

JOINT OPERATIONAL ACCESS CONCEPT (JOAC)



**VERSION 1.0
17 January 2012**

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

THIS PAGE INTENTIONALLY LEFT BLANK

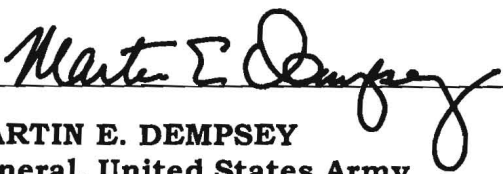
FOREWORD

The *Joint Operational Access Concept* (JOAC) describes in broad terms my vision for how joint forces will operate in response to emerging antiaccess and area-denial security challenges. Due to three major trends - the growth of antiaccess and area-denial capabilities around the globe, the changing U.S. overseas defense posture, and the emergence of space and cyberspace as contested domains - future enemies, both states and nonstates, see the adoption of antiaccess/area-denial strategies against the United States as a favorable course of action for them.

The JOAC describes how future joint forces will achieve operational access in the face of such strategies. Its central thesis is *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—to establish superiority in some combination of domains that will provide the freedom of action required by the mission. The JOAC envisions a greater degree of integration across domains and at lower echelons than ever before. Embracing cross-domain synergy at increasingly lower levels will be essential to generating the tempo that is often critical to exploiting fleeting local opportunities for disrupting the enemy system. The JOAC also envisions a greater degree and more flexible integration of space and cyberspace operations into the traditional air-sea-land battlespace than ever before.

Each Service has an important role in ensuring Joint Operational Access. The JOAC was developed by representatives from each of the Services and the Joint Staff in coordination with the combatant commands, multinational partners, and other stakeholders. The JOAC development was supported by an experimentation campaign including a multi-scenario wargame, multiple Service-sponsored events, and other concept development venues.

The strategic challenge is clear: the Joint Force must maintain the freedom of action to accomplish any assigned mission. The Joint Operational Access Concept is a critical first step in ensuring the joint force has the requisite capabilities to do so.


MARTIN E. DEMPSEY
General, United States Army
Chairman, Joint Chiefs of Staff

THIS PAGE INTENTIONALLY LEFT BLANK

JOINT OPERATIONAL ACCESS CONCEPT (JOAC)

EXECUTIVE SUMMARY

This paper proposes a concept for how joint forces will achieve operational access in the face of armed opposition by a variety of potential enemies and under a variety of conditions, as part of a broader national approach.

Operational access is the ability to project military force into an operational area with sufficient freedom of action to accomplish the mission. Operational access does not exist for its own sake, but rather serves our broader strategic goals, whether to ensure access to commerce, demonstrate U.S. resolve by positioning forces overseas to manage crisis and prevent war, or defeat an enemy in war. Operational access is the joint force contribution to *assured access*, the unhindered national use of the global commons and select sovereign territory, waters, airspace and cyberspace.

Enduring requirement for force projection. As a global power with global interests, the United States must maintain the credible capability to project military force into any region of the world in support of those interests. While the requirement for operational access applies to any mission, the most difficult access challenge—and therefore the subject of this concept—is operational access contested by armed opposition.

Distinction between antiaccess and area-denial. As used in this paper, *antiaccess* refers to those actions and capabilities, usually long-range, designed to prevent an opposing force from entering an operational area. *Area-denial* refers to those actions and capabilities, usually of shorter range, designed not to keep an opposing force out, but to limit its freedom of action within the operational area.

Importance of preconditions. The challenge of operational access is determined largely by conditions existing prior to the onset of combat operations. Consequently, success in combat often will depend on efforts to shape favorable access conditions in advance, which in turn requires a coordinated interagency approach. The joint force will attempt to shape the operational area in advance of conflict through a variety of security and engagement activities (as described in the *Capstone Concept for Joint Operations*), such as multinational exercises, access and support agreements, establishment and improvement of overseas bases, prepositioning of supplies, and forward deployment of forces.

Emerging trends. Three trends in the operating environment promise to complicate the challenge of opposed access for U.S. joint forces:

- (1) The dramatic improvement and proliferation of weapons and other technologies capable of denying access to or freedom of action within an operational area.
- (2) The changing U.S. overseas defense posture.
- (3) The emergence of space and cyberspace as increasingly important and contested domains.

Enemy adoption of antiaccess/area-denial strategies. Events of recent decades have demonstrated the decisive results U.S. joint forces can achieve when allowed to flow combat power into an operational area unimpeded. Yet, few if any enemies perceived that they possessed the ability to deny U.S. access by armed opposition, and U.S. operational access during that period was essentially unopposed. The combination of the three major trends described above has altered that calculus dramatically. Increasingly capable future enemies will see the adoption of an antiaccess/area-denial strategy against the United States as a favorable course of action for them. The ability to ensure operational access in the future is being challenged—and may well be the most difficult operational challenge U.S. forces will face over the coming decades.

The Military Problem. The essential access challenge for future joint forces is to be able to project military force into an operational area and sustain it in the face of armed opposition by increasingly capable enemies when U.S. overseas defense posture is changing and space and cyberspace are becoming increasingly important and contested domains.

The Central Idea: Cross-domain synergy. To meet that challenge, future joint forces will leverage *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—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, depending on the enemy’s capabilities and the requirements of the mission. Superiority in any domain may not be widespread or permanent; it more often will be local and temporary.

Attaining cross-domain synergy to overcome future access challenges will require a greater degree of integration than ever before. Additionally this integration will have to occur at lower echelons, generating the tempo that is often critical to exploiting fleeting local opportunities for disrupting the enemy system, and will require the full inclusion of space and cyberspace operations into the traditional air-land-sea battlespace.

Precepts. Several general principles amplify the central idea in describing how future joint forces could achieve operational access in the face of armed opposition.

- Conduct operations to gain access based on the requirements of the broader mission, while also designing subsequent operations to lessen access challenges.
- Prepare the operational area in advance to facilitate access.
- Consider a variety of basing options.
- Seize the initiative by deploying and operating on multiple, independent lines of operations.
- Exploit advantages in one or more domains to disrupt or destroy enemy antiaccess/area-denial capabilities in others.
- Disrupt enemy reconnaissance and surveillance efforts while protecting friendly efforts.
- Create pockets or corridors of local domain superiority to penetrate the enemy's defenses and maintain them as required to accomplish the mission.
- Maneuver directly against key operational objectives from strategic distance.
- Attack enemy antiaccess/area-denial defenses in depth rather than rolling back those defenses from the perimeter.
- Maximize surprise through deception, stealth, and ambiguity to complicate enemy targeting.
- Protect space and cyber assets while attacking the enemy's cyber and space capabilities.

