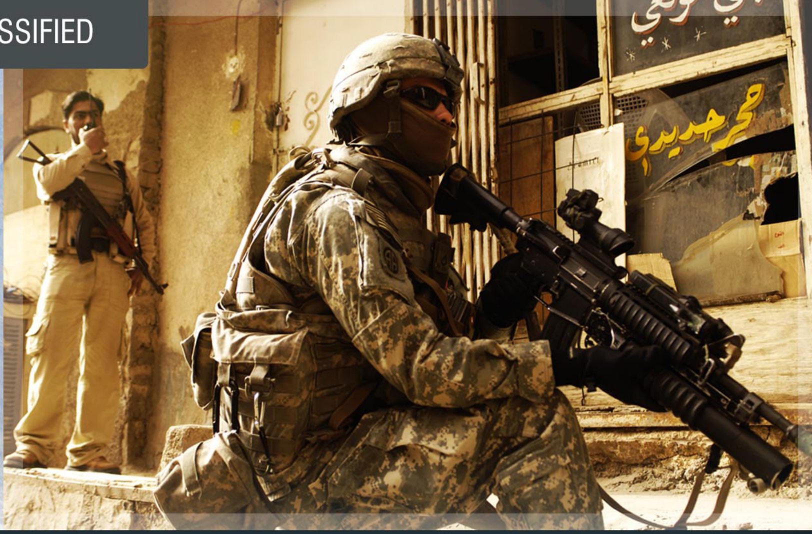
UNCLASSIFIED



Cross-Domain Synergy in Joint Operations

• PLANNER'S GUIDE •

United States Joint Staff Joint Force Development (J7) - Future Joint Force Development

14 January 2016

PREFACE

1. Introduction

Today's security environment continues to change with adversaries more able to challenge U.S. military capabilities. It is imperative the U.S. joint force develop ways to combine its powerful capabilities across all domains (air, land, maritime, space, and cyberspace). The application of cross-domain solutions requires developing joint planning experience to enhance the Joint Force Commanders' (JFC) capabilities against a wide array of adversaries.

2. Purpose

The purpose of the planner's guide is to provide information and approaches to integrate efficiently and effectively each domain's capabilities to accomplish the JFC's mission.

3. Development

The Chairman of the Joint Chiefs of Staff directed the development of the planner's guide to operationalize cross-domain synergy as described in the Joint Operational Access Concept (JOAC). The guide is neither authoritative nor does it represent consensus across the Joint Force. However, it is grounded in a comprehensive literature review and over one hundred interviews with Combatant Command staff officers and Services' academic faculty.

4. Application

The guide organizes cross-domain planning information for the use of planning staffs. It applies to the planning activities of the Joint Staff, Combatant Commands, sub-unified commands, joint task forces, subordinate components of these commands, the Services, and Department of Defense (DOD) agencies supporting joint operations.

5. Contact Information

Please direct suggestions for improvement to Major Kevin Schieman, Joint Staff J-7, FJFD, JCD; kevin.p.schieman.mil@mail.mil, (757) 203-5221.

Paul E Bauman

PAUL E. BAUMAN
Brigadier General, U.S. Air Force
Deputy Director, J-7
Future Joint Force Development

TABLE OF CONTENTS

LIST OF FIGURE (cont.)

LIST OF TABLE

Intentionally Blank

CHAPTER 1

CROSS-DOMAIN SYNERGY OVERVIEW

A. General

1. Introduction

The United States currently enjoys significant overmatch in the air, land, maritime, and space domains. However, adversaries are challenging that overmatch by creatively avoiding traditional U.S. strengths. This inventiveness allows adversaries to achieve their objectives in spite of U.S. military dominance in individual domains.

Military operations are becoming more complex with the rise in the number and variety of options available to commanders. Today's warriors must contend with computers and satellites in addition to bayonets and bullets. The expansion of military activity beyond the air, sea, and land domains to space and cyberspace has broadened the community of warfighters to include computer scientists and astrophysicists. Integrating this expertise to achieve operational effectiveness against an adaptive, complex enemy is the mission of Joint Force Commanders (JFCs) and their staffs.

> *…**future Joint Forces will leverage better integration to improve cross-domain synergy-the complementary vice merely additive employment of capabilities across domains time and space. While the U.S. military maintains unique advantages in every domain, it is our ability to project force across domains that so often generates our decisive advantage.***
> ***Capstone Concept for Joint Operations: Joint Force 2020,* (Washington, DC: U.S. Department of Defense, 2012, page 7).**

Cross-domain synergy is *"the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others*.*"[1] In the conduct of joint operations, the JFC routinely employs air, land, maritime, space, and/or cyberspace capabilities to overwhelm an adversary's ability to decide and act.[2] The commander seeks to optimize the balance between effectiveness and efficiency when combining joint capabilities. This requires employing capabilities so that they reinforce each other without undue redundancy or overlap. Synergy occurs when two or more of these actions combine to produce an effect greater than the sum of their individual effects. The JFC increases the likelihood of achieving a synergistic effect with the integrated employment of joint capabilities across multiple domains.

Cross-domain synergy is not an end in itself, but a by-product of effective joint planning. On rare occasions, a single domain solution is appropriate and better suited to accomplishing the mission. However, most missions call for capabilities from all five domains thus generating the need for competence in the integration of cross-domain capabilities. The planner's efforts to

[1] U.S. Department of Defense, *Joint Operational Access Concept (JOAC) Version 1.0.* (Washington, DC: United States Department of Defense, 2012), Foreword. http://www.defense.gov/pubs/pdfs/JOAC_Jan%2012_Signed.pdf.
[2] U.S. Department of Defense, *JOAC,* ii.

integrate and synergize cross-domain capabilities will allow the JFC to attain the ultimate desired goal: mission accomplishment.

Throughout this planner's guide, the adjective "cross-domain" describes operations, capabilities, and solutions which employ tools from one domain to create effects in another domain (air, land, maritime, space, and cyberspace). The guide highlights the importance of cross-domain solutions, the nuances of the domains, and the requirement for strong partnerships. It offers methods to engender innovative solutions from a large, diverse group and then merge their ideas into the planning process. While the planner's guide will assist all staffs, it targets coordinating staff (numbered J-directorate) members responsible for orchestrating the contributions from multiple domains. The planner's guide is both a ready reference for joint procedures and a basic source of information about each domain. Improved understanding of each domain will improve the employment of cross-domain capabilities and increase the potential for achieving cross-domain synergy.[3]

The planner's guide is structured for quick retrieval of information.

- Chapter 2 addresses the challenges to cross-domain synergy.
- Chapter 3 discusses means to foster cross-domain synergy via the Joint Operations Planning Process (JOPP).
- Chapter 4 describes each domain along with A) how the DOD has organized to operate within that domain and B) what it means to a joint planner trying to integrate that domain's capabilities into a comprehensive plan.
- Appendix A provides several recommended planning practices. These maxims are useful practices followed by experienced planners and should be deviated from only after careful consideration of risks.
- Appendix B discusses the agencies and partners that a joint staff planner may encounter and how each can be used to develop and improve cross-domain solutions.
- Appendix C is the bibliography of publications cited in this guide.
- Appendix D provides a tailored reference list. Beyond a mere listing, Appendix D describes publications for staff officers who would like to learn more on a given topic (e.g. planning, cyberspace).
- Glossary provides a listing of abbreviations (Part I) and terms and definitions (Part II).

2. Historical Background and Examples

History demonstrates that skillful blending of combat arms can achieve decisive effects.[4] The idea of combining weapons systems in battle is age old: from the coordination of chariots, archers, and spearmen in the armies of the ancient world to the cavalry, musketeers, and pikemen at the dawn of the age of gunpowder. In the early 17th century, King Gustavus Adolphus of Sweden combined improved firearms technology with innovative organization to create the world's first modern combined arms army. The Swedish monarch employed infantry brigades comprised of infantry, mobile field artillery, and heavy cavalry in a manner that combined fire, maneuver, and shock effect in a single fighting unit. Each arm of one of Gustavus Adolphus' brigades supported and enhanced each other's effectiveness.[5] The integration of cross-domain

[3] U.S. Department of Defense, *Capstone Concept for Joint Operations: Joint Force 2020*, Washington, DC: U.S. Department of Defense, 2012, 7.

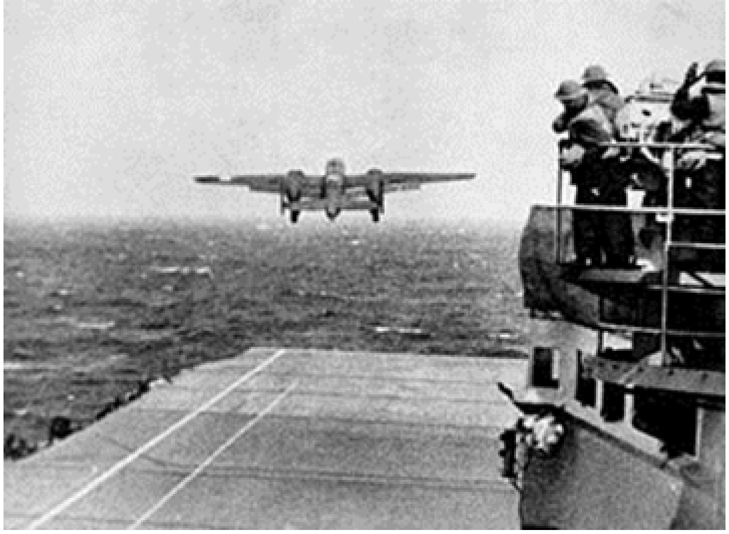
[4] Michael Evans and Alan Ryan (Editors), *From Breitenfeld to Baghdad: Perspectives on Combined Arms Warfare, Land Warfare Studies Centre Working Paper No.122,* (Dunmore, Australia: Land Warfare Studies Centre, 2003), 9.

[5] Evans and Ryan, *From Breitenfeld to Baghdad: Perspectives on Combined Arms Warfare,* 9.

capabilities is merely an extension of the principles behind combining arms – the whole can be greater than the sum of the parts when skillfully integrated and employed.

Cross-domain operations have been a strength of the U.S. Joint Force for decades.[6] Before the invention of manned-flight, the U.S. military combined land- and sea-based capabilities to win pivotal victories at Yorktown (1781), Vicksburg (1863), and Santiago (1898). With the advent of flight, the Joint Force added air-based capabilities to their growing and rapidly modernizing arsenals. In World War II and Korea, amphibious landings exemplified cross-domain operations.[7] Below are two examples of successful (Figures I-1 and I-2) cross-domain approaches.

Cross-Domain Synergy Success: The Doolittle Raid 18 April 1942



The 18 April 1942 Doolittle Raiders attack represents an example of innovative thinking leading to a cross-domain solution. In one of World War II's first truly joint operations, 80 crewmembers of the U.S. Army Air Forces trained under the guidance of U.S. Navy pilots to master taking off in a B-25 Mitchell medium bomber from the deck of an aircraft carrier. Their efforts resulted in the first aerial attack of the Japanese home islands by U.S. bombers. Thinking out-of-the-box as a true cross-domain planner, Captain Francis Low, United States Navy (USN), a submarine officer and member of the Chief of Naval Operations staff, conceived the idea and worked closely with the Army Air Forces to turn his idea into reality. Sixteen B-25s took off from the USS Hornet to bomb military targets in Japan. Led by then-Lieutenant Colonel Jimmy Doolittle, the Raiders brought the war to the enemy and, while not inflicting serious damage, the mission's impact upon American morale was incalculable. Moreover, the mission compelled the Japanese to reallocate some of their forces to homeland defense and led Admiral Yamamoto to the Battle of Midway, a disaster for the Japanese navy which turned the tide of the war in the Pacific. The Doolittle Raid is a great example of integrating the capabilities of two domains to achieve an effect greater than they could do individually.

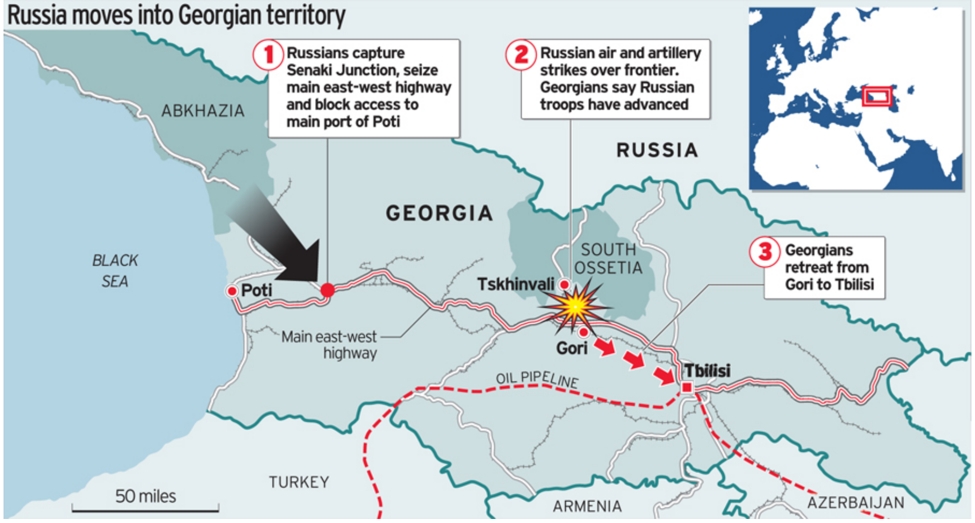
Figure I-1. LtCol Jimmy Doolittle takes off in B-25 from the USS Hornet[8]

[6] U.S. Department of Defense, *JOAC,* 16.

[7] William O. Odom and Christopher D. Hayes, "Cross-Domain Synergy: Advancing Jointness", *Joint Forces Quarterly 73 2nd Quarter 2014*, 124.

[8] National Museum of the United States Air Force. "The Doolittle Raiders – 18 April 1942"

Cross-Domain Synergy Success: Russian Cyber Actions against Georgia August 2008


Russia moves into Georgian territory
1 Russians capture Senaki Junction, seize main east-west highway and block access to main port of Poti
2 Russian air and artillery strikes over frontier. Georgians say Russian troops have advanced
3 Georgians retreat from Gori to Tbilisi
ABKHAZIA
RUSSIA
GEORGIA
BLACK SEA
SOUTH OSSETIA
Poti
Tskhinvali
Gori
Tbilisi
Main east-west highway
OIL PIPELINE
TURKEY
ARMENIA
AZERBAIJAN
50 miles

(Source: Perry-Castaneda Library Map Collection University of Texas www.lib.utexas.edu/maps/georgia_war_2008.html)

The war between Georgia, Russia, and the Russian-backed self-proclaimed republics of South Ossetia and Abkhazia saw some 35,000-40,000 Russian and allied forces, augmented by significant air and naval forces, confront some 12,000-15,000 Georgian forces with little air and minimal naval capability. Although a short and limited conflict, it was historic and precedent setting. This appears to be the first coordinated cyberspace attacks synchronized with major combat actions in the other warfighting domains, primarily land and air.

Russian offensive cyberspace operations began several weeks before the outbreak of kinetic operations. Russian cyber intelligence units conducted reconnaissance on important sites and infiltrated Georgian military and government networks in search of data useful for the upcoming campaign. During this period, the Russian government began organizing the work of Russian cyberspace militias - irregular hackers outside the government - that would support the campaign and provide cover for some of the government’s operations. Russian government and cyberspace militias conducted rehearsals of attacks against Georgian targets. When the kinetic battle started on 7 August, Russian government and irregular forces conducted distributed denial-of-service attacks on Georgian government and military websites. These attacks disrupted the transmission of information between military units and between offices in the Georgian government. Russian cyberspace forces attacked civilian sites near the action of kinetic operations with the goal of creating panic in the civilian population. For example, in the town of Gori, Russians disabled government and news websites with distributed denial-of-service attacks just prior to an air attack. Cyberspace interdiction (attacks concentrated on tactical data links and data fusion centers) degraded and disrupted the Georgians’ decision cycle limiting their military response. Russian forces also attacked Georgian hacker forums in order to pre-empt a retaliatory response against Russian cyberspace targets.

The Russians were very sophisticated in their target selection. For example, Russians refrained from attacking Georgia’s most important asset, the Baku-Ceyhan oil pipeline and associated infrastructure. By holding this target in reserve, the Russians gave Georgian policymakers an incentive to quickly end the war. Faced by overwhelming Russian air power, armored attacks on several fronts, an amphibious assault on its Black Sea coastline, and devastating cyber-attacks, Georgia had little capability of kinetic resistance. Its best hope lay with strategic communications: transmitting to the world a sympathetic message of rough treatment at the hands of Russian military aggression. But Russia effectively used cyberspace operations to disrupt the Georgian government’s ability to assemble and transmit such a plea thus removing Georgia’s last hope for international support.

In summary, Russian planners tightly integrated cyberspace operations with their kinetic, diplomatic, and strategic messaging operations. The Russo-Georgian war provides a case study for joint planners preparing for a future conflict, involving the new domain of cyberspace.

Figure I-2. Russia-Georgia War 2008[9]

[9] David M. Hollis, “Cyberwar Case Study: Georgia 2008,” Small Wars Journal, Modified January 2011/Accessed November 2015. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

3. Overview of Contemporary Domains

Currently, Joint Force Commanders integrate the traditional air, land, and maritime domains more easily into joint operations than the newer domains of space and cyberspace. Several reasons exist for this uneven integration, including staff officers' unfamiliary with the new domains and a centralized command and control (C2) structure for the capabilities of new domains.

Air

The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible. Source: JP 3-30

Land

The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals. Source: JP 3-31

Maritime

The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. Source: JP 3-32

Space

A medium like the land, sea, and air within which military activities shall be conducted to achieve US national security objectives. JP 1-02

Cyberspace

A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Source: JP 3-12

B. Cross-Domain Synergy

1. Introduction

The term "cross-domain synergy" first appeared in the 2012 *Joint Operational Access Concept* (JOAC) as a solution to anti-access/area denial threats (A2/AD). However, because it applies in nearly all military situations, it also became a key element of the *Capstone Concept for Joint Operations: Joint Force 2020* (CCJO). This ability to operate in multiple domains provides JFCs with many opportunities to apply force against enemy weaknesses. Cross-domain approaches enable JFCs to overwhelm an adversary with many, difficult problems at multiple points in time and space. The disruption of the adversary's ability to observe, orient, decide, and act (OODA) achieves synergy when the cross-domain activities result in second- and third-order effects on the adversary's ability to fight.

Cross-domain operations require interoperability and routine integration of cross-domain capabilities. Cross-domain operations are more complex than single domain options, but they have advantages. The Joint Force maintains extensive C2 networks and mechanisms to offset the complexity inherent in coordinating cross-domain operations. JFCs use those networks and staff expertise (joint, interagency, and multinational) to implement innovative cross-domain solutions to overwhelm their adversaries and achieve objectives. Proficiency hinges on habitual integration of capabilities from all domains.

2. Anti-Access/Area Denial (A2/AD)

A2/AD strategies are a defining characteristic of today's operational environment. Confronting this challenge will require more integration – across all domains and at all echelons – than ever before.[10]

The JOAC defines **anti-access** as "those capabilities, usually long-range, designed to prevent an advancing enemy from entering an operational area."[11] **Area denial** consists of "those actions and capabilities, usually of shorter range, designed not to keep an opposing force out, but to limit its freedom of action within in an operational area."[12]

Since the end of the Cold War, the Joint Force has enjoyed largely unhindered access to and freedom of action within nearly every theater of operation. A constellation of alliances and partnerships, dominant forward posture, and unchallenged military-technical advantages vis-à-vis potential military competitors provided U.S. military forces with persistent regional influence and points of entry into contested theaters of operation. The United States enjoyed unchallenged operational access to Iraq and Afghanistan. Supplying operations in landlocked Afghanistan, in particular, would have been much more difficult without unfettered access to the seaports of Karachi and Kuwait. The Joint Force's remotely piloted aircraft roamed the skies of Iraq and Afghanistan free from antiaircraft artillery and surface-to-air missile threats to find, surveil, and strike insurgent targets. These advantages are eroding due to adversary adoption of sophisticated A2/AD strategies that combine technical and nontechnical capabilities.[13]

A2/AD strategies undermine U.S. power projection by denying freedom of movement and freedom of action in and around areas of interest. Implications of A2/AD, however, reach far beyond that of conflict. A2/AD not only increases the dangers of conventional war, but also offers non-state actors options to increase the effectiveness of irregular or hybrid warfare.[14] To successfully operate in an A2/AD environment, the U.S. military must prepare by understanding the operational implications presented by modern technology and weaponry.[15] The proliferation of A2/AD weapon systems and asymmetric capabilities strongly suggests the U.S. military must develop innovative concepts and employ cross-domain solutions to address potential A2/AD contingencies. A future adversary is unlikely to make the same mistake that Saddam Hussein made - twice - when he allowed a U.S. led coalition to mass a large, decisive military force on Iraq's borders.[16]

[10] GEN Martin Dempsey, U.S. Army, Chairman of the Joint Chiefs of Staff, "Release of the Joint Operational Access Concept", DOD Live, January 12, 2012. http://www.dodlive.mil/index.php/2012/01/release-of-the-joint-operational-access-concept-joac/

[11] U.S. Department of Defense, *JOAC*, i.

[12] U.S. Department of Defense, *JOAC*, i.

[13] Nathan Freier, "Challenges to American Access: The Joint Operational Access Concept and Future Military Risk," Center for Strategic and International Studies csis.org, Published January 5, 2012. http://csis.org/publication/challenges-american-access-joint-operational-access-concept-and-future-military-risk

[14] Maj Christopher J. McCarthy USAF, *Anti-Access/Area Denial: The Evolution of Modern Warfare*, (Newport, RI: U.S. Naval War College, 2012), 10.

[15] McCarthy, *Anti-Access/Area Denial*, 9.

[16] Mark Gunzinger with Chris Dougherty, *Outside-In: Operating from Range to Defeat Iran's Anti-Access and Area-Denial Threats,* (Washington, DC: Center for Strategic and Budgetary Assessments, 2011), 19.

3. Joint Operational Access Concept (JOAC)

The JOAC foreshadows an era of increased constraints on U.S. military actions abroad. U.S. military power now competes on a substantially more complicated playing field in a number of important regions around the world. Consequently, U.S. policymakers and military commanders should anticipate novel obstacles to global access emerging from some combination of improved adversary military and paramilitary capability. In short, the comprehensive A2/AD challenge is rapidly compounding, necessitating innovative U.S. military responses.

The JOAC proposes the concept of cross-domain synergy to achieve operational access in the face of armed opposition under a variety of conditions.[17] Operational access is the ability to project military force into an operational area with sufficient freedom of action to accomplish the mission.[18] Operational access does not exist for its own sake, but rather serves the United States' broader strategic interests, whether to ensure access to commerce, demonstrate U.S. resolve, or defeat an adversary in combat. Operational access is the Joint Force's contribution to assured access: the unhindered national use of the global commons and select sovereign territory, waters, airspace, and cyberspace.[19] Confronting this challenge will require more integration – across all domains – than ever before.[20]

The ability to integrate capabilities from across multiple domains affords JFCs with numerous, powerful options.[21] For example, undersea operations can be used to defeat air defense systems, air forces can be used to eliminate submarine or maritime mine threats, ground forces can defeat threats to space systems, or cyberspace capabilities can be used to disrupt adversary command and control. Put simply, traditional understandings of Service missions, functional responsibilities, and employment of capabilities from particular domains must not hamper imaginative joint operational planning.[22]

JOAC cites the goal of cross-domain synergy is to establish superiority in some combination of domains that will provide the freedom of action required by the mission. The combination of domain superiorities will vary with the situation, the adversaries' capabilities, and the mission. Superiority in any domain may not be widespread or permanent; it will usually be local and temporary. Additionally, domain integration must occur at lower echelons, generating the tempo that is often critical to exploiting fleeting local opportunities for disrupting the adversaries' systems, and will require the full inclusion of space and cyberspace operations into the traditional air-land-maritime battlespace.[23] Chapter 2 describes challenges to cross-domain synergy in more detail and how JFCs and their staffs might overcome them.

[17] The use of *operational* in this context refers to military operations broadly and is not restricted to the operational level of war. The 2015 *National Military Strategy* (NMS) describes the national strategy for defeating hostile anti-access/area-denial strategies. Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011; Redefining America's Military Leadership,* (Washington, DC: Department of Defense, 2011), 8.

[18] U.S Department of Defense, *JOAC,* i.

[19] U.S Department of Defense, *JOAC,* i.

[20] U.S. Department of Defense, *JOAC,* i.

[21] Air-Sea Battle Office, *Air-Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges*, (Washington, DC: Air-Sea Battle Office, 2013), 5. http://www.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf

[22] Air-Sea Battle Office, *Air-Sea Battle*, 5.

[23] U.S. Department of Defense, *JOAC*, ii.

CHAPTER 2

ADDRESSING CHALLENGES TO CROSS-DOMAIN SYNERGY

A. General

Cross-domain solutions inherently incur additional command and control burdens. By comparison, single domain operations will have less to plan and orchestrate, minimizing C2 friction. However, single domain operations rarely occur. Overcoming the friction of employing multiple domains requires practice and habitual interaction with domain experts. The primary challenge to cross-domain synergy is institutionalizing participation in the JFCs' decision making processes from a diverse community of warfighters. Other challenges include training and education shortfalls, sub-optimal manning, and classification/compartmentalization of many cross-domain capabilities.

CHALLENGES TO CROSS-DOMAIN SYNERGY

1. **Primary Challenge: Bringing varied and specific expertise to bear on the problem**
2. **Secondary Challenges:**
    a. **Training and education shortfalls**
    b. **Manning**
    c. **Classification and compartmentalization of capabilities**

B. Primary Challenge

The major challenge JFCs face is obtaining domain expertise and integrating it into planning and operations. It requires greater inclusion of many, diverse subject matter experts in JFC decision making processes. JFC's must assess the level of experience and knowledge resident in their staffs. Ideally, staff membership includes experts from across the warfighting communities and each domain who represent their domain during planning and operations. To this end, JFCs must recruit subject matter experts (SMEs) and incorporate their contributions within their activities.

C. Addressing the Primary Challenge

JFCs must aggressively secure wide expertise and integrate it into their staff processes. Fortunately, DOD provides multiple mechanisms for accessing expertise. Through a manning document, joint staffs may request domain experts from the Services. Several agencies also offer support for staffs with inadequate resident expertise. Liaison officers help knit headquarters and organizations by enhancing coordination. Once on board, the JFC must integrate the subject matter experts into the staff. Again, several mechanisms are available to build cohesion, including boards, bureaus, centers, cells, working groups (B2C2WG), planning groups, and battle rhythm. By carefully structuring and tailoring the interaction of the headquarters staff, JFC's and staff leads can leverage the best expertise from many diverse elements.

A listing of common mission partners is provided in Appendix B, JP 2-01, JP 3-08, and JP 3-16.

1. Core Staff, Augmentation, Support Elements and Liaison Requirements

a. The Core Staff. Combatant Commands (CCMDs) or Joint Task Forces (JTFs) **core staff may lack the expertise to address all aspects of the mission**. A JTF formed around a single Service component or headquarters will usually augment the core staff with outside experts based on the mission and force composition. **Mission analysis should consider necessary HQ capabilities and other related functions**.

MISSION ANALYSIS FACTORS

1. **Likely duration of the mission.**
2. **Geographic scope of the mission.**
3. **Interagency requirements.**
4. **Multinational involvement.**
5. **Campaign or joint operation phasing.**
6. **Communication strategy requirements.**
7. **Logistic support requirements.**

An assessment of the core staff's expertise will determine the type and amount of augmentation required to fill the gaps. The assessment occurs at initial formation of the staff and throughout the duration of the mission. Generally, the **staff mirrors the JTF composition** in proportion of membership, experience, and influence of position and rank of members among participating Services, functional components, subordinate task forces, supporting commands, and multinational forces.

(1) For example, a JTF formed around an Army Corps HQ for a ground combat mission will likely augment the core staff with experts to assist with planning and executing air, space, cyberspace, and special operations not to mention the probability of integrating a significant number of multinational liaisons.

(2) United States led JTFs should expect to participate as part of a Multi-National Force (MNF) (i.e., a coalition or alliance) in most future military endeavors. Such participation with multi-national forces may complicate normal unilateral organization, planning, and operations.

There are several sources for building on a core staff that are depicted in Figure II-1 below:

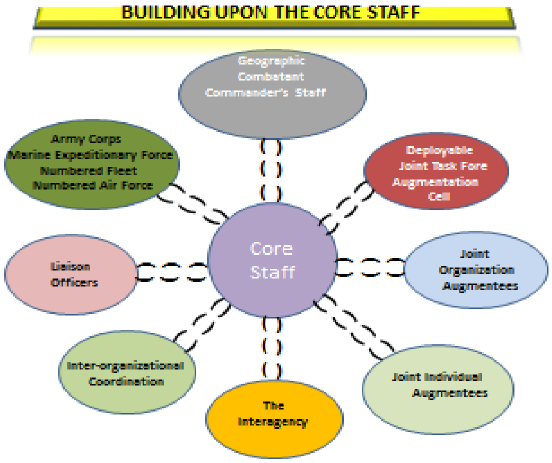

BUILDING UPON THE CORE STAFF
Geographic Combatant Commander's Staff
Army Corps
Marine Expeditionary Force
Numbered Fleet
Numbered Air Force
Deployable Joint Task Fore Augmentation Cell
Liaison Officers
Core Staff
Joint Organization Augmentees
Inter-organizational Coordination
The Interagency
Joint Individual Augmentees

Figure II-1. Building Upon the Core Staff

[1] U.S. Joint Chiefs of Staff, *Joint Publication 3-33 Joint Task Force Headquarters*, (Washington, DC: U.S. Joint Chiefs of Staff, 2012), II-3.

When determining requirements to augment the staff, the Commander, J-5, and the Joint Planning Group (JPG) Lead should look to assemble subject matter expertise from across all five domains. This will mitigate one of the initial challenges of ensuring the JPG includes the right mix of domain expertise.

b. Augmentation. Individual staff officer augmentation is an important mechanism for providing personnel to a joint staff. The core staff or establishing Combatant Command identifies individual augmentation requirements and publishes them in a joint manning document. Augmentation considerations should include core competencies not resident on the core staff or special subject matter expertise. Often augmentees arrive at the headquarters requiring additional training to prepare them to serve as functional members of the staff.

Linguists and interpreters often are critical to JTF operations. It is important to identify the numbers and types of linguists required for an operation early in the planning cycle to facilitate their procurement and integration.

c. Support Elements. In contrast to individual augmentees, support elements often arrive at the headquarters as a mission-tailored detachment. Listed below are a number of possible joint organizations that may provide support elements to bolster a core staff. The list is not all-inclusive but should provide some insight into the types of augmentation the core staff can receive and the purpose behind that augmentation.

