield of the Future," October 4, 2016. As of August 1, 2019: https://www.defense.gov/Newsroom/News/Article/Article/963806/work-details-multidomain-battlefield-of-the-future/

———, "Air Force, Army Developing Multidomain Doctrine," January 25, 2018. As of August 1, 2019: https://www.defense.gov/Newsroom/News/Article/Article/1424263/air-force-army-developing-multidomain-doctrine/

———, "U.S. Military Must Develop All-Domain Defenses, Mattis, Dunford Say," n.d. As of August 1, 2019: https://www.jcs.mil/Media/News/News-Display/Article/1493778/us-military-must-develop-all-domain-defenses-mattis-dunford-say/

Garner, Bryan A., *Black's Law Dictionary*, 10th ed., St. Paul, Minn.: Thomson West, 2014.

Goff, Stan, "Russia Jammed GPS Signals During NATO Military Exercise Involving U.S. Troops," *Inside GNSS*, November 14, 2018. As of August 1, 2019: https://insidegnss.com/russia-jammed-gps-signals-during-nato-military-exercise-involving-us-troops/

Goldfein, Dave, *CSAF Focus Area: Enhancing Multi-Domain Command and Control . . . Tying It All Together*, Washington, D.C.: U.S. Air Force, March 2017.

Gould, Joe, "Eyeing Russia, Army Fields Jam-Resistant GPS in Europe," *C4ISRNET*, June 6, 2019. As of August 1, 2019: https://www.c4isrnet.com/show-reporter/c4isrnet-conference/2019/06/06/eyeing-russia-army-fields-jam-resistant-gps-in-europe/

Government Accountability Office, *Warfight Support: An Assessment of DoD Documents Used in Previous Efforts to Rebalance to the Pacific*, Washington, D.C.: Government Accountability Office, GAO-18-192, May 2018.

Hague Convention of 1907 ("Hague IV"), Articles 22–41.

Hallion, Richard P., *Storm over Iraq: Air Power and the Gulf War*, Washington, D.C.: Smithsonian Institute Press, 1992.

Harrell, Margaret C., and Melissa A. Bradley, *Data Collection Methods: Semi-Structured Interviews and Focus Groups*, Santa Monica, Calif.: RAND Corporation, TR-718-USG, 2009. As of June 4, 2020: https://www.rand.org/pubs/technical_reports/TR718.html

Harvard, James W., "Airmen and Mission Command," *Air and Space Power Journal*, March–April 2013, pp. 131–146.

Hayden, Michael V., "The Making of America's Cyberweapons," *Christian Science Monitor*, February 24, 2016. As of August 1, 2019: https://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0224/The-making-of-America-s-cyberweapons

Heininger, Clare, "Army, Air Force Team on Sensor to Shooter Prototype for Multi-Domain Battle," 2018. As of August 1, 2019: https://www.army.mil/article/209672/army_air_force_team_on_sensor_to_shooter_prototype_for_multi_domain_battle

Hendrix, Jerry, *Filling the Seams in U.S. Long-Range Penetrating Strike*, Washington, D.C.: Center for a New American Security, September 10, 2018. As of August 1, 2019: https://www.cnas.org/publications/reports/filling-the-seams-in-u-s-long-range-penetrating-strike

Hitchens, Theresa, "Navy, Air Force Chiefs Agree to Work on All Domain C2," *Breaking Defense*, November 12, 2019a. As of January 23, 2020: https://breakingdefense.com/2019/11/exclusive-navy-air-force-chiefs-agree-to-work-on-all-domain-c2/

———, "STRATCOM Move to Space Command: 2 Years, 100s of People," *Breaking Defense*, August 6, 2019b. As of August 1, 2019: https://breakingdefense.com/2019/08/stratcom-move-to-space-command-2-years-100s-of-people/

———, "Gen. Goldfein Launches Air Force Doctrine for Joint All-Domain Ops," *Breaking Defense*, March 18, 2020.

Huyck, Kevin A., "ACC Operationalizing Multi-Domain," Briefing at the USAF Air Combat Command-U.S. Army Training and Doctrine Command Multi-Domain Operations Symposium, Joint Base Langley-Eustis, Va., April 29, 2019.