Required capabilities. The concept identifies 30 operational capabilities the future joint force will need to gain operational access in an opposed environment. The implications of creating and maintaining these capabilities in the necessary capacity are potentially profound.

Adoption of this concept will establish a common intellectual framework for the challenge of opposed access, will inform subsequent joint and Service concepts, and will result in doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) solutions.

Table of Contents

EXECUTIVE SUMMARY.....	i
1. Introduction.....	1
2. Purpose	2
3. Scope.....	3
4. The Nature of Operational Access.....	4
5. Operational Access in the Future Operating Environment	8
6. The Military Problem: Opposed Operational Access in an Advanced Antiaccess/Area-Denial Environment.....	14
7. A Concept for Joint Operational Access	14
8. Operational Access Precepts.....	17
9. Joint Operational Access and the Joint Functions	27
10. Capabilities Required by this Concept	33
11. Risks of Adopting this Concept.....	36
12. Conclusion.....	38
ANNEX A Glossary	40
ANNEX B Assessment Plan.....	46
ANNEX C Bibliography	60

List of Figures

Figure 1. Antiaccess and area-denial capabilities as part of a layered, integrated defense	11
Figure 2. Cross-Domain Synergy	15
Figure 3. JOAC Project Framework.....	46
Figure 4. JOAC SOOPA Model	47
Figure 5. JOAC Development Architecture	48

– This page intentionally left blank –

1. Introduction

This paper proposes a concept for how joint forces will achieve operational access in the face of armed opposition by a variety of potential enemies and under a variety of conditions, as part of a broader national approach.¹

Operational access is the ability to project military force² into an operational area with sufficient freedom of action to accomplish the mission. As war is the extension of politics by other means, operational access does not exist for its own sake, but rather serves our broader strategic goals, whether to ensure strategic access to commerce, demonstrate U.S. resolve by positioning forces overseas to manage crisis and prevent war, or defeat an enemy in war.³ Operational access is the joint force contribution to *assured access*, the unhindered national use of the global commons and select sovereign territory, waters, airspace and cyberspace. The *global commons*, in turn, are areas of air, sea, space, and cyberspace that belong to no one state.⁴ While operational access is achieved through the projection of military force, assured access is achieved by projecting all the elements of national power.⁵

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

Assured access: The unhindered national use of the global commons and select sovereign territory, waters, airspace and cyberspace, achieved by projecting all the elements of national power.

Global commons: Areas of air, sea, space, and cyberspace that belong to no one state.

¹ The use of *operational* in this context refers to military operations broadly and is not restricted to the operational level of war. The 2011 *National Military Strategy* (NMS) describes the national strategy for defeating hostile antiaccess/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, 8Feb11), p. 8.

² **Force projection:** "The ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations." *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 2Jun11].

³ *On War* Carl Von Clausewitz. <http://www.clausewitz.com/readings/Principles/#Intro> [accessed 22Apr11].

⁴ Barry R. Posen defined global commons as areas of air, sea, and space that "belong to no one state and that provide access to much of the globe." "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security*, Vol. 28, No. 1 (Summer 2003), p. 8. The same description can apply to cyberspace, which provides access to much of the globe's information. Posen attributes the origin of the term to Alfred Thayer Mahan, who described the sea as "a wide common, over which men may pass in all directions." *The Influence of Sea Power upon History: 1660-1783*. (Boston: Little, Brown and Co., 1890), p. 25.

⁵ **Power projection:** "The ability of a nation to apply all or some of its elements of national power - political, economic, informational, or military - to rapidly and effectively deploy and

As a global power with global interests, the United States must maintain the credible capability to project military force into any region of the world in support of those interests. This includes the ability to project force both into the global commons to ensure their use and into foreign territory as required. Moreover, the credible ability to do so can serve as a reassurance to U.S. partners and a powerful deterrent to those contemplating actions that threaten U.S. interests. For decades, the American ability to project military force from the United States to an operational area has gone essentially unopposed. During the Gulf War of 1990-1991, for example, Coalition forces flowed into the operational area unhindered for six months in the build-up to Operation Desert Storm. Coalition forces similarly deployed uncontested into Afghanistan in 2001 for Operation Enduring Freedom and into Kuwait in 2003 for Operation Iraqi Freedom.

This paper asserts that such unopposed operational access will be much less likely in the future, as potential enemies, exploiting weapons and other systems that are increasingly effective against an advancing enemy, will resource and adopt antiaccess strategies against U.S. forces. It is that emerging challenge—increasingly opposed operational access—that this concept addresses. That challenge may be one of the most difficult that joint forces will face in the coming decades—and also one of the most critical, since a military that cannot gain the operational access needed to bring force to bear loses utility as an instrument of national power.

2. Purpose

This concept describes how a future joint force will overcome opposed access challenges. Its purpose is to guide force development by:

- Establishing a common intellectual framework for military professionals, policymakers, and others interested in the challenge of opposed access.
- Invigorating interest in and study of an operational challenge that a generation of military leaders, focused on other missions, has not had to consider in recent years.
- Establishing a basis for subsequent joint and Service concepts and doctrine.
- Identifying the broad capabilities required to gain operational access in the face of armed opposition.
- Informing study, evaluation, wargaming, and experimentation that will result in changes to doctrine, organization, training, materiel, leadership

sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability.” *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 17Jan11].

and education, personnel, and facilities (DOTMLPF).

3. Scope

This concept applies to combatant commands, joint task forces, and subordinate commands. It addresses operational access within the context established by the *Capstone Concept for Joint Operations* (CCJO)⁶, which describes a future operating environment characterized by uncertainty, complexity, and rapid change. As a solution to those conditions, the CCJO proposes a process of operational adaptation involving the dynamic combination of four broad categories of military activity: combat, security, engagement, and relief and reconstruction. The concept proposed here exists within the context of that adaptation process.

