RESEARCH BRIEF

Multiple Dilemmas for the Joint Force

Joint All-Domain Command and Control

To counter increasingly capable near-peer competitors, the U.S. military services have been developing new concepts for multi-domain operations (MDOs)—operations that involve two or more of the five domains: air, land, maritime, space, and cyber. The joint force already conducts MDOs today, but U.S. military leaders argue that MDOs have been episodic and that operations in different domains have often been deconflicted rather than truly integrated. Also, the joint force is grappling with how to integrate space and cyber, which are emerging as more important warfighting domains. The Air Force is now leading the joint initiative to assess how the current command and control (C2) construct might need to adapt to enable MDOs.

This brief summarizes research results that identified potential impediments to MDOs in the current operational C2 construct for joint operations. The study drew on joint warfighting principles to identify C2 characteristics that could prevent MDO options from being considered, could make MDOs too time-consuming to plan, or could create too much planning uncertainty. Researchers analyzed current laws, regulations, and joint doctrine and conducted more than 150 interviews to identify specific aspects of the current C2 structure that have these characteristics. The study also developed four alternative joint all-domain C2 (JADC2) constructs for further analysis and experimentation.

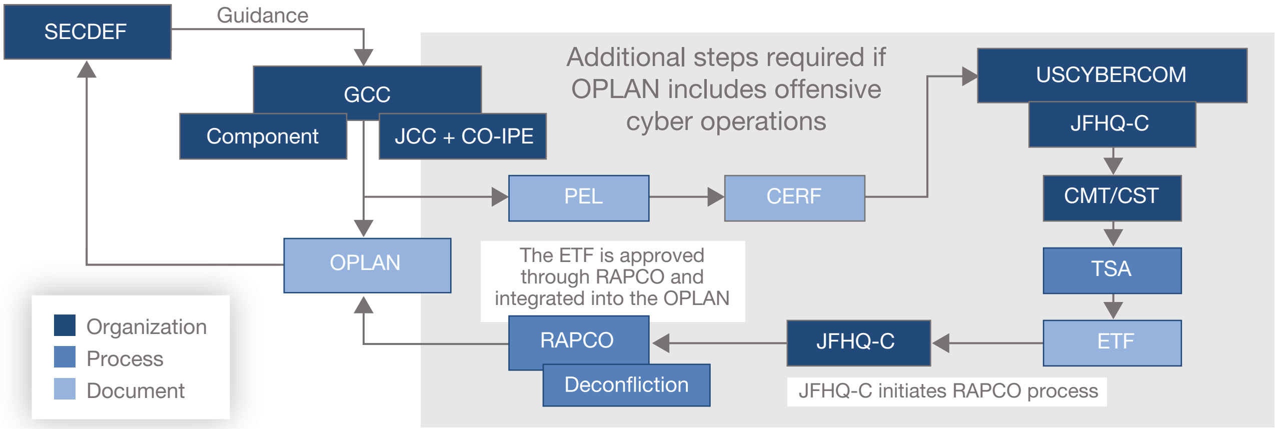
Potential Impediments to MDOs in the Current C2 Construct

More Steps and Approvals Are Sometimes Required to Integrate Multiple Domains

The Air Force vision of faster decisionmaking might not be realized if planning, executing, or assessing multidomain options requires more time or involves more complexity than single-domain alternatives. RAND researchers found that integrating multiple domains can involve additional steps and approvals when MDOs involve capabilities controlled by multiple organizations. For example, as shown in Figure 1, if the air component wanted to include offensive cyber operations in its suppression of enemy air defense plans, it would need to account for all steps in the offensive cyber operations request and approval process shown, as well as typical approvals for air operations plans.

FIGURE 1

Offensive Cyber Request and Approval Process


SECDEF
Guidance
GCC
Component
JCC + CO-IPE
Additional steps required if OPLAN includes offensive cyber operations
USCYBERCOM
JFHQ-C
PEL
CERF
CMT/CST
OPLAN
The ETF is approved through RAPCO and integrated into the OPLAN
TSA
Organization
Process
Document
RAPCO
JFHQ-C
ETF
Deconfliction
JFHQ-C initiates RAPCO process

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

NOTES: 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—Cyber; OPLAN = Operation Plan; PEL = Priority Effects List; RAPCO = Review and Approval Process—Cyberspace Operations; SECDEF = Secretary of Defense; TSA = Target System Analysis; USCYBERCOM = U.S. Cyber Command.

Planners Have Insufficient Expertise or Access to Information on Relevant Domains

To generate multidomain options, planners must understand the capabilities and limitations of operations in all domains. They also need information about what forces are available and 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 situational awareness. 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 multidomain planners at the operational level need access to enough expertise and information to know what options are available and appropriate in a given situation. Component planning staffs specialize in certain domains and do not have resident experts or easy access to information on all domains. Coordination with other components can produce multidomain options, but some options might be missed because planners with expertise on multiple domains are not working together to tackle an operational problem.

MDOs Can Increase Dependence on Vulnerable Communications

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 (CONUS), are considered most vulnerable because 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, although the larger number of communications links and redundant communications options make these communications harder to degrade. Air Force leaders aspire to develop a C2 construct that is more resilient to attacks on both long-distance and local communications. An impediment exists when the current C2 construct requires planning, executing, or assessing an MDO to rely more heavily on communications than on single-domain operations. MDOs that involve detailed coordination with CONUS-based space or cyber organizations, for example, could be more vulnerable to disruption than MDOs that involve in-theater forces.