(1) Joint Communications Support Element (JCSE). The JCSE provides connectivity both to and from the JTF HQ. Its purpose is to provide a temporary solution to JTF communications requirements. The JCSE can support up to two JTFs and two joint special operations task forces (JSOTFs) simultaneously. The JCSE normally redeploys when unit or commercial equipment replace its functions. http://www.jcse.mil/

(2) Joint Enabling Capabilities Command (JECC). The JECC provides mission-tailored, joint capability packages to CCMDs to facilitate rapid establishment of joint force headquarters, fulfill Global Response Force execution, and bridge joint operational requirements. http://www.jecc.mil/

(a) The **Joint Planning Support Element (JPSE)** provides rapidly deployable, tailored, joint planners who bring the expertise to accelerate the formation and increase the effectiveness of a joint force headquarters during emerging operations. http://www.jecc.mil/Portals/21/Documents/JPSE-Trifold-Web.pdf

(b) The **Joint Public Affairs Support Element (JPASE)** provides rapidly deployable joint public affairs professionals who can launch, land, and within minutes implement the commander's communication strategy in order to drive the narrative. http://www.jecc.mil/Subordinates/JointPublicAffairsSupportElement.aspx

(3) Defense Threat Reduction Agency (DTRA). DTRA's mission is to safeguard America and its allies from weapons of mass destruction (WMD) (chemical, biological, radiological, nuclear, and high-yield explosives [CBRNE]) by providing capabilities to reduce, eliminate, and counter the threat, and mitigate its effects. DTRA has the capacity to provide specialists to support JTF operations. http://www.dtra.mil/

(4) Joint Information Operations (IO) Warfare Command (JIOWC). The joint information operations warfare command is the principal field agency for joint IO support of Combatant Commands. The joint information operations warfare command fulfills this role by planning, coordinating, and executing DOD IO. https://en.wikipedia.org/wiki/Joint_Information_Operations_Warfare_Center

(5) Joint Communications Security Monitoring Activity (JCMA). JCMA can provide information security monitoring and analysis support to JTFs. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA297770

(6) Joint Personnel Recovery Agency (JPRA). JPRA is the principal joint DOD agency for coordinating and advancing personnel recovery (PR). http://www.jpra.mil/

(7) Joint Warfare Analysis Center (JWAC). JWAC assists in preparation and analysis of joint OPLANs and Service chiefs' analysis of weapons effectiveness. JWAC normally provides this support to JTFs through the supported Combatant Command. http://www.jwac.mil/

(8) Defense Logistics Agency (DLA). DLA will support the JTF using a variety of capabilities. DLA has robust logistic planning experience, logistic surge and sustainment expertise, forward (such as DLA regional commanders and staff, deployable distribution capability) and expeditionary forces (DLA contingency support teams, liaison officers [LNOs], and other experts) imbedded physically and virtually with the warfighting and support organizations. http://www.dla.mil/Pages/default.aspx

(9) National Guard Bureau (NGB). The NGB provides coordination with the ARNG/ANG elements that are critical for non-federal domestic cross-domain coordination

(10) Liaison Requirements. JFCs generally have to manage significant liaison requirements both to and from their HQ. Liaison is the contact by which communications can be maintained between elements of military forces or other organizations and agencies to ensure mutual understanding and unity of purpose and action. Direct Liaison Authorized (DIRLAUTH) among military organizations facilitates innovative collaboration. This collaboration generates cross-domain solutions. JFCs should only withhold DIRLAUTH from their subordinates in very specific situations to avoid stifling the collaborative environment which produces cross-domain synergy. Furthermore, JFCs should pursue DIRLAUTH from their superiors to effectively build relationships with mission partners.

d. Liaisons: Liaison Officers (LNOs) enhance interoperability and contribute significantly to mission success. The JFC must identify the requirement for liaison personnel based on command relationships and mission support requirements. LNOs must be requested at the earliest opportunity and should be of sufficient rank (recommend equal rank to primary staff officers) to influence the decision-making process. Ideally, LNOs should possess the requisite skill sets (technical training or language) to liaise and communicate effectively with receiving organizations.

(1) The JFC should establish a familiarization program for all liaison personnel. A joint reception center (JRC) could perform this requirement. The JFC must determine what staff officer or staff section will exercise overall responsibility for liaison personnel reporting to the joint staff for duty (e.g., Deputy Commander, Joint Task Force (DCJTF), chief of staff, or J-3). Regardless of which staff section manages the LNO program, liaison personnel perform their duties within the joint staff directorate that is responsible for functions related to the liaison personnel's assigned duties.

(2) With the addition of space and cyberspace domains, where actions have global effects, liaisons from these domains' proponents become much more important. JFCs and their staffs should seek assistance in these two domains from two of U.S. Strategic Command's (USSTRATCOM) subordinates, Joint Functional Component Command SPACE (JFCC-Space) and U.S. Cyber Command (USCYBERCOM), to secure critical domain subject matter expertise.

In general, liaison requirements may include (but are not limited to) the following:

(a) Liaison to the CCMD or subordinate Joint Force Commanders.

(b) Liaison to or from supporting commands.

(c) Liaison to or from DOD or other interagency organizations.

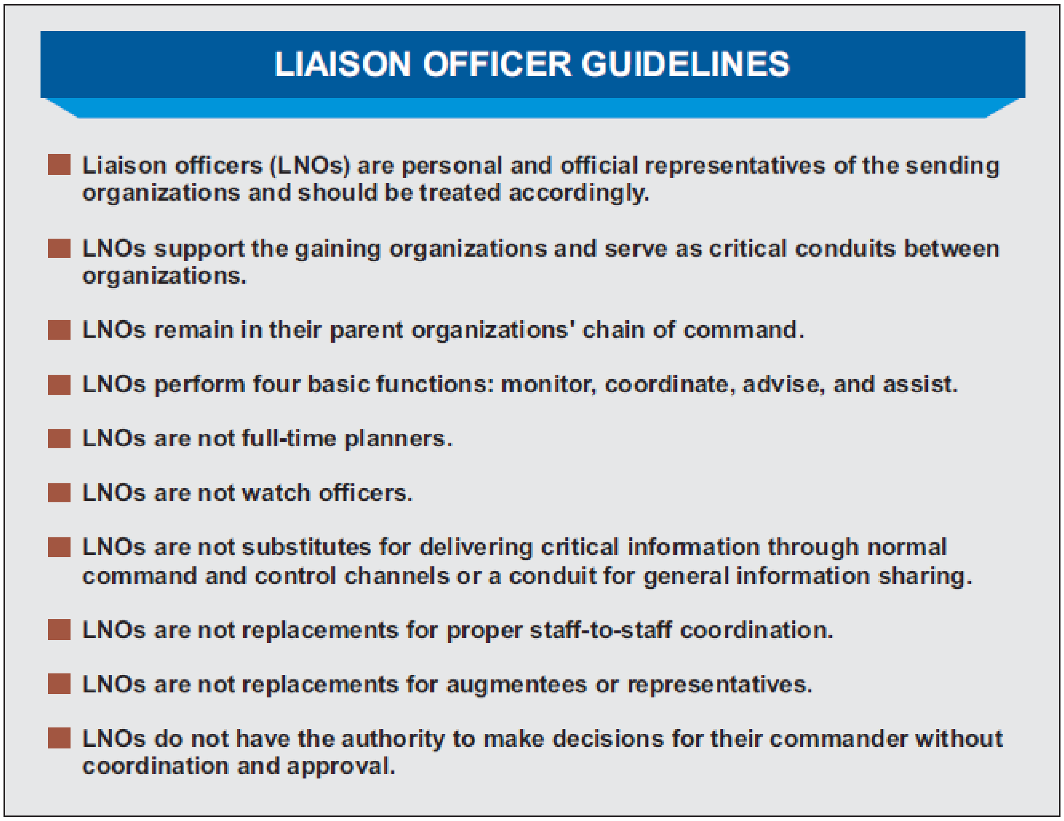
(d) Liaison to a U.S. embassy.

(e) Liaison to or from foreign military organizations.

(f) Liaison from JTF components or major subordinate commands

(g) Liaison to and from state or local governments for Defense Support Civilian Agencies (DSCA) operations.

Some guidelines for the utilization of liaison officers are provided in Figure II-2.



LIAISON OFFICER GUIDELINES

- Liaison officers (LNOs) are personal and official representatives of the sending organizations and should be treated accordingly.
- LNOs support the gaining organizations and serve as critical conduits between organizations.
- LNOs remain in their parent organizations' chain of command.
- LNOs perform four basic functions: monitor, coordinate, advise, and assist.
- LNOs are not full-time planners.
- LNOs are not watch officers.
- LNOs are not substitutes for delivering critical infomation through normal command and control channels or a conduit for general information sharing.
- LNOs are not replacements for proper staff-to-staff coordination.
- LNOs are not replacements for augmentees or representatives.
- LNOs do not have the authority to make decisions for their commander without coordination and approval.

Figure II-2. Liaison Officer Guidelines[24]

2. Inter-Agency Considerations. LNOs from non-DOD agencies are sometimes different from military organizations' LNOs. Some of these differences are listed below:

a. Most U.S. Government (USG) agencies, IGOs, and NGOs are not equipped and organized to create separate staffs at the strategic, operational, and tactical levels, resulting in the necessity for joint staff personnel to interface with individuals who are coordinating their organization's activities at more than one level.

b. The **unique aspects of the interagency**, Intergovernmental Organization (IGO), and Non-Governmental Organization (NGO) coordination process require the joint staff to be especially flexible, responsive, and cognizant of the capabilities of these entities, including participating host nations (HNs) and multinational partners.

c. The **joint staff must establish organizational structures**, processes, and procedures to consider interagency, IGO, and NGO perspectives and positions into its planning, execution, and assessment process.

d. Depending on the type of contingency operation, the extent of military operations, and degree of interagency involvement, the **focal point for operational and tactical level coordination** with civilian agencies may occur at the joint staff, the Civil Military Operations Center (CMOC), or the humanitarian operations center.

[24] U.S. Joint Chiefs of Staff, *Joint Publication 3-33, Joint Task Force Headquarters*, II-18.

e. The JFC's **Joint Interagency Coordination Group (JIACG)** is an element that can assist the JTF with an **increased capability to coordinate with other** USG agencies and departments. The JIACG, an element of a JFC's staff, is an interagency staff group that establishes regular, timely, and collaborative working relationships between civilian and military operational planners.

f. Composed of USG civilian and military experts assigned to joint staffs and tailored to meet the JFCs' specific needs, the JIACG **provides the capability to collaborate at the operational level with other USG civilian agencies and departments.** JIACG members participate in theater campaign planning (including theater security cooperation), contingency planning, and crisis action planning. They provide a collaborative conduit back to their parent organizations to help synchronize joint operations with the efforts of non-military organizations.

3. Boards, Bureaus, Centers, Cells, Working Groups (B2C2WG), Planning Teams, and Battle Rhythm

a. B2C2WG and planning teams. Effective cross-domain solutions require close coordination, synchronization, and information sharing across the staff directorates. The most common technique for promoting this cross-functional collaboration is the formation of boards, bureaus, centers, cells, groups, offices, elements, working groups, planning teams, and other enduring or temporary organizations that manage specific processes and accomplish tasks in support of mission accomplishment. In designing the joint staff's B2C2WG schedule, staff leads must find a balance between the inclusivity which generates innovative solutions and the efficiency which neatly tailors meetings to time constraints. **Distinctions between lethal and non-lethal effects B2C2WG tend to isolate and marginalize space and cyberspace capabilities.** By eliminating the distinction between lethal and non-lethal effects B2C2WG and rigidly enforcing meetings' agendas, staff leads may garner the benefits of both inclusivity and efficiency.

b. These B2C2WG facilitate planning by the staff, decision-making by the commander, and execution by the Joint Force. Although **cross-functional in their membership, most B2C2WG, and planning teams fall under the principal oversight of the staff directorates**. The B2C2WG definitions are included below:

(1) A **board** is an organized group of individuals within a joint staff, appointed by the commander (or other authority) that meets with the purpose of gaining guidance or decision. Its responsibilities and authority are governed by the authority, which established the board. Boards are chaired by a senior leader with members representing major staff elements, subordinate commands, LNOs, and other organizations as required. There are two different types of boards:

(a) Command Board. A command board is chaired by the commander and its purpose is to gain guidance or decision from the commander.

(b) Functional Board. A functional board's purpose is to gain functionally specific guidance and decisions from the commander (or designated representative) based on a staff recommendation. These boards often focus on:

1. Synchronizing a particular function (e.g., Information Operations (IO), targeting, collection, and distribution) across multiple planning initiatives.

2. Allocation of resources between ongoing or future operations.

3. Maintaining continuity of purpose across ongoing operations.

(2) A **bureau** is a long-standing functional organization, with a supporting staff designed to perform a specific function or activity within a joint staff. A joint visitor's bureau is an example of a bureau common to many joint staffs.

(3) A **center** is an enduring functional organization, with a supporting staff, designed to perform a joint function within a joint force commander's headquarters.

(4) A **cell** is a subordinate organization formed around a specific process, capability, or activity within a designated larger organization of a joint force commander's headquarters. A cell usually is part of both a functional and traditional staff structures.

(5) A **group** is an enduring functional organization, which is formed to support a broad HQ function within a JFC's HQ. Normally, groups within a joint staff consist of one or more planning groups. The planning group manages joint staff planning. The functions of joint staff planning groups include:

(a) Managing designated planning efforts.

(b) Resourcing planning teams.

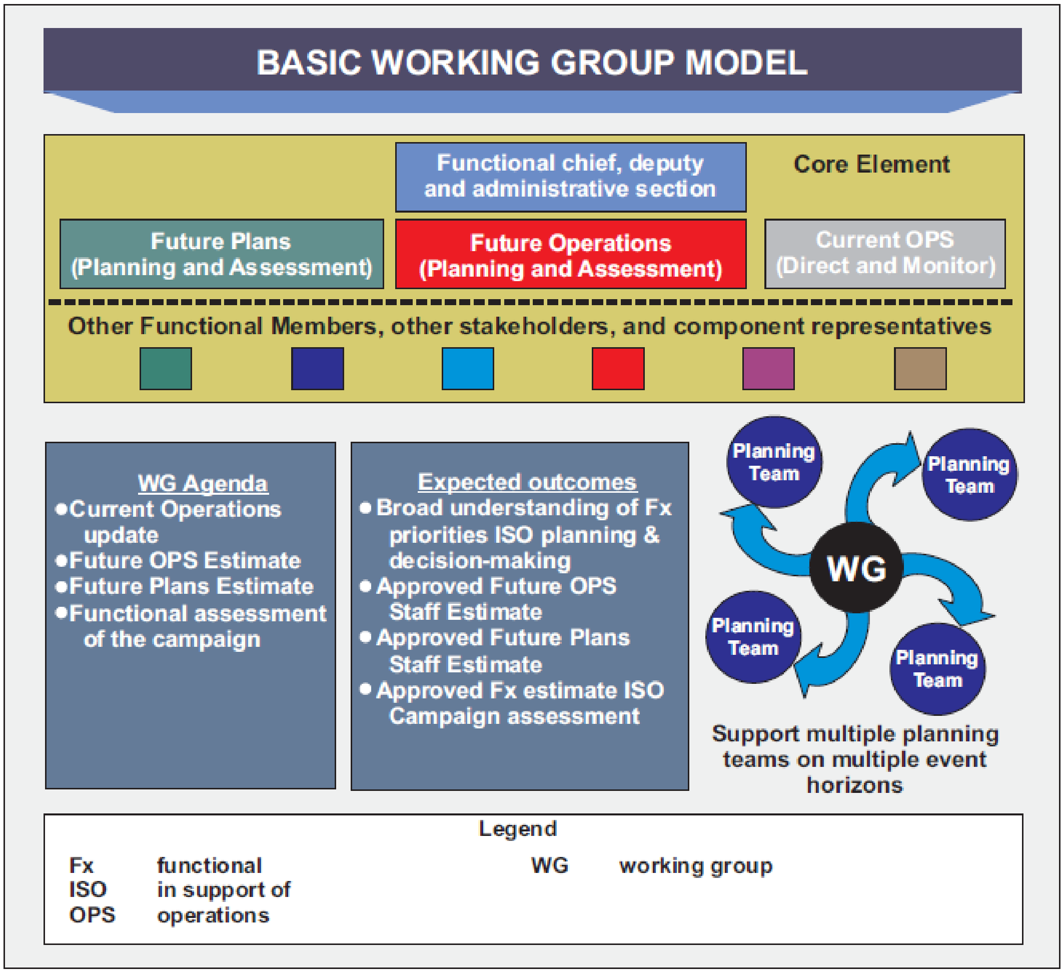
(c) Coordinating planning activities with other staff directorates.

(d) Managing the subordinate planning teams' conduct of the operational planning process.

(6) An **office** is an enduring organization that is formed around a specific function within a joint staff to coordinate and manage support requirements. An example of an office is the Joint Mortuary Affairs Office (JMAO).

(7) An **element** is an organization formed around a specific function within a designated directorate of a joint staff. The subordinate components of an element usually are functional cells. An example of an element is the Joint Fires Element (JFE).

(8) Working Group (WG) is an enduring or ad hoc organization within a joint staff formed around a specific function whose purpose is to provide analysis to users. The WG consists of a core functional group and other staff and component representatives. Members of a WG meet to discuss specific problems. The WG's members, then, provide insights on that problem back to the staff's decision-making processes. See Figure II-3.



BASIC WORKING GROUP MODEL

Functional chief, deputy and administrative section
Core Element
Future Plans (Planning and Assessment)
Future Operations (Planning and Assessment)
Current OPS (Direct and Monitor)
Other Functional Members, other stakeholders, and component representatives
Planning Team
Planning Team
WG
Planning Team
Planning Team
Support multiple planning teams on multiple event horizons

WG Agenda
- Current Operations update
- Future OPS Estimate
- Future Plans Estimate
- Functional assessment of the campaign

Expected outcomes
- Broad understanding of Fx priorities ISO planning & decision-making
- Approved Future OPS Staff Estimate
- Approved Future Plans Staff Estimate
- Approved Fx estimate ISO Campaign assessment

Legend

Fx	functional	WG	working group
ISO	in support of		
OPS	operations		

Figure II-3: Basic Working Group Model[25]

(9) Planning Team. A planning team is a functional element formed within the joint staff to solve problems related to a specific task or requirement. The planning team is not an enduring element and dissolves upon completion of the assigned task. Planning teams and WGs are complementary. WGs enhance planning through their provision of functional staff estimates to multiple planning teams. In contrast, planning teams integrate the functional concepts of multiple functional WGs into plans and orders.

The staff proponent for a meeting is responsible for clearly communicating the purpose of that meeting to its participants. From that purpose, other structural components for the meeting will be derived (e.g. agenda, attendees, inputs, outputs). Communicating a meeting's organization and construct can be accomplished through the use of a simple "meeting design." Drafting and adhering to a "meeting design" will also ensure participants' time is used wisely. An example of a generic "meeting design" is provided in Figure II-4.

[25] U.S. Joint Chiefs of Staff, *Joint Publication 3-33, Joint Task Force Headquarters*, II-13.

Purpose / Frequency	**Name: Name of Board, working group, etc.** **Purpose: What does this meeting accomplish?** **Frequency / Location: Date Time Group (DTG) when (in the Battle Rhythm) and where (potentially, virtual)**	
Composition	**Lead J-Code, Chair: Who receives, compiles and delivers information**	
	Attendees: Membership codes, who has to attend (task staff to provide reps)	
Inputs / Outputs	**Inputs: Suspense DTG for inputs. Staff sections and/or B2C2WG required to provide products.**	**Outputs: Products and links to other B2C2WG. DTG when outputs are due.**
Agenda		

Figure II-4: B2C2WG and planning team - "Meeting Design"[26]

After beginning with a core staff and augmenting that staff with the requisite expertise, JFCs organize the staff and staff leads determine the B2C2WGs to best support the mission. A typical example of this staff organization, including B2C2WGs, is shown in Figure II-5.

[26] U.S. Joint Chiefs of Staff, *CJCS Wargame, Iron Crucible*, (Unpublished manuscript dated May 2014).

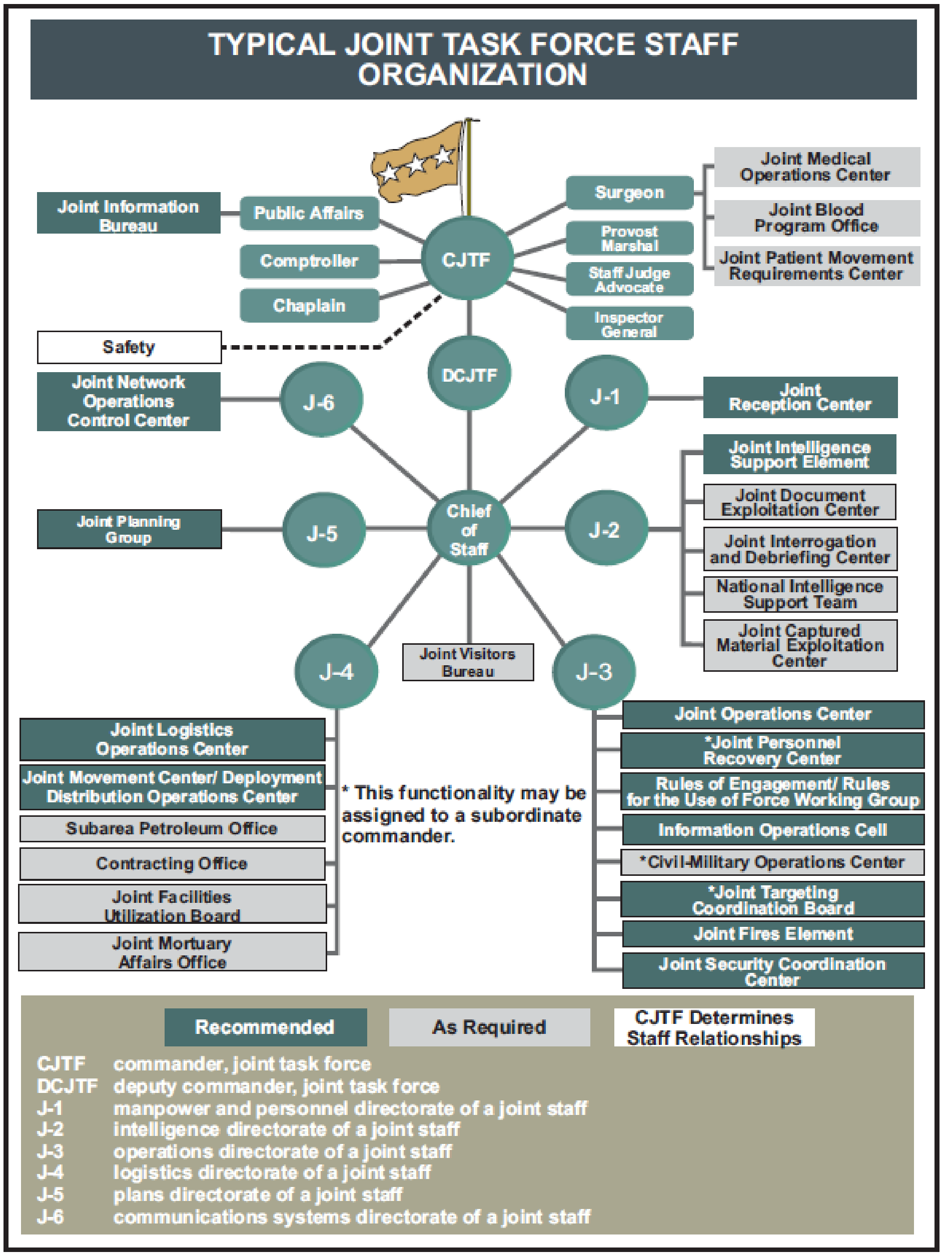

TYPICAL JOINT TASK FORCE STAFF ORGANIZATION
Joint Information Bureau
Public Affairs
Comptroller
Chaplain
Safety
CJTF
Surgeon
Provost Marshal
Staff Judge Advocate
Inspector General
Joint Medical Operations Center
Joint Blood Program Office
Joint Patient Movement Requirements Center
DCJTF
Joint Network Operations Control Center
J-6
J-1
Joint Reception Center
Joint Intelligence Support Element
Joint Document Exploitation Center
Joint Interrogation and Debriefing Center
National Intelligence Support Team
Joint Captured Material Exploitation Center
Joint Planning Group
J-5
Chief of Staff
J-2
J-4
Joint Visitors Bureau
J-3
Joint Logistics Operations Center
Joint Movement Center/ Deployment Distribution Operations Center
Subarea Petroleum Office
Contracting Office
Joint Facilities Utilization Board
Joint Mortuary Affairs Office
* This functionality may be assigned to a subordinate commander.
Joint Operations Center
*Joint Personnel Recovery Center
Rules of Engagement/ Rules for the Use of Force Working Group
Information Operations Cell
*Civil-Military Operations Center
*Joint Targeting Coordination Board
Joint Fires Element
Joint Security Coordination Center
Recommended
As Required
CJTF Determines Staff Relationships
CJTF commander, joint task force
DCJTF deputy commander, joint task force
J-1 manpower and personnel directorate of a joint staff
J-2 intelligence directorate of a joint staff
J-3 operations directorate of a joint staff
J-4 logistics directorate of a joint staff
J-5 plans directorate of a joint staff
J-6 communications systems directorate of a joint staff

Figure II-5: Typical Joint Task Force Staff Organization w/B2C2WG[27]

4. Battle Rhythm.

a. The JFCs and their staffs use a number of processes that support the commands' requirements, activities, and products. The joint staff battle rhythm is especially important for the efficient management of day-to-day operations. **Battle rhythm** is the sequencing and execution of actions and events within a joint staff that are regulated by the flow and sharing of information

[27] U.S. Joint Chiefs of Staff, *Joint Publication 3-33 Joint Task Force Headquarters*, IV-17.

that support all decision cycles.[28] A poorly designed battle rhythm will waste staff officers' time and paralyze the staff through inefficiency. The benefits of a well-designed battle rhythm include:

(1) Routinizing staff interaction and coordination.

(2) Routinizing commander and staff interaction.

(3) Synchronizing B2C2WG and planning team's activities.

(4) Facilitating planning by the staff and decision-making by the commander.

b. Factors that Shape a Battle Rhythm. Typically, the chief of staff (COS) manages a joint staff's battle rhythm and considers several factors in its design. These factors include (but are not limited to) the following:

(1) The higher HQ battle rhythm and reporting requirements.

(2) The subordinate HQ battle rhythm requirements.

(3) The duration of the operation.

(4) The intensity of the operation.

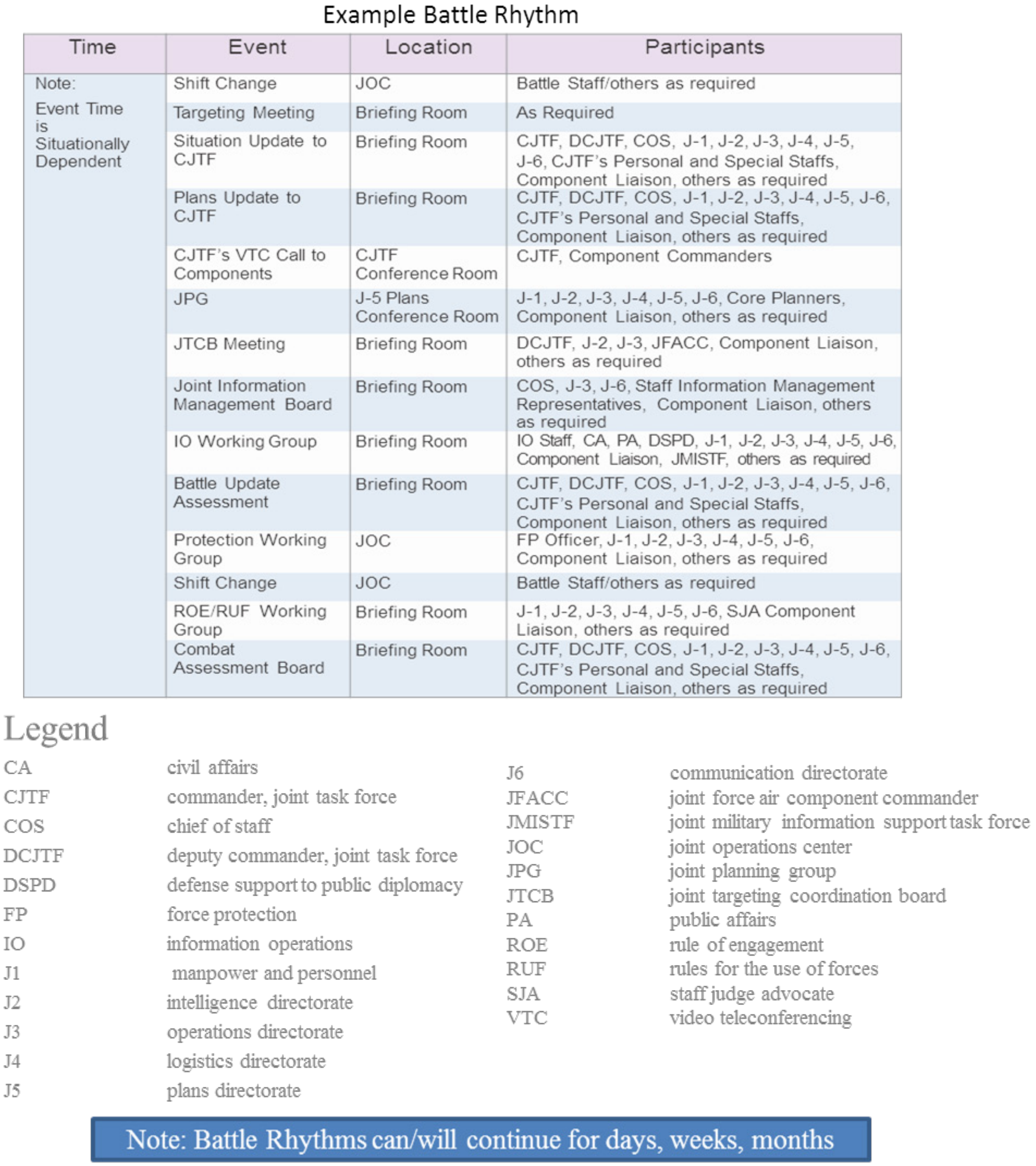
(5) The planning requirements within the joint staff (e.g., future plans, future operations, and current operations).

(6) Rest requirements for the planners (it is important to plan rest into the battle rhythm).

(7) The joint staff's internal battle rhythm.

Figure II-6, provides an example of what a JFC battle rhythm might look like. As with the battle rhythm itself, the JFC dictates times based on the situation and operational tempo.

[28] U.S. Joint Chiefs of Staff, *Joint Publication 3-33, Joint Task Force Headquarters,* IV-16.