This is a warfighting concept. It addresses *opposed access*, those situations requiring the use of force to gain access against an enemy trying to deny that access through the use of force. While even benign missions such as foreign humanitarian assistance can pose access challenges, this concept takes the position that opposed access presents the most difficult access challenge and that unopposed access constitutes a lesser included challenge. That said, many of the noncombat aspects of this concept may apply to unopposed access situations, such as disaster relief in an inaccessible region. Moreover, this concept emphasizes warfare against highly capable enemies with advanced, multidomain antiaccess/area-denial capabilities on the premise that this is the greatest access challenge of all. Although not specifically addressed in this paper, the effects of weapons of mass destruction remain a critical consideration.

This concept acknowledges that joint operations will occur in support of a broader national strategy employing all the elements of national power. Comprehensive national and multinational efforts are critical but beyond the scope of this paper, which limits itself to the actions of military forces. Additionally, this concept applies to both unilateral joint operations and multinational operations, the latter being the more likely context.⁷ The cross-domain synergy that is the central idea of this concept can be the product of internal joint interactions or integration with foreign military powers.

This concept addresses opposed access in conceptual terms; it does not

⁶ Department of Defense, *Capstone Concept for Joint Operations*, v3.0, 15Jan09.

⁷ **Multinational operations:** “A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance.” *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 26May11]. According to the NMS (p. 1): “In some cases, the joint force will serve in an enabling capacity to help other nations achieve security goals that advance common interests.”

provide tactics, techniques, or procedures for defeating specific antiaccess and area-denial systems, although it is intended to inform subsequent efforts to develop those methods. Nor does it establish specific programmatic requirements, although it does identify the broad capabilities required to implement the described approach fully.

This is an overarching concept, under which can nest other concepts dealing with more specific aspects of antiaccess/area-denial challenges, such as the *Air-Sea Battle* concept already under development, or concepts on entry operations or littoral operations as possible examples. It is envisioned that

Air-Sea Battle

Recognizing that antiaccess/area-denial capabilities present a growing challenge to how joint forces operate, the Secretary of Defense directed the Department of the Navy and the Department of the Air Force to develop the Air-Sea Battle Concept. The intent of Air-Sea Battle is to improve integration of air, land, naval, space, and cyberspace forces to provide combatant commanders the capabilities needed to deter and, if necessary, defeat an adversary employing sophisticated antiaccess/area-denial capabilities. It focuses on ensuring that joint forces will possess the ability to project force as required to preserve and defend U.S. interests well into the future.

The Air-Sea Battle Concept is both an evolution of traditional U.S. power projection and a key supporting component of U.S. national security strategy for the 21st Century. However, it is important to note that Air-Sea Battle is a limited operational concept that focuses on the development of integrated air and naval forces in the context of antiaccess/area-denial threats. The concept identifies the actions needed to defeat those threats and the materiel and nonmateriel investments required to execute those actions.

There are three key components of Air-Sea Battle designed to enhance cooperation within the Department of the Air Force and the Department of the Navy. The first component is an *institutional* commitment to developing an enduring organizational model that ensures formal collaboration to address the antiaccess/area-denial challenge over time. The second component is *conceptual* alignment to ensure that capabilities are integrated properly between Services. The final component is doctrinal, organizational, training, materiel, leadership and education, personnel, and facilities *initiatives* developed jointly to ensure they are complementary where appropriate, redundant when mandated by capacity requirements, fully interoperable, and fielded with integrated acquisition strategies that seek efficiencies where they can be achieved.

such concepts would deal with their subject matter areas in greater specificity while remaining compatible with this concept.

4. The Nature of Operational Access

The requirement for operational access has existed since the first army crossed the sea to fight in a foreign land. For the United States, separated as it is from most of the world by two oceans, operational access has been an enduring

requirement and a primary concern throughout its history.

Projecting U.S. military force invariably requires extensive use of international waters, international airspace, nonsovereign cyberspace, space, and the electromagnetic spectrum. U.S. access to and freedom of navigation within these global commons are vital to its national interests, both because the American way of life requires free access to the global marketplace and as a means for projecting military force into hostile territory. Even where the ultimate objective is the latter, operations in the global commons may be critical if an enemy attempts to gain strategic depth by pushing armed opposition out into international spaces. In fact, the contest over operational access can dominate practically all other considerations in warfare, as it did throughout the Pacific theater and in the battle for the North Atlantic during the Second World War.

Gaining and maintaining operational access in the face of armed opposition involves two tasks inseparable in practice. The first is the combat task of overcoming the enemy's antiaccess and area-denial capabilities through the application of combat power. The second is moving and supporting the necessary combat power over the required distances, essentially a logistical task that can be a challenge in itself. Each depends on the other. Any concept for opposed operational access must reconcile both.

As with practically all combat actions, time can be a critical factor in operations to defeat opposed access. The temporal dimension can range from political imperatives that could impose extremely short timelines, to operational requirements to reinforce forward-deployed forces before they are destroyed, to tactical requirements to locate and neutralize antiaccess and area-denial weapons before they inflict unacceptable losses. Moreover, many enemies attempting to deny access will seek to impose delays on an advancing force by trading space for time and inflicting losses in the process.

As used in this paper, *antiaccess* refers to those actions and capabilities, usually long-range, designed to prevent an opposing force from entering an operational area.⁸ Antiaccess actions tend to target forces approaching by air and sea predominantly, but also can target the cyber, space, and other forces that support them. *Area-denial* refers to those actions and capabilities, usually of shorter range, designed not to keep an opposing force out, but to limit its freedom of action within the operational area. Area-denial capabilities target forces in all domains, including land forces. The distinction between antiaccess and area-denial is relative rather than strict, and many capabilities can be employed for both purposes. For example, the same submarine that performs an area-denial mission in coastal waters can be an antiaccess capability when employed on distant patrol.

Antiaccess: Those actions and capabilities, usually long-range, designed to prevent an opposing force from entering an operational area.

Area-denial: Those actions and capabilities, usually of shorter range, designed not to keep an opposing force out, but to limit its freedom of action within the operational area.

Advancing across open ocean and through open airspace to overcome prepared defenses is by nature a very challenging form of warfare, tending to impose higher-than-normal losses on the attacker, and therefore requiring the resolve to absorb those losses. Any concept for defeating opposed access should acknowledge that reality.

Maintaining and expanding operational access may require entry of land forces into hostile territory for a number of reasons.⁹ These may range from limited-objective attacks, such as raids to eliminate land-based threats to friendly air and naval forces, to seizing a lodgment for a sustained land campaign. Neither of these necessarily implies the deliberate establishment of a static beachhead or

Establishing operational access may require **forcible entry**, the projection of land forces onto hostile territory in the face of armed opposition. The subsequent land operations may vary in scope and duration, from small-scale raids to sustained campaigns.