A Single-Domain-Centric or Single-Service-Centric Mindset Is Present

Another potential threat to the Air Force vision for JADC2 is a mindset that prevents planners 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 use helicopters and request air support, and the joint force air component commander is concerned about interdicting adversary forces on the ground. Still, functional and service components might have cultural biases or organizational structures that lead them to focus on solutions that employ forces from their primary domain. These biases could lead planners to overlook or eschew solutions in other domains.

Establishing Priorities for the High-End Fight

Specific concepts for MDOs are still emerging, so it is not yet clear which C2 changes to address the above impediments are most important or how beneficial such changes would be. At the same time, the joint force has not decided how to prioritize C2 changes to enable MDOs with those needed to meet two other C2 challenges in a conflict with a near-peer threat:

- **Global integration for transregional conflict:** A conflict with a near-peer competitor will likely cross combatant command (CCMD) boundaries. For example, the adversary could launch an attack on countries near its periphery, conduct cyberattacks on the U.S. homeland, contest U.S. space communications, and harass U.S. forces in a third region. The joint force has been testing nascent concepts for global integration to manage priorities, synchronize effects, and follow a coherent global strategy. Such changes could be in tension with C2 changes to reduce the number of steps and approvals for MDOs.
- **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. Concepts for distributed control therefore aim to give forward forces the authority and capability to make decisions based on the intent of higher headquarters. Pacific Air Forces, in particular, has been developing a concept and has taken steps to empower wings to act as distributed control nodes, but there is still much work to be done. It is unclear whether these concepts would give forward forces the authority or capability to plan and execute joint all-domain operations.

Four C2 Constructs

Given the nascent state of all-domain operations concepts and unresolved questions about how to balance the two other C2 challenges, the joint force should—before making major changes to structures—investigate and experiment with alternative C2 constructs and assess possible impacts on warfighting effectiveness. The RAND team developed four GCC JADC2 constructs that span the range from small changes in the current C2 construct to more significant ones that could be the basis for this future analysis. Each of the constructs has advantages and drawbacks, as shown in Table 1.

A combatant commander (CCDR) could use aspects of some of the constructs described here in a hybrid approach to JADC2. For example, CCDRs might want to conduct contingency planning "sprints" at the CCMD level that draw resources from the components for short durations but continue to use functional components during wartime.

Conclusions

The results above yield the following 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.
- Three emerging C2 concepts for conflict against a near-peer competitor—global integration, JADC2, and distributed control—are developing in parallel and need to be investigated to determine how they might fit together in a high-end fight.
- Operational planning is component-centered, creating the risk of insufficient expertise on all domains and a preference for solutions in certain domains.
- MDOs often involve forces controlled by multiple organizations, increasing C2 complexity.

TABLE 1

Advantages and Disadvantages of Alternative JADC2 Constructs

Alternative Construct	Main Advantages	Main Disadvantages
Incremental Change Experts from all domains are embedded in all component planning staffs; control of capabilities remains divided among components	• Increases the likelihood that multidomain options will be considered • Builds on existing approach; as such, it is the least disruptive • Increases planning redundancy at dispersed locations, thus likely improving resilience and ability to reconstitute planning capabilities	• Might not overcome domain-centric bias of components given small number of additional planners • Might still involve additional steps and approvals from relevant components to plan and execute MDOs • Increases staff size with likely increased costs and decreased mobility
Air, Space, and Cyber Component A single component plans for and controls in-theater forces in three domains and coordinates for support in these domains from outside the theater	• Reduces the number of steps required for planning MDOs that involve air, space, and cyber operations • Builds on expertise and relationships already present in the air operations center	• Having multidomain rather than all-domain planning could undervalue other domains
CCDR-Centric Involves all-domain operational planning and control of forces at the combatant commander (CCDR) level; components focus on tactical planning and execution	• Reduces steps and processes for MDOs • Involves joint, all-domain expertise and culture	• Could overtask CCDR and staff because of greater span and control • If collocated, increases vulnerability to adversary attack
Line-of-Effort Components Organizes components around lines of effort instead of domains during wartime	• Has many of the same advantages of the CCDR-centric approach but places authorities at a lower echelon of command	• Has more-involved peacetime to wartime transition • Makes it more difficult to move forces between mission areas

- Single-service initiatives cannot resolve C2 impediments to MDOs that involve forces from multiple CCMDs or services.
- Reducing the number of steps and approvals for space, cyber, and intelligence operations might facilitate MDOs but reduce efficiency and increase risk.
- MDOs that rely on planning, approval, or execution from outside the theater could be particularly vulnerable in a communications-contested environment.

Recommendations

Based on these conclusions, the authors offer the following recommendations:

- Specify MDO concepts and thoroughly assess operational costs and benefits to inform JADC2 changes and investments.
- Set priorities among concepts for global integration, JADC2, and distributed control.
- Experiment with alternative JADC2 constructs to assess their 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.

This brief describes research conducted in RAND Project AIR FORCE and documented in *Multiple Dilemmas: Challenges and Options for All-Domain Command and Control*, by Miranda Priebe, Douglas C. Ligor, Bruce McClintock, Michael Spirtas, Karen Schwindt, Caitlin Lee, Ashley L. Rhoades, Derek Eaton, Quentin E. Hodgson, and Bryan Rooney, RR-A381-1, 2020 (available at www.rand.org/t/RRA381-1). To view this brief online, visit www.rand.org/t/RBA381-1. The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.