Huyck, Kevin, and Mark Odom, "ACC/TRADOC TXX Series: Results and Insights," October 23, 2018.

Igl, Chadwick D., Candy S. Smith, Daniel R. Fowler, and William L. Angermann, "568 Balls in the Air: Planning for the Loss of Space Capabilities," *Joint Force Quarterly*, No. 90, July 3, 2018. As of October 8, 2020: https://www.ndu.edu/Portals/68/Documents/jfq/jfq-90/jfq-90_24-29_igl-et-al.pdf?ver=2018-04-11-125441-307

International Committee of the Red Cross, *Geneva Convention Relative to the Treatment of Prisoners of War*, August 12, 1949. As of August 1, 2019: https://www.refworld.org/docid/3ae6b36c8.html

JCS—*See* Joint Chiefs of Staff.

Johnson, David, "Cluster Munitions and Rearming for Great Power Competition," *War on the Rocks*, May 9, 2019. As of December 3, 2019: https://warontherocks.com/2018/05/cluster-munitions-and-rearming-for-great-power-competition/

Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, Washington, D.C.: Joint Chiefs of Staff, March 16, 2018. As of June 10, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257

———, *Current List of CJCS Guides, Instructions, Manual, and Notices*, Washington, D.C.: Joint Chiefs of Staff , June 20, 2019. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Library/SupportDocs/CJCS%20Reports/CJCS%20CURRENT%20DIRECTIVES%20-%2022%20Jan%202020.pdf?ver=2020-01-24-141719-760

Joint Force Space Component Command Public Affairs, "Combined Space Operations Center Established at Vandenberg AFB," Vandenberg, Va.: U.S. Strategic Command, July 19, 2018. As of August 1, 2019: https://www.stratcom.mil/Media/News/News-Article-View/Article/1579497/combined-space-operations-center-established-at-vandenberg-afb/

Joint Publication 1, *Doctrine of the Armed Forces of the United States*, Washington, D.C.: Joint Chiefs of Staff, March 25, 2013, Incorporating Change 1, July 12, 2017. As of October 8, 2020: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf?ver=2019-02-11-174350-967

Joint Publication 2-0, *Joint Intelligence*, Washington, D.C.: Joint Chiefs of Staff, October 22, 2013. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, Washington, D.C.: Joint Chiefs of Staff, July 5, 2017. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_01_20170705v2.pdf

Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, Washington, D.C.: Joint Chiefs of Staff, May 21, 2014.

Joint Publication 2-03, *Geospatial Intelligence in Joint Operations*, Washington, D.C.: Joint Chiefs of Staff, July 5, 2017. As of October 8, 2020: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_03_20170507.pdf

Joint Publication 3-0, *Joint Operations*, January 17, 2017, Incorporating Change 1, Washington, D.C.: Joint Chiefs of Staff, October 22, 2018. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910

Joint Publication 3-01, *Countering Air and Missile Threats*, Washington, D.C.: Joint Chiefs of Staff, April 21, 2017. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_01_pa.pdf?ver=2018-05-16-175020-290

Joint Publication 3-05, *Special Operations*, Washington, D.C.: Joint Chiefs of Staff, July 16, 2014. As of October 8, 2020: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_05.pdf?ver=2018-03-15-111255-653

Joint Publication 3-09, *Joint Fire Support*, Washington, D.C.: Joint Chiefs of Staff, April 10, 2019. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf

Joint Publication 3-12, *Cyberspace Operations*, Washington, D.C.: Joint Chiefs of Staff, June 8, 2018. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Joint Publication 3-14, *Space Operations*, Washington, D.C.: Joint Chiefs of Staff, April 10, 2018. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf

Joint Publication 3-30, *Joint Air Operations*, Washington, D.C.: Joint Chiefs of Staff, July 25, 2019. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf

Joint Publication 3-31, *Command and Control for Joint Land Operations*, Washington, D.C.: Joint Chiefs of Staff, February 24, 2014.