⁸ This is not to say that there are no friendly forces within the theater. Forward-deployed or other forces might already be present when conflict starts and can be critical in defeating hostile antiaccess efforts to support the approach of follow-on forces. At the same time, those forward-deployed forces can be at considerable risk if not reinforced quickly enough, which introduces a potentially critical time element. This situation might be a simple result of the timing of the conflict, although it also might reflect a deliberate operational choice by the enemy to allow some U.S. forces into the operational area before “closing the door” to follow-on forces.

⁹For the purposes of this paper, *forcible entry* is defined as: “The projection of land forces onto hostile territory in the face of armed opposition. Cf. the doctrinal definition: **Forcible entry:** “Seizing and holding of a military lodgment in the face of armed opposition.” *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 17Jan11]. The distinction is important because, depending on the mission, future land forces might not seize and hold a lodgment, but might maneuver directly against the objective.

airhead in the traditional sense. While the access ultimately required in a situation may require forcible entry, forcible-entry operations themselves rely on some level of pre-existing access in the other domains.

In some cases, the enemy also must project military force into the operational area from a distant home base. In such cases, gaining friendly operational access can involve interdicting the enemy's force projection through the employment of one's own antiaccess capabilities.

The challenge of operational access is determined largely by conditions existing prior to the actual operation. These conditions can be influenced by both friendly and hostile activities conducted prior to and during the development of a crisis. Geography, particularly distance, arguably determines the access challenge more than any other factor, as military power historically has tended to degrade over distance. Advances in airpower and long-range weapons have mitigated the degrading effects of distance to some extent but have not eliminated them, while cyber capabilities are unaffected by distance. Those advancements apply not only to the attacker but also to the defender, who can exploit those capabilities to engage the enemy at greater ranges.

Historically, a key way to mitigate the degrading effects of distance has been to establish forward bases in the anticipated operational area, thereby maintaining some of the capabilities of a home base at a distant location. The more capability and capacity that a military can amass at the forward base, the more it can mitigate the effects of distance. Moreover, permanent or long-term forward bases can assure partners and deter adversaries. The ability to establish new expeditionary bases, or to improve those already in existence, also can serve as deterrent options. Conversely, a forward base becomes a resource requiring protection and sustainment and can even become a political liability, often by causing friction with the host nation or within the region.

Some operations to gain access will occur in austere environments lacking the advanced infrastructure typical of modern societies. In the antiaccess case in particular, even if the objective area is well-developed in terms of infrastructure, the most desirable approaches may well be austere. In the area-denial case, many conflicts will arise in failed or failing states where infrastructure is lacking. In such cases an advancing force will have no option other than to operate under austere conditions. At the same time, the ability to operate effectively in such conditions can confer an advantage to an advancing force because it increases operational flexibility by freeing the force from major ports, airfields, and other infrastructure and thereby also complicates enemy intelligence collection efforts.

Political conditions also can mitigate or amplify access challenges. Foreign partners willing to provide military and political support (including access to infrastructure, territorial waters, or airspace) can be critical. The

employment of forces in engagement activities often years prior to a crisis may be critical to success by encouraging willing and capable partners. Conversely, an adversary who has successfully built a strong network of partnerships throughout and en route to the region can make gaining operational access extremely challenging.

The presence of forward-deployed or other in-range combat forces at the beginning of a crisis can facilitate operational access—and sometimes even deter acts of aggression in the first place. Naval forces, which can remain on station in international waters almost indefinitely, are especially suited to such missions, as could be special operations forces inserted clandestinely. Air and space forces can exploit speed and global range to move quickly into position in response to an emerging crisis. That said, forward-deployed forces, like advanced bases, can be vulnerable to attack, particularly given a lack of advanced warning.

The more a joint force commander can promote favorable access conditions in advance, the more likely success will be. While such preparations can be invaluable and a priority for combatant commanders, it is important to keep in mind that numerous constraints—political, strategic, resource, legal, and others—can severely limit the commander’s latitude. Moreover, there are limits to what military engagement can achieve. Even long-standing allies may, for political reasons, deny access for a particular operation. In the end, joint forces must be able to gain by force the operational access needed to accomplish the mission regardless of the initial conditions.

While the United States must project and sustain military force at global distances—and therefore must protect its lines of communications¹⁰ back to home bases—most adversaries operating in their own region will not be so burdened. While U.S. joint forces almost always will need to transit international waters and airspace, many adversaries will not, although they may attack U.S. forces there. These requirements create potential vulnerabilities for U.S. forces not shared by most adversaries.

5. Operational Access in the Future Operating Environment

While operational access itself is not new, some of the conditions under which joint forces will operate to gain it in the future are. The *Joint Operating*

¹⁰ **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. Also called LOC.” *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 17Jan11].

*Environment 2010*¹¹ envisions a future characterized by complexity, uncertainty, and rapid change, all of which will influence future joint operational access. In addition, three particular trends in the operating environment promise to complicate the challenge of opposed access for U.S. joint forces: (1) the dramatic improvement and proliferation of weapons and other technologies capable of denying access to or freedom of action within an operational area, (2) changing U.S. overseas defense posture, and (3) the emergence of space and cyberspace as increasingly important and contested domains. These trends were identified based on the sources listed in Annex C and were supported by the assessment campaign described in Annex B.

The first trend is the **dramatic improvement and proliferation of weapons and other technologies capable of denying access to or freedom of action within an operational area**, which come not only from advanced technologies, but also from the innovative use of basic, even crude, capabilities.¹²

Key *antiaccess* capabilities include:

- A variety of surface-, air- and submarine-launched ballistic and cruise missiles able to accurately attack forward bases and deploying U.S. forces and their supporting logistics at ranges exceeding 1,000 nautical miles.
- Long-range reconnaissance and surveillance systems that provide necessary targeting information, including satellites, aircraft, and land- and ship-based radar.
- Kinetic and nonkinetic antisatellite weapons that can disable space systems vital to U.S. force projection.
- Submarine forces able to interdict U.S. and friendly sea lines of communications in both sovereign and international waters between U.S. bases and the theater of operations.
- Cyber attack capabilities designed to disrupt U.S. command and control systems and critical infrastructure, both civilian and military.
- Terrorists willing to attack U.S. or partner bases and deploying forces, even at points of origin in the continental United States or other regions.