Example Battle Rhythm

Time	Event	Location	Participants
Note: Event Time is Situationally Dependent	Shift Change	JOC	Battle Staff/others as required
	Targeting Meeting	Briefing Room	As Required
	Situation Update to CJTF	Briefing Room	CJTF, DCJTF, COS, J-1, J-2, J-3, J-4, J-5, J-6, CJTF's Personal and Special Staffs, Component Liaison, others as required
	Plans Update to CJTF	Briefing Room	CJTF, DCJTF, COS, J-1, J-2, J-3, J-4, J-5, J-6, CJTF's Personal and Special Staffs, Component Liaison, others as required
	CJTF's VTC Call to Components	CJTF Conference Room	CJTF, Component Commanders
	JPG	J-5 Plans Conference Room	J-1, J-2, J-3, J-4, J-5, J-6, Core Planners, Component Liaison, others as required
	JTCB Meeting	Briefing Room	DCJTF, J-2, J-3, JFACC, Component Liaison, others as required
	Joint Information Management Board	Briefing Room	COS, J-3, J-6, Staff Information Management Representatives, Component Liaison, others as required
	IO Working Group	Briefing Room	IO Staff, CA, PA, DSPD, J-1, J-2, J-3, J-4, J-5, J-6, Component Liaison, JMISTF, others as required
	Battle Update Assessment	Briefing Room	CJTF, DCJTF, COS, J-1, J-2, J-3, J-4, J-5, J-6, CJTF's Personal and Special Staffs, Component Liaison, others as required
	Protection Working Group	JOC	FP Officer, J-1, J-2, J-3, J-4, J-5, J-6, Component Liaison, others as required
	Shift Change	JOC	Battle Staff/others as required
	ROE/RUF Working Group	Briefing Room	J-1, J-2, J-3, J-4, J-5, J-6, SJA Component Liaison, others as required
	Combat Assessment Board	Briefing Room	CJTF, DCJTF, COS, J-1, J-2, J-3, J-4, J-5, J-6, CJTF's Personal and Special Staffs, Component Liaison, others as required

Legend

CA	civil affairs
CJTF	commander, joint task force
COS	chief of staff
DCJTF	deputy commander, joint task force
DSPD	defense support to public diplomacy
FP	force protection
IO	information operations
J1	manpower and personnel
J2	intelligence directorate
J3	operations directorate
J4	logistics directorate
J5	plans directorate
J6	communication directorate
JFACC	joint force air component commander
JMISTF	joint military information support task force
JOC	joint operations center
JPG	joint planning group
JTCB	joint targeting coordination board
PA	public affairs
ROE	rule of engagement
RUF	rules for the use of forces
SJA	staff judge advocate
VTC	video teleconferencing

Note: Battle Rhythms can/will continue for days, weeks, months

Figure II-6: JFC Battle Rhythm Example[29]

For more information, refer to Joint Publication 3-33, Joint Task Force Headquarters.

With the staff assembled, B2C2WG's defined, and the Battle Rhythm set, staff leads should (considering time available) foster creative interaction amongst the HQ's diverse communities to cultivate multi-disciplinary thought, leading to cross-domain solutions.

[29] U.S. Joint Chiefs of Staff, *JP 3-33, Joint Task Force Headquarters,* IV-24.

D. Secondary Challenges

Training shortfalls, education deficiencies, sub-optimal manning, and capability classification/compartmentalization can create unnecessary friction and stifle cross-domain synergy.

1. Training and Education. Before staff officers can work efficiently on a joint staff, they must be prepared through experience, training, and education. Staff officers gain experience though Service assignments. Service assignments tend to develop expertise in one domain with only limited exposure to the other domains. Service experience rarely involves exposure to space and cyberspace capabilities. As a result, staff officers learn to solve problems using the capabilities in which they are most confident, and overlook some cross-domain solutions.

Training in preparation for assignment to a joint staff is available through: **1) Joint Professional Military Education Phase 2 (JPME II)** offered by the Joint Forces Staff College in Norfolk, VA; **2)** the **onboarding training** offered at the joint staff as a new staff officer arrives; and **3) Joint Knowledge Online (JKO)**, a large repository of online training lessons maintained by the Joint Staff J-7. Building familiarity through training and education empowers new joint staff officers to create innovative cross-domain solutions.

For more information on available training/courses, refer to Joint Knowledge On-line (JKO) at https://jkodirect.jten.mil/Atlas2/faces/page/login/Login.seam.

2. Manning. Services may opt to assign an unqualified officer to a joint billet rather than leave it unfilled. This practice degrades staff efficiency as the newly assigned officer requires time and additional training to develop the skills required by the billet. Close coordination between the Services' assignment managers and joint staff personnel sections can help mitigate this challenge.

The gaining command may opt to assign an officer to a different billet to perform special duties. This sometimes occurs when commanders divert trained planners from the planning staff. This practice drains the staff of personnel who are specially trained to develop cross-domain solutions.

3. Classification/compartmentalization. Classification and compartmentalization hinder cross-domain planning, especially in the cyberspace domain where capabilities are closely guarded and security classification guidance is not well understood. To mitigate this challenge, lead staff officers should include all domain representatives in their activities. While these domain representatives may not describe their classified capabilities to the entire staff team, they will build an understanding of the staff's effort. From that understanding, they can discreetly work to integrate their capabilities while informing only those with the appropriate clearance and need-to-know. In this manner, lead staff officers can build cross-domain synergy using classified capabilities.

CHAPTER 3

CROSS-DOMAIN SYNERGY VIA THE JOINT OPERATION PLANNING PROCESS (JOPP)

A. General

Planning blends the collective knowledge of the many diverse communities within the joint staff into a single, coherent plan which accomplishes the JFCs' missions. It transforms national strategic objectives into activities by development of operational products that include planning for the mobilization, deployment, employment, sustainment, redeployment, and demobilization of joint forces. This flexible and adaptable process is applicable to planners across all domains and mirrors Service planning processes.

Planning involves a combination of conceptual planning and detailed processes. Joint Publication (JP) 5-0 recognizes this dynamic by describing the benefits of operational art and design in chapter III before describing the JOPP in chapter IV. Conceptual planning enables cross-domain and cross-functional collaboration which fosters innovative, cross-domain solutions. Operational art and the application of operational design provide the conceptual basis for structuring campaigns and operations.[30] Detailed methods are used to help provide form and function to the planning process. This section will look at how conceptual planning can feed detailed planning through discussion, debate, and brainstorming. These methods in combination assist the joint planner understand the problem and to develop creative solutions.

JOPP is an orderly, analytical, structured process, which consists of a set of logical steps to examine a mission; develop, analyze, and compare alternative COAs; select the best COA; and produce a plan or order.[31] JOPP provides a proven process to organize the work of the commander, staff, subordinate commanders, and other partners, to develop plans that will appropriately address the problem. It focuses on defining the military mission and development and synchronization of detailed plans to accomplish that mission.

Joint Operational Planning integrates military actions with those of the other instruments of national power in time, space, and purpose to achieve the specified objectives.

B. Conceptual Planning

Conceptual planning, or "brainstorming," occurs early, often, and regularly throughout the planning process to generate as many different options for solving the military problem as possible within the allocated time. Brainstorming sessions should inspire creative thinking, encourage open discussion from all participants, and drive consideration of many, wide-ranging options. They should assemble experts with differing perspectives to account for all available capabilities and elicit novel approaches to solving the problem prior to detailed planning. While less time and fewer planners may be available for Crisis Action Planning (CAP), planners should

[30] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, (Washington, DC: U.S. Joint Chiefs of Staff, 2011), IV-1.

[31] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, IV-1.

still attempt to allocate time for unstructured, unconstrained thinking. Figure III-1 depicts a brainstorming technique.

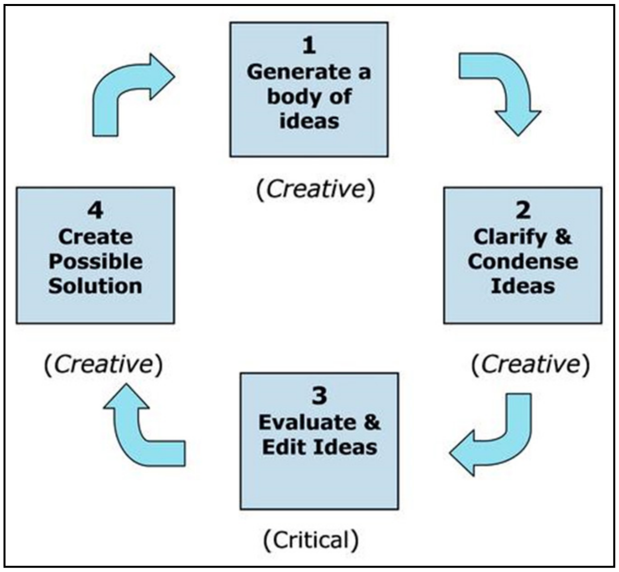


Figure III-1: Creative Brainstorming Technique

Cyberspace, space, and SOF planners are particularly important participants due to their expertise in employing these specialized capabilities. LNOs from the U.S. interagency and foreign nations can add unique experiences. The range of perspectives gained by including many different subject matter experts in the planning process facilitates the development of cross-domain solutions. These conceptual sessions will provide dividends to planners through exchanging knowledge, collaborating on like ideas, and debating differences that can lead to innovative thought and solutions. The results will assist planners during JOPP or CAP to create the best possible plan in support of the JFC.

C. Detailed Planning

Joint operation planning occurs within the Adaptive Planning and Execution (APEX) system, which is the department-level system of joint policies, processes, procedures, and reporting structures. Chairman of the Joint Chiefs of Staff Guide (CJCSG) 3130 Adaptive Planning and Execution Overview and Policy Framework defines APEX as “the Joint Capability to create and revise plans rapidly and systematically, as circumstances require.” APEX is supported by communications and information technology that is used by the Joint Planning and Execution Community (JPEC) worldwide to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint operations. Figure III-2 shows the JPEC members. All domain planners are members of the JPEC.

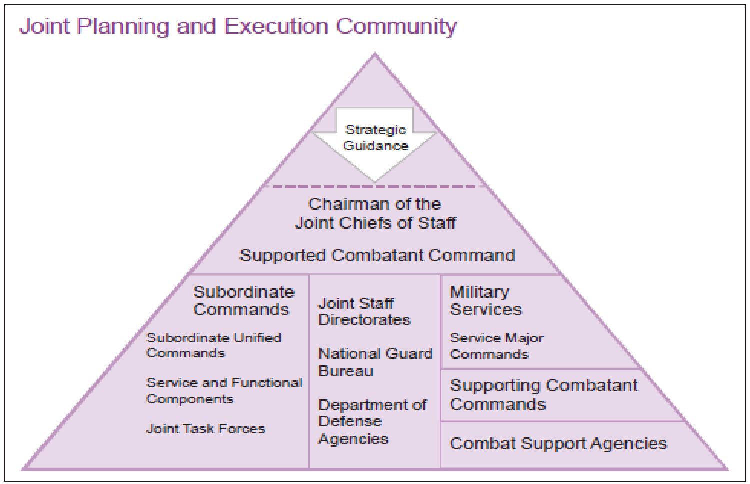

Joint Planning and Execution Community
Strategic Guidance
Chairman of the Joint Chiefs of Staff
Supported Combatant Command
Subordinate Commands
Subordinate Unified Commands
Service and Functional Components
Joint Task Forces
Joint Staff Directorates
National Guard Bureau
Department of Defense Agencies
Military Services
Service Major Commands
Supporting Combatant Commands
Combat Support Agencies

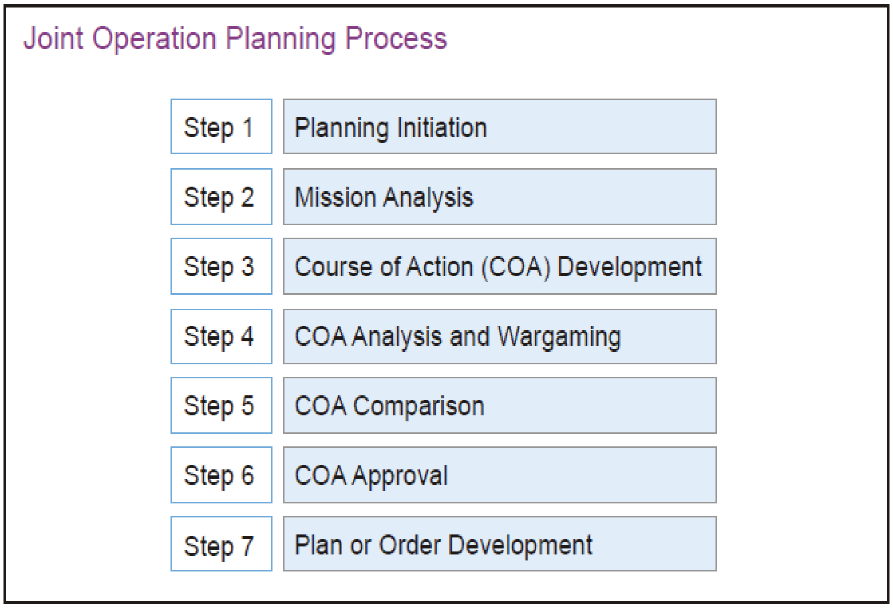
Figure III-2: Joint Planning and Execution Community[32]

JFCs and the Joint Operation Planning Process (JOPP). The JFC gains an understanding of the operational environment, defines the problem, and develops an operational approach for the campaign or operation. JFCs communicate their operational approach to their staff, subordinates, supporting commands, agencies, and multinational/nongovernmental entities in their initial planning guidance. The JFC's timely communication with subordinates ensures their approach can be translated into executable plans. This iterative process between the JFC's maturing operational approach and the development of the mission and concept of operations (CONOPS) through JOPP facilitates the continuing development of possible COAs and their refinement into eventual CONOPS and executable plans.

D. JOPP

Planners use JOPP to translate the creative thinking developed through conceptual planning into a plan or order. It is a seven-step process that culminates with a published operations order (OPORD) in CAP and results in an operations plan (OPLAN), concept plan (CONPLAN), Base Plan, or commander estimate during contingency planning.[33] The JOPP starts with Mission Analysis (MA) followed by Course of Action (COA) Development, COA Analysis, COA Comparison, and COA Selection and ends with OPLAN production and rehearsals. **Lead planners direct these efforts, and all supporting planners analyze, simulate, exercise, and critique to produce the best plan.** The resulting plan should support the foreign and/or domestic theater campaign plan and global synchronizing plans. The JOPP steps are provided at Figure III-3.

[32] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, II-12.
[33] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, IV-44.



Joint Operation Planning Process

Step 1	Planning Initiation
Step 2	Mission Analysis
Step 3	Course of Action (COA) Development
Step 4	COA Analysis and Wargaming
Step 5	COA Comparison
Step 6	COA Approval
Step 7	Plan or Order Development

Figure III-3: Joint Operation Planning Process[34]

1. Planning Initiation. "Joint operation planning begins when an appropriate authority recognizes potential for military capability to be employed in response to a potential or actual crisis. At the strategic level, that authority-the President, SecDef, or CJCS-initiates planning by deciding to develop military options. The Guidance for Employment of Force (GEF), Joint Strategic Capabilities Plan (JSCP), Unified Command Plan (UCP), and related strategic documents provide initial guidance for deliberate planning."[35] Planners from all domains must understand the guidance in these documents.

Conceptual planning activity is best scheduled during this step in the JOPP. By deliberately bringing together a diverse range of planners in a free flowing dialogue, the lead planner can begin to comprehend the requirements of the mission and potential approaches.

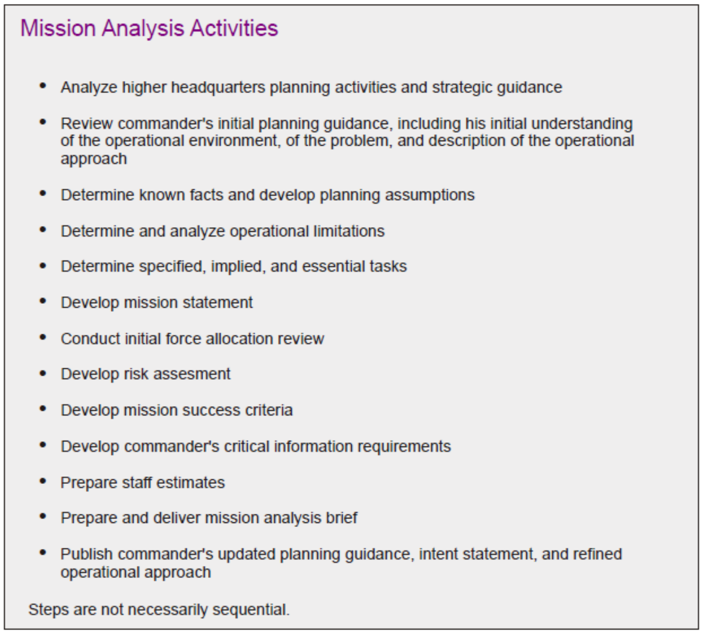
JFCs and lead planners must integrate all domain planners (air, land, maritime, space, and cyberspace) as soon as possible. It is particularly important to include space and cyberspace planners due to the unique authority levels, requirements, processes, and time-sensitivities associated with employment of their domain capabilities. Some space and cyberspace employment options could require an inordinate amount of time to gain approval for execution. JFCs and lead planners must understand the capabilities and limitations early in the planning process.

2. Mission Analysis. Mission analysis helps the JFC understand the problem and purpose of the operation and allows the JFC to issue guidance. The first step is defining the problem**. It is the most difficult and the most important step.** It involves diagnosing the situation to focus on the real problem and not on its symptoms.

[34] U.S. Joint Chiefs of Staff, *Joint Publication 5-0, Joint Operation Planning*, IV-2.
[35] U.S. Joint Chiefs of Staff, *Joint Publication 5-0, Joint Operation Planning,* IV-2.

Domain planners will accomplish all the steps outlined in Figure III-4 for their domain. Planners should understand that the steps do not necessarily happen sequentially. Although some activities occur before others, mission analysis typically involves substantial parallel processing of information by the JFC and staff, particularly in a CAP situation.

During mission analysis, it is essential that the tasks (specified and implied) and their purposes are clearly stated to ensure planning encompasses all requirements; limitations (restraints-cannot do, or constraints-must do) on actions that the JFC or subordinate forces may take are understood; and the correlation between the JFC's mission and intent and those of higher and other commanders is understood. It is at the end of the mission analysis process that all domain planners produce their staff estimates. They are the result of the Key Inputs and Key Outputs seen in Figure III-5. During this step, planners build on their understanding of the problem developed in conceptual planning activities.



Mission Analysis Activities

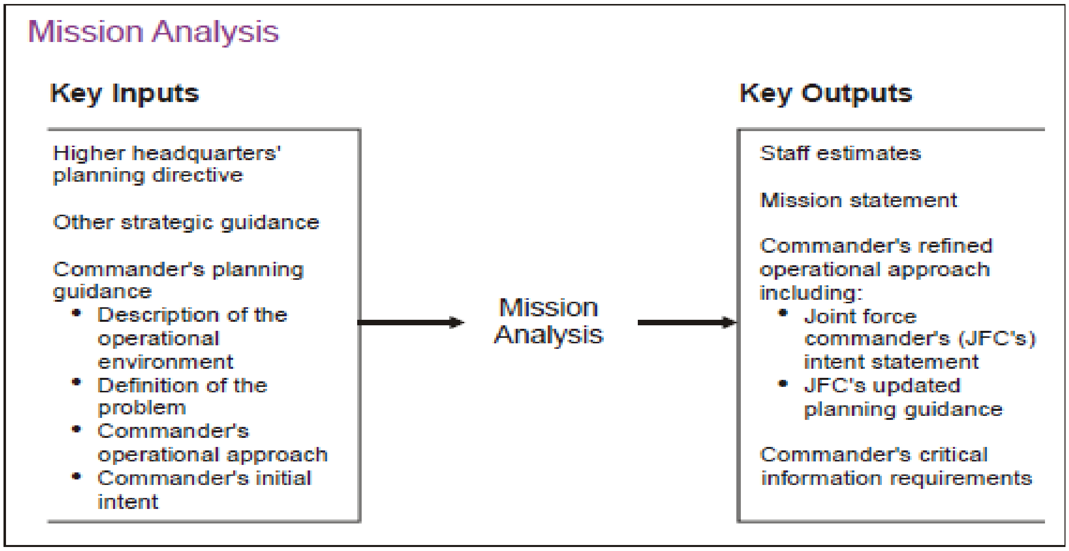
- Analyze higher headquarters planning activities and strategic guidance
- Review commander's initial planning guidance, including his initial understanding of the operational environment, of the problem, and description of the operational approach
- Determine known facts and develop planning assumptions
- Determine and analyze operational limitations
- Determine specified, implied, and essential tasks
- Develop mission statement
- Conduct initial force allocation review
- Develop risk assesment
- Develop mission success criteria
- Develop commander's critical information requirements
- Prepare staff estimates
- Prepare and deliver mission analysis brief
- Publish commander's updated planning guidance, intent statement, and refined operational approach

Steps are not necessarily sequential.

Figure III-4: Mission Analysis Activities[36]

If planners fail to account for each of the domains - air, land, maritime, space, and cyberspace - staff estimates will be incomplete and the resulting COAs, OPORDs, and plans will be sub-optimal.

[36] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning,* IV-6.



Mission Analysis

Key Inputs

Higher headquarters' planning directive

Other strategic guidance

Commander's planning guidance
- Description of the operational environment
- Definition of the problem
- Commander's operational approach
- Commander's initial intent

Mission Analysis

Key Outputs

Staff estimates

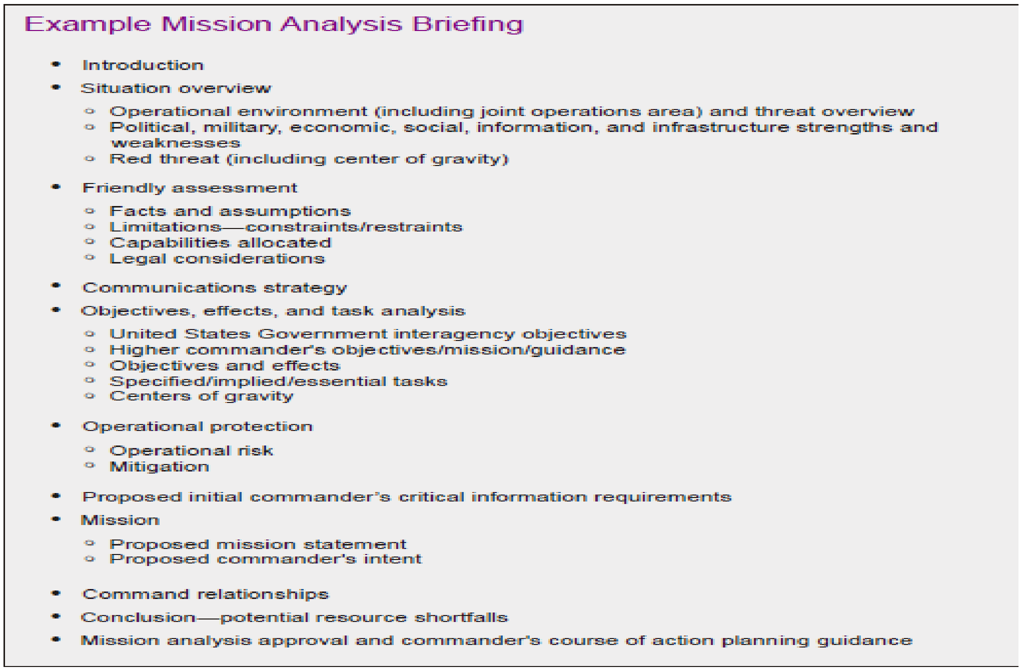
Mission statement

Commander's refined operational approach including:
- Joint force commander's (JFC's) intent statement
- JFC's updated planning guidance

Commander's critical information requirements

Figure III-5: Mission Analysis[37]

Once mission analysis is complete, the JFC receives a mission analysis brief. An example of how the brief might be structured is provided at Figure III-6.



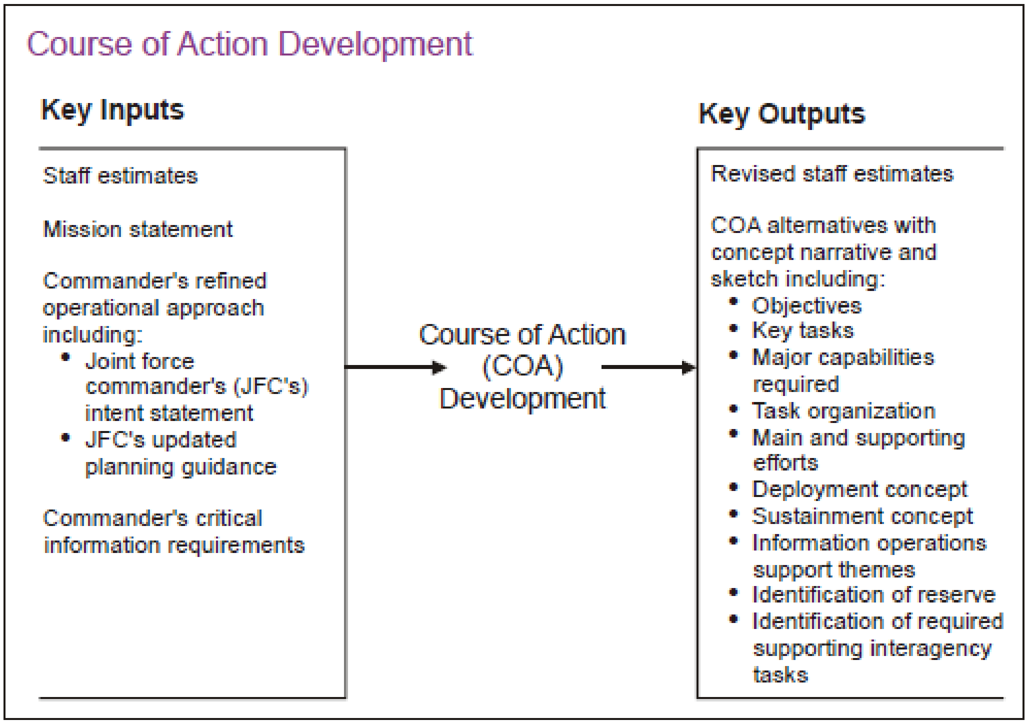
Example Mission Analysis Briefing

- Introduction
- Situation overview
  - Operational environment (including joint operations area) and threat overview
  - Political, military, economic, social, information, and infrastructure strengths and weaknesses
  - Red threat (including center of gravity)
- Friendly assessment
  - Facts and assumptions
  - Limitations—constraints/restraints
  - Capabilities allocated
  - Legal considerations
- Communications strategy
- Objectives, effects, and task analysis
  - United States Government interagency objectives
  - Higher commander's objectives/mission/guidance
  - Objectives and effects
  - Specified/implied/essential tasks
  - Centers of gravity
- Operational protection
  - Operational risk
  - Mitigation
- Proposed initial commander's critical information requirements
- Mission
  - Proposed mission statement
  - Proposed commander's intent
- Command relationships
- Conclusion—potential resource shortfalls
- Mission analysis approval and commander's course of action planning guidance

Figure III-6: Example Mission Analysis Briefing[38]

[37] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning,* IV-5.
[38] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, IV-15.

3. Course of Action Development (COA Dev). "A COA is a potential way (solution, method) to accomplish the assigned mission. The staff develops COAs to provide unique choices to the commander, all oriented on accomplishing the military end state. A good COA accomplishes the mission within the commander's guidance, provides flexibility to meet unforeseen events during execution, and positions the joint force for future operations. It also gives components the maximum latitude for initiative."[39] Figure III-7 provides key inputs and outputs for COA Dev. The products of *mission analysis* drive COA development. Since the *operational approach* contains the JFC's broad vision to solving the problem, the role of COA development is to expand this concept with the additional details. These details must describe **who** will take the action, **what type** of military action will occur, **when** the action will begin, **where** the action will occur, **why** the action is required (purpose), **how** the action will occur (method of employment of forces), and upon **whom** will the action be directed. COAs must be substantially distinguishable from each other. The JFC's involvement in the early operational design process can help ensure that only viable options are considered. If time and personnel resources permit, different COAs could be developed by different teams to ensure they are unique. During this step, planners screen the viable options proposed during conceptual planning and further develop the COAs considered acceptable, feasible, suitable, and distinct.



Course of Action Development

Key Inputs

Staff estimates

Mission statement

Commander's refined operational approach including:
- Joint force commander's (JFC's) intent statement
- JFC's updated planning guidance

Commander's critical information requirements

Course of Action (COA) Development

Key Outputs

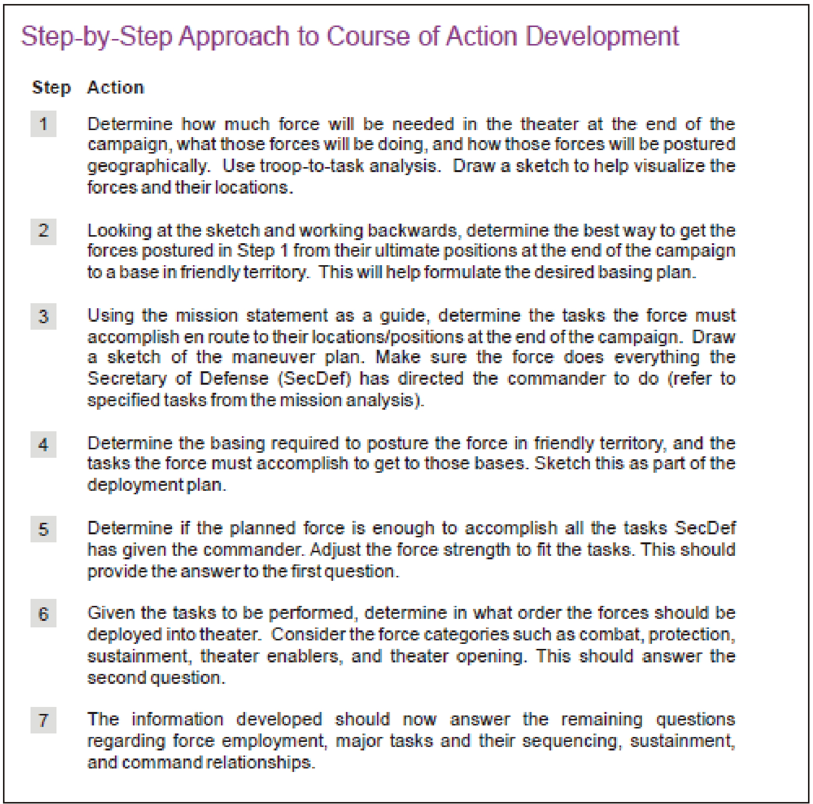
Revised staff estimates

COA alternatives with concept narrative and sketch including:
- Objectives
- Key tasks
- Major capabilities required
- Task organization
- Main and supporting efforts
- Deployment concept
- Sustainment concept
- Information operations support themes
- Identification of reserve
- Identification of required supporting interagency tasks

Figure III-7 Course of Action Development Inputs and Outputs

Bringing the capabilities of different domains together mandates that planners from all domains participate and characterize the potential contributions and limitations of their area of expertise.

[39] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, IV-17.