Joint Publication 3-32, *Joint Maritime Operations*, Washington, D.C.: Joint Chiefs of Staff, June 8, 2018. As of October 8, 2020: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_32.pdf?ver=2019-03-14-144800-240

Joint Publication 3-33, *Joint Task Force Headquarters*, Washington, D.C.: Joint Chiefs of Staff, January 31, 2018. As of August 1, 2020: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_33.pdf

Joint Publication 3-60, *Joint Targeting*, Washington, D.C.: Joint Chiefs of Staff, January 31, 2013.

Joint Publication 5-0, *Joint Planning*, Washington, D.C.: Joint Chiefs of Staff, June 16, 2017. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf

Joint Staff J7, "Insights and Best Practices Focus Paper: Integration and Synchronization of Joint Fires," July 2018. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/int_and_sync_jointfires.pdf?ver=2018-09-18-102801-350

Joint Staff J7 Deployable Training Division, "Insights and Best Practices Focus Paper: Design and Planning," Suffolk, Va., July 2013. As of August 1, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/design_and_planning_fp.pdf

Joint Warfighting Center, *Commander's Handbook for an Effects-Based Approach to Joint Operations*, Norfolk, Va.: U.S. Joint Forces Command, February 24, 2006.

JP—*See* Joint Publication.

Keller, Cole, "AF, Navy Conduct Joint Air Defense Exercise," November 1, 2016. As of August 1, 2019: https://www.af.mil/News/Article-Display/Article/992085/af-navy-conduct-joint-air-defense-exercise/

Kiser, Aaron, Jacob Hess, El Mostafa Bouhafa, and Shawn Williams, *The Combat Cloud: Enabling Multi-Domain Command and Control Across the Range of Military Operations*, Maxwell Air Force Base, Ala.: Air University, 2017. As of August 1, 2019: https://apps.dtic.mil/dtic/tr/fulltext/u2/1042210.pdf

Kondra, Alex A., and Deborah C. Hunt, "Institutional Processes of Organizational Culture," *Culture and Organization*, Vol. 15, No. 1, pp. 39–58.

Kouba, Dustin, ed., *Operational Law Handbook*, Charlottesville, Va.: The Judge Advocate General's Legal Center and School, 2018.

Lacey, Jim, "The 'Dumbest Concept Ever' Just Might Win Wars," *War on the Rocks*, July 29, 2019. As of August 1, 2019: https://warontherocks.com/2019/07/the-dumbest-concept-ever-just-might-win-wars/

LaGrone, Sam, "Successful F-35, SM-6 Live Fire Test Points to Expansion in Networked Naval Warfare," *USNI News*, September 13, 2016. As of August 1, 2019: https://news.usni.org/2016/09/13/video-successful-f-35-sm-6-live-fire-test-points-expansion-networked-naval-warfare

Lamothe, Dan, "How the Pentagon's Cyber Offensive Against ISIS Could Shape the Future for Elite U.S. Forces," *Washington Post*, December 16, 2017. As of August 1, 2019: https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/

Lee, Connie, "News from AUSA Global: Army Sharpens Focus on Multi-Domain Warfare," *National DEFENSE*, March 27, 2019. As of August 1, 2019: https://www.nationaldefensemagazine.org/articles/2019/3/27/army-integrates-multi-domain-task-force-unit

Lyle, David J., *Seeing the Forest from the Sky: Joint Airpower Through the Lens of Complex Systems Theory*, Maxwell Air Force Base, Ala.: Air University, 2010. As of August 1, 2019: https://apps.dtic.mil/dtic/tr/fulltext/u2/1019205.pdf

McCullough, Amy, "Facing the Unknown in a Multi-Domain Command and Control Environment," *Air Force Magazine*, November 11, 2017. As of October 8, 2020: https://www.airforcemag.com/facing-the-unknown-in-a-multi-domain-command-and-control-environment/

———, "USAF Looks to Create New Command and Control Structure," *Air Force Magazine*, June 6, 2018. As of August 1, 2019: http://www.airforcemag.com/Features/Pages/2018/June%202018/USAF-Looks-to-Create-New-Command-and-Control-Structure.aspx

McGhee, James E., "Liberating Cyber Offense," *Strategic Studies Quarterly*, Winter 2016, pp. 48–49. As of August 1, 2019: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-10_Issue-4/McGhee.pdf

Mehta, Aaron, "Space Command to Launch Aug. 29," *Defense News*, August 20, 2019. As of September 1, 2019: https://www.defensenews.com/space/2019/08/20/space-command-to-launch-aug-29/

Miles, Anne Daugherty, *Intelligence Community Programs, Management, and Enduring Issues*, Washington, D.C.: Congressional Research Service, R44681, November 8, 2016.