¹¹ The *Joint Operating Environment* (JOE) forecasts emerging security challenges based on current trends in the world. Joint Future Group (J59), U.S. Joint Forces Command (Suffolk, VA, 18Feb10).

¹² While these capabilities could be employed for various purposes, they will be referred to as “antiaccess and area-denial capabilities” hereafter since that is the subject of this concept.

- Special operations forces capable of direct action and unconventional warfare in the approaches to the operational area.

As a result of improvements in these antiaccess capabilities, deploying forces will find themselves at risk at ever greater ranges. Deploying to the theater while under attack is a challenge that U.S. joint forces have not had to deal with in recent decades. Personnel, supplies, and equipment located in rear areas once thought to be secure increasingly will be targeted.

Key *area-denial* capabilities include:

- Air forces and air defense systems, both fixed and mobile, designed to deny local U.S. air superiority.
- Shorter-range antiship missiles and submarines employing advanced torpedoes to deny U.S. maritime superiority in the objective area.
- Precision-guided rockets, artillery, missiles, and mortars (G-RAMM) designed to attack surface targets, including landing forces, with much greater accuracy and lethality than their “dumb” predecessors.
- Chemical and biological weapons to deny the use of select areas.
- Computer and electronic attack capabilities to degrade, neutralize, or destroy U.S. command and control in the operational area.
- Abundant land and naval mines capable of quickly closing straits, land passes, long stretches of coastline, or airfields.
- Armed and explosives-laden small boats and craft in cluttered and restricted coastal waters and straits.
- Land maneuver forces.
- Special operations forces capable of direct action and unconventional warfare in the objective area.
- Unmanned systems, such as unmanned aircraft and unmanned underwater vehicles, which could loiter to provide intelligence collection or fires in the objective area.

The above capabilities, many once available only to powerful states, are now increasingly available to weaker states and even non-state actors. Some enemies will possess limited numbers of only a few of these capabilities, but others will deploy fully integrated and layered advanced antiaccess/area-denial systems comprising air, naval, land, space, and cyber forces guided by a single command and control system and employed in mutual support such that to

defeat one capability an attacker must expose himself to others. See Figure 1.

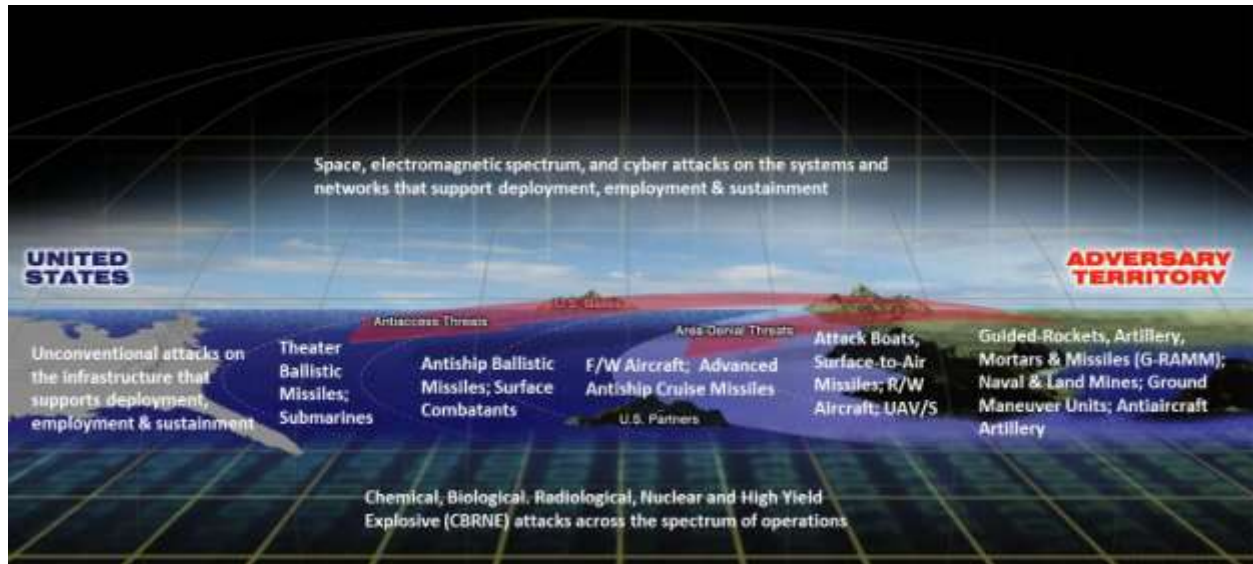


Figure 1.

Antiaccess and area-denial capabilities as part of a layered, integrated defense

Some enemies with layered, multidomain antiaccess systems, and the geographical depth within which to employ them, may actually attempt to defeat a U.S. advance before it reaches its objective area. Other enemies have no chance of physically keeping the United States out of an operating area but may instead attempt to inflict greater losses than U.S. resolve will tolerate.

The second trend affecting future operational access is **the changing U.S. overseas defense posture**, which itself is the result of several related factors. The first factor is markedly *decreased support abroad for an extensive network of U.S. military bases around the globe*. In an increasingly globalized world, there is much greater international competition for regional influence and access. Immediately after the Cold War, states had few partnership options other than the United States, but today numerous rising powers provide alternatives. Whether due to coercive threats or inducements offered by other powers, many states will be unwilling to offer the kind of long-term basing rights the United States enjoyed during the Cold War. Gaining basing rights for expeditionary operations is already a primary concern for U.S. military planners and diplomats, and that challenge is likely to grow.

The second factor is projections of *severely contracting resources*. Even were there an international appetite for it, the United States simply could not afford to establish garrisons around the globe in response to every plausible threat, especially in an era of dynamic uncertainty in which threats could emerge unpredictably.

The third factor is *force protection*. In an age of increased terrorism, increasingly affordable precision weapons, and heightened sensitivity to perceived impositions on national sovereignty, U.S. garrisons on foreign soil become both causes of friction and inviting targets. American sensitivity to casualties, especially to a garrison force outside a war zone, only exacerbates the problem.

The third trend is **the emergence of space and cyberspace as increasingly important and contested domains** with critical importance for the projection of military force. Arguably, this emergence is the most important and fundamental change in the opposed access challenge over the past several decades.