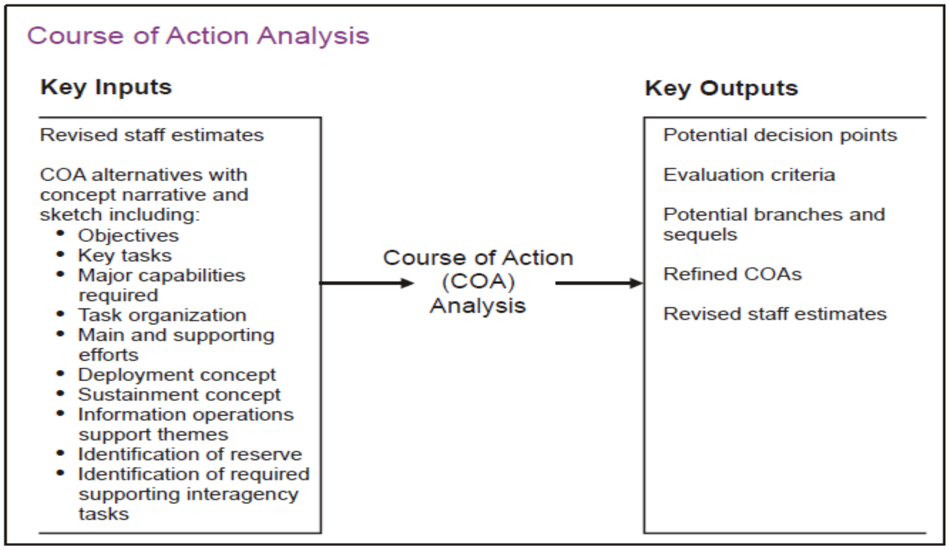


Step-by-Step Approach to Course of Action Development

Step	Action
1	Determine how much force will be needed in the theater at the end of the campaign, what those forces will be doing, and how those forces will be postured geographically. Use troop-to-task analysis. Draw a sketch to help visualize the forces and their locations.
2	Looking at the sketch and working backwards, determine the best way to get the forces postured in Step 1 from their ultimate positions at the end of the campaign to a base in friendly territory. This will help formulate the desired basing plan.
3	Using the mission statement as a guide, determine the tasks the force must accomplish en route to their locations/positions at the end of the campaign. Draw a sketch of the maneuver plan. Make sure the force does everything the Secretary of Defense (SecDef) has directed the commander to do (refer to specified tasks from the mission analysis).
4	Determine the basing required to posture the force in friendly territory, and the tasks the force must accomplish to get to those bases. Sketch this as part of the deployment plan.
5	Determine if the planned force is enough to accomplish all the tasks SecDef has given the commander. Adjust the force strength to fit the tasks. This should provide the answer to the first question.
6	Given the tasks to be performed, determine in what order the forces should be deployed into theater. Consider the force categories such as combat, protection, sustainment, theater enablers, and theater opening. This should answer the second question.
7	The information developed should now answer the remaining questions regarding force employment, major tasks and their sequencing, sustainment, and command relationships.

Figure III-8: Course of Action Development[40]

4. Course of Action Analysis and Wargaming. COA analysis is the process of closely examining potential COAs to reveal details that will allow the JFC and staff to tentatively identify COAs that are valid, and then compare these COAs. The JFC and staff analyze each tentative COA separately according to the JFC's guidance. While time-consuming, COA analysis should answer two primary questions: ***Is the COA feasible, and is it acceptable?*** Key inputs and outputs of COA analysis are provided in Figure III-8.



Course of Action Analysis

Key Inputs

Revised staff estimates

COA alternatives with concept narrative and sketch including:
- Objectives
- Key tasks
- Major capabilities required
- Task organization
- Main and supporting efforts
- Deployment concept
- Sustainment concept
- Information operations support themes
- Identification of reserve
- Identification of required supporting interagency tasks

Course of Action (COA) Analysis

Key Outputs

Potential decision points

Evaluation criteria

Potential branches and sequels

Refined COAs

Revised staff estimates

Figure III-9: Course of Action Analysis[41]

[40] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, IV-17.

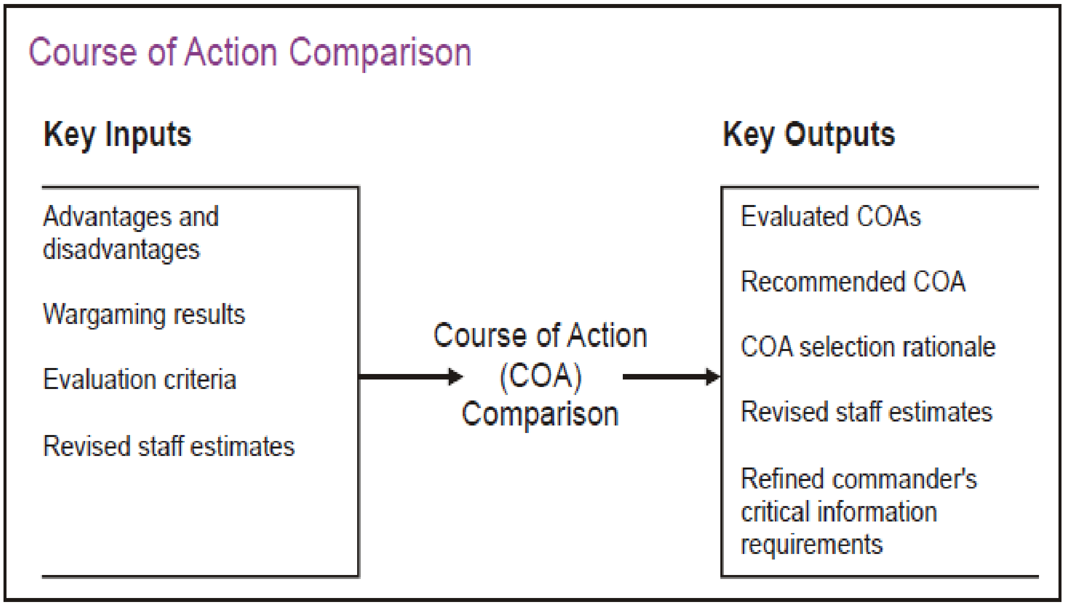
[41] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, V-28.

Wargaming is the primary means to conduct this analysis. Wargaming is a disciplined process, with rules and steps that attempt to visualize the flow of the operation. The process considers friendly dispositions, strengths, and weaknesses; enemy assets and probable COAs; and characteristics of the physical environment.

To accurately consider all aspects of the mission, each domain must be adequately represented for friendly forces, adversary forces, and wargame control groups.

When time permits, planners should wargame each critical event within a proposed COA using the action, reaction, and counteraction method of friendly and/or opposing force interaction. Wargaming is a critical portion of the planning process and should be allocated more time than any other step. At a minimum, each retained COA should be wargamed against both the most likely and most dangerous enemy COAs. When considering these enemy COAs, the analysis must consider all domains to ensure JFCs have a complete understanding of the COA they approve for execution.

5. Course of Action Comparison. COA comparison is a subjective process in which planners study each COA independently and evaluate/compare it against a set of criteria established by the staff and JFC. The goal is to identify and recommend the COA that has the highest probability of success against the enemy COA that is of the most concern to the JFC. Figure III-9 depicts inputs and outputs for COA comparison.



Course of Action Comparison

Key Inputs

- Advantages and disadvantages
- Wargaming results
- Evaluation criteria
- Revised staff estimates

Course of Action (COA) Comparison

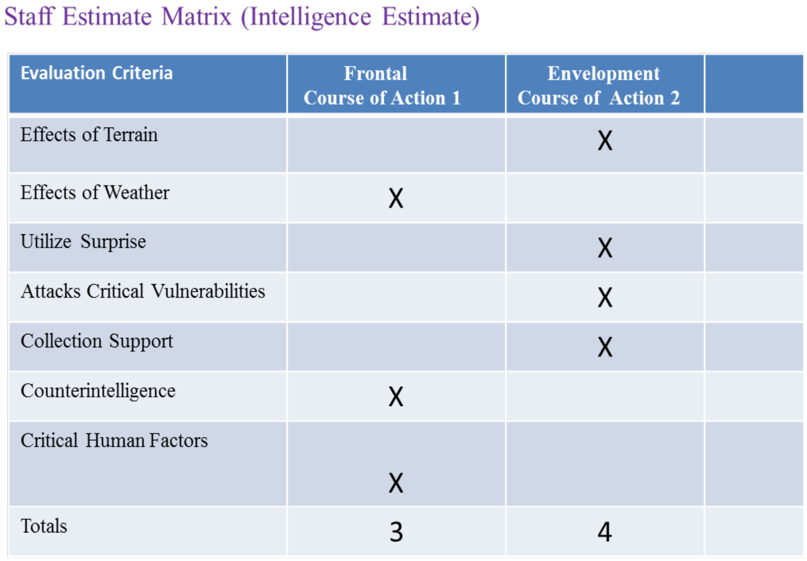
Key Outputs

- Evaluated COAs
- Recommended COA
- COA selection rationale
- Revised staff estimates
- Refined commander's critical information requirements

Figure III-10: Course of Action Comparison[42]

[42] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, IV-37.

JFCs modify the criteria list as required. Normally, staff officers use a matrix, such as the example in Figure III-10 to compare COAs with respect to their functional areas.



Staff Estimate Matrix (Intelligence Estimate)

Evaluation Criteria	Frontal Course of Action 1	Envelopment Course of Action 2	
Effects of Terrain		X	
Effects of Weather	X		
Utilize Surprise		X	
Attacks Critical Vulnerabilities		X	
Collection Support		X	
Counterintelligence	X		
Critical Human Factors	X		
Totals	3	4	

Figure III-11: Staff Estimator Matrix (Intelligence Estimate)

6. COA Approval. In this step, the staff briefs the COA analysis and comparison results, then recommends a COA to the JFC. The COA brief include the following:

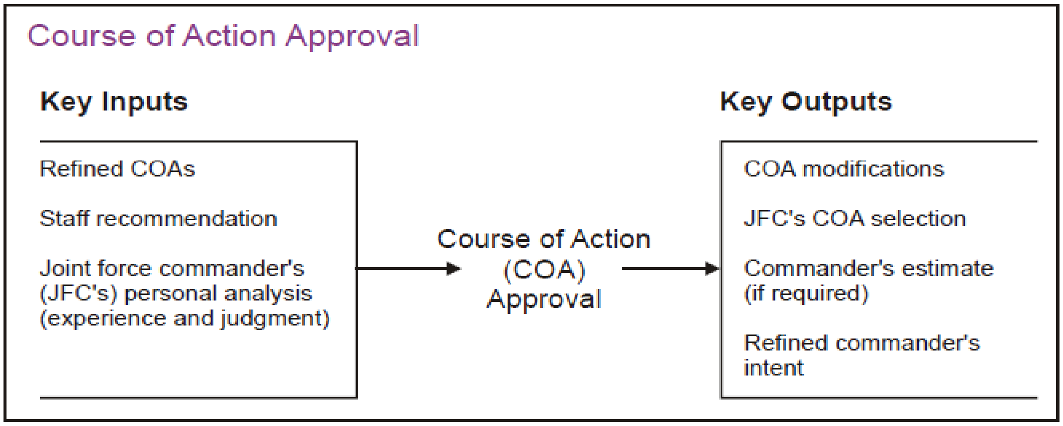
a. Prepare and present the COA decision briefing.

b. Commander selects/modifies the COA.

c. Refine Selected COA.

d. Prepare the Commander's Estimate.

Figure III-12 depicts the key inputs and outputs of COA approval.



Course of Action Approval

Key Inputs

Refined COAs

Staff recommendation

Joint force commander's (JFC's) personal analysis (experience and judgment)

Course of Action (COA) Approval

Key Outputs

COA modifications

JFC's COA selection

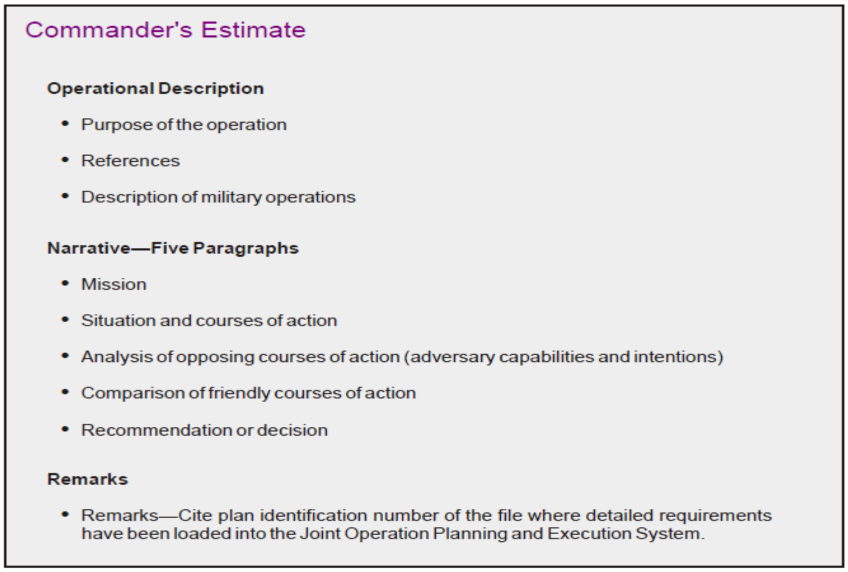
Commander's estimate (if required)

Refined commander's intent

Figure III-12: Course of Action Approval[43]

[43] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, IV-40.

Commanders Estimate. The Commander's estimate is prepared in the format shown in Figure III-13.



Commander's Estimate

Operational Description

- Purpose of the operation
- References
- Description of military operations

Narrative—Five Paragraphs

- Mission
- Situation and courses of action
- Analysis of opposing courses of action (adversary capabilities and intentions)
- Comparison of friendly courses of action
- Recommendation or decision

Remarks

- Remarks—Cite plan identification number of the file where detailed requirements have been loaded into the Joint Operation Planning and Execution System.

Figure III-13: Commander's Estimate[44]

7. Plan/Order Development. From the JFC's COA selection, the staff must now produce an OPLAN or OPORD. Deliberate planning will produce an OPLAN, while CAP typically will result in an OPORD.

The JFC and staff, in collaboration with mission partners and planners from across all domains, accomplish plan/order development. The JOPP transforms the selected COA into a Concept of the Operations (CONOPS) that accomplishes the JFC's mission. It describes how the actions of the joint force components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission, including branches and sequels.

From the CONOP, staff planners from all domains develop (or graphically portray) the OPLAN or OPORD in sufficient detail so that subordinate and supporting commanders understand their mission, tasks, and other requirements.

The *CJCSM 3130.03 series that provide detailed guidance on CONOPS content and format.*

[44] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, IV-44.

CHAPTER 4

DOMAINS

A. General

1. Introduction

The employment of cross-domain capabilities to exploit adversaries' weaknesses and achieve decisive victory is not a new idea, but much has changed in recent years. Cross-domain operations have expanded beyond the combination of air, land, and maritime operations to include capabilities delivered from space and cyberspace. Modern technology has vastly increased the number of capabilities with military applications. These capabilities are no longer "owned" by a single Service. Moreover, other government organizations and foreign partners bring unique capabilities to the battle space. While the problems we face are more complex, we have a greater quantity, quality, and variety of tools with which to fix them – our potential to achieve cross-domain synergy is at an all-time high.[45]

Cross-domain integration requires familiarity with all the domains. For each domain, this chapter describes important characteristics, how the DOD organizes and operates within that domain, and the key implications staff officers need to understand. Staff officers can develop deeper knowledge by studying the references in Appendix D.

B. Air

1. Introduction.

Air operations will be essential for any intervention operation, providing rapid access to the theater of operations and enabling air superiority in support of land and maritime forces. While only the richest nations can afford large air forces, the declining costs of unmanned aerial vehicles afford even non-state actors use of the air domain. Countering adversary Unmanned Aerial System (UASs) and other novel developments will require ingenuity.[46]

2. Unique Air Capabilities and Characteristics.

Beyond interdicting strategic targets in isolation, air superiority provides the ability to prevent adversary air and missile threats from effectively interfering with operations of friendly air, land, maritime, space, and special operations forces. This facilitates freedom of action and movement. The characteristics of air domain capabilities are:

(a) Speed: Modern air assets can move quickly between locations often engaging adversary forces before other domains' capabilities are within range. Speed is also a combat multiplier in the defense allowing quick responses to enemy activities.

[45] William O. Odom and Christopher D. Hayes, "Cross-domain synergy: Advancing Jointness", *Joint Forces Quarterly 73 2nd Quarter 2014*, 124.

[46] Elizabeth Quintana, Joanne Mackowski, and Adam Smith, *Occasional Paper July 2012: Cross-Domain Operations and Interoperability*, (London: Royal United Services Institute www.rusi.org , July 2012), 6.

(b) Range: Air assets can cross vast distances, deliver munitions, and return to bases outside the area of operations (AOR). Range and loiter times may be extended through refueling. These long range capabilities afford the nation a strategic advantage not available to most adversaries.

(c) Detection: Air operations are generally difficult to conceal and vulnerable to enemy air defenses. However, use of advanced materials and deception operations can reduce detection by adversary sensors.

(d) Airspace Overflight: Obtaining permission to fly over through another nation's airspace can delay operations.

3. Operations.

Within DoD, the United States Air Force (USAF) is principally responsible for strategic, operational, and tactical air and space assets.[47] While all Services have air capabilities, the USAF maintains the preponderance of air and space assets. It coordinates with the other services to plan and execute joint missions.

These forces are tasked through the JOPP process. The USAF functions in both strategic and operational roles based on requirements and tasking from DOD. The USAF's organization reflects its dual support and operational responsibilities. It consists of major commands (MAJCOMs), groups, wings, and squadrons. The USAF assigns MAJCOMs to CCMDs to support air operations. **The MAJCOMs provide air and space operations planning and support elements to the AOR's CCDR** to ensure integrated air and space planning.

Gaining and maintaining **air superiority is one of the air domain planner's top priorities.** Attaining air superiority – and air supremacy when required – helps provide both the freedom to attack and freedom from attack. Operating without it increases risk to maritime and land operations. The JFC draws air support from USAF Air Expeditionary Wings (AEW's) from an assigned Air Expeditionary Task Force (AETF), Naval Aviation from Carrier Strike Groups (CSG's) and land based Naval Aviation assets, United States Marine Corps (USMC) aviation assets from an assigned Marine Air Ground Task Forces (MAGTF), and United States Army (USA) aviation assets.

The Joint Forces Air Component Command (JFACC) is responsible for planning joint air operations as well as providing space planning for the AOR. The JFACC uses the Joint Operation Planning Process Air (JOPPA) to develop a Joint Air Operations Plan (JAOP) for employment of air assets. The JFC normally designates the component with the preponderance of air assets and the ability to manage air operations as the JFACC. Common JFACC responsibilities are to:

(a) Develop a JAOP.

(b) Recommend air apportionment priorities.

[47] U.S. Joint Chiefs of Staff, *Joint Publication 3-01 Countering Air and Missile Threats*, (Washington, DC: U.S. Joint Chiefs of Staff, 2012), II-5.

(c) Allocate and task the joint air capabilities and forces provided by the Service components based on the JFC's air apportionment decision.

(d) Provide the JFACC's guidance in the Air Operations Directive (AOD) for the use of joint air capabilities. The JFACC updates the AOD periodically and uses it throughout the planning and execution of the joint air tasking cycle (ATC). Figure IV-1 depicts the ATC process.

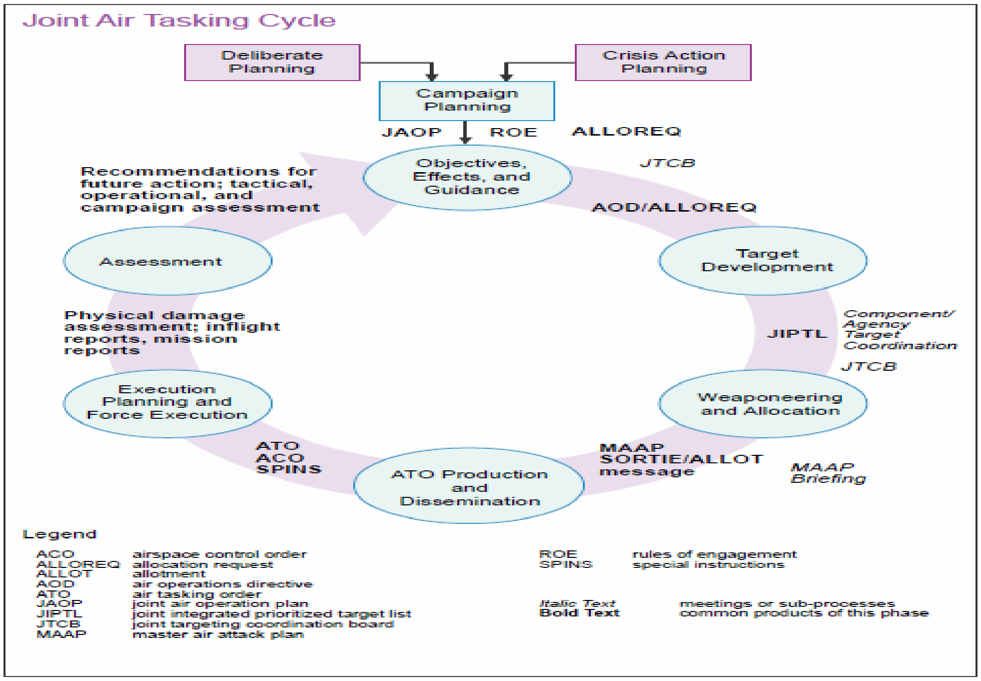

Joint Air Tasking Cycle
Deliberate Planning
Crisis Action Planning
Campaign Planning
JAOP
ROE
ALLOREQ
Objectives, Effects, and Guidance
JTCB
AOD/ALLOREQ
Target Development
JIPTL
Component/ Agency Target Coordination
JTCB
Weaponeering and Allocation
MAAP SORTIE/ALLOT message
MAAP Briefing
ATO Production and Dissemination
ATO ACO SPINS
Execution Planning and Force Execution
Physical damage assessment; inflight reports, mission reports
Assessment
Recommendations for future action; tactical, operational, and campaign assessment
Legend
ACO airspace control order
ALLOREQ allocation request
ALLOT allotment
AOD air operations directive
ATO air tasking order
JAOP joint air operation plan
JIPTL joint integrated prioritized target list
JTCB joint targeting coordination board
MAAP master air attack plan
ROE rules of engagement
SPINS special instructions
Italic Text meetings or sub-processes
Bold Text common products of this phase

Figure IV-1: Joint Air Tasking Cycle[48]

(e) Perform the duties of the Airspace Control Authority (ACA). ACA is a commander designated by the JFC to assume **overall responsibility for the operation of the airspace control system** in the airspace control area. JP 3-30, *Command and Control Joint Air Operations*, 10 Feb 2014, pg. I-4 describes this function.

(f) Perform the duties of the Area Air Defense Commander (AADC). AADC is **responsible for Defensive Counter-Air (DCA) operations**, which include the integrated air defense system for the joint operations area. DCA and offensive counter-air operations comprise the counter-air mission, which is designed to attain and maintain the degree of air superiority desired by the JFC. In coordination with the component commanders, the AADC develops, integrates, and distributes a JFC-approved joint area air defense plan.

(g) Perform the duties of the Space Coordinating Authority (SCA). See the section on the space domain for a complete discussion on the SCA.

The JFACC will normally operate from a Combined Air Operations Center (CAOC). The CAOC is structured to operate as a fully integrated command center and should be staffed by members from all participating components, to include key staff positions, to fulfill the JFACC's responsibilities. Elements common to all CAOCs are a strategy division, combat plans division, ISR division, air mobility division, and combat operations division.

[48] U.S. Joint Chiefs of Staff, *Joint Publication 3-30 Command and Control of Joint Air Operations*, (Washington, DC: U.S. Joint Chiefs of Staff, 2014), III-21.

The Joint Air Operations Command and Control System is the C2 system for joint air operations. **The C2 system for air operations will vary depending on the operational area and missions**. The Air Force's theater air control system, the Army's air-ground system, the Navy's composite warfare commander/Navy tactical air control system, Marine's air command and control system, or the special operations air-ground system typically serves as the nucleus for C2 of joint air operations.

The JFACC **uses the entire staff to compare air capabilities and explore adversary and friendly COAs**. The JFACC must ensure that planners collaborate with other components. Figure IV-2 depicts the joint air operations planning process.

The **JAOP integrates and coordinates** joint air operations. It addresses all air capabilities and forces supported by, and in support of, other joint force components. The JFACC's planners **must anticipate the need to make changes** to plans (e.g., sequels or branches) in a dynamic and time-constrained environment. Planners should include representatives from all components providing air capabilities or forces in their efforts to enable their effective integration.

JOPPA parallels the JOPP described in *JP 5-0, Joint Operations Planning*. The JFACC utilizes JOPPA during deliberate and crisis action planning to produce JAOPs, and supporting plans and orders. The air planning staffs coordinate the JOPPA and the JAOP with the overall plan.

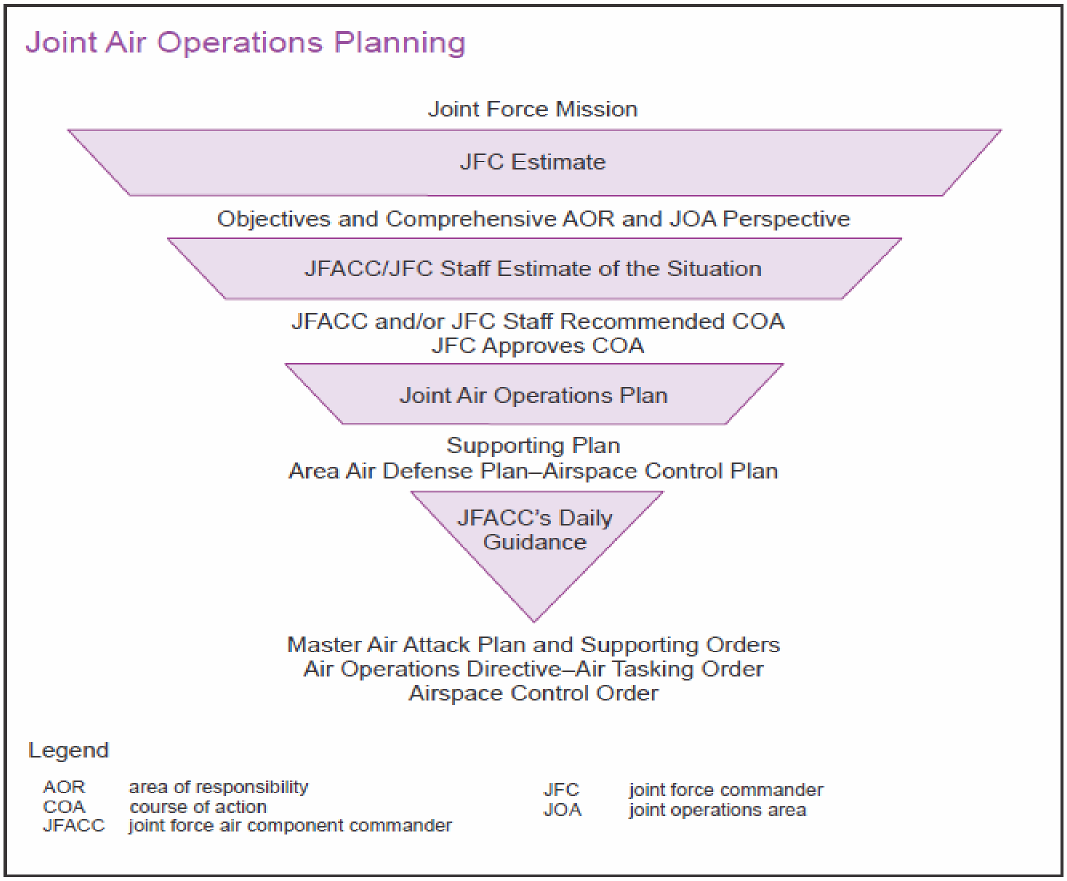

Joint Air Operations Planning
Joint Force Mission
JFC Estimate
Objectives and Comprehensive AOR and JOA Perspective
JFACC/JFC Staff Estimate of the Situation
JFACC and/or JFC Staff Recommended COA
JFC Approves COA
Joint Air Operations Plan
Supporting Plan
Area Air Defense Plan–Airspace Control Plan
JFACC's Daily Guidance
Master Air Attack Plan and Supporting Orders
Air Operations Directive–Air Tasking Order
Airspace Control Order
Legend
AOR area of responsibility
COA course of action
JFACC joint force air component commander
JFC joint force commander
JOA joint operations area

Figure IV-2: Joint Air Operations Planning

The use of personal contact, established communications and information support systems, and liaison personnel ensures all staff planners have continuous access to the JFACC and the JFACC's staff.

For more information on Liaisons, refer to Section 4 of this planner's guide *and JP 3-33, Joint Task Force Headquarters, 30 July 2012.*

4. Planning Considerations. Joint planners integrating air operations into a joint planning process, should first seek the expertise of:

(a) Air planners on the joint staff (potentially, the space planners as well)

(b) LNOs from the JFACC or Air Force Service Component Command

(c) Lead planners from the JFACC's staff

From these experts, gaining insight and understanding of available air capabilities enables planners to merge these capabilities with the other domains.

Understanding the **JFACC's role is to plan joint air operations in support of the developed JFC COAs is critical for a joint planner.** The joint planner must also recognize that most often the planning and coordination of space assets are directly linked with air.

As a joint staff planner, it is important to have a basic understanding the internal operational flow of the JFACC and to maintain awareness of the JFACC's planning progress. The JFACC operates on an air tasking cycle; to integrate air capabilities with the other domains, understanding the JFACC's tasking cycle is crucial.

For more information refer to Appendix D.

C. Land

1. Introduction.

The land domain is where most humans live. **By controlling land, military forces can force adversary forces to retreat, disperse, reposition, or collapse**. Occupation of an adversary's land enables military forces to sustain influence on the indigenous population over a long period of time and increase the likelihood of a permanent solution to the military problem.[49]

2. Unique Land Capabilities and Characteristics.

Wars have been decided on land since the beginning of recorded history. The characteristics of fighting on land are:

(a) Extreme variations in climate and terrain – urban, forest, desert, jungle, mountain, and arctic – present dramatically different operational environments

[49] U.S. Joint Chiefs of Staff, *Joint Publication 3-31 Command and Control for Joint Land Operations*, (Washington, DC: U.S. Joint Chiefs of Staff, 2014), ix.

(b) Presence of people, especially non-combatants, effects options for use of military force.

(c) The ability to sustain operations over long periods of time.

(d) The speed and duration of movement on land is slower and more arduous than movement by air and sea.

(e) "With respect to non-lethal effects, only land forces have directly useful capability that can be precisely applied in complex, human terrain. Non-lethal effects work through example and the potential threat of violence rather than the execution of that threat. Although all services have the ability to affect their counterparts through security assistance activities, only land forces can achieve the position (close to the population dispersed in complex land clutter) and duration (persistence) that permits sustained non-lethal effect."[50]

3. Operations.

The U.S. Army, U.S. Marine Corps, and U.S. Special Operations Command are the DOD's premier land forces. Joint Force Land Component Commanders (JFLCCs) lead the fight on land, but also support operations in other domains. Coordinated planning between the JFC and JFLCC staffs is critical to achieving cross-domain synergy.

The **JFLCC integrates planning for land operations beneath the level of the JFC**. The designation of a JFLCC enhances the integration and synchronization of operational maneuver with fires by making the JFLCC the supported commander within their area of operations (AO).[51] The **JFLCC's overall responsibilities and roles are to plan, coordinate, and employ forces in support of the JFC's mission**. They include:

(a) Advising the JFC on the employment of forces**.** Developing, integrating, maintaining, and sharing with the JFC the land common operational picture (COP) (people, objects, and events) within the JFLCC's operational area, as an input to the JFC's COP.

(b) Developing the joint land operation plan (OPLAN)/operation order (OPORD) in support of the JFC's mission and optimizing land operations. The JFLCC issues planning guidance to all subordinate and supporting elements and analyzes proposed COAs.

(c) Executing land operations as directed by the JFC, which includes adjusting tasks to forces and capabilities and coordinating with affected component commanders.