Murray, Hurcules, "Cyber Requirements," briefing delivered at Armed Forces Communications and Electronics Association TechNet: Achieving Force 2025 Rough Signals and Cyber, Augusta, Ga., September 10, 2014. As of August 1, 2019: https://www.afcea.org/events/augusta/14/documents/T2S2AFCEATechnetCyberRequirements.pdf

Nakashima, Ellen, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *Washington Post*, September 20, 2018. As of August 1, 2019: https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?noredirect=on

National Air and Space Intelligence Center, *Competing in Space*, Wright-Patterson Air Force Base, Oh., December 2018. As of August 1, 2019: https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF

Northrop Grumman, Communications, *Navigation, and Identification (CNI) Avionics for the F-35 Lightning II: New Dimensions for the Warfighter in Digital Battlespace*, San Diego, Calif.: Northrup Grumman, 2012. As of August 1, 2019: https://www.northropgrumman.com/Capabilities/F35Lightning/Documents/asq242_datasheet.pdf

Office of the Chairman of the Joint Chiefs of Staff, *DoD Dictionary of Military and Associated Terms*, Washington, D.C.: Joint Staff, June 2020. As of October 26, 2020: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Office of General Council, *Department of Defense Law of War Manual*, Washington, D.C.: Department of Defense, 2015, updated December 2016. As of October 8, 2020: https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190

———, *Missile Defense Review*, Washington, D.C.: Department of Defense, 2019. As of August 1, 2019: https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf

Orye, Erwin, and Olaf M. Maennel, "Recommendations for Enhancing the Results of Cyber Effects," 11th International Conference on Cyber Conflict, Tallinn, Estonia, 2019. As of August 1, 2019: https://ccdcoe.org/uploads/2019/06/Art_06_Recommendations-for-Enchasing-the-Results-of-Cyber-Effects.pdf

O'Shaughnessy, T. J., and Matthew Strohmeyer, *Multi-Domain Command and Control: Ensuring Offensive Initiative at the Theater AOC and Below in a Contested Environment*, Joint Base Pearl Harbor-Hickam, Hi.: Pacific Air Forces, Strategic Thinking White Papers, 2018.

Osborn, Kris, "Cross-Domain Fires: US Military's Master Plan to Win the Wars of the Future," *The National Interest*, July 19, 2016. As of August 1, 2019: https://nationalinterest.org/blog/the-buzz/cross-domain-fires-us-militarys-master-plan-win-the-wars-the-17029

Park, Francis J. H., "Chairman's Vision of Global Integration," unpublished briefing created by the Strategy Development Division, Directorate for Strategy, Plans, and Policy, Joint Staff, May 24, 2018.

Parsons, Dan, "Why the US Needs a Marine Corps: Multi-Domain Before It Was Cool," *Rotor & Wing International*, August 3, 2018. As of August 1, 2019: https://www.rotorandwing.com/2018/08/03/us-needs-marine-corps-multi-domain-cool/

Perkins, David G., "Multi-Domain Battle: The Advent of Twenty-First Century War," *Military Review*, November–December 2017, pp. 8–13.

Perkins, David G., and James M. Holmes, "Multidomain Battle: Converging Concepts Toward a Joint Solution," *Joint Forces Quarterly*, Vol. 88, January 10, 2018, pp. 54–57.

Pierce, William G., *Span of Control and the Operational Commander: Is It More Than Just a Number?*, Leavenworth, Ka.: School of Advanced Military Studies, September 12, 1994. As of August 1, 2019: https://apps.dtic.mil/dtic/tr/fulltext/u2/a240178.pdf

Poisson, Alain, "MDC2 Overview," unpublished briefing, Washington, D.C., U.S. Air Force, n.d.