Space and cyberspace are increasingly important both for supporting operations in the other domains and as operational domains in their own rights when directed. In a support role, space systems provide satellite communications, missile warning, intelligence collection, satellite reconnaissance advanced warning, and position, navigation and timing, among other support. Cyberspace, meanwhile, provides the information infrastructure upon which the command and control of practically all military operations rests. This is especially true for U.S. forces projecting military force globally, but it is increasingly true for practically all modern militaries, especially since capabilities can be purchased commercially and relatively cheaply. In fact, U.S. space and cyberspace capabilities depend significantly on commercial systems and adversaries in some cases will purchase space capabilities on the same platforms used by U.S. joint forces.

Because of that increased importance, many future enemies will seek to contest space control and cyberspace superiority as means to denying operational access to U.S. joint forces. In fact, space and cyberspace will be priority domains for many future adversaries, both state and nonstate, because U.S. forces critically depend on them, because the capabilities are readily available and relatively affordable, and because the effects of operations can be difficult to trace and even perceive.

Moreover, because the critical support provided by space and cyberspace generally must be in place in advance and because many operations in those domains, especially offensive operations, require significant lead time, space and cyberspace operations likely will commence well in advance of other operations. In fact, even in the absence of open conflict, operations to gain and maintain cyberspace superiority and space control will be continuous requirements.

U.S. military operations conducted in the past several decades have demonstrated the decisive results U.S. joint forces are capable of when allowed to flow combat power into an operational area unimpeded. Yet, few if any

enemies perceived that they possessed the ability to deny U.S. access by armed opposition, and U.S. operational access during that period was essentially unopposed. The combination of the three major trends described above—the growth of antiaccess and area-denial capabilities around the globe, the changing U.S. overseas defense posture, and the emergence of space and cyberspace as contested domains—has altered that calculus dramatically. Future enemies, both states and nonstates, will see the adoption of an antiaccess/area-denial strategy against the United States as a favorable course of action for them. Those able to field layered and fully integrated antiaccess/area-denial defenses in multiple domains may attempt to deny U.S. operational access altogether, while others with less robust and comprehensive capabilities may simply attempt to inflict greater losses than they perceive the United States will tolerate politically.

Future enemies, both states and non-state actors, will see the adoption of an antiaccess/area-denial strategy against the United States as a favorable course of action for them.

Any example of such a strategy likely will exhibit some common critical elements, to include:

- Long-term shaping operations prior to conflict, including information operations, designed to increase influence and build up antiaccess/area-denial capabilities in a region and to encourage regional actors to deny the United States the political conditions that facilitate access.
- Imposing a steeper cost than the United States is willing to bear—either through a catastrophic attack or an attrition-based defeat mechanism designed to create substantial casualties.
- Creating as much strategic and operational depth as possible within which to inflict casualties, even interdicting deploying U.S. forces by sabotage at their points of origin or ports of embarkation.
- Attacking U.S. forward bases, whether by missiles, special operations units, or irregular forces—to include the use of weapons of mass destruction.
- Attacking U.S. command and control and communications, especially long-range capabilities, to include space and cyber capabilities.
- Attacking U.S. distribution operations at either fixed points or vulnerable choke points in the lines of communications or through cyber attacks that disrupt logistics command and control.
- Employing antiaccess and area-denial capabilities in combination to contest local air and maritime superiority and land freedom of maneuver.

Beyond those common elements, any example of an antiaccess strategy will conform itself uniquely to the capabilities of the enemy and other situational factors.

6. The Military Problem: Opposed Operational Access in an Advanced Antiaccess/Area-Denial Environment

The essential problem for future joint forces is to be able to project military force into an operational area and sustain it in the face of armed opposition when three trends apply:

- Antiaccess and area-denial weapons and technologies are dramatically improving and proliferating.
- U.S. overseas defense posture is changing.
- Space and cyberspace are becoming increasingly important and contested domains.

Meeting that challenge increasingly will require defeating integrated antiaccess/area-denial systems of growing lethality and sophistication.

7. A Concept for Joint Operational Access

To meet the challenge described above, future joint forces will leverage *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—to establish superiority in some combination of domains that will provide the freedom of action required by the mission. See Figure 2.

Future joint forces will leverage *cross-domain synergy* to establish superiority in some combination of domains that will provide the freedom of action required by the mission.

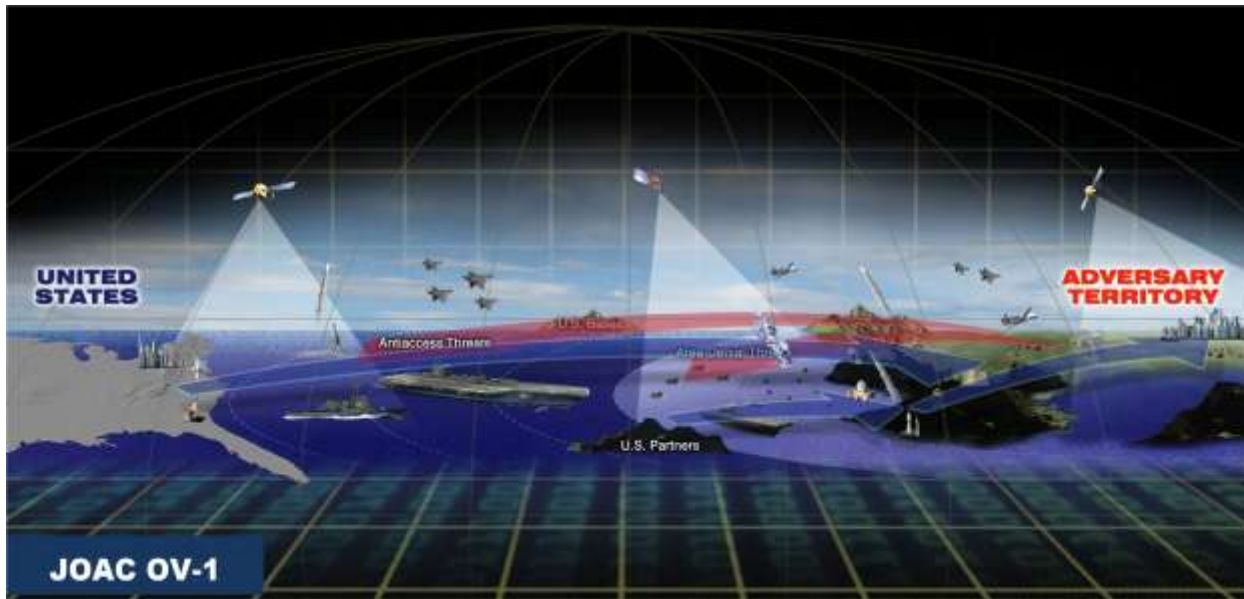


Figure 2.
Cross-Domain Synergy

Superiority here refers to 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.¹³ The combination of domain superiorities will vary with the situation, depending on the enemy’s capabilities and the requirements of the mission. Determining that combination in any situation is a function of operational design. Superiority in any domain may not be widespread or permanent; it more often will be local

¹³Adapted from doctrinal definitions of air superiority and maritime superiority. **Air superiority:** “That degree of dominance in the air battle of one force over another that permits the conduct of 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.” **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.” **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, sea and space forces at a given time and sphere of operations without prohibitive interference by an adversary.”