(d) Evaluating the results of land operations to include the effectiveness of interdiction operations, and forwarding these results to the JFC for inclusion in the combat assessment.

(e) **Designating the target** priorities, effects, and timing for joint land operations.

(f) Performing duties of the joint force supported commander for PR, if designated.

[50] MG David A. Fastabend, U.S. Army (Retired), *Mechanism of Joint Synergy Version 3,* (Unpublished manuscript last modified December 12, 2012)
[51] U.S. Joint Chiefs of Staff, *Joint Publication 3-31 Command and Control for Joint Land Operations*, I-9.

(g) Providing **mutual support to other components** by conducting operations such as suppression of enemy air defenses and suppression of threats to maritime operations.

(h) Coordinating with other functional and Service components' sustainment support in accomplishment of JFC objectives. (Such as: Bulk Fuel, Airfield outer security, Theater C2, etc.)

(i) Providing an assistant or deputy to the area air defense coordinator (AADC) for land-based joint theater integrated air missile defense operations and coordination as determined by the JFC.

(j) Supporting the JFCs IO by developing the IO requirements that support land operations and synchronizing the land force information-related capabilities (IRCs) when directed.

(k) Providing inputs into the JFC-approved joint operational **area air defense plan (AADP)** and the **airspace control plan (ACP).**

The interface between JFLCC planners and their peers in other commands is provided below in the Table below.

JFLCC Interface With Other Joint Force Command and Control Mechanisms

C2 Mechanism	Role/Function	JFLCC Interface
JFC's Joint Targeting Coordination Board (JTCB)	Meets daily to provide broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance and priorities, and refining the Joint Intelligence Prioritized Target List (JIPTL).	JFLCC's representative attends JTCB meetings to represent land component interests. JFLCC's targeting coordination board provides input.
JFC'S Joint Planning Group (JPG)	Meets daily or as required to conduct crisis action planning (to include course of action development and refinement), coordination of joint force operation order development, and planning for future operations (e.g., transition, termination, follow-on).	JFLCC's representative participates in all planning activities.
JFC's Joint Intelligence Operation Center	An interdependent, operational intelligence organization at the combatant command or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment.	JFLCC's J-2 and staff maintain daily communication with the JIOC to provide, request, and receive intelligence products as needed.
JFC's Information Operations Cell	Meets daily or as required to integrate and synchronize information-related capabilities with other elements of the operation plan.	JFLCC's representative to this IOWG participates and coordinates with the JFLCC's JPG representative and other staff members.

JFC's Joint Transportation Board	Communicates JFC's priorities and adjudicates competing requirements for intra-theater lift assets and helps resolve other issues that negatively impact the Defense Transportation System.	JFLCC's representative participates.
JFC's Joint Movement Center	Coordinates the employment of all means of transportation (including that provided by allies or host nations) daily to support the concept of operations.	JFLCC's representative participates.
JFC's Joint Petroleum Office	Plans and manages wholesale theater bulk petroleum support and develops the petroleum logistic support plan.	JFLCC's logistics directorate (J-4) coordinates and provides assistance as needed.
JFC's Civil-Military Operations Center	Meets daily and will coordinate all civil-military operations (CMO) among other USG departments and agencies, intergovernmental organizations, nongovernmental organizations, coalition, and host nation members; and plays an integration and synchronization role with other elements of the operation plan.	JFLCC's representative participates.
JFACC's Targeting Effects Team	Processes all potential targets to balance component priorities with the JFC's objectives. Competing concerns are prioritized against available assets to produce the JIPTL, apportionment recommendations, and close air support allocation.	JFLCC provides input and participates, coordinates with targeting effects team.
JFACC's Air Tasking Order (ATO) Development Processes	Produces a tasking document transmitted to components, subordinate units, and C2 agencies on projected sorties, capabilities, and specific missions. The ATO normally provides specific instructions to include call signs, targets, controlling agencies, etc., as well as general instructions.	JFLCC provides input, participates, and coordinates for JFLCC-retained air assets (i.e. rotary and available fixed wing).
Airspace Control Authority Airspace Control Order (ACO) Development Process	Produces an ACO transmitted to components, subordinate units, and C2 agencies on joint use of airspace. The ACO normally provides specific instructions for airspace de-confliction by time, altitude, or routes as well as general instructions.	JFLCC provides input and participates. Marine Direct Air Support Center provides input and participates. - Army Theater Air Operations Group provides input and participates.

Joint Security Coordination Committee (JSCC)	Coordinates and oversees overall security operations within the AOR/ JOA. Monitors emergency service, force protection, antiterrorism, physical security, and base /base cluster plans.	JFLCC security coordinator is typically designated principal staff officer for the planning of joint security operations throughout the AOR/JOA.
Joint Lines of Communication Security Board	Assesses and reports LOC status and security capability shortfalls.	JFLCC/JSCC leads and provides transportation, intelligence, and provost marshal representatives.
Joint Deployment and Distribution Operations Center	A combatant command movement control organization designed to synchronize and optimize national and theater multimodal resources for deployment, distribution, and sustainment.	JFLCC coordinates and utilizes JDDOC.
Joint Interagency Coordination Group	Interagency staff group that establishes regular, timely, collaborative working relationship between civilian and military organizations and other agencies.	JFLCC's representative participates.
CCMD's Joint Cyberspace Center	Combines input from United States Cyber Command and CCMDs to provide a regional/functional cyberspace situation awareness/common operational picture. Facilitates the coordination and de-confliction of CCDR directed cyberspace operations.	JFLCC's representative coordinates to provide/request cyberspace operations products.

Legend

ACO	airspace control order	JIPTL	joint integrated prioritized target list
AOR	area of responsibility	JOA	joint operations area
ATO	air tasking order	JPG	joint planning group
BCD	battlefield coordination detachment	JSCC	joint security coordination center
C2	command and control		
JTCB	joint targeting coordination board J-2	intelligence directorate of a joint staff	
JFACC	Joint Force Air Component Commander	MARLE	Marine liaison element
JFC	joint force commander		
JFLCC:	Joint Force Land Component Commander		

Table IV-1: JFLCC Interface with Other Joint Forces C2 Mechanism[52]

4. **Planning Considerations.** The planning efforts required to command and control joint land operations are extensive. The JFC and JFLCC have processes and procedures to optimize the use of all capabilities and facilitate cross-domain coordination.[53] Planners integrating land operations into a joint planning process, should first seek the expertise of:

(a) Land planners on the joint staff.

(b) LNOs from the JFLCC.

(c) LNOs from the Army and Marine Corps Service Component Commands.

(d) LNOs from the CCMD's theater special operations command (TSOC).

(e) Lead planners from the JFLCC's or the TSOC's staff.

These experts can provide information on available land capabilities and how to combine their effects with other capabilities based in other domains.

Land forces provide much of the support for other domains' forces (bulk fuel, base security, long haul transportation, theater network support, air defense artillery, etc.) requiring coordination with other components and prioritization by the JFC.

Land forces provide the ultimate fidelity on battle damage assessment.

Every activity on land requires security - every patrol, every new base, and every convoy - must have a land security force, which comes from the overall budget of land forces.

For more information refer to Appendix D.

[52] U.S. Joint Chiefs of Staff, *Joint Publication 3-31 Command and Control for Joint Land Operations,* II-19.
[53] U.S. Joint Chiefs of Staff, *Joint Publication 3-31 Command and Control for Joint Land Operations*, 18.

D. Maritime

1. Introduction.

Despite an exponential rise in air traffic, over 90 percent of all freight is still shipped by sea. Piracy in the Horn of Africa and in the Straits of Malacca punctuate the need to secure maritime trade routes. In addition, with 80 percent of the world's population living within 100 miles of the sea, landlocked theaters will be an exception. Furthermore, due to the high bandwidth capacity of fiber-optic cables, much of the world's *cyberspace traffic* flows through the maritime domain via undersea cables. **The ability to access the maritime domain enhances a nation's ability to interact with other nations**. The application of naval power can also deny adversaries this same capability.

Maritime power is military, diplomatic, and economic power or influence exerted through use of the sea. The JFC employs maritime power to influence events on land directly through power projection (e.g., amphibious assault) or indirectly through control of the maritime domain.

2. Unique Maritime Capabilities and Characteristics.

(a) Movement is relatively inexpensive and constrained only by land formations (islands, coastlines) and water depth.

(b) Sea lines of communication are vulnerable to subsurface attack. The vast spaces of the ocean can hide naval forces from detection, however movement on the ocean surface is more easily detected with modern sensing capabilities.

(c) Maritime capabilities **can operate far from home bases more flexibly and at greater distances than air forces**. Additionally, they can assault land objectives from the sea. However, sea-based capabilities have distinct range and sortie generation disadvantages relative to land-based capabilities.

(d) The **maritime domain also has unique economic, diplomatic, military, and legal aspects** (see figure IV-3).[54] Diplomatic and political issues related to the maritime domain have increased as many nations have tried to extend their claims over offshore resources. These **claims have led to disputes over the extent of maritime borders and Exclusive Economic Zones (EEZs).** This is highlighted in diplomatic and legal tension over some archipelagic waters and international straits. Naval forces may face constraints and restrictions when operating in territorial seas, contiguous zones, EEZs, and continental shelves claimed by coastal states.

[54] U.S. Joint Chiefs of Staff, *Joint Publication 3-32 Command and Control for Joint Maritime Operations,* (Washington, DC: U.S. Joint Chiefs of Staff, 2013), I-7.

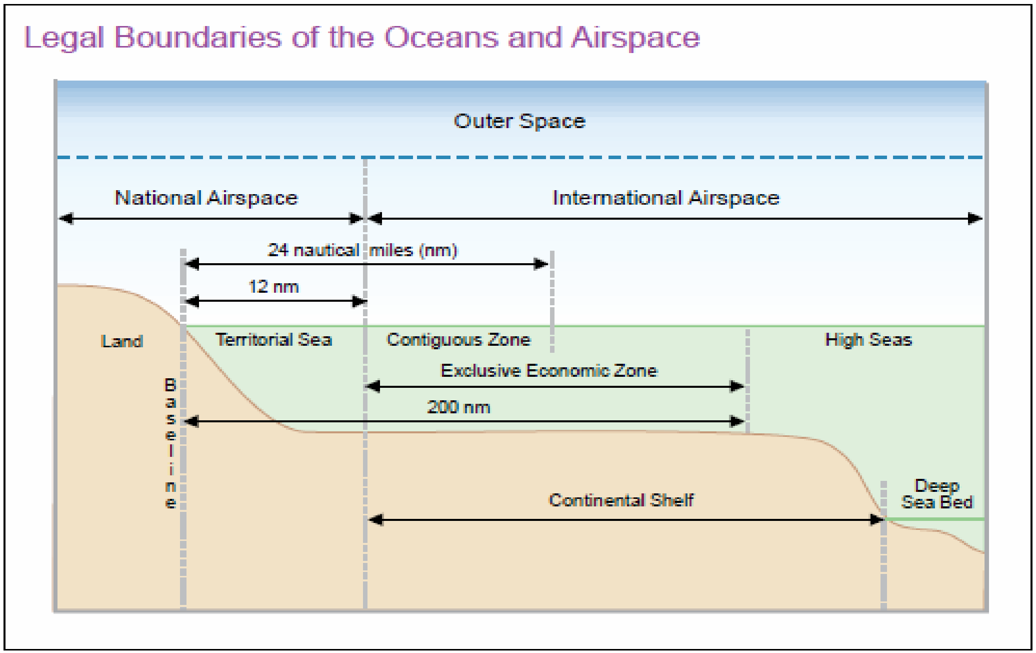


Figure IV-3: Legal Boundaries of the Ocean and Airspace[55]

(e) The world's oceans contain about 200 **chokepoints and lines of communications (LOCs)** control of which can restrict access or disrupt passage. In the event of regional conflict, small coastal navies operating in the proximity of these chokepoints can challenge naval operations and merchant shipping.

3. Operations.

The **five core capabilities** of U.S. naval forces are: **all domain access, deterrence, sea control, power projection, and maritime security**. Additional naval capabilities include foreign humanitarian assistance (FHA), naval aviation, strategic sealift, sea basing, and homeland security support. These unique capabilities afford several options to creatively employ the maritime domain in JFCs' warfighting efforts. Below are listed several constructs the Joint Force employs to address the uniqueness of the maritime domain.

(a) Joint Maritime Operations (JMO) are operations performed with maritime forces and other forces assigned, attached, or made available, in support of the JFC's operation or campaign objectives, or in support of other components of the Joint Force. The JFC may designate a Joint Force Maritime Component Commander (JFMCC) to C2 a JMO. As a functional component commander, the JFMCC has authority over assigned and attached forces and forces made available for tasking.

(b) The degree of integration and coordination between components varies depending on the situation. For some JMO, the JFMCC will likely operate without the support of other component forces (e.g., submarine operations in blue water) whereas for others there may be detailed

[55] U.S. Joint Chiefs of Staff, *Joint Publication 3-32 Command and Control for Joint Maritime Operations,* I-7.

integration between components (e.g., attack of enemy submarines in port or their supporting critical infrastructures ashore).

(c) The JFMCC's staff planning process is consistent with the JOPP as outlined in JP 5-0, *Joint Operation Planning* and in conjunction with JP 3-32 *Command and Control for Joint Maritime Operations*. The JFMCC's staff uses a synchronization process similar to a JFC's staff to ensure coordination between subordinates.[56]

(d) JFMCCs and their staffs not only contribute to the JFC's planning efforts but also contribute to the development of other components' and multinational supporting plans and OPORDs. Therefore, maritime staffs should be well versed in the JOPP and multinational procedures. North Atlantic Treaty Organization (NATO) Standardization Agreements (STANAGs) and Allied Joint Publications (AJPs) may impact the maritime components.[57] Maritime staffs may need to refer to NATO publications, such as AJP-3.1, *Allied Joint Maritime Operations*, AJP-3.3.3, *Air Maritime Co-ordination*, *Maritime Tactical Publication-01, Multinational Maritime Tactical Instructions and Procedures*, and *Maritime Procedural Publication-01, Multinational Maritime Voice Reporting Procedures*.

(e) A JFC should consider the advantages of establishing a sea base to stage or support joint operations. **Joint sea basing** reduces the footprint ashore and allows support and sustainment to be landed in sufficient quantities, as required, without necessarily placing it in a vulnerable and essentially immobile location. Additional information related to establishing, maintaining, and operating from a sea base can be found in *Naval Warfare Publication (NWP) 3-62M, Sea Basing*.

(f) Most maritime platforms are multi-mission capable and are routinely multi-tasked to support different missions and commanders. **JFMCCs recognize and prioritize requirements, address conflicts and limitations, and integrate the various capabilities of assigned and attached forces and those made available for tasking.**

(g) Maritime forces use some unique C2 structures. While afloat, Marines and SOF remain independent of the ship's captain, but utilize the ship's communication systems. Similarly, a CSG commander will have separate commanders for the carrier and the carrier's air wing.

For more information on Maritime Operations and Legal boundaries, refer to Joint Publication (JP) 3-32, Command and Control for Joint Maritime Operations, 7 August 2013.

4. Planning Considerations.

Joint planners integrating maritime operations into a joint planning process should first seek the expertise of:

(a) Maritime planners on the joint staff.

(b) LNOs from the JFMCC.

(c) LNOs from the Service Component Commands of applicable maritime Services.

[56] U.S. Joint Chiefs of Staff, *Joint Publication 5-0 Joint Operation Planning*, xxv.

[57] For further information refer to Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122 Series, *Joint Operation Planning and Execution System;* CJCSM 3130 Series, *Adaptive Planning and Execution,* JP 3-0, *Joint Operations;* JP 5-0, *Joint Operation Planning;* approved joint terminology; and the amphibious planning process contained in JP 3-02, *Amphibious Operations.*

(d) Lead planners from the JFMCC's staff.

These experts can provide information on available maritime capabilities and how to combine their effects with other capabilities based in other domains.

Joint planners should understand the implications of multi-mission tasking (e.g., Anti-Submarine Warfare (ASW), Surface Tactical Warfare (STW), CAS, Maritime Air Support, sea control) on individual platforms and personnel.

Maritime domain awareness (MDA) is the extent of a planner's understanding of the maritime domain. Accurate MDA is a key enabler of an active, layered maritime defense. MDA facilitates expeditious and precise actions by the JFC, the JFMCC, and subordinate commanders.

For more information refer to Appendix D.

E. Space

1. Introduction.

Space is becoming increasingly important and contested. In this global common, over sixty nations rely on space assets for a growing number of services. Anti-satellite technologies, destructive space weather, and damage from space debris potentially threaten space assets. JFCs and their staffs must plan for the disruption of space services.[58]

2. Unique Space Forces Capabilities and Characteristics.

Joint staff officers must understand the environment in which space forces operate and their relationship to military operations. These forces have the following unique characteristics:

(a) There are no geographical boundaries in space. As a **Global Commons**, space overcomes the international law aspect of a nation's territorial sovereignty.

(b) Satellites are subject to the laws of orbital mechanics. Adjustments to orbits expend fuel and reduce asset life span.

(c) Environmental considerations place demands on satellites' characteristics to include size, weight, and power further hindering the spacecraft's performance and life span.

(d) Though space is infinite in expanse, certain altitudes and orbital patterns are advantageous. These portions of space are becoming crowded.

(e) **Electromagnetic spectrum** access is vital to space operations because it is the sole medium for space-based assets to transmit and receive information and/or signals. Therefore, JFCs must sufficiently control the EMS to interact with space systems.[59]

[58] Quintana et al., *Occasional Paper July 2012: Cross-Domain Operations and Interoperability,* 6.
[59] U.S. Joint Chiefs of Staff, *Joint Publication 3-14 Space Operations*, (Washington, DC: U.S. Joint Chiefs of Staff, 2013), x.

(f) Space is no longer a domain exclusively transited by state actors. Many non-state actors maintain assets in orbit and often military capabilities (Iridium satellite phones, Virgin space tourism, etc.) employ these non-state assets.

3. Operations.

(a) Space Mission Areas: The space mission areas are:[60]

1. **Space Situational Awareness (SA)** characterizes capabilities within the space domain.

2. **Space Force Enhancement** operations improve the effectiveness of military operations. They include intelligence, surveillance, and reconnaissance; integrated tactical warning and attack assessment; command, control, and communications; position, velocity, time, and navigation; and environmental monitoring.[61]

3. **Space Support** provides essential capabilities, activities, tasks, and functions vital to operate and sustain all elements of space forces. Its components include Satellite Operations, Space Lift, and Space Forces Reconstitution.

4. **Space Control** enables the freedom of action for friendly forces and, when required, negates or defeats interfering adversary capabilities and efforts. Space Control involves the offensive and defensive actions required for U.S. and friendly forces' space operations. Offensive control entails multiple negating actions to include deception, disruption, denial, degradation, or destruction.

5. **Space Force Application** covers the execution of combat operations in, through, and from space. It includes ballistic missile defense and employment of intercontinental ballistic missiles.

The most important mission area for a joint staff planner to consider is Space Force Enhancement. While the other mission areas are important, the Geographic Combatant Command (GCC) and JTF planners will have little control over Space Force Application or Space Support. Space Force Enhancement increases joint force effectiveness by enhancing operational awareness, providing joint force support, and increasing the force's combat potential. Its critical advantage is reducing confusion inherent within combat. Space Force Enhancement also gives JFCs visibility into denied areas and persistence not obtainable by air, land, or maritime capabilities. However, space force enhancement dependency is a potential vulnerability. **Planning redundancy for space-dependent systems is crucial when adversaries disrupt, degrade, or deny joint force space capabilities and operations.**

For further information on Space Missions refer to JP 3-14 and AF Annex 3-14, *Space Operations.*

[60] U.S. Joint Chiefs of Staff, *Joint Publication 3-14, Space Operations*, II-1.

[61] U.S. Joint Chiefs of Staff, *Joint Publication 1-02 DOD Dictionary of Military and Associated Terms,*(Washington, DC: U.S. Joint Chiefs of Staff, 2010 (as amended through 15 March 2015)), 226.

(b) Space Organizational Structure: Command and control of space assets and capabilities differs from C2 in the traditional domains in that it is globally focused on supporting worldwide missions and requirements. Planners must coordinate with Commander, United States Strategic Command (CDRUSSTRATCOM) for use of space assets. Consolidating the DOD's space responsibilities under USSTRATCOM establishes the unity of command, effort, and purpose needed to achieve joint force and national security objectives.[62] CDRUSSTRATCOM delegates the daily management of space operations to the Commander, Joint Functional Component Command-Space (JFCC-Space) but maintains authority to delegate operational control (OPCON) or tactical control (TACON). GCCs have the following responsibilities:

1. Provide their prioritized space requirements to CDRUSSTRATCOM.

2. Provide joint force guidance and objectives for space operations for integration into plans and annexes.

3. Specify Offensive Space Control (OSC) and Defensive Space Control (DSC) objectives, and provide guidance for the employment of C2 systems, communications systems, intelligence, logistics, and attack operations for inclusion in plans and annexes.

4. Consolidate, validate, and prioritize subordinates and component commanders' space operations requirements.

5. Consider designating a space coordinating authority (SCA) and delegating appropriate authorities for planning, integrating, and coordinating space operations within the operational area.[63]

(c) Space Organizational Structure: The SCA is responsible for all aspects of integrating space capabilities and coordinating joint space operations. The SCA's roles and responsibilities may include:

1. Planning, coordinating, and synchronizing space operations in the operational area and incorporating input from the joint force staff and components.

2. Maintaining situational awareness of theater space operations and coordinating with other commands' SCAs or JFCC-SPACE to integrate theater space operations into DOD space operations.

3. Consolidating space requirements through the JFC for coordination.[64]

For further information on Space Force Command, Roles and Responsibilities refer to JP 3-14*, Space Operations* and AF Annex 3-14*, Space Operations.*

[62] U.S. Joint Chiefs of Staff, *Joint Publication 3-14, Space Operations*, III-1.
[63] U.S. Joint Chiefs of Staff, *Joint Publication 3-14 Space Operations*, III-1.
[64] U.S. Joint Chiefs of Staff, *Joint Publication 3-14 Space Operations*, III-2.

4. Planning Considerations.

Joint planners integrating space operations into a joint planning process should first seek the expertise of:

(a) Space planners on the joint staff (and potentially air planners).

(b) The JFC's designated SCA.

(c) LNOs from JFCC-SPACE or USSTRATCOM.

(d) Lead planners from JFCC-SPACE.

These experts can provide information on available space capabilities and how to combine their effects with other capabilities based in other domains.

Considering **space operations and assets are global in nature**, it is important to understand these assets can and will be used simultaneously for multiple commanders.

Space operations approvals and capabilities require long lead times. Consider and **request space assets and capabilities early to ensure effective integration.**

Anticipate degraded access to the space domain. Understand which systems rely on space and plan alternatives.

Expect taskings to either protect friendly ground stations or target adversary ground stations. While such taskings may drain other domains' combat power, they ultimately further the JFC's objectives.

Continuous information flow on space capabilities allows planners at different levels to proactively assess subordinate commanders' needs against available assets.

For further information on Space Planning refer to JP 3-14*, Space Operations* and AF Annex 3-14*, Space Operations.*

For more information refer to Appendix D.

F. Cyberspace

1. Introduction.

The ability to operate in cyberspace has emerged as a vital national security requirement. The growing impact of information warfare on military operations further increases the importance of cyberspace. As technological capabilities and instantaneous access to information continue to grow, the opportunities for real-time communication and information sharing expand. These capabilities are vital to economic and national development. However, reliance on these capabilities demands protection of the networks and information. Adversary activity in cyberspace could threaten the United States' dominance in the air, land, maritime, and space domains as they become increasingly interconnected and dependent on cyberspace technology.[65]

Cyberspace comprises the Internet, networks, systems, associated peripherals, and users in the information environment. This interconnected environment is important to global governance, commercial, military, and national security. A major challenge for the United States and its allies is protecting and defending the environment from adversaries. The host of cyberspace adversaries and threats include state actors, non-state actors, criminal organizations, general users, rogue individual hackers, and, in many cases, internal personnel. Conversely, many of these threats may also be vulnerable through cyberspace.

2. Unique Cyberspace Capabilities and Characteristics.

(a) Cyberspace is a **global** enabler for expedient, dynamic information exchange impacting all aspects of life. It allows instantaneous information flow across the globe for financial transactions as well as the movement and tracking of products and goods. However, it also allows adversaries to access this information and disrupt vital operations from any location. Cyberspace is difficult to regulate due to ease of accessibility. From a military perspective, cyberspace activities rarely require movement of forces, allowing engagement from extended stand-off ranges. It also enables the influence of populations that are inaccessible through the other domains.

(b) ***Can be reverse engineered:*** Unlike munitions, which are normally destroyed upon use, cyberspace activities include code that can be saved, analyzed, and recoded for use against allies or friendly nations. Planners must account for the possibility of a "boomerang effect" in which cyber activities are turned against the originator through reverse engineering.

(c) ***No Single National/International Ownership:*** While someone owns each physical component of cyberspace, the whole of cyberspace is not under any single nations' or entities' complete control. The infrastructure is a disparate combination of public and private networks without standardized security or access controls. This arrangement enables free information flow, but the lack of controls hinders global accountability, standardization, and security.

(d) ***Lack of Cooperation/Collaboration:*** The lack of international laws and regulations governing the environment complicates responses to actions in this domain. The difficulty in tracing the source of a cyberattack makes them easily deniable, especially if conducted by individual "hackers." Further hindering collaboration is the tendency to deny that a cyberspace attack has occurred to prevent loss of trust in an organization's cyber security measures.

(e) ***Low Cost:*** Cyberspace is the most affordable domain through which to attack the United States. Viruses, malicious code, and training are readily available over the Internet at no cost. Adversaries can develop, edit, and reuse current tools for network attacks. Inexpensive tools and training allow an adversary to compete without costly ships, aircraft, or missiles. Furthermore, an adversary can impose significant financial burdens on nations that rely heavily on cyberspace

[65] LCDR Sean Brandes, U.S. Navy, "The Newest Warfighting Domain: Cyberspace", *Synesis: A Journal of Science, Technology, Ethics, and Policy*. Published 2013. Accessed June 2015, G:90 http://www.synesisjournal.com/vol4_g/Brandes_2013_G90-95.pdf

by forcing them to invest in cyberspace defense. Currently, “military-grade” cyberspace capabilities remain too expensive for most malign actors, but they can buy relatively inexpensive services of professional hackers.

(f) ***Volatile:*** Successful cyberspace attacks depend on vulnerabilities within the adversary’s network. Identifying these vulnerabilities and creating cyberspace capabilities sometimes require great expense. If an adversary discovers the targeted network’s vulnerability and closes it, the cyberspace attack technique is rendered immediately and unexpectedly useless despite the development expense. For this reason, great care must be taken to prevent alerting adversaries to vulnerabilities in their networks.

(g) ***Speed:*** Cyberspace operations occur quickly. However, preparation for those operations is often extensive. An intense study of the adversary’s network may be required to learn system specifications and understand patterns of life. Therefore, a cyberspace unit operating on one adversary’s networks may not be able to shift focus to another target without substantial preparation.

(h) ***Unintentional cascading effects:*** Another unique characteristic of cyberspace is the potential for unintended cascading effects. Capabilities and munitions in the natural domains lose momentum the greater distance from impact. However, physical distance means very little in cyberspace. While cyberspace capabilities are developed and evaluated in computer labs and cyberspace ranges, there can never be complete assurances as to how a capability will behave or where it might spread when introduced to the great expanse of cyberspace.

(i) ***Layers:*** Cyberspace consists of three layers: Physical Network, Logical Network, and Cyber-Persona as reflected in Figure IV-4.

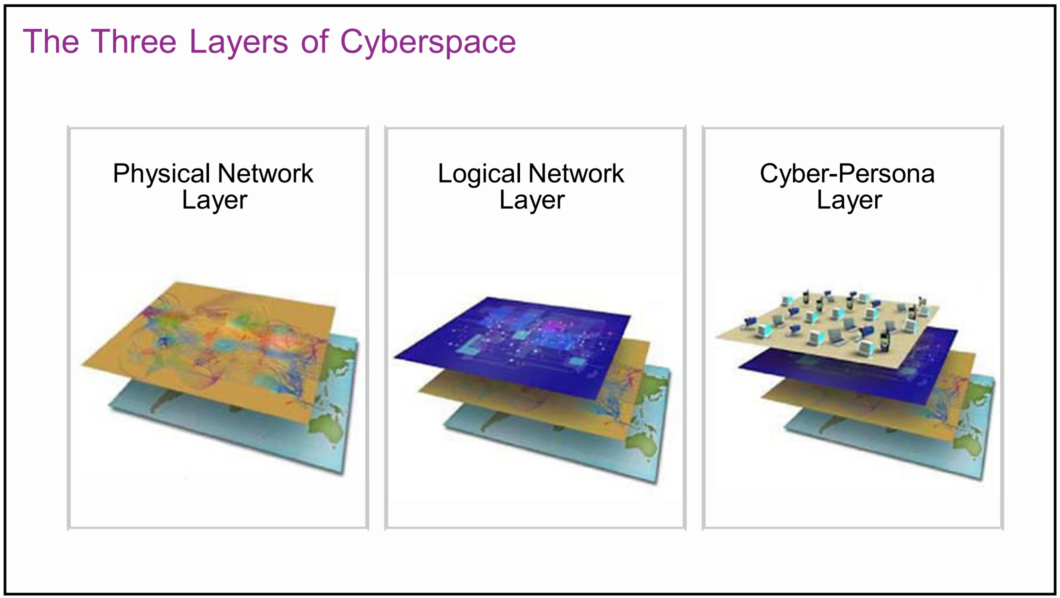
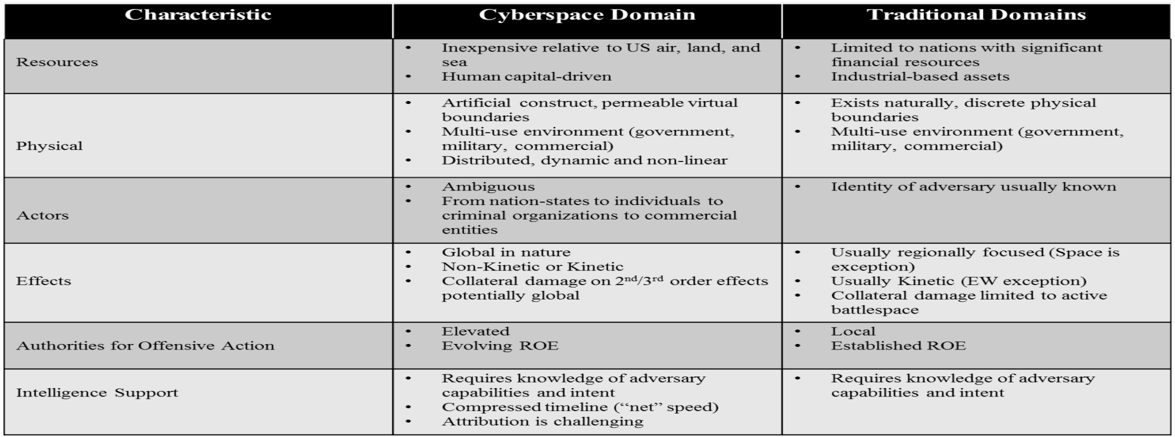


Figure IV-4: Three Layers of Cyberspace[66]

[66] U.S. Joint Chiefs of Staff, *Joint Publication 3-12 (R) Cyberspace Operations*, (Washington, DC: U.S. Joint Chiefs of Staff, 2013, I-3.