Pomerleau, Mark, "Authorities Complicate Use of Cyber Capabilities," *Fifth Domain*, January 9, 2017a. As of August 1, 2019: https://www.fifthdomain.com/home/2017/01/09/authorities-complicate-the-use-of-cyber-capabilities/

———, "Marines Take Multi-Domain Battle to the Littorals," *C4ISRNET*, September 21, 2017b. As of August 1, 2019: https://www.c4isrnet.com/digital-show-dailies/modern-day-marine/2017/09/21/marines-taking-multi-domain-battle-to-the-littorals/

———, "The 'Real Strength' in Cyber Command's Recent Work," *Fifth Domain*, February 27, 2018a. As of August 1, 2019: https://www.fifthdomain.com/dod/cybercom/2018/02/27/the-real-strength-in-cyber-commands-recent-work/

———, "DoD Makes Significant Updates to Cyber Operations Doctrine," *Fifth Domain*, June 22, 2018b. As of August 1, 2019: https://www.fifthdomain.com/dod/2018/06/22/dod-makes-significant-updates-to-cyber-operations-doctrine/

———, "How the Air Force's New Software Team Is Proving Its Worth," *C4ISRNET*, January 14, 2019. As of August 1, 2019: https://www.c4isrnet.com/it-networks/2019/01/14/how-the-air-forces-new-software-team-is-proving-its-worth/

Pope, Charles, "Goldfein Details Air Force's Move Toward a 'Fully Networked,' Multi-Domain Future," September 17, 2019. As of September 20, 2019: https://www.af.mil/News/Article-Display/Article/1963310/goldfein-details-air-forces-move-toward-a-fully-networked-multi-domain-future/

Porche, Isaac R., III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, Santa Monica, Calif.: RAND Corporation, RR-1600-A, 2017. As of June 4, 2020: https://www.rand.org/pubs/research_reports/RR1600.html

Priebe, Miranda, Alan J. Vick, Jacob L. Heim, and Meagan L. Smith, *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation*, Santa Monica, Calif.: RAND Corporation, RR-2959-AF, 2019. As of June 4, 2020: https://www.rand.org/pubs/research_reports/RR2959.html

Public Law 108-458, Intelligence Reform and Terrorism Prevention Act, December 17, 2004.

Public Law 113-291, National Defense Authorization Act of 2015, December 19, 2014.

Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, August 13, 2018.

The Public-Private Analytic Exchange Program, *The Threats to Undersea Communications*, Washington, D.C.: U.S. Department of Homeland Security and Office of the Director of National Intelligence, September 28, 2017. As of October 20, 2020: https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf

Rumbaugh, Devin M., "WPC Executes Milestone Air Force–Army Integration Exercise," April 25, 2018. As of August 1, 2019: https://www.af.mil/News/Article-Display/Article/1502725/wpc-executes-milestone-air-force-army-integration-exercise/

Russo, Joe, "A Lethal Combination: F-35 Joint Strike Fighter and M142 HIMARS Sensor-to-Shooter Integration," *Fires*, November–December 2017, pp. 37–42. As of October 23, 2020: https://sill-www.army.mil/fires-bulletin-archive/archives/2017/nov-dec/nov-dec.pdf

Sadusky, Aaron, James Ford, and Arthur Wilas, "Link 16 and AFATDS Interoperability: Addressing the Critical Gap in the Sensor to Shooter Chain," *Redleg Update*, March–April 2019, pp. 15–16. As of August 1, 2019: https://sill-www.army.mil/USAFAS/redleg/archive/2019/mar-apr-2019.pdf

Saltzman, Chance, "Multi-Domain Command & Control," unpublished briefing slides, Washington, D.C.: United States Air Force, November 27, 2017.

———, "Multi-Domain Ops in the 13OXX," Briefing Prepared for 705 Training Squadron, U.S. Air Force, November 13, 2018a.