Note that superiority applies to a “given time and place” and need not be permanent or widespread throughout a domain. Superiority is distinct from *supremacy*, which is that degree of superiority in a domain wherein the opposing force is incapable of effective interference. See **air supremacy:** “That degree of air superiority wherein the opposing force is incapable of effective interference.” And **maritime supremacy:** “That degree of maritime superiority wherein the opposing force is incapable of effective interference.” All definitions taken from *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 18Nov10], except *cyberspace superiority*, taken from “Joint Terminology for Cyberspace Operations,” VCJCS memo for the Service chiefs, combatant commanders and directors of Joint Staff directorates, undated, p. 8.

and temporary.

This concept envisions a greater degree of integration of actions and capabilities across domains and at lower echelons than ever before. Embracing cross-domain synergy at increasingly lower levels will be essential to generating the tempo that is often critical to exploiting fleeting local opportunities for disrupting the enemy system. This concept also envisions the fuller and more flexible integration of space and cyberspace operations into the traditional air-sea-land battlespace than ever before.

This concept envisions a greater degree of integration of actions and capabilities across domains and at lower echelons than ever before, to include the full and flexible integration of space and cyberspace operations into the traditional air-sea-land battlespace.

Cross-domain synergy creates and exploits asymmetrical advantages inherent in a joint force—airpower to defeat antiship weapons, naval power to neutralize air defenses, ground forces to neutralize land-based threats to air and naval forces, cyber operations to defeat space systems, and so on (although by no means does this suggest that a joint force should forgo symmetrical advantages). Nowhere is that more critical than in defeating a multidomain antiaccess/area-denial strategy. The relationships between operations in the various domains, and the specific asymmetries to be exploited, will vary with the situation.

This synergy applies not only to joint forces deploying to the operational area—that is, attacking the enemy antiaccess system from the outside in—but also to forward-deployed forces already in the operational area attacking the enemy system from the inside out. The latter can be critical in neutralizing key enemy capabilities to support the approach of the former. Reachback capabilities able to contribute from distant stations without deploying to the operational area, such as space and cyber forces, will support both. Moreover, this synergy can result not only from integration within the joint force, but also from integration with foreign military partners contributing various capabilities and capacities to the multinational effort. Joint forces must also be able to integrate with those partners.

The CCJO introduced the idea of *joint synergy*, the combination of Service capabilities such that each enhances the effectiveness and compensates for the vulnerabilities of the others. Joint synergy is the expansion of the idea of combined arms to multiple Services. Joint synergy has been a strength of U.S. joint forces for decades. Whereas joint synergy focuses on the integration of Service capabilities, cross-domain synergy requires the integration

Joint synergy has been a strength of U.S. joint forces for decades. Whereas joint synergy focuses on the integration of Service capabilities, **cross-domain synergy** requires the integration across domains without regard for which Service provides the action or capability.

across domains without regard for which Service provides the action or capability. The concept thus envisions a seamless application of combat power between domains, with greater integration at dramatically lower echelons than joint forces currently achieve.

The level at which capabilities are integrated to achieve cross-domain synergy will range from the component (for example, airborne or amphibious forces securing forward air bases to extend the range of air power) to the low-level tactical (individual aerial, naval, space, cyber, and land-based capabilities cooperating in an attack against a single antiaccess system).

The concept applies to practically any opposed access situation, but its specific application will vary widely depending on the domains in which the enemy operates, the number and type of the enemy's antiaccess and area-denial capabilities, and the level and manner of the integration of those capabilities.

8. Operational Access Precepts

The central idea, cross-domain synergy, describes in the broadest terms how the joint force will gain operational access in the face of armed opposition. The following general principles, when applied to each situation through planning and execution, amplify that basic concept with an additional level of description. They are not a checklist but rather a guide to judgment based on an understanding of the unique factors of any situation. These precepts flow from the conditions and challenges described earlier. Coupled with the central idea of cross-domain synergy, they provide a description of how joint forces will operate to gain access in the face of armed opposition.

Operational Access Precepts

- Conduct operations to gain access based on the requirements of the broader mission, while also designing subsequent operations to lessen access challenges.
- Prepare the operational area in advance to facilitate access.
- Consider a variety of basing options.
- Seize the initiative by deploying and operating on multiple, independent lines of operations.
- Exploit advantages in one or more domains to disrupt enemy antiaccess/area-denial capabilities in others.
- Disrupt enemy reconnaissance and surveillance efforts while protecting friendly efforts.
- Create pockets or corridors of local domain superiority to penetrate the enemy's defenses and maintain them as required to accomplish the mission.
- Maneuver directly against key operational objectives from strategic distance.
- Attack enemy antiaccess/area-denial defenses in depth rather than rolling back those defenses from the perimeter.
- Maximize surprise through deception, stealth, and ambiguity to complicate enemy targeting.
- Protect space and cyber assets while attacking the enemy's space and cyber capabilities.

- **Conduct operations to gain access based on the requirements of the broader mission, while also designing subsequent operations to lessen access challenges.** Since operational access does not exist for its own sake, joint forces should conduct access operations in accordance with the broader objectives and ideally in conjunction with the other elements of national power. Importantly, a joint force commander should avoid over-committing forces or projecting combat power deeper into hostile territory than is required by the objective. This is especially true of major land forces, which can be difficult to withdraw once committed.

At the same time, because of the mounting lethality of emerging antiaccess and area-denial weapons, commanders should design campaigns that do not require attacking into the teeth of an enemy's antiaccess/area-denial defenses where possible. Moreover, due to this lethality, commanders and political leaders should consider the potentially rapid escalatory effect the employment of such weapons in the early stages of a situation could have. Finally, to the extent that other elements of national power can achieve the national objectives, they are preferable to military forces employed in combat because of the risks of the latter in the emerging environment.