The **physical layer** includes all hardware assets – computers, servers, routers, satellite links, etc. – enabling the movement of information in and through cyberspace. Related to the physical layer is cyberspace's reliance on the electromagnetic spectrum (EMS), where much of cyberspace's code moves and is, therefore, vulnerable to jamming or manipulation. The **logical layer** is the abstract portion of the physical layer. This layer reflects information represented and accessible in multiple locations through Internet Protocol and uniform resource locator (URLs). The **cyber-persona** layer is an extension of the logical layer and represents the users, entities, and organizations on the network. This layer applies the same rules that govern the logical layer.[67] **Adversaries might attack any of these layers to disrupt, degrade, or destroy cyberspace capability. Conversely, each of these layers presents a means to attack adversaries' use of cyberspace.** The table below highlights differences and similarities between the cyberspace domain, and those of land, air, and sea.



Characteristic	Cyberspace Domain	Traditional Domains
Resources	• Inexpensive relative to US air, land, and sea • Human capital-driven	• Limited to nations with significant financial resources • Industrial-based assets
Physical	• Artificial construct, permeable virtual boundaries • Multi-use environment (government, military, commercial) • Distributed, dynamic and non-linear	• Exists naturally, discrete physical boundaries • Multi-use environment (government, military, commercial)
Actors	• Ambiguous • From nation-states to individuals to criminal organizations to commercial entities	• Identity of adversary usually known
Effects	• Global in nature • Non-Kinetic or Kinetic • Collateral damage on 2nd/3rd order effects potentially global	• Usually regionally focused (Space is exception) • Usually Kinetic (EW exception) • Collateral damage limited to active battlespace
Authorities for Offensive Action	• Elevated • Evolving ROE	• Local • Established ROE
Intelligence Support	• Requires knowledge of adversary capabilities and intent • Compressed timeline ("net" speed) • Attribution is challenging	• Requires knowledge of adversary capabilities and intent

Table TIV-2: Cyberspace vs. Traditional Warfare Domain Characteristics[68]

Control of cyberspace is a vital component of national security. The importance of cyberspace operations is on par with kinetic operations.[69]

3. Operations.

Cyberspace is similar to the space domain in its global expanse. Because the information environment affects all aspects of society, control of cyberspace must consider the global ramifications of actions within this domain. **Cyberspace, unlike the other domains, does not yet have a permanently defined C2 structure**.

(a) DOD information networks (DODIN) are the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.[70]

[67] U.S. Joint Chiefs of Staff, *Joint Publication 3-12 (R) Cyberspace Operations,* I-3.
[68] Brandes, "The Newest Warfighting Domain: Cyberspace", G:94.
[69] Brandes, "The Newest Warfighting Domain: Cyberspace", G:93.
[70] U.S. Joint Chiefs of Staff, *Joint Publication 3-12 (R) Cyberspace Operations*, A-51.

(b) The DOD sub-divides all cyberspace operations in to one of three categories: DODIN Operations, Defensive Cyberspace Operations, or Offensive Cyberspace Operations. Figure IV-5 depicts DOD's view of the range of actions in cyberspace.

- ***Cyberspace Security*** – install, (re)configure, train, update, monitor, etc. in order to maintain configuration, integrity, and availability.
- ***Cyberspace Defense*** – detect, characterize, counter, mitigate specific threat within a defended network. These are the actions we take when our cyber security has failed.
- ***Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR)*** – monitor a target in support of future operations.
- ***Cyberspace Operational Preparation of the Environment (OPE)*** – modify the cyber terrain to prepare for future operations.
- ***Cyberspace Attack*** – functional denial, or manipulation leading to denial in Cyberspace or other domains.
- ***Defensive Cyberspace Operations Response Actions (DCO-RA)***
- ***Defensive Cyberspace Operations Internal Defensive Measures (DCO-IDM)***

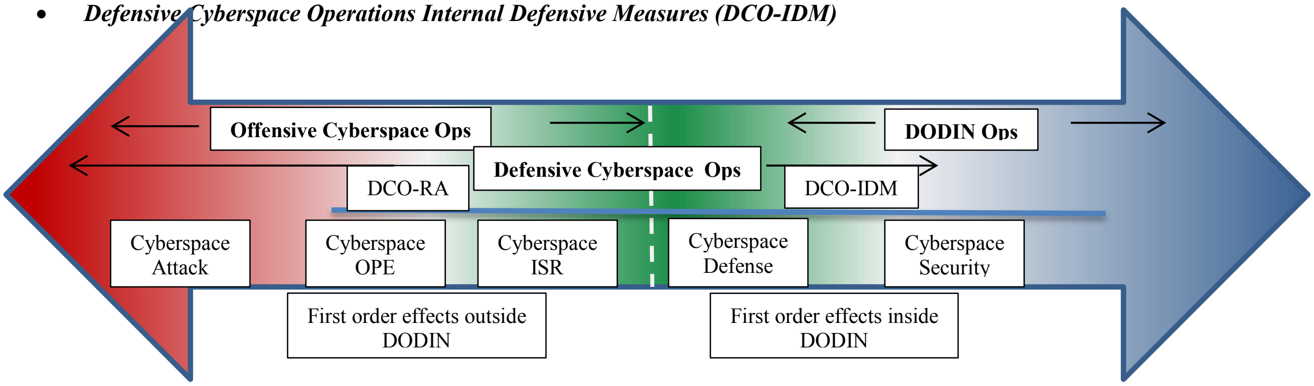


Figure IV-5: Cyberspace Actions

1. DODIN operations (DODIN Ops): Operations to design, build, control, secure, operate, maintain, and sustain DOD networks to create information assurance on the DODIN.[71]

2. Defensive Cyberspace Operations (DCO): Passive and active CO intended to preserve the ability to utilize friendly cyberspace capabilities and protect DOD data, networks, and capabilities and other designated systems.[72]

a) DCO Internal Defensive Measure (DCO-IDM) activities involve assessing the DODIN for advanced internal threats and the responses to those threats. IDM responds to unauthorized alert information and activity occurring in the DODIN.

b) DCO Response Action (DCO-RA) activities occur external to the DODIN to counter those ongoing or imminent threats to the DODIN, DOD cyberspace capabilities, and other systems. RA's deliberate defensive events must be authorized in accordance with standard rules of engagement (ROE) and other rules.[73]

3. Offensive Cyberspace Operations (OCO): Cyberspace operations intended to project power by the application of force in or through cyberspace.[74]

[71] U.S. Joint Chiefs of Staff, *Joint Publication 3-12(R) Cyberspace Operations,* II-3.
[72] U.S. Joint Chiefs of Staff, *Joint Publication 3-12(R) Cyberspace Operations,* II-2.
[73] U.S. Joint Chiefs of Staff, *Joint Publication 3-12(R) Cyberspace Operations*, II-3.
[74] U.S. Joint Chiefs of Staff, *Joint Publication 3-12(R) Cyberspace Operations,* II-2.

The **authorities** for performing defensive and offensive operations are different. For **DODIN Ops and DCO-IDM**, the Joint Force may operate without external coordination. However, **DCO-RA and OCO** require more coordination with other governmental agencies and to prevent the Joint Force from exceeding its authority by infringing on the Department of Homeland Security's or Department of Justice's (DOJ's) authority. Centralized control allows authorities to consider potential second and third order effects.

For additional information on cyberspace related authorities refer to JP 3-12, Cyberspace Operations.

(c) Organization Structure: The current cyberspace command structure begins with the POTUS and the SecDef. Below the SecDef, USSTRATCOM and its sub-unified command, USCYBERCOM, serve as global synchronizers for cyberspace operations. USCYBERCOM has several subordinates, including a Joint Force Headquarters-DODIN to focus on DODIN operations and service component commands (Marine Forces Cyber Command, U.S. Air Force Cyber Command, U.S. Fleet Cyber Command, and U.S. Army Cyber Command). Additionally, the Joint Force is developing four varieties of cyber mission forces (CMF) to conduct cyberspace operations:

<u>1.</u> **The Cyber National Mission Force (CNMF)** is the national element for cyberspace activities. CNMF and its associated teams are focused on overall national strategic cyberspace threats that potentially stem from all AOR.

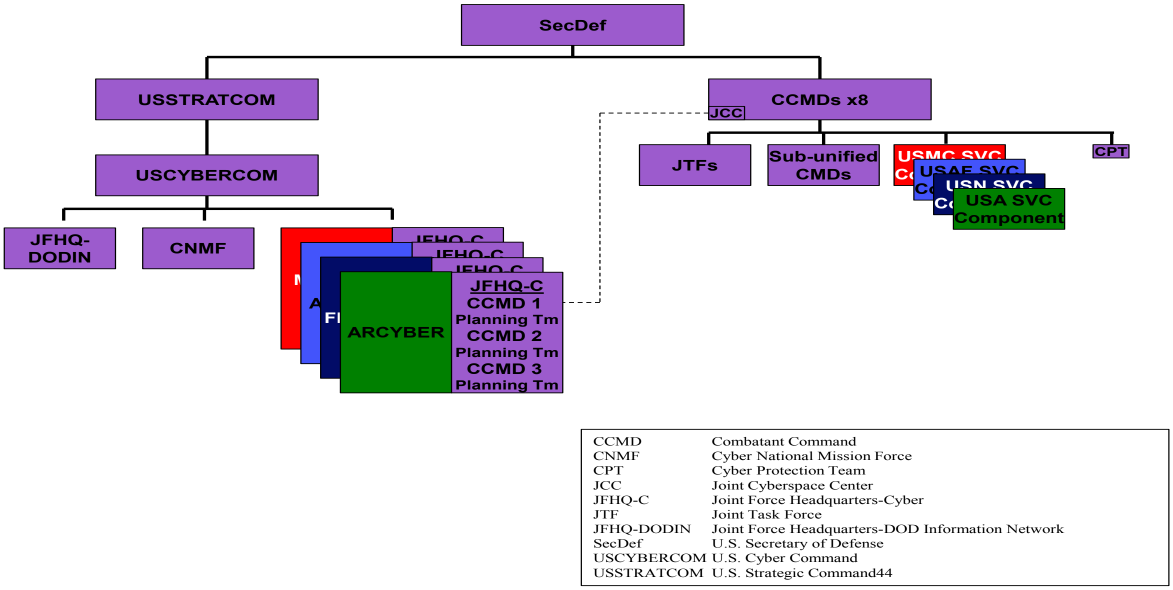
<u>2.</u> **Cyber Combat Mission Forces (CCMF)** are tasked according to regions and responsible for providing offensive cyberspace operations when approved and authorized through the proper authorities.

<u>3.</u> **Cyber Support Teams (CST)** are the unit assigned within the CCMF to provide developers, analysts, programmers, linguists, and engineers in support of offensive operations.

<u>4.</u> **Cyber Protection Teams (CPT)** are assigned across DOD to provide defensive operations across the DODIN and, sometimes, outside the DODIN. This team manages, monitors, and defends the assigned networks and applications within their assigned region while continuously coordinating with the Defense Information Systems Agency (DISA). CPTs are imbedded at all levels of the DODIN to ensure defensive mechanisms are in place and working correctly.

To C2 the different CCMTs, USCYBERCOM dual-hatted its service component commands as **Joint Force Headquarters-Cyber (JFHQ-C)**. In this capacity, those commands are assigned

CCMTs and cooperate with two or three designated CCMDs to plan and conduct cyberspace operations. Internal to each CCMD, a **Joint Cyberspace Center (JCC)** is established to coordinate the cyberspace operations relevant to that CCMD. Currently, there is no standardized JCC structure describing how a JCC is manned. Nor are there standardized operating procedures dictating how a JCC interacts with mission partners. Consequently, CCMDs have taken different approaches to developing their JCC, including differences in how much manpower to assign the JCC and which staff directorate should serve as proponent (J-3 or J-6).



CCMD	Combatant Command
CNMF	Cyber National Mission Force
CPT	Cyber Protection Team
JCC	Joint Cyberspace Center
JFHQ-C	Joint Force Headquarters-Cyber
JTF	Joint Task Force
JFHQ-DODIN	Joint Force Headquarters-DOD Information Network
SecDef	U.S. Secretary of Defense
USCYBERCOM	U.S. Cyber Command
USSTRATCOM	U.S. Strategic Command44

Figure IV-6: Cyberspace C2 Concept

4. Planning Considerations. Joint planners integrating cyberspace operations into a joint planning process should first seek the expertise of:

(a) Cyberspace planners on their joint staff

(b) Their CCMD's JCC

(c) LNOs from USCYBERCOM or USSTRATCOM

(d) The commander of a CPT assigned to their CCMD

(e) Lead planners from the JFHQ-C with planning responsibility for their CCMD
From these experts, gaining insight and understanding of available cyberspace capabilities enables planners to merge these capabilities with the other domains. **Avoid symmetric thinking.** Merely because the adversary attacks through cyberspace, does not restrict the Joint Force to solely cyberspace response options. Cyberspace has a physical layer.

Similar to the space domain, cyberspace capabilities require long approval chains and, sometimes, long development timelines. **Identify potential cyberspace needs early** in the planning process and set cyberspace planners working to secure the necessary permissions.

Tailor **requests for cyberspace operations.** Given cyberspace operations' global nature and potential for cascading effects, authorities rarely grant broad permissions. Planners should craft requirements which are specific (used only in certain situations, limited in duration, and limited networks affected). By requesting a discrete operation, planners increase the likelihood of approval and, potentially, shorten approval time. Planners should coordinate and socialize desired cyber activities with the IA as early as possible in planning.

Conducting cyberspace battle damage assessment (BDA) through cyberspace is difficult. A friendly cyberspace operator may report mission accomplishment. However, unlike physical munitions, there will not be a blast crater to verify results. Planners must use other ways to the measure success of a cyberspace operation. One approach is to layer assessments. For example, if a cyberspace operator reports disarming an adversary through cyberspace, probe the adversary's system with a remotely piloted vehicle before launching a risky major assault.

All cyberspace operations require branch plans to accomplish similar effects. Because OCO are often disapproved and susceptible to failure, planners must understand the intent of those cyberspace operations and develop a branch plan to accomplish that intent through other domains. Similarly, joint staff officers must understand that most of today's operating systems are vulnerable to attack. The Joint Force should prepare to operate with degraded cyberspace capabilities.

Many cyberspace capabilities are highly classified to avoid exposing vulnerabilities. Lack of sufficient security clearances will hinder a planner's ability to integrate cyberspace capabilities. To mitigate this challenge, lead planners should include cyberspace experts in planning team meetings to inform them of the plan's objectives and intent. This enables planners to discreetly integrate classified capabilities while informing only those with the appropriate clearance and need-to-know.

For more information refer to Appendix D.

G. Wrap-Up

In today's dynamic strategic environment the United States faces adversaries capable of integrated attacks from multiple domains. To counter this, Joint Forces must conduct cross-domain operations to engage adversaries where the Joint Force holds advantage and present them with multiple problems.

The planner's guide provides a ready reference for integrating all domains during planning and other staff activities. It identifies key internal and external relationships officers should establish upon joining a joint staff and suggests methods for developing them. Ultimately, the guide will contribute to the achievement of synergy through employment of efficient, effective cross-domain operations.

Intentionally Blank

APPENDIX A
RECOMMENDED PLANNING PRACTICES

The following are "Suggestions for Planners," that may make the job a little easier:

1. If possible, get frequent feedback and guidance from the Joint Force Commander. Get this feedback throughout the planning process and not just during the formal interactions or decision briefings.

2. People are not inclined to read lengthy documents thoroughly. Normally, they will only read what applies to themselves directly. The whole plan may be long. But each section needs to be as brief as possible. When detail and long explanations are required, put them into Annexes and Appendixes. This also means the base plan should be very brief, built on simple task and purpose statements.

3. The role of "Assumptions" in planning is more important than JP 5-0 indicates. They must be few in number, account for gaps in information that cannot be ignored, and have a collection plan to confirm or deny them. A failed assumption realized means a new plan is required.

4. The planning process is more important than the plan. The planning team and collective understanding developed during the planning process are critical to effective adaptation during execution.

5. The planning staff is a team – build it carefully and train it regularly.

6. Leading the planning process is based on peer leadership, that is persuasive not authoritarian.

7. Learn to discern competence from confidence.

8. Remember to take breaks. The planning process tends to run people into the ground.

9. Always take great care to maintain version control of the plan and associated planning documents.

10. Standing Operating Procedures (SOPs) are not helpful unless they are simple, used often, and come with concrete examples.

Intentionally Blank

APPENDIX B
AGENCIES AND PARTNERS

The following provides a quick reference to the agencies and partners that the staff planner may encounter during the planning process.

1. Department of Defense (DOD): The mission of DOD is to provide the military forces needed to deter war and to protect the security of our country. Additionally, the purpose of the Armed Forces is to fight and win the Nation's wars. http://www.defense.gov/

a. Secretary of Defense (SecDef): SecDef is the principal assistant to the President for all DOD matters, with authority, direction, and control over the entire DOD.

b. Chairman of the Joint Chiefs of Staff (CJCS): CJCS is the principal military advisor to the President, the NSC, and SecDef. CJCS functions under the authority, direction, and control of SecDef, transmits communications between SecDef and CCDRs, and oversees activities of CCDRs as directed by SecDef.

c. The Military Departments. The authority vested in the Secretaries of the Military Departments in the performance of their role to organize, train, equip, and provide forces runs from the President through SecDef to the Secretaries. Then, to the degree established by the Secretaries or specified in law, this authority runs through the Service Chiefs to the Service component commanders assigned to the combatant commands and to the commanders of forces not assigned to the combatant commands. This administrative control provides for the preparation of military forces and their administration and support, unless such responsibilities are specifically assigned by SecDef to another DOD component.

The Military Departments are the Departments of the Army, Navy (including the Marine Corps), and Air Force. Each Military Department is separately organized under a civilian Secretary, who supervises the Chief (or Chiefs) of the Service in matters of a Service nature. The Secretaries of the Military Departments exercise authority, direction, and control (through the individual Chiefs of the Services) of their forces not specifically assigned to CCDRs. The Military Departments are responsible for training, organizing, providing, and equipping forces for assignment to combatant commands.

d. Combatant Commanders (CCDRs): CCDRs exercise combatant command (command authority) over assigned forces and are directly responsible to SecDef for the performance of assigned missions and the preparedness of their commands to perform assigned missions. Combatant commands typically have geographic or functional responsibilities.

e. Defense Information Systems Agency (DISA): The mission requires that DISA remains purposeful in planning, acquisition, operations, and execution. http://www.disa.mil/ As the provider for defensive cyberspace and IT combat support for the DOD, DISA will:

(1) Focus on our global infrastructure of telecommunications and services delivery — comprised of a hybrid cyberspace ecosystem of mobile, collaboration, internal clouds, and commercial clouds.

(2) Synchronize command and control (C2) and senior leadership support to effectively streamline decision making within all echelons of National and DOD leadership.
(3) Enable warfighter capabilities from a sovereign cyberspace domain, focused on speed, agility, and access.
(4) Reduce costs by eliminating duplication in production and operations.

f. U.S. Air Force Intelligence, Surveillance, and Reconnaissance (USAF ISR): USAF ISR Enterprise is America's leading provider of finished intelligence derived from airborne, space, and cyberspace sensors. The USAF ISR Enterprise delivers decision advantage in order to enable commanders to achieve kinetic and non-kinetic effects on targets anywhere on the globe in support of national, strategic, operational, and tactical requirements. The AF/A2 is the USAF's Senior Intelligence Officer and is responsible for functional management of all Air Force global integrated ISR capabilities, including oversight of planning, programming, and budgeting, developing and implementing the Air Force policies and guidance for managing Air Force global integrated ISR activities. www.af.mil

g. Intelligence and Security Command (INSCOM): The Army's principal intelligence staff officer and functional manager for intelligence is the Assistant Chief of Staff for Intelligence, also known as the Army G-2. Within the IC, the Army's Intelligence and Security Command (INSCOM), headquartered at Ft. Belvoir, Virginia, represent the Army. INSCOM provides all-source intelligence to Army Commands and other IC agencies at all levels. www.army.mil and www.inscom.army.mil

h. Marine Corps Intelligence Activity: The Marine Corps' intelligence department conducts intelligence, CI, terrorism, and cryptologic activities. The Marine Corps' Director of Intelligence is its principal intelligence staff officer. The Marine Corps Intelligence Activity in Quantico, Virginia is the service production center. www.usmc.mil

i. Office of Naval Intelligence (ONI): ONI is the leading provider of maritime intelligence to the U.S. Navy and joint warfighting forces, as well national decision makers and other consumers in the Intelligence Community. Established in 1882, ONI **specializes in the** analysis, production and dissemination of vital, timely and accurate scientific, technical, geopolitical and military intelligence information to key consumers worldwide. While ONI is the largest Naval Intelligence organization with the largest concentration of Naval Intelligence civilians, most of Naval Intelligence is comprised of active duty military personnel serving throughout the world. www.navy.mil

j. National Geospatial-Intelligence Agency (NGA): The National Geospatial Agency (NGA) is the manager for all imagery intelligence activities, both classified and unclassified, within the government including the Department of Defense. The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial Intelligence (GEOINT) consists of imagery, imagery intelligence, and geospatial information. GEOINT supports the multidirectional flow and integration of geospatially referenced data from all sources to achieve shared situational understanding of the operational environment, near real-time tracking, and collaboration between forces. The GEOINT cell in a J-2 interfaces directly with the user to define user requirements. Then the cell interfaces with the National System for Geospatial Intelligence to obtain and provide the best quality GEOINT product possible to support planners and warfighters. www.nga.mil

2. Department of State (DOS):

The Department's mission is to shape and sustain a peaceful, prosperous, just, and democratic world and foster conditions for stability and progress for the benefit of the American people and people everywhere. This mission is shared with the USAID, ensuring we have a common path forward in partnership as we invest in the shared security and prosperity that will ultimately better prepare us for the challenges of tomorrow. DOS manages America’s relationships with foreign governments, international organizations, and the people of other countries. The management of all of these relationships is called diplomacy. DOS diplomats carry out the President’s foreign policy and help build a freer, prosperous, and secure world. http://www.state.gov/s/d/rm/index.htm#mission DOS is a vital part of the U.S. foreign policy because it:

- Represents the United States overseas and conveys US policies to foreign governments and international organizations through American embassies and consulates in foreign countries and diplomatic missions;
- Negotiates and concludes agreements and treaties on issues ranging from trade to nuclear weapons;
- Coordinates and supports international activities of other US agencies, hosts official visits, and performs other diplomatic missions;
- Leads interagency coordination and manages the allocation of resources for foreign relations; and
- Promotes mutual understanding between the people of the United States and the people of other countries around the world.

a. United States Agency for International Development (USAID): The USAID is an independent federal agency that receives overall foreign policy guidance from the Secretary of State. It is the principal US agency to extend assistance to countries recovering from disaster, trying to escape poverty, and engaging in democratic reforms. USAID supports long-term and equitable economic growth and advances US foreign policy objectives by supporting economic growth, agriculture, and trade; global health; and democracy, conflict prevention, and humanitarian assistance. USAID works in agriculture, democracy and governance, economic growth, the environment, education, health, global partnerships, and humanitarian assistance in more than 100 countries to provide a better future for all. http://www.usaid.gov

b. Bureau of Intelligence and Research (INR): INR provides the Secretary of State with timely, objective analysis of global developments as well as real-time insights from all-source intelligence. It serves as the focal point within the Department of State for all policy issues and activities involving the Intelligence Community (IC). The INR Assistant Secretary reports directly to the Secretary of State and serves as the Secretary's principal adviser on all intelligence matters. INR's expert, independent foreign affairs analysts draw on all-source intelligence, diplomatic reporting, INR's public opinion polling, and interaction with U.S. and foreign scholars. Their strong regional and functional backgrounds allow them to respond rapidly to changing policy priorities and to provide early warning and in-depth analysis of events and trends that affect U.S. foreign policy and national security interests. www.state.gov

3. Department of Justice (DOJ):
The DOJ, represents the citizens of the United States in enforcing the law in the public interest and plays a key role in providing protection against criminal activity.
http://www.justice.gov/

a. Federal Bureau of Investigation (FBI): The FBI's mission is to uphold the law through the investigation of violations of federal criminal law; to protect the United States from foreign intelligence and terrorist activities; to provide leadership and law enforcement assistance to federal, state, local, and international agencies; and to perform these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution of the United States.

b. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF): The ATF is a principal LEA within the DOJ dedicated to preventing terrorism, reducing violent crime, and protecting our Nation. The men and women of ATF perform the dual responsibilities of enforcing federal criminal laws and regulating the firearms and explosives industries. ATF is committed to working directly, and through partnerships, to investigate and reduce crime involving firearms and explosives, acts of arson, and illegal trafficking of alcohol and tobacco products.

c. Drug Enforcement Administration (DEA): The DEA is the primary narcotics enforcement agency for the USG. The mission of the DEA is to enforce the controlled substances laws and regulations of the United States and bring to the criminal and civil justice system of the United States, or any other competent jurisdiction, those organizations and principal members of organizations, involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States; and to recommend and support no enforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets.

DEA's Office of National Security Intelligence (ONSI) became a member of the IC in 2006. ONSI facilitates full and appropriate intelligence coordination and information sharing with other members of the U.S. Intelligence Community and homeland security elements. Its goal is to enhance the United States' efforts to reduce the supply of drugs, protect national security, and combat global terrorism. DEA has 21 field divisions in the U.S. and more than 80 offices in more than 60 countries worldwide. www.dea.gov

d. International Criminal Police Organization, United States National Central Bureau (INTERPOL-USNCB): INTERPOL-USNCB serves as the United States' representative to the

INTERPOL. The INTERPOL-USNCB is the central POC for all INTERPOL matters in the United States, including secure communications with police authorities in INTERPOL's 187 member countries and access to INTERPOL's various databases containing information on wanted persons, terrorists, missing persons, stolen and lost passports and travel documents, stolen vehicles, and other law enforcement information. On a daily basis, the INTERPOL-USNCB coordinates and transmits requests for criminal investigative and humanitarian assistance between United States federal, state, and local law enforcement authorities and their foreign counterparts. http://www.interpol.int/

4. Department of Homeland Security (DHS):

The Department of Homeland Security has a vital mission: to secure the nation from the many threats the nation faces. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cyberspace security analyst to chemical facility inspector.

DHS/FEMA will often be the primary federal agency involved in federal response to emergencies which may involve cross-domain response involving active and reserve component non-federalized forces. DHS' Office of Intelligence and Analysis is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States. DHS Intelligence focuses on four strategic areas:

- Promote understanding of threats through intelligence analysis
- Collect information and intelligence pertinent to homeland security
- Share information necessary for action
- Manage intelligence for the homeland security enterprise.