———, "MDC2 Overview," paper presented at C2 Summit, Dubai, United Arab Emirates, 2018b. As of August 1, 2019: https://www.mitre.org/sites/default/files/publications/Special-Presentation-Gen%20Chance-Saltzman%20MDC2%20Overview%20for%20MITRE-June-2018.pdf

Sanger, David E., and Eric Schmitt, "U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS," *New York Times*, June 12, 2017. As of August 1, 2019: https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html

Schaar, Steven, Joint Targeting Effects Cell Update, unpublished briefing slides, Ramstein Air Force Base, Germany: U.S. Air Forces Europe and Air Forces Africa, January 24, 2019.

Schlight, John, *Help from Above: Air Force Close Air Support of the Army: 1946–1973*, Washington, D.C.: Air Force History and Museums Program, 2003. As of August 1, 2019: https://media.defense.gov/2010/May/26/2001330295/-1/-1/0/AFD-100526-039.pdf

Schoka, Andrew, "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat," *War on the Rocks*, April 3, 2019. As of August 1, 2019: https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/

Schubert, Frank, and Theresa Krause, *The Whirlwind War*, Washington, D.C.: Center for Military History, 1995. As of October 8, 2020: https://history.army.mil/html/books/070/70-30-1/cmhPub_70-30-1.pdf

Schwartz, Michael, "Leader Development: The Air Defense Artillery Transformation's Biggest Challenge," *Fires*, March–April 2017, pp. 15–17. As of August 1, 2019: https://sill-www.army.mil/fires-bulletin-archive/archives/2017/mar-apr/mar-apr.pdf

Smith, Grant J., "Multi-Domain Operations: Everyone's Doing It, Just Not Together," *Over the Horizon*, June 24, 2019. As of August 1, 2019: https://othjournal.com/2019/06/24/multi-domain-operations-everyones-doing-it-just-not-together/

Spirtas, Michael, "Are We Truly Prepared for a War with Russia or China?," *The Hill*, October 5, 2018a. As of December 3, 2019: https://thehill.com/opinion/national-security/410047-are-we-prepared-for-a-war-with-russia-or-china

———, "Toward One Understanding of Multiple Domains," *C4ISRNet*, May 1, 2018b. As of June 11, 2020: https://www.c4isrnet.com/opinion/2018/05/01/toward-one-understanding-of-multiple-domains/

Strout, Nathan, "Government Leaders Worry About GPS Spoofing, Hacking," *C4ISRNET*, May 17, 2019. As of August 1, 2019: https://www.c4isrnet.com/c2-comms/satellites/2019/05/17/government-leaders-worry-about-gps-spoofing-hacking/

Thornhill, Paula, and Mara Karlin, "The Chairman the Pentagon Needs," *War on the Rocks*, January 5, 2018. As of August 1, 2019: https://warontherocks.com/2018/01/chairman-pentagon-needs/

Townsend, Stephen, "Accelerating Multi-Domain Operations: Evolution of an Idea," West Point, N.Y.: Modern War Institute, July 23, 2018. As of August 1, 2019: https://mwi.usma.edu/accelerating-multi-domain-operations-evolution-idea/

TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, Joint Base Langley-Eustis, Va.: U.S. Army Training and Doctrine Command, December 6, 2018. As of August 1, 2019: https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

Trump, Donald J., "Establishment of the United States Space Force, Space Policy Directive-4," Washington, D.C.: Office of the President, February 19, 2019.

United Nations Charter, Article 2(4).

United Nations Charter, Article 51.

U.S. Air Force Central Command, "Joint Air Defense Exercise Sharpens Skills, Strengthens Partnerships," February 22, 2019. As of August 1, 2019: https://www.af.mil/News/Article-Display/Article/1765425/joint-air-defense-exercise-sharpens-skills-strengthens-partnerships/

U.S. Army Europe, "Summer 2019 Series of Exercises," webpage, 2019. As of August 1, 2019: https://www.eur.army.mil/SummerExercises/

U.S. Code, Title 10, Section 164.

U.S. Code, Title 10, Sections 801–964a.

U.S. Code, Title 50, Chapter 44 (National Security), 3001–3238.

U.S. Code, Title 50, Chapter 45 (Miscellaneous Intelligence Community Authorities), 3301–3383.