The Under Secretary for Information and Analysis (I&A) also serves as DHS' chief intelligence officer and is responsible to both the secretary of Homeland Security and the director of National Intelligence. http://www.dhs.gov/

a. Customs and Border Protection (CBP): CBP protects US borders from terrorism, human and drug smuggling, illegal migration, and agricultural pests while simultaneously facilitating the flow of legitimate travel and trade. CBP's priority mission is to prevent terrorists and terrorists' weapons, including WMD, from entering the United States. http://www.cbp.gov

b. US Immigration and Customs Enforcement (ICE): ICE's primary mission is to protect national security, public safety, and the integrity of the U.S. borders through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. ICE has approximately 19,000 employees in over 400 offices, including 63 Attaché offices in 44 countries around the world. The agency's law enforcement authorities encompass more than 400 US federal statutes that ICE is responsible for enforcing in its commitment to ensuring national security and public safety. http://www.ice.gov

c. Transportation Security Administration (TSA): The TSA protects the Nation's transportation systems to ensure freedom of movement for people and commerce. http://www.tsa.gov

d. US Citizenship and Immigration Services (USCIS): USCIS is the government agency that oversees lawful immigration to the United States. Refugee status or asylum may be granted to people who have been persecuted or fear they will be persecuted on account of race, religion, nationality, and/or membership in a particular social group or political opinion. US Citizenship and Immigration Services (USCIS) officers conduct interviews overseas, so the military could be interacting with them in some joint operations. For example, officers were interviewing Iraqi nationals, many of whom had associations with the USG and the US military in particular, for refugee resettlement to the United States. In some cases a USCIS officer may believe a refugee has information that the military should hear, or USCIS may request information from the military that might support an applicant's refugee claim or identify a ground of ineligibility. USCIS asylum officers posted to one of eight domestic asylum offices interview aliens physically present in the United Sates who are applying for asylum status. http://www.uscis.gov

e. U.S. Coast Guard (USCG): U.S. Coast Guard (USCG): The USCG is the Nation's primary maritime operating agency with resources organized, trained, and equipped to be "multi-mission capable." while carrying out its Homeland Security or Homeland Defense mission. The USCG is unique as it is a branch of the Armed Forces at all times and an agency within DHS. The USCG may also operate under the Department of the Navy during time of war or when directed by the President. The USCG protects the public, the environment, and US economic interests—in the Nation's ports and waterways, along the coast, on international waters, or in any maritime region as required to support national security. Its broad responsibilities include protecting citizens from the sea (maritime safety), protecting America from threats delivered by the sea (maritime security) including terrorists and terrorist weapons (i.e., WMD), and protecting the sea itself (maritime stewardship). http://www.uscg.mil

f. Federal Emergency Management Agency (FEMA): The primary mission of FEMA is to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters, by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation. http://www.fema.gov

g. U.S. Secret Service (USSS): The USSS safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy and protects national leaders, visiting heads of state and government, designated sites, and national special security events. When an event is designated by the Secretary of Homeland Security as a national special security event, the USSS assumes its mandated role as the lead agency for the design and implementation of the operational security plan. The USSS has developed a core strategy to carry out its security operations, which relies heavily on its established partnerships with law enforcement and public safety officials at the local, state, and federal levels. The goal of the cooperating agencies is to provide a safe and secure environment for USSS protectees, other dignitaries, the event participants, and the general public. There is a tremendous amount of advance planning and coordination in preparation for these events, particularly in the areas of venue and motorcade route security, communications, credentialing, and training. http://www.secretservice.gov

5. Office of the Director of National Intelligence (ODNI)

The Office of the Director of National Intelligence (ODNI) was established by a 2004 act of Congress to lead the integration of the U.S. Intelligence Community (IC). The Director of National Intelligence (DNI) serves as the head of the IC. The DNI is responsible for the performance of the nation's intelligence capability, even though it is dispersed across six governmental departments. The DNI is appointed by the President to serve as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security. The staff elements of ODNI include the National Counterterrorism Center, the Office of the National Counterintelligence (CI) Executive, and the National Counter-proliferation Center, each responsible for IC-wide coordination and support, as well as offices that set policy for the IC. The ODNI's focus is to promote its vision of a more integrated and collaborative IC. www.dni.gov

a. **Defense Intelligence Agency (DIA)**: DIA is an intelligence combat support agency. The Director, DIA reports to the SECDEF through the Chairman of the Joint Chiefs of Staff (CJCS). DIA's mission is to satisfy the military and military-related intelligence requirements of the SECDEF, the CJCS, and the DNI, and provide the military intelligence contribution to the National Foreign Intelligence Program (NFIP) and CIA. DIA serves as the DOD lead for coordinating intelligence support to meet combatant command requirements. DIA also leads efforts to align ISR activities, and links and synchronizes national, defense, and military intelligence. DIA also provides analytical and operational support in areas such as CI, counterterrorism, counterdrug operations, computer network operations, personnel recovery, proliferation of Weapons of Mass Destruction (WMD), United Nations peacekeeping and coalition support, MASINT, Noncombatant Evacuation Operation (NEO) efforts, Indications and Warning (I&W), targeting, Battle Damage Assessment (BDA), current intelligence, collection management, intelligence architecture and systems support, and document and media exploitation capability. The Director, DIA is dual-hatted as the Director, Defense Intelligence Operations Coordination Center and also serves as the Commander, Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance (JFCC-ISR) under USSTRATCOM. www.dia.mil

b. **Central Intelligence Agency (CIA):** CIA's primary areas of expertise are in HUMINT collection, all-source analysis, and the production of political and economic intelligence. The Director, CIA, also serves as the national Human Intelligence (HUMINT) manager and the National Clandestine Service Director. The CIA has three Deputy Directors: Deputy Director for Intelligence, Deputy Director for Science and Technology (S&T), and Deputy Director for Support. CIA is the largest producer of all-source national security intelligence to senior U.S. policymakers and provides extensive political and economic intelligence to DOD senior decision makers. CIA also oversees the Open Source Intelligence Center. www.cia.gov

c. **National Reconnaissance Office (NRO):** NRO designs, builds and operates the nation's reconnaissance satellites. NRO products, provided to an expanding list of customers like the CIA and the DOD, can warn of potential trouble spots around the world, help plan military operations, and monitor the environment. As part of the Intelligence Community, the NRO plays a primary role in achieving information superiority for the U.S. Government and Armed Forces. A DOD agency, the NRO is staffed by DOD and CIA personnel. It is funded through the

National Reconnaissance Program, part of the National Foreign Intelligence Program. www.nro.mil

d. National Security Agency (NSA): NSA is an intelligence combat support agency under the SECDEF and is also a member of the IC under the DNI. The Director, NSA, exercises operational control over the United States Cryptologic System (USCS). The Director is the principal SIGINT advisor to the Secretary of Defense (SecDef), the DNI, and the JCS, and is designated as the national manager responsible for securing the government's national security telecommunications and information systems. USCS is the term that describes both the SIGINT and information assurance activities of the U. S. Government. The Central Security Service (CSS) is comprised of the Service cryptologic elements of the military services. NSA/CSS is a unified organization structured to provide for the Signals Intelligence (SIGINT) mission of the United States and to ensure the protection of national security systems for all departments and agencies of the U.S. Government. The Director, NSA is also Commander, United States Cyber Command, a sub unified command subordinate to USSTRATCOM. NSA provides direct support to the combatant command Joint Intelligence Operations Centers (JIOCs) through the CSS. www.nsa.gov

6. Department of Energy (DOE): DOE's Office of Intelligence and Counterintelligence (CI) are responsible for the intelligence and CI activities throughout the DOE complex, including nearly 30 intelligence and CI offices nationwide. The mission is to protect, enable, and represent the vast scientific brain trust resident in DOE's laboratories and plants. The office protects vital national security information and technologies, representing intellectual property of incalculable value, and provides unmatched scientific and technical expertise to the U.S. government to respond to foreign intelligence, terrorist and cyber threats, to solve the hardest problems associated with U.S. energy security, and to address a wide range of other national security issues. www.energy.gov

7. Department of the Treasury (DOT): The Department of the Treasury (TREAS) strengthens national security by managing the USG's finances effectively, promoting economic growth and stability, and ensuring the safety, soundness, and security of the U.S. and international financial systems. TREAS also performs a critical and far-reaching role in enhancing national security by implementing economic sanctions against foreign threats to the United States, identifying and targeting the financial support networks of national security threats and improving the safeguards of our financial system. http://www.ustreas.gov

a. Office of Intelligence and Analysis (OIA): OIA, a sub-directorate of the Department of Treasury (DOT), was established by the Intelligence Authorization Act for fiscal 2004. OIA is responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign CI information related to the operation and responsibilities of the Department of the Treasury. OIA is a component of the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence (TFI). TFI marshals the Department's intelligence and enforcement functions with the twin aims of safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, weapons of mass destruction proliferators, money launderers, drug kingpins, and other national security threats. www.treasury.gov

8. Department of Commerce (DOE): The mission of the Department of Commerce (DOC) is to promote job creation, economic growth, sustainable development, and improved living standards for all Americans by working in partnership with businesses, universities, communities, and workers. DOC is a participant in the whole-of-government approach to Reconstruction & Stabilization operations led by the Department of State Office of the Coordinator for Reconstruction and Stabilization. DOC provides ongoing technical assistance in many countries and can develop coordinated Department of Defense Civil-Military Operations and DOC projects for given countries or regions. DOC has demonstrated ability to support post-conflict operations through its actions in Iraq and Afghanistan. https://www.commerce.gov

9. Other Pertinent Agencies and Partners:

a. North Atlantic Treaty Organization (NATO): NATO is an alliance of 28 countries from North America and Europe committed to fulfilling the goals of the North Atlantic Treaty. In accordance with the Treaty, the fundamental role of NATO is to safeguard the freedom and security of its member countries by political and military means. It provides a forum in which countries from North America and Europe can consult together on security issues of common concern and take joint action in addressing them. The Alliance is committed to defending its member states against aggression or the threat of aggression and to the principle that an attack against one or several members would be considered as an attack against all.

For more information, refer to Allied Joint Publication (AJP)-01(C), Allied Joint Doctrine, and Annex A, "North Atlantic Treaty Organization," to Appendix B, "Intergovernmental Organizations."

b. Nongovernmental Organizations (NGO): Working alone, alongside the US military, with other US agencies, or with multinational partners, NGOs are assisting in many of the world's trouble spots where humanitarian or other assistance is needed. NGOs may range in size and experience from those with multimillion dollar budgets and decades of global experience in developmental and humanitarian relief to newly created small organizations dedicated to a particular emergency or disaster. The capability, equipment and other resources, and expertise vary greatly from one NGO to another. NGOs seek to address humanitarian needs first and are often unwilling to subordinate their objectives to achievement of an end state, which they had no part in determining. Many NGOs view their relationship with the military under the United Nations Office for Coordination of Human Affairs (UNOCHA) *Guidelines on the Use of Military and Civil Defense Assets in Disaster Relief,* commonly referred to as the "*Oslo Guidelines,*" that emphasize the principle of "humanitarian space" (humanitarianism, neutrality, and impartiality) as defined in the "*Oslo Guidelines.*"

The Secretary of Defense (SecDef) may determine that it is in the national interest to task US military forces with missions that bring them into close contact with (if not support of) NGOs. In such circumstances, it is mutually beneficial to closely coordinate the activities of all participants. A climate of cooperation between NGOs, and military forces should be the primary goal. The secondary goal would be establish as good a rapport as possible with NGOs maintaining neutrality. The tertiary goal (although often critical) is to monitor openly hostile NGOs and, when applicable, develop mitigation strategies. The *Guidelines for Relations between US Armed Forces and Non-Governmental Humanitarian Organizations in Hostile or Potentially Hostile Environments* agreed by the DOD, and the United States Institute of Peace should facilitate interaction between the Armed Forces of the United States and NGOs.

c. Interagency Relationships: DOD has a major role in the interagency arena. It interacts with almost every government agency and department and is involved in interagency coordination at the strategic, operational, and tactical levels. SecDef is a member of the National Security Council (NSC), Chairman of the Joint Chiefs of Staff (CJCS), and serves as an advisor to the NSC. DOD is significantly involved in the entire NSC interagency process, with representatives (i.e., Office of the Under Secretary of Defense (Policy)(OUSD[P]) and joint staff (JS)) assigned to all NSC subgroups (i.e., National Security Council/Principals Committee (NSC/PC) and Deputies Committee of the National Security Council (NSC/DC)) and most National Security Council/interagency policy committees (NSC/IPCs).

For further information see Joint Publication 2-01 *Joint and National Intelligence Support to Military Operations*, 5 January 2012 and Joint Publication 3-08 *Interorganizational Coordination During Joint Operations*, 24 June 2011.

Intentionally Blank

APPENDIX C
BIBLIOGRAPHY

Ballard, William H. Maj, USAF and Col Mark C. Harysch, USAF (Retired). "Operationalizing Air-Sea Battle in the Pacific." *Air & Space Power Journal January-February 2015.*

Brandes, Sean LCDR, USN. "The Newest Warfighting Domain: Cyberspace." *Synesis: A Journal of Science, Technology, Ethics, and Policy Volume 4, 2013.*

Dempsey, Martin GEN, USA Chairman of the Joint Chiefs of Staff. *Release of the Joint Operational Access Concept.* DOD Live. January 12, 2012. http://www.dodlive.mil/index.php/2012/01/release-of-the-joint-operational-access-concept-joac/

Eassa, Charles N. COL, USA. "Research Paper: Enabling Combatant Commander's Ability to Conduct Operations in the Cyber Domain." Research Paper, U.S. Army War College, 2012.

Evans, Michael and Ryan, Alan (Editors). *From Breitenfeld to Baghdad: Perspectives on Combined Arms Warfare, Land Warfare Studies Centre.* Duntroon, Australia: The Land Warfare Studies Centre, 2003.

Fastabend, David MG USA (Retired). *Domain Power.* Unpublished manuscript, date unknown.

Fastabend, David MG USA (Retired). *Mechanism of Joint Synergy.* Unpublished manuscript, last modified December 12, 2012.

Freier, Nathan. "Challenges to American Access: The Joint Operational Access Concept and Future Military Risk." Center for Strategic and International Studies csis.org. Published January 5, 2012. http://csis.org/publication/challenges-american-access-joint-operational-access-concept-and-future-military-risk

Gallemore, John B. Maj, USAF. *Cross-Domain Synergy: Warfare in the 21st Century.* Quantico, VA: U.S. Marine Corps Command and General Staff College, 2013.

GlobalSecurity.org. July 2013. "Report on US Military Power 2012." *GlobalSecurity.org.* July 2013. "Report on US Military Power 2012." http://www.globalsecurity.org/military/library/report/2013/us-military-power2012_cscpa04.htmp://www.globalsecurity.org/military/library/report/2013/us-military-power2012_cscpa04.htm

Gordon IV, John and John Matsumura. *The Army's Role in Overcoming Anti-Access and Area Denial Challenges.* Santa Monica, CA: RAND Corporation, 2013.Gunzinger, Mark with Chris Dougherty. *Outside-In: Operating from Range to Defeat Iran's Anti-Access and Area-Denial Threats.* Washington, DC: Center for Strategic and Budgetary Assessments, 2011.

Hollis, David. "Cyberwar Case Study: Georgia 2008." Small Wars Journal. Modified January 2011/Accessed November 2015. http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Mahan, Alfred Thayer. *The Influence of Sea Power Upon History: 1660-1783.* Gretna, LA: Pelican Publishing, 2003 (First published in 1890).

McCarthy, Christopher J Maj, USAF. "Chinese Anti-Access/Area Denial: The Evolution of Warfare in the Western Pacific." Paper submitted in partial satisfaction of the requirements of the Department of Joint Operations, U.S. Naval War College, 2010.

National Museum of the U.S. Air Force. "The Doolittle Raiders – April 18, 1942." Accessed June 1, 2015. http://www.nationalmuseum.af.mil/shared/media/document/AFD-150417-021.pdf

Odom, William O. and Christopher D. Hayes. "Cross-Domain Synergy: Advancing Jointness." *Joint Forces Quarterly Number 73 2nd Quarter 2014.*

Quintana, Elizabeth, Joanne Mackowski, and Adam Smith. "Cross-Domain Operations and Interoperability." *Royal United Services Institute Occasional Paper July 2012.*

Tangredi, Sam J. *Anti-Access Warfare: Countering A2/AD Strategies.* Annapolis, MD: U.S. Naval Institute Press, 2013.

U.S. Department of Defense. *Air-Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges.* Washington, DC: Air-Sea Battle Office, 2013.

——. *Capstone Concept for Joint Operations: Joint Force 2020.* Washington, DC: U.S. Department of Defense, 2012.

——. *Joint Operational Access Concept Version 1.0.* Washington, DC: U.S. Department of Defense, 2012.

U.S. Joint Chiefs of Staff. *CJCS Wargame Iron Crucible 2014.* Unpublished manuscript dated May 2014.

Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms. Washington, DC: U.S. Joint Chiefs of Staff, 2015.

——. *Joint Publication 3-0 Operations.* Washington, DC: U.S. Joint Chiefs of Staff, 2011.

——. *Joint Publication 3-01 Countering Air and Missile Threats.* Washington, DC: U.S. Joint Chiefs of Staff, 2012.

——. *Joint Publication 3-13 Information Operations.* Washington, DC: U.S. Joint Chiefs of Staff, 2014.

——. *Joint Publication 3-15.1 Counter-Improvised Explosive Device Operations.* Washington, DC: U.S. Joint Chiefs of Staff, 2012.

——. *Joint Publication 3-31 Command and Control for Joint Land Operations.* Washington, DC: U.S. Joint Chiefs of Staff, 2014.

——. *Joint Publication 3-32 Command and Control for Joint Maritime Operations.* Washington, DC: U.S. Joint Chiefs of Staff, 2013.

——. *Joint Publication 3-33 Joint Task Force Headquarters.* Washington, DC: U.S. Joint Chiefs of Staff, 2012.

——. *Joint Publication 5-0 Joint Operation Planning.* Washington, DC: U.S. Joint Chiefs of Staff, 2011.

Intentionally Blank

APPENDIX D
REFERENCES FOR FURTHER PROFESSIONAL EDUCATION

This appendix is intended to offer greater professional education in each of the individual domains as well as planning in general. Each reference is briefly described along with its bibliographical information.

1. United States Laws

a. Title 10, USC: Gives the responsibility to the services to man, train, and equip forces to support the mission and operation of the DOD and CCMD. http://www.gpo.gov/

b. Titles 22, USC: Outlines the role of foreign relations and interaction with the U.S. http://www.gpo.gov/

c. Title 32, USC: Outlines the role of the National Guard in defense of the U.S. http://www.gpo.gov/

d. Title 50, USC: Governs how the United States conducts wars and intelligence operations in defense of the United States to include cyberspace. http://www.gpo.gov/

2. Strategic Guidance and Policy.

a. Sustaining U.S. Global Leadership: Priorities for the 21st Century. Washington, D.C: President of the United States, January 2012.

Description: Sustaining U.S. Global Leadership: Priorities for the 21st Century is the President of the United States' guidance to the Department of Defense for engagement of forces for the future. It is based off the 2011 Congressional Budget and potential adversaries.

b. The National Military Strategy of the United States of America 2015. Washington, DC: U.S Joint Chiefs of Staff, June 2015.

Description: The National Military Strategy describes how the United States will employ its military forces to protect and advance its national interests. The 2015 NMS continues the call for greater agility, innovation, and integration. The NMS discusses projecting power across all domains to stop aggression and win our Nation's wars by decisively defeating adversaries and the need for cross-domain synergy.

3. Chairman of the Joint Chiefs of Staff Publications.

a. Chairman of the Joint Chiefs of Staff Manual 3130.01A: Campaign Planning Procedures and Responsibilities. Washington, DC: Chairman of the Joint Chiefs of Staff, Joint Staff, J-5, November 2014. http://www.dtic.mil/cjcs_directives/cdata/unlimit/m313001.pdf

Description: Establishes procedures and responsibilities for the preparation of strategies and campaign plans. A campaign plan operationalizes the CCDR's strategy by organizing and aligning all operations, activities, and investments with resources to achieve the CCMD's objectives and complement related USG efforts in the theater, functional area, or domain over an approximately five year time frame.

b. U.S. Department of Defense. Joint Operational Access Concept (JOAC) Version 1.0. Washington, DC: United States Department of Defense, January 17, 2012. http://www.defense.gov/pubs/pdfs/JOAC_Jan%202012_Signed.pdf

Description: The JOAC describes how joint forces will operate in response to emerging anti-access and area denial security challenges. The JOAC describes how future joint forces will achieve operational access in the face of such strategies. The JOAC's central tenet to achieve access is cross-domain synergy.

c. U.S. Joint Chiefs of Staff. Operating Procedures for Joint Operation Planning and Execution System (JOPES) – Information Systems Governance. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.05. Washington, DC: U.S. Joint Chiefs of Staff, December 15, 2011 (current as of November 18, 2014). http://www.dtic.mil/cjcs_directives/cdata/unlimit/m312205.pdf

Description: The current JOPES IT is a solution developed by the Defense Information Systems Agency (DISA), whose goal was to solve the data synchronization issues inherent in the JOPES Classic architecture and modernize the database architecture for JOPES. The Block IV JOPES v4.0 release provides a more robust infrastructure and a greatly enhances the method of synchronization for the Joint Planning and Execution Community (JPEC).

d. U.S. Joint Chiefs of Staff. Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms. Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 as amended March 15, 2015.

e. Joint Publication 2-0 Joint Intelligence. Washington, DC: U.S. Joint Chiefs of Staff: October 22, 2013. Pages IV-13 (Air, Land, and Maritime)

f. Joint Publication 2-01 Joint and National Intelligence Support to Military Operations. Washington, DC: U.S. Joint Chiefs of Staff, January 5, 2012.

g. Joint Publication 2-01.3 Intelligence Preparation of the Operational Environment (JIPOE). Washington, DC: U.S. Joint Chiefs of Staff: May 21, 2014. Pages IV-14 (Air, Land, and Maritime)

h. Joint Publication 2-03 Geospatial Intelligence in Joint Operations. Washington, DC: U.S. Joint Chiefs of Staff, October 31, 2013.

i. Joint Publication 3-0 Operations. Washington, DC: U.S. Joint Chiefs of Staff: August 11, 2011. Pages III-2, III-3, III-5, III-6, VI-26, and (Joint C2)

j. Joint Publication 3-01 Countering Air and Missile Threats. Washington, DC: U.S. Joint Chiefs of Staff: March 23, 2012.

k. Joint Publication 3-02 Amphibious Operations. Washington, DC: U.S. Joint Chiefs of Staff: July 18, 2014.

l. Joint Publication 3-09 Joint Fire Support. Washington, DC: U.S. Joint Chiefs of Staff: December 12, 2014.

m. Joint Publication 3-10 Joint Security Operations in Theater. Washington, DC: U.S. Joint Chiefs of Staff, November 13, 2014. Pages I-1, I-2, I-3, I-5, and I-6 (Protection)

n. Joint Publication 3-12 *(R)* Cyberspace Operations. Washington, DC: U.S. Joint Chiefs of Staff, February 5, 2013. Pages vii, vii, ix, x, ix, xii (Air, Land, Maritime, Space, Cyberspace, Joint C2, Fires, Protection), pages; II-7, II-9, II-11, (Air, Land, Maritime, Joint C2, Fires, Protection, Sustainment)

o. Joint Publication 3-13 Information Operations. Washington, DC: U.S. Joint Chiefs of Staff: November 27, 2012 with Change 1 November 20, 2014.

p. Joint Publication 3-14 Space Operations. Washington, DC: U.S. Joint Chiefs of Staff, May 29, 2013.

q. Joint Publication 3-15.1 Counter-Improvised Explosive Device Operations. Washington, DC: U.S. Joint Chiefs of Staff, January 9, 2012.

r. Joint Publication 3-30 Command and Control of Joint Air Operations. Washington, DC: U.S. Joint Chiefs of Staff, February 10, 2014.

s. Joint Publication 3-31 Command and Control for Joint Land Operations. Washington, DC: U.S. Joint Chiefs of Staff, February 24, 2014. Page: ix, II-19, II-20 (Land- B2C2WG)

t. Joint Publication 3-32 Command and Control for Joint Maritime Operations. Washington, DC: U.S. Joint Chiefs of Staff, August 7, 2013.

u. Joint Publication 3-33 Joint Task Force Headquarters. Washington, DC: U.S. Joint Chiefs of Staff, July 30, 2012. Page III-2, II-18 (Land), II-10 – II-18 (B2C2WG, Liaison, Support Elements, Augmentees)

v. Joint Publication 3-60 Joint Targeting. Washington, DC: U.S. Joint Chiefs of Staff, 2013.

w. Joint Publication 4-0 Joint Logistics. Washington, DC: U.S. Joint Chiefs of Staff, October 16, 2013. Pages II-15, IV-16, and VII-2, IX-11 (Air, Land, and Maritime)

x. Joint Publication 5-0 Joint Operation Planning. Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011. Pages x-ii, xix, xxv, III-3, III-8, IV-3, IV-6, (Air, Land, Maritime, B2C2WG, and Battle Rhythm)

y. Joint Publication 6-0 Joint Communications. Washington, DC: U.S. Joint Chiefs of Staff, Aug 11, 2011.

z. Joint Publication 6-01 Joint Electromagnetic Spectrum Management Operations. Washington, DC: U.S. Joint Chiefs of Staff, March 20, 2012.

4. Other References.

Planning

a. Santacroce, Mike. *Joint Strategic & Operational Planning: Planning for Planners.* Lakeland, FL: The Lightning Press, 2014.

Description: Volume 1 of the Joint/Interagency Smartbook series. The book was developed to assist planners at all levels in understanding how to plan utilizing the Joint Operational Planning Process. *Planning for Planners* has been used since 2007 by war colleges, joint staffs, Services, and combatant commands as a step-by-step guide to understanding the complex world of global planning and force management. The goal of the book is to help develop flexible planners who can cope with the inevitable changes that occur during the planning process.

b. *Ballistic Missile Defense Operational Planning Solution Guide*. 2012. Suffolk, VA: Joint Staff, J-7 Future Joint Force Development, 2012. https://portal.js.mil/sites/J7/DC/Documents/(U)-BMD-C2I-BMDOperationalPlanningSolutionGuide-2012.pdf

Description: The purpose of the BMD Operational Planning Solution Guide is to provide planners new approaches to solve gaps and shortfalls for Combatant Command and Component BMD planners. The Guide will help better integrate air and missile defense planning across joint air and maritime operations centers within and across geographic combatant commands.

c. *Theater Campaign Planning: Planners' Handbook.* Washington, DC: Office of the Under Secretary of Defense for Policy, February 2012. https://portal.js.mil/sites/J4/DC/Documents/Planners_Handbook_Master__Final Draft 02-22-12.pdf

Description: This handbook is intended to provide combatant command planners with a conceptual approach to developing theater campaign plans (TCPs). It is based on insights from a variety of sources over the last several years. This booklet is designed to assist planners by presenting a broad approach to TCPs and country-level planning that considers ongoing security cooperation efforts, current operations, the Phase 0 component of contingency plans, and resourcing constraints as part of the combatant commander's implementation of his strategic approach to the area of responsibility.

d. *Commander's Handbook for the Joint Interagency Coordination Group (JIACG),* United States Joint Forces Command Joint Warfighting Center Joint Innovation & Experimentation Directorate, 1 March 2007.
http://www.dtic.mil/doctrine/

> **Description:** This handbook serves as a bridge between the evolving JIACG and its migration into doctrine. As such, it is intended to inform doctrine writers, educators, and trainers about the JIACG and its potential for further inclusion in joint doctrine, education, and training. It fills the existing void between emerging concepts and published joint doctrine. It also presents well developed definitions that have been harmonized with current and evolving joint doctrine and discusses those "best practices" that have proven of value during on-going military operations, exercises, and experimentation. This handbook provides potential joint and Service users a definitive publication on "how" a JIACG may be organized and employed to support interagency coordination at the operational level, particularly during the planning and execution of a joint operation.

e. *Commander's Handbook for Assessment Planning and Execution. Version 1.0.* Washington, DC: Joint Staff, J-7 - Joint and Coalition Warfighting - 9 September 2011.
www.dtic.mil/doctrine/doctrine/jwfc/assessment_hbk.pdf

> **Description:** This handbook provides an understanding of the processes and procedures being employed by joint force commanders and their staffs to plan and execute assessment activities. It provides fundamental principles, techniques, and considerations related to assessment that are being employed in the field and are evolving toward incorporation in joint doctrine. Furthermore, this handbook supplements doctrinal publications by providing detailed guidance to conduct effects assessment, task assessment, and deficiency analysis. This handbook provides users with a pre-doctrinal reference describing how to conduct assessment execution and planning. Its primary purpose is to improve the U.S. military's assessment process through educating the user on basics, best practices, and processes. This handbook complements and expands upon the overarching concepts and principles that have been incorporated into keystone joint doctrinal publications, to include joint publications 3-0, *Joint Operations*; 5-0, *Joint Operation Planning*; and 2-0, *Joint Intelligence*. It supports requirements of joint operation planning and offers techniques and procedures currently used in the field. It is intended as a reference for joint forces conducting assessment as an element of a joint operation.

Cross-domain synergy

a. Cordesman, Anthony H. with George Sullivan and William D. Sullivan. *"Lessons of the 2006 Israeli-Hezbollah War CSIS Significant Issues Series Volume 29 Number 4.* (Washington, DC: Center for Strategic and International Studies Press, 2007)
http://csis.org/files/publication/120720_Cordesman_LessonsIsraeliHezbollah.pdf

> **Description:** The Israeli-Hezbollah conflict shows that every effort must be made to learn from experience. The war showed that high-technology forces, optimized to defeat conventional enemies, can be vulnerable to asymmetric attacks and can create political problems that offset their military advantages.

Israeli reliance on high technology applied to force transformation efforts based on using technology – particularly precision long-range strike capabilities and advanced ISR capabilities – as a substitute for force numbers and for human skills and presence. The Israelis failed to properly employ Joint Synergy, much less cross-domain synergy, in the conflict.

b. Kreuder, Gregory. "The Joint Operational Access Concept and Joint Doctrine." *Joint Forces Quarterly Issue 69, (2nd Quarter 2013)* http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-69/JFQ-69_103-108_Kreuder.pdf

Description: This article discusses how the changing operational environment, combined with emerging anti-access/area-denial (A2/AD) threats, is creating doctrinal gaps. It then discusses the relationship between doctrine, policy, and concepts, along with ways to accelerate the transition from concept to doctrine. Finally, this article draws current concepts from the JOAC and suggests tools that proponents can use to make their concept reality and to ensure U.S. operational access for future joint operations.

c. Luck, Gary GEN, U.S. Army (Retired) and the JS J7 Deployable Training Division. *Insights and Best Practices Focus Paper – Mission Command and Cross-Domain Synergy.* Suffolk: Deployable Training Division, Deputy Director Joint Staff J7, March 2013. http://www.dtic.mil/doctrine/fp/joint_operations_fp.pdf

Description: The juxtaposing of *mission command* and *cross-domain synergy* has clear utility at theater-strategic and operational level for operating at the *speed of the problem*. *Mission command* is important in setting conditions for military subordinates. *Cross-domain synergy* leverages the capabilities of our many mission partners to increase overall effectiveness.

d. Odom, William O., Ph.D., COL, U.S. Army (Retired) and Christopher D. Hayes, LCDR, U.S. Navy. "Cross-Domain Synergy: Advancing Jointness." *Joint Forces Quarterly* 73, 2nd Quarter 2014. http://ndupress.ndu.edu/JFQ/JointForceQuarterly73.aspx

Description: Achieving cross-domain synergy is ultimately about evolving the understanding of jointness, which cross-domain perspectives on military problems advances. Improved jointness enables more effective combination of the capabilities of the Armed Forces and the achievement of cross-domain synergy in joint operations. To improve jointness the military needs to shift from Service-centric approaches to a mindset that holistically views the military problem and considers the full range of available capabilities. It also requires changes in the way the military accesses and integrates capabilities, essentially transcending Service and combatant command ownership of capabilities and assuming a global perspective on military operations to achieve globally integrated operations.

e. Quintana, Elizabeth, Joanne Mackowski, and Adam Smith. "Occasional Paper: Cross-Domain Operations and Interoperability." London: Royal United Services Institute (RUSI), July 2012. https://www.rusi.org/publications/occasionalpapers/ref:O4FF47E156E9D7/

Description: RUSI and the Royal Air Force convened two workshops to look at the evolving relationship between the RAF and industry in the light of the new structural changes within the UK Ministry of Defense, and the implications of the U.S. Joint Operational Access Concept – and associated Air-Sea Battle and Joint Forced Entry Concepts – for the UK and other forces. This paper, looking at cross-domain capabilities and interoperability, is the result of the second workshop and explores some of the concepts, capabilities and force structures that might be adopted. Smaller countries like the UK with fewer military resources than the U.S. have made good use of cross-domain synergy to maximize capabilities.

f. Both Air Land Sea Application Center (ALSA) and Joint Knowledge On-Line (JKO) provide a myriad of articles that complement the topics of this planner's guide. http://www.alsa.mil/library/mttps/airfield_opening.html; https://portal.js.mil/sites/Matrix/JKO/SitePages/Home.aspx

Description: Provides the reader an understanding of the planning factors that should be considered for airfield opening in a hostile or permissive environment. In particular, it addresses the specific expertise that is required to build an effective plan and the need to designate a senior airfield authority (SAA).

Air Domain

a. *Air Force Doctrine Document (AFDD) 2-0 Global Integrated Intelligence, Surveillance, & Reconnaissance (ISR) Operations.* Washington, DC: Chief of Staff of the Air Force, January 6, 2012. http://www.airpower.maxwell.af.mil/digital/Doctrine/du_afdd2-0.pdf

Description: AFDD 2-0 Global Integrated Intelligence, Surveillance, and Reconnaissance (ISR) Operations, is the Air Force's keystone doctrinal publication on global integrated ISR and defines how the Service plans and conducts these operations to enable Joint Operations. It compiles the best practices of how an Airman conducts and employs ISR capabilities and why global integrated ISR is unique. Global integrated ISR is defined as cross-domain synchronization and integration of the planning and operation of ISR assets.

b. "Cross-Domain Integration" *U.S. Air Force Annex 3-0 Operations & Planning to Joint Publication 3-0.* Maxwell AFB, AL: Curtis E. Lemay Center for Doctrine and Education, November 9, 2012. https://doctrine.af.mil/download.jsp?filename=3-0-D08-OPS-Cross-Domain.pdf

Description: Military operations take place in and through the air, land, maritime, space, and cyberspace domains and the information environment. The Air Force exploits advantages in the air, space, and cyberspace domains to achieve joint force commander (JFC) and national objectives in all domains and the information environment. In either a supporting or supported role, these functions can be conducted independently from, or in concert with, land and maritime operations. Air Force operations are crucial to the success of operations in all domains.

c. *U.S. Air Force Strategic Master Plan*. Washington, DC: Secretary of the Air Force and Chief of Staff of the Air Force May 2015. http://www.af.mil/Portals/1/documents/Force%20Management/Enlisted/Strategic%20Master%20Plan%20May%202015.pdf?timestamp=1432224521926

Description: This Strategic Master Plan (SMP) translates the United States Air Force's 30-year strategy, *America's Air Force: A Call to the Future,* into comprehensive guidance, goals, and objectives. The SMP discusses pursuing a "Multi-Domain" approach to Air Force missions integrating and employing capabilities operating in or through the cyberspace and space domains in addition to the traditional air domain.

Land Domain

a. Gordon IV, John and John Matsumura. *The Army's Role in Overcoming Anti-Access and Area Denial Challenges.* Santa Monica, CA: Rand Arroyo Center, 2013. http://www.rand.org/pubs/research_reports/RR229.html

Description: The U.S. military has become increasingly concerned about the challenges it could face in gaining access to an operational area. Given their global responsibilities, the U.S. armed forces must be prepared to deploy to a wide range of locations that include almost any type of terrain and confront adversaries that span the threat spectrum from very poorly armed bands to peer-level foes. Research indicates that, in most situations, anti-access challenges require a joint solution, in which the capabilities of the different services can be brought to bear based on the threat and the mission. This study examines the nature of those future challenges and the Army's role as part of a larger joint or combined force.

b. Lindsey, Eric. *Beyond Coast Artillery: Cross-Domain Denial and the Army*. Washington, DC: Center for Strategic and Budgetary Assessments (CSBA), October 15, 2014. http://csbaonline.org/publications/2014/10/beyond-coast-artillery-cross-domain-denial-and-the-army/

Description: In this brief, CSBA Research Fellow Eric Lindsey argues that Army missiles forces can do far more than defend coastlines. By enhancing its land-based anti-air, anti-ship and surface-to-surface strike capabilities, he says, the Army could field a forward-deployed anti-access/area-denial force that would deny adversaries sanctuary and freedom of action and help the Army deter and prevail in a wider spectrum of conflict.

c. Shunk, Dave. "Area Denial & Falklands War Lessons Learned. *Small Wars Journal* (December 12, 2014). http://smallwarsjournal.com/jrnl/art/area-denial-falklands-war-lessons-learned-implications-for-land-warfare-2030-2040-after-the

Description: In 1982 Great Britain fought Argentina over the Falkland Islands in the South Atlantic. The Falklands war forced Britain to fight an expeditionary conflict 8,000 miles away from home station. It is one of the best examples of lessons learned for both anti-access and area denial in a modern conventional conflict. As such, it may prove far more relevant for the future than any conflict in the past three decades.

d. U.S. Army Training and Doctrine Command. *TRADOC Pamphlet 525-3-1 The U.S. Army Operating Concept: Win in a Complex World 2020-2040.* Fort Eustis, VA: U.S. Army Training and Doctrine Command, October 31, 2014. http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf

Description: Army operations are inherently cross-domain operations. U.S. forces depend on and complement joint efforts in the land, air, maritime, space, and cyberspace domains to enable operations on land. Because joint force freedom of movement and action across all domains are increasingly challenged by elusive land-based threats, this concept emphasizes Army operations to gain, sustain, and exploit control over land, to deny its use to the enemy. Future Army forces will support joint force freedom of movement and action through the projection of power from land across the maritime, air, space, and cyberspace domains.

e. *TRADOC Pamphlet 525-3-6 US Army Functional Concept for Movement and Maneuver 2016-2028*. Fort Monroe, VA: U.S. Army Training and Doctrine Command, October 13, 2010. http://www.tradoc.army.mil/tpubs/pams/tp525-3-6.pdf

Description: TRADOC Pam 525-3-6 describes corps, division, and brigade operations in the future. It identifies the capabilities required to enable them to conduct combined arms maneuver and wide area security successfully. The document requires the Army to develop adaptive and agile soldiers and leaders to lead combined arms formations capable of functioning effectively in predicted complex operational environments as integral members of a joint, interagency, intergovernmental, and multinational team.

Maritime Domain

a. *A Cooperative Strategy for 21st Century Seapower.* Washington, DC: Chief of Naval Operations, Commandant of the Marine Corps, and Commandant of the Coast Guard, March 2015. http://www.navy.mil/local/maritime/150227-CS21R-Final.pdf

Description: This maritime strategy describes how the United States will design, organize, and employ the Sea Services in support of national defense and homeland security strategies. The document discusses all domain access as the ability to project military force in contested areas with sufficient freedom of action to operate effectively. In today's security environment, that access is increasingly contested by state and non-state actors that can hold even our most advanced forces and weapon systems at risk with their own sophisticated anti-access/area denial strategies. Employed in coordination with the Navy–Marine Corps team's sea control and power projection capabilities, all domain access allows Joint Force Maritime Component Commanders to provide cross-domain capability to the Joint Force.

b. Greenert, Jonathan, ADM, U.S. Navy. "Opening Remarks at the Brookings Institution Air-Sea Battle Doctrine Conference." Washington, DC: Brookings Institution, May 16, 2012.

http://www.navy.mil/navydata/people/cno/Greenert/Speech/120516%20Air%20Sea%20Battle_Brookings.pdf

Description: On May 16, 2012 the 21st Century Defense Initiative at The Brookings Institution hosted Air Force Chief of Staff General Norman Schwartz and Chief of Naval Operations Admiral (ADM) Jonathan Greenert for a discussion of the Air-Sea Battle Concept and their joint efforts to assure access and maintain stability. ADM Greenert stressed the need for cross-domain synergy to ensure access in the Global Commons, especially the Maritime Domain.

c. Mahan, Alfred Thayer. *The Influence of Sea Power Upon History: 1660-1783.* Gretna, LA: Pelican Publishing, 2003 (First published in 1890).

Description: One of the most important treatises written about the Maritime Domain. The essence of Mahan from a naval viewpoint is that a great navy is a prerequisite of national greatness. Geopolitical principles, to include geographic position, population size, character of the people, extent of territory, and character of the government underlie national and maritime greatness. The Chinese People's Liberation Army Navy has closely studied Mahan as it expands its fleet, blue water capabilities, and A2/AD weapon systems.

Space Domain

a. Air Command and Staff College Space Research Electives Seminars. *AU-18 Space Primer*. Maxwell AFB, AL: Air University Press, 2009. http://www.au.af/au/awc/space/au-18-2009/index.htm

Description: This primer is a useful tool both for individuals who are not "space aware" – unacquainted with space capabilities, organizations, and operations – and for those who are "space aware", especially individuals associated with the space community, but not familiar with space capabilities, organizations, and operations outside their particular areas of expertise.

b. Association of the U.S. Army. "U.S. Army Space Capabilities: Enabling the Force of Decisive Action: An AUSA Torchbearer National Security Report." Washington, DC: Association of the United States Army. May 2012. https://www.ausa.org/publications/torchbearercampaign/tnsr/Documents/TB_SMDC_web.pdf

Description: This document discusses how Army space-based capabilities fit within land power. A discussion of warfighting integration, force structure, training and materiel development provides a snapshot where Army space is now and where it must go in the future.

c. Berkowitz, Mark J. "Protecting America's Freedom of Action in Space." *High Frontier The Journal for Space and Missile Professionals Volume 3, Number 2. March 2007.* http://www.afspc.af.mil/shared/media/document/AFD-070322-103.pdf

Description: As a matter of national policy, U.S. space systems are sovereign property with the right of passage through and operations in space without interference. The preservation of this right will be *the* space policy issue for the United States in the coming years. The article discusses challenges to the freedom of space and proposed measures to protect it.

d. George C. Marshall Institute. "A Day Without Space: What would happen with a day without space?" Accessed July 15, 2015. https://adaywithoutspace.wordpress.com/

Description: Space systems provide significant benefits to American commerce and national security. The George C. Marshall Institute and the Space Enterprise Council have co-hosted a series of events called *"A Day Without Space"* to discuss the implications of losing access to space-borne assets and information for the U.S. economy and national security. The website contains archives of the findings of the seminars.

e. Office of the President of the United States of America. *National Space Policy of the United States of America.* Washington, DC: The White House, 2010. https://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf

Description: The National Space Policy expresses the President's direction for the Nation's space activities. The policy articulates the President's commitment to reinvigorating U.S. leadership in space for the purposes of maintaining space as a stable and productive environment for the peaceful use of all nations.

f. Shipp, Jac W. "Space and Cyberspace: Key Areas of Intersection." *Fires May – June 2012.* http://www.dtic.mil/dtic/tr/fulltext/u2/a559424.pdf

Description: Article discusses how space and cyberspace domains and their associated operations overlap and intersect, and the synergies and opportunities created by each. Article goes on to describe ways to improve integrated space and cyberspace to full spectrum operations.

g. U.S. Air Force. *Air Force Tactics, Techniques, and Procedures 3-1: Air Force Satellite Control Network*. February 2013. *Doctrine Annex 3-14 Space Operations.* Published June 19, 2012. *https://doctrine.af.mil/DTM/dtmspace.htm*

Description: Airmen should understand space capabilities are vital to joint campaign and operational planning. Integration of space capabilities occurs within Air Force, joint, and combined operations in uncontested, contested, and denied environments, and throughout the range of military operations. Since space assets like Global Positioning System (GPS) complement existing capabilities (e.g., navigation aids, long-haul communication), space capabilities are inherently cross-domain. Integration of space capabilities requires diligent establishment of command relationships.

h. U.S. Strategic Command (USSTRATCOM). "Joint Functional Component Command for Space Factsheet." Published December 2011. https://www.stratcom.mil/factsheets/7/JFCC_Space/

Description: Factsheet describes the Mission, Background, Current Operations, Personnel, and Budget of the Joint Functional Component Command for Space (JFCC Space), a component of USSTRATCOM. JFCC Space is responsible for executing continuous, integrated space operations to deliver theater and global effects in support of national and combatant commander objectives. JFCC Space coordinates space operational-level planning, integration, and coordination to ensure unity of effort in support of military and national security operations, and support to civil authorities.

Cyberspace Domain

a. U.S. Department of Defense. The DOD Cyber Strategy April 2015. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_for_web.pdf

Description: The purpose of this cyberspace strategy, the Department's second, is to guide the development of DOD's cyberspace forces and strengthen U.S. cyberspace defense and cyberspace deterrence posture. It focuses on building cyberspace capabilities and organizations for DOD's three cyberspace missions: to defend DOD networks, systems, and information; defend the U.S. homeland and U.S. national interests against cyberspace attacks of significant consequence; and support operational and contingency plans.

b. U.S. Fleet Cyber Command/Tenth Fleet. *Strategic Plan 2015-2020.* Published 2015. http://www.fcc.navy.mil

Description: This Plan plots Fleet Cyber Command's course to deliver on its responsibilities by leveraging its strengths and shrinking the Navy's vulnerabilities. The Plan lays out five pivotal strategic goals: (1) Operate the Network as a Warfighting Platform; (2) Conduct Tailored Signals Intelligence; (3) Deliver Warfighting Effects through Cyberspace; (4) Create Shared Cyber Situational Awareness; and (5) Establish and Mature the Navy's Cyber Mission Forces. The Plan describes a detailed Execution Plan to achieve those goals.

c. U.S. Air Force. *Doctrine Annex 3-12 Cyberspace Operations*. 30 November 2011 https://doctrine.af.mil/DTM/dtmcyberspaceops.htm

Description: Contains chapters on the integration of cyberspace operations across domains, design of cyberspace operations, and considerations across the range of military operations.

d. Ackerman, Robert K. "Destructive Cyber Attacks Increase in Frequency, Sophistication." *Signal,* July 2015. http://www.afcea.org/content/?q=Article-destructive-cyber-attacks-increase-frequency-sophistication

Description: Short, recent, unclassified article discussing cyberspace threats and attacks including the hack into OPM data. A more diverse group of players is generating a growing threat toward all elements of the critical infrastructure through cyberspace. New capabilities have stocked the arsenals of cyber-marauders, who now are displaying a greater variety of motives and desired effects as they target governments, power plants, financial services and other vulnerable sites.

e. Bae, Sebastian J. "Cyber Warfare: Chinese and Russian Lessons for U.S. Cyber Doctrine." Georgetown Security Studies Review. Published May 7, 2015. http://georgetownsecuritystudiesreview.org/2015/05/07/cyber-warfare-chinese-and-russian-lessons-for-us-cyber-doctrine/

Description: As Sun-Tzu said, "Know your enemy." The victors in cyberspace will not be the states with the best technology, but those who effectively manipulate and control information. China and Russia have already demonstrated their ability to wage information warfare in the digital age – understanding cyberspace is a means to an end. Without a strategic overhaul in conceptualizing cyber warfare, the U.S. will be unable to compete in cyberspace where information superiority will define success. The first step in winning the cyber wars of the future will be understanding ends, ways, and means – a lesson the United States could learn from China and Russia.

f. Bender, Jason M. "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations." *Small Wars Journal.* Published November 5, 2013. http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner

Description: While this monograph does not answer "What is a cyber-planner?" it does present multiple points for discussion based on existing challenges in doctrine, training, and leader development. In light of these challenges, the Services must approach solutions at both the individual and institutional levels. In the case of the individual planner, the requirement is for units to identify those personnel who show shown an aptitude for planning and target them for specific functional training and development. In the case of the institution, the Services must pursue broad and comprehensive education for all potential commanders and planners regarding cyberspace operations. Article concludes with an outstanding Recommended Professional Reading List for Commanders, Staffs, and Planners (Especially Offensive Cyberspace Operations Planners).

g. Brewster, William M., Maj., USMC and Gerald W. Kearney, Jr., LtCol., USMC. "Integrating Cyber Fires into MAGTF Operations: Putting the enemy on the horns of a dilemma." *Marine Corps Gazette,* July 2015.

Description: The article provides a realistic NEO scenario in which cyber fires can be incorporated into expeditionary MAGTF operations. The article focuses on the process as well as the roles and responsibilities to plan, request, integrate, and execute cyber fires. The goal of the article is to demystify U.S. Cyber Command's process to request cyber fires and develop an understanding of the role each organization plays in the planning and execution of offensive cyber operations (OCO).

h. Chavana, Staff Sgt. Jarrod USAF. "Airmen train for 'new wild, wild west in cyber domain." Air Force Space Command *Inside AFSPC.* Published October 2014. http://www.afspc.af.mil/news/story.asp?id=123427359

Description: Article describes activities at the 39th Information Operations Squadron located at Hulbert Field, FL to train cyber warfare operators for the Air Force. "Cyber is the new wild, wild west," said Gen. John E. Hyten, Air Force Space Command Commander. "It took us 30 years to figure out how to make space a real warfighting domain and operate in it accordingly. We do not have that time in cyber, because cyber is under threat every day."

i. Corrin, Amber. "Army experiments now underway that integrate cyber and land operations." *C4ISR & Networks,* (July 10, 2015). http://www.c4isrnet.com/story/military-tech/cyber/2015/07/10/army-testing-cyber-integration-in-land-operations/29976545/

Description: The Army is conducting a series of experiments to find the best ways to integrate cyber operations into more traditional land operations, including in the formations closest to the ground. The experimental initiative, known as "cyberspace operations corps and below" started with a first event held in the May-June 2015 timeframe with a brigade combat team at the Joint Readiness Training Center at Fort Polk, LA.

j. Denning, Dorothy E. "Rethinking the Cyber Domain and Deterrence." *Joint Forces Quarterly Number 77 2nd Quarter 2015.* http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/581864/jfq-77-rethinking-the-cyber-domain-and-deterrence.aspx

Description: Article starts with a discussion of two key attributes of cyberspace resembling traditional domains: Man & Nature and the malleability of the domain. Article then moves to a discussion of deterrence in cyberspace including the differences between deterrence in cyberspace and deterrence in the traditional domains. Because cyberspace is such a rich domain, studies of "cyber deterrence" raise as many problems as would be raised by a comparable study of "land deterrence." This does not mean that deterrence in cyberspace is impossible, only that a more focused approach is needed, as has been followed in traditional domains of warfare.

k. Eom, Jung ho. "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace. *International Journal of Software Engineering and its Applications Volume 8 Number 9 (2014).* http://www.sersc.org/journals/IJSEIA/vol8_no9_2014/11.pdf

Description: This paper focuses on the roles and responsibilities of cyberspace intelligence in each phase of cyberspace operations. Cyberspace intelligence must properly support cyberspace commanders and units for ensuring cyberspace intelligence superiority. Cyberspace intelligence is a cyber-discipline that exploits a number of information collection and analysis approaches to provide direction and decision to the cyberspace commander and units.

l. Headquarters, U.S. Army Cyber Command/2nd Army. *U.S. Army Landcyber White Paper: 2012-2030.* Published September 14, 2012. https://www.milsuite.mil/book/docs/DOC-171583

Description: This white paper describes Army cyberspace operations in the 2012-2030 timeframe, to include Army cyberspace operations needs and required capabilities. The white paper informs future Army cyberspace force development and serves as the conceptual basis for developing solutions to the future force pertaining to Army cyberspace operations across the DOTMLPF.

m. Rivera, Jason. "A Theory of Cyber warfare: Political and Military Objectives, Lines of Communication, and Targets. *Georgetown Security Studies Review*. Published June 10, 2014. http://georgetownsecuritystudiesreview.org/2014/06/10/a-theory-of-cyberwarfare-political-and-military-objectives-lines-of-communication-and-targets/

Description: This paper develops a framework that military planners can use to understand cyberspace as a battlefield terrain upon which cyber forces secure, exercise, and dispute control of computer systems and networks in order to achieve political and military objectives. The paper's theory of Cyber warfare is undergirded by three critical assumptions. First, all state-sponsored military operations are conducted for the purpose of accomplishing nation-state political or military or objectives. Second, cyberspace, inherent to the initial design of the Internet, is formulated upon lines of communication designed to transport information from Point A to Point B. Third, like military concepts of key terrain or centers of gravity, there are key targets within cyberspace for which positon and possession yield a decisive military advantage. Using the theory presented, the paper concludes by illustrating three lines of effort necessary for a state to effectively engage in cyberspace.

n. Samad, Musa A., Maj., USMC. "Cyber Operations: Putting MAGTF commanders in control." *Marine Corps Gazette,* July 2015.

Description: In terms of the Marine Corps, the basic premise behind cyber teams should be to enable a commander to apply military cyber power within the commander's area of operations. For that to happen, commanders need to be taught the capabilities and limitations of what cyber operations can provide. The article discusses the potential for conducting cyberspace operations in support of Marine missions.

o. Singer, Peter W. *Ghost Fleet: A Novel of the Next World War.* New York: Houghton Mifflin Harcourt, 2015.

Description: Ghost Fleet tells of a near-future world war, using a large and diverse cast of well-developed characters. Even the most unexpected developments and plot twists are based on real-world trends and technologies. Cyberspace plays an especially prominent role, and much of the action revolves around how the flow of ones and zeros affects strategy and operations. One review states the book should be required reading for the entire Pentagon.

p. VanDriel, Martha S. H., COL, USA. "Bridging the Planning Gap: Incorporating Cyberspace into Operational Planning. U.S. Army War College Strategic Studies Institute. Published May 4, 2015. http://strategicstudiesinstitute.army.mil/index.cfm/articles/Bridging-the-planning-gap/2015/05/04

Description: While there are examples of how cyberspace support to military operations has advanced over the last decade, one gap has not been addressed in detail- operational planning. Incorporating cyberspace operations into operational-level planning has proven more difficult than anticipated. Joint and Army senior leaders have identified operational-level cyberspace planners to be a critical shortage. Several major systemic problems hinder the incorporation of cyberspace into operational planning. The Army needs to take actions now to successfully incorporate cyberspace operations into operational-level planning.

q. Williams, Brett T, Major General, USAF. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Forces Quarterly Number 73 January 2014.* http://ndupress.ndu.edu/News/NewsArticleView/tabid/7849/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations.aspx

Description: The intent of this article is to advocate for making cyberspace operations part of the powerful synergy we currently create with joint force operations. Today's commanders must be prepared to defend the Nation in all domains including cyberspace. They cannot do so without trained and ready forces, situational awareness of cyberspace, effective command and control, defensible architecture, appropriate delegation of authority for execution, and an operational approach to tie it all together. The operational approach described in the article provides a starting point for commanders to integrate cyberspace operations within the joint doctrinal framework employed every day to accomplish their assigned missions.

Intentionally Blank

APPENDIX G
GLOSSARY
PART I—ABBREVIATIONS AND ACRONYMS

A2	Anti-Access
A2/AD	Anti-Access/Area Denial
AADC	Area Air Defense Command
AADP	Area Air Defense Plan
ACA	Airspace Control Authority
ACO	Airspace Control Order
ACP	Airspace Control Plan
AD	Area Denial
ADM	Admiral
AEF	Air Expeditionary Forces
AEW	Air Expeditionary Wings
AJP	Allied Joint Publication
AO	Area of Operations
AOD	Air Operations Directive
AOR	Area of Operations/Area of Responsibility
APEX	Adaptive Planning and Execution
ASW	Anti-Submarine Warfare
ATC	Air Tasking Cycle
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
ATO	Air Tasking Order
B2C2WG	Boards, Bureaus, Centers, Cells and Working Groups
BCD	Battlefield Coordination Detachment
BDA	Battle Damage Assessment
C2	Command and Control
CA	Civil Affairs
CAOC	Combined Air Operations Center
CAP	Crisis Action Plan
CAS	Close Air Support
CBP	Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear and high-yield Explosives
CCDR	Combatant Commander
CCJO	Capstone Concept for Joint Operations
CCMD	Combatant Command
CCMF	Cyberspace Combat Mission Force
CDRUSSTRATCOM	Commander, United States Strategic Command
CI	Counterintelligence
CIA	Central Intelligence Agency
CJCS	Chairman of the Joint Chiefs of Staff

CJTF	Commander, Joint Task Force
CMF	Cyberspace Mission Forces
CMO	Civil-Military Operations
CMOC	Civil-Military Operations Center
CNMF	Cyberspace National Mission Force
COA	Course of Action
COA Dev	Course of Action Development
COIN	Counterinsurgency
CONOPS	Concept of Operations
CONPLAN	Concept Plan
COP	Common Operational Picture
COS	Chief of Staff
CPT	Cyberspace Protection Team
CSG	Carrier Strike Group
CSS	Central Security Service
CST	Cyberspace Support Team
CYBERCOM	Cyber Command

DCA	Defensive Counter-Air
DCJTF	Deputy Commander, Joint Task Force
DCO	Defensive Cyberspace Operations
DCO IDM	Defensive Cyberspace Operations Internal Defensive Measures
DCO RA	Defensive Cyberspace Operations Response Actions
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIRLAUTH	Direct Liaison Authorized
DISA	Defense Information System Agency
DLA	Defense Logistics Agency
DNI	Director of National Intelligence
DOD	Department of Defense
DODIN	Department of Defense Information Network
DODIN Ops	Department of Defense Information Network Operations
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DSC	Defensive Space Control
DTG	Date Time Group
DTRA	Defense Threat Reduction Agency

EEZ	Exclusive Economic Zone
EMS	Electromagnetic Spectrum

FBI	Federal Bureau of Investigation
FDO	Foreign Disclosure Office/Officer
FEMA	Federal Emergency Management Agency

FHA	Foreign Humanitarian Assistance
GCC	Geographic Combatant Command
GEF	Guidance for Employment of Force
GPS	Global Positioning System
HN	Host Nation
HQ	Headquarters
HUMINT	Human Intelligence
I&W	Indications and Warning
IC	Intelligence Community
ICE	US Immigration and Customs Enforcement
IDF	Israeli Defense Force
IGO	Intergovernmental Organizations
INR	Intelligence and Research
INSCOM	Intelligence and Security Command
INTERPOL-USNCB	International Criminal Police Organization, United States National Central Bureau
IO	Information Operations
IRC	Information Related Capabilities
ISR	Intelligence, Surveillance and Reconnaissance
JAOP	Joint Air Operations Plan
JCC	Joint Cyber Center
JCMA	Joint Communications Security Monitoring Activity
JCSE	Joint Communications Support Element
JECC	Joint Enabling Capabilities Command
JFACC	Joint Force Air Component Commander
JFC	Joint Force Commander
JFCC	Joint Functional Component Commander
JFCC – ISR	Joint Functional Component Command – Intelligence, Surveillance, and Reconnaissance
JFCC – Space	Joint Functional Component Command - Space
JFE	Joint Fires Element
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JIACG	Joint Interagency Coordination Group
JIOC	Joint Intelligence Operations Center
JIOWC	Joint Information Operations Warfare Command
JIPOE	Joint Intelligence Preparation of the Environment
JIPTL	Joint Integrated Prioritized Target List
JKO	Joint Knowledge On Line
JMAO	Joint Mortuary Affairs Office
JMO	Joint Maritime Operations
JOA	Joint Operations Area
JOAC	Joint Operational Access Concept

JOPES	Joint Operation Planning and Execution System
JOPP	Joint Operation Planning Process
JOPPA	Joint Operation Planning Process for Air
JP	Joint Publication
JPASE	Joint Public Affairs Support Element
JPEC	Joint Planning and Execution Community
JPG	Joint Planning Group
JPME	Joint Professional Military Education
JPRA	Joint Personnel Recovery Agency
JRC	Joint Reception Center
JSCP	Joint Strategic Capabilities Plan
JS	Joint Staff
JSCC	Joint Security Coordination Committee
JPSE	Joint Planning Support Element
JSOTF	Joint Special Operations Task Force
JTCB	Joint Targeting Coordination Board
JTF	Joint Task Force
JWAC	Joint Warfare Analysis Center
LNO	Liaison Officer
LOC	Line of Communication
MA	Mission Analysis
MAGTF	Marine Air Ground Task Force
MAJCOMS	Major Commands
MARLE	Marine Liaison Element Joint Force Commander
MDA	Maritime Domain Awareness
MNF	Multi-National Force
MOE	Measures of Effectiveness
MOP	Measures of Performance
NATO	North Atlantic Treaty Organization
NATO STANAG	North Atlantic Treaty Organization Standardization Agreement
NEO	Non-combatant Evacuation Operation
NFIP	National Foreign Intelligence Program
NGA	National Geospatial-Intelligence Agency
NGO	Non-Governmental Organizational
NIST	National Intelligence Support Team
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
NSC/DC	Deputies Committee of the National Security Council
NSC/IPC	National Security Council/Interagency Policy Committee
NSC/PC	National Security Council/Principals Committee
NWP	Naval Warfare Publication
OCO	Offensive Cyberspace Operations
ODNI	Office of the Director of National Intelligence

OIA	Office of Intelligence and Analysis
ONI	Office of Naval Intelligence
ONSI	Office of National Security Intelligence
OODA	Observe, Orient, Decide, and Act
OPCON	Operational Control
OPLAN	Operational Plan
OPORD	Operation Order
OSC	Offensive Space Control
OSINT	Open Source Intelligence
OUSD[P]	Office of the Under Secretary of Defense (Policy)
PA	Public Affairs
S&T	Science and Technology
SA	Situational Awareness
SCA	Space Coordinating Authority
SecDef	Secretary of Defense
SIGINT	Signals Intelligence
SME	Subject Matter Expert
SOF	Special Operations Forces
SOP	Standing Operating Procedures
STW	Surface Tactical Warfare
TACON	Tactical Control
TFI	Terrorism and Financial Intelligence
TSA	Transportation Security Administration
TSOC	Theater Special Operations Command
UAV	Unmanned Aerial Vehicle
URL	Uniform Resource Locator
U.S.	United States
USA	United States Army
USAF	United States Air Force
USAF ISR	United States Air Force Intelligence, Surveillance, and Reconnaissance
USAID	United States Agency for International Development
USCG	Unites States Coast Guard
USCIS	US Citizenship and Immigration Services
USCS	United States Cryptologic Systems
USCYBERCOM	United States Cyber Command
USD(P)	Under Secretary of Defense for Policy
USG	United States Government
USMC	United States Marine Corps
USN	United States Navy
USS	United States Ship
USSS	U.S. Secret Service
USSTRATCOM	United States Strategic Command

WG	Working Group
WMD	Weapons of Mass Destruction

PART II—TERMS AND DEFINITIONS

Unless otherwise stated, all definitions are from JP 1-02, DOD Dictionary of Military Terms, http://www.dtic.mil/doctrine/dod_dictionary/.

Acceptability: The joint operation plan review criterion for assessing whether the contemplated course of action is proportional, worth the cost, consistent with the law of war; and is militarily and politically supportable. See also adequacy; feasibility. Source: JP 1-02.

Assumption: A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action. Source: JP 1-02

Cross-domain synergy: The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others. Source: JOAC.

Cyberspace: A global domain within the information environment consisting of the interdependent networks of information technology infrastructures, and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Source: JP 3-12 (Approved for incorporation into JP 1-02.)

Cyberspace superiority: The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. JP 3-12 (Approved for inclusion in JP 1-02.)

Cyberspace operations: The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Source: JP 3-0.

Domain superiority: That degree of dominance of one force over another in a domain that permits the conduct of operations by the former at a given time and place without prohibitive interference by the latter. Source: JOAC.

Joint synergy: The combination of Service capabilities such that each enhances the effectiveness and compensates for the vulnerabilities of the others. Source: CCJO v3.0.

Line of communications: A route, either land, water, and/or air, that connects an operating military force with a base of operations and along which supplies and military forces move. Source: (JP 2-01.3)

Maritime superiority: That degree of dominance of one force over another that permits the conduct of maritime operations by the former and its related land, sea, and air forces at a given time and place without prohibitive interference by the opposing force. Source: JP 3-32

Maritime supremacy: That degree of maritime superiority wherein the opposing force is incapable of effective interference. Source: JP 3-32

Military options: A range of military force responses that can be projected to accomplish assigned tasks. Options include one or a combination of the following: civic action, humanitarian assistance, civil affairs (CA), and other military activities to develop positive relationships with other countries; confidence building and other measures to reduce military tensions; military presence; activities to convey threats to adversaries as well as truth projections; military deceptions and psychological operations; quarantines, blockades, and harassment operations; raids; intervention operations; armed conflict involving air, land, maritime, and strategic warfare operations; support for law enforcement authorities to counter international criminal activities (terrorism, narcotics trafficking, slavery, and piracy); support for law enforcement authorities to suppress domestic rebellion; and support for insurgency, counterinsurgency (COIN), and civil war in foreign countries. See also civil affairs; foreign humanitarian assistance; military civic action. Source: JP 5-01.3.

Objective Area: A defined geographical area within which is located an objective to be captured or reached by the military forces. This area is defined by competent authority for purposes of command and control. Source: JP 3-06

Operational Access: The ability to project military force into an operational area with sufficient freedom of action to accomplish the mission. Source: JOAC

Operational Area: An overarching term encompassing more descriptive terms (such as area of responsibility and joint operations area) for geographic areas in which military operations are conducted. Source: JP 3-0

Sea Basing: The deployment, assembly, command, projection, reconstitution, and re-employment of joint power from the sea without reliance on land bases within the operational area. Source: JP 3-02

Space: A medium like the land, sea, and air within which military activities shall be conducted to achieve US national security objectives. Source: JP 1-02.

Space Situational Awareness: The requisite current and predictive knowledge of the space environment and the operational environment upon which space operations depend - including physical, virtual, and human domains - as well as all factors, activities, and events of friendly and adversary space forces across the spectrum of conflict. Source: JP 3-14

Staging: Assembling, holding, and organizing arriving personnel, equipment, and sustaining materiel in preparation for onward movement. The organizing and preparation for movement of personnel, equipment, and materiel at designated areas to incrementally build forces capable of meeting the operational commander's requirements. Source: JP 3-35

Strategic Distance: A descriptor for action originating outside the operational area, often from home station. Source: JOAC.

Weapons of Mass Destruction: Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. Also called WMD. Source: JP 3-40

Unmanned Aircraft: An aircraft or balloon that does not carry a human operator and is capable of flight under remote control or autonomous programming. Source: JP 3-52

Distribution Statement A: Approved for public release; distribution is unlimited.