U.S. Code, Title 50, Chapter 46 (Central Intelligence Agency), 3501–3524.

U.S. Code, Title 50, Chapter 47 (National Security Agency), 3601–3618.

U.S. Code, Title 50, Section 3023, Director of National Intelligence.

U.S. Code, Title 50, Section 3024(a)(1)(C).

U.S. Cyber Command, "Mission and Vision," webpage, n.d. As of August 1, 2019: https://www.cybercom.mil/About/Mission-and-Vision/

U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision," *Joint Force Quarterly*, Vol. 80, No. 1, 2016, pp. 86–93. As of August 1, 2019: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_86-93_CyberCom.pdf

U.S. House of Representatives, "National Defense Authorization Act for Fiscal Year 2017, Conference Report," Washington, D.C.: U.S. Government Printing Office, November 30, 2016. As of August 1, 2019: https://www.congress.gov/114/crpt/hrpt840/CRPT-114hrpt840.pdf

U.S. Joint Staff Joint Force Development (J-7), *Cross-Domain Synergy in Joint Operations*, January 14, 2016.

U.S. Marine Corps Concepts and Programs, "Expeditionary Advanced Base Operations," webpage, n.d.-a. As of September 8, 2019: https://www.candp.marines.mil/Concepts/Subordinate-Operating-Concepts/Expeditionary-Advanced-Base-Operations/

———, "Littoral Operations in a Contested Environment," webpage, n.d.-b. As of September 8, 2019: https://www.candp.marines.mil/Concepts/Subordinate-Operating-Concepts/Littoral-Operations-in-a-Contested-Environment/

U.S. Navy, "A Design for Maintaining Maritime Superiority," January 2016. As of August 1, 2019: https://www.navy.mil/cno/docs/cno_stg.pdf

U.S. Transportation Command, "About USTRANSCOM," webpage, n.d. As of August 1, 2019: https://www.ustranscom.mil/cmd/aboutustc.cfm

Vick, Alan J., Richard M. Moore, Bruce R. Pirnie, and John Stillion, *Aerospace Operations Against Elusive Ground Targets*, Santa Monica, Calif.: RAND Corporation, MR-1398-AF, 2001. As of June 4, 2020: https://www.rand.org/pubs/monograph_reports/MR1398.html

Vick, Alan J., Sean M. Zeigler, Julia Brackup, and John Speed Meyers, *Air Base Defense: Rethinking Army and Air Force Roles and Functions*, Santa Monica, Calif.: RAND Corporation, RR-4368-AF, 2020. As of September 29, 2020: https://www.rand.org/pubs/research_reports/RR4368.html

Wall, Andru E., "Demystifying the Title 10–Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard Law School National Security Journal*, Vol. 3, No. 1, 2011, pp. 85–142. As of August 1, 2019: https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf

Watts, Barry, *The Military Use of Space: A Diagnostic Assessment*, Washington, D.C.: Center for Strategic and Budgetary Assessments, 2001. As of October 8, 2020: https://csbaonline.org/research/publications/the-military-use-of-space-a-diagnostic-assessment

Zetter, Kim, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014. As of August 1, 2019: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

PROJECT AIR FORCE

To counter increasingly capable near-peer competitors, the U.S. military services have been developing new concepts for multidomain operations (MDOs), which aim to more fully integrate operations in the air, land, maritime, space, and cyber domains, as well as the electromagnetic spectrum and information environment. Although the joint force already conducts some MDOs, current initiatives aim to expand the scope and scale of such operations and to change command-and-control (C2) constructs to better enable MDOs.

To identify potential impediments to MDOs, the authors reviewed joint warfighting principles; current laws, regulations, and doctrine; and interview responses. The authors identified aspects of the current C2 construct for joint operations that could prevent multidomain options from being considered, make MDOs too time consuming to plan, or create too much planning uncertainty. The authors propose four alternative approaches to joint all-domain command and control (JADC2) and provide criteria for assessing alternative constructs.

$38.00

ISBN-10 1-9774-0628-9
ISBN-13 978-1-9774-0628-6

www.rand.org

RR-A381-1