- **Prepare the operational area in advance to facilitate access.** As mentioned, the challenge presented by opposed access will be determined largely by conditions created prior to combat. Much of that shaping is a national or even multinational effort, and joint forces will find themselves operating in support of other agencies and departments, in particular the U.S. State Department. Preparing the operational area will be a continuous priority effort for combatant commanders, commencing well in advance of combat and continuing after combat begins, and combatant commanders will have to coordinate with other agencies and departments in that effort.

This precept comprises a wide range of actions designed to strengthen regional partnerships and partners, which include not only foreign militaries but also other agencies and nongovernmental organizations. These actions include engagement activities such as bilateral and multinational exercises to improve multinational operations; key leader engagements; missions to train, advise and equip foreign forces to improve their national ability to contribute to regional access; negotiations to secure basing and transit rights and to establish command relationships, roles and responsibilities, and support agreements; freedom-of-navigation exercises with regional partners; the use of grants and contracts to improve relationships with and strengthen host-nation and other regional partners; and planning conferences to develop multinational plans. Additionally, this effort can include military information support operations and other information activities designed to foster support for U.S. efforts in a region. This effort also can include establishing, improving, and hardening forward and intermediate bases critical to the projection of military force into the region as well as prepositioning supplies and equipment. Finally,

this effort can include the forward deployment of forces, whether conducting security activities on a routine basis or deploying for combat in response to a developing crisis. These steps can all signal U.S. commitment to a region.

The effort to shape advantageous access conditions is part of a larger, long-term effort to improve security cooperation in a region and will benefit from that broader effort. Actions to secure access will be included within each theater and appropriate country security cooperation plan. Even seemingly unrelated missions such as humanitarian assistance can contribute indirectly to securing access by engendering goodwill in the region. That said, commanders must anticipate that agreements made during routine security cooperation may not endure during actual crisis or conflict, and therefore they should develop options based on varying degrees of pre-existing access.

Another critical and continuous effort to improve access conditions in advance will be on-going intelligence, surveillance, and reconnaissance activities to improve situational awareness, both overall and in the various domains, and to uncover adversary antiaccess/area-denial capabilities, plans, and preparations in the region. Operations in space, cyberspace, and across the electromagnetic spectrum likewise will be continuous to ensure that support to navigation, command and control, targeting, sustainment, and intelligence are in place when needed. Moreover, computer network operations, both offensive and defensive, likely will commence long before lethal combat begins and even before combat forces begin to deploy.

- ***Consider a variety of basing options.*** As mentioned, the use of forward bases is a primary means for mitigating the effect of distance on force projection. Forward bases, including mobile seabases, constitute critical “access infrastructure” which supports the deployment of forces and supplies. The greater the capabilities and capacity that can be established at or flowed through the base, the greater the force that ultimately can be projected. Future enemies consequently can increasingly be expected to attack those bases as part of an antiaccess/area-denial strategy in an attempt to restore the penalty of distance. They will employ a variety of means ranging from missiles to terror attack—any of which might employ weapons of mass destruction. Therefore, while undeniably valuable in the context of opposed access, forward bases are maintained at potentially considerable risk.

Since this concept calls for some elements of a joint force to maneuver against key operational objectives directly from ports of embarkation, reliance on forward bases will decrease while also increasing employment options. The greater the proportion of such elements in the joint force, the less an enemy attack on any bases will endanger the mission. This capability is especially valuable in initial assault forces.

Not all forces will be able to deploy directly into combat, however, and

sustained operations eventually will require robust bases in the operational area. Several options exist for resolving this dilemma. The practical solution in any given situation likely will consist of a combination of them. The first option is to protect and harden permanent bases so they can withstand attack and retain their functionality. The loss of a forward base could be catastrophic, and since abandoning a base generally is not politically viable, forward bases must be protected. A second option is to disaggregate large bases into a greater number of smaller bases, decreasing vulnerability through redundancy and complicating the enemy's targeting efforts. This option, however, tends to increase the logistical burden and protection requirements. A third option, in conjunction with disaggregation, is to employ austere temporary bases as opposed to sophisticated permanent bases. The ability to operate effectively from such locations can confer a significant advantage to a joint force. Especially for small or specialized forces, this can include the use of remote or even abandoned bases, airfields, ports, or other military or civilian facilities. Such locations present a less lucrative and less obvious target for the enemy, improving survivability and complicating the enemy's targeting. Moreover, the ability to dismantle and relocate facilities also can improve security and operational flexibility. The disadvantage of such locations is that they tend to lack the capabilities and capacity of permanent installations. The greater the proportion of the force able to operate from austere forward locations, the less will be the threat posed by enemy attack against permanent forward bases—and the greater will be the operational choices. A fourth option is the use of seabasing,¹⁴ which reduces sovereignty issues that often can preclude the establishment of forward bases. The inherent mobility of seabasing can complicate the enemy's defensive preparations by making the objective remain ambiguous through holding a large coastal area at risk. It can enhance security by complicating the enemy's detection and targeting. Seabasing options may be limited by capacity. One other option is to emphasize capabilities with minimal dependence on forward bases, such as amphibious, long-range strike, cyber, electronic, or space capabilities, either in primary or supporting roles.

- ***Seize the initiative by deploying and operating on multiple, independent lines of operations.*** Seizing and maintaining the initiative is critical to any combat operation. One key advantage of U.S. joint forces over most potential enemies is their ability to manage complex operations. Operating on multiple lines in multiple domains simultaneously can help joint forces to seize that initiative by overloading an enemy's ability to cope. Moreover, it increases friendly employment options while forcing the enemy to

¹⁴ **Seabasing:** "The deployment, assembly, command, projection, reconstitution, and re-employment of joint power from the sea without reliance on land bases within the operational area." *Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 17Jan11].

defend multiple avenues of approach, especially if the joint force is not dependent on major infrastructure nodes but has the ability to operate effectively in austere environments. Operating on multiple lines also improves a joint force's ability to exploit unforeseen opportunities and to overcome setbacks. Finally, the dispersal of joint forces also will mitigate the risk posed by enemy weapons of mass destruction.

Correspondingly, this concept envisions that future joint forces will organize tactically into tailored joint formations able to deploy, operate, and survive autonomously. For land forces especially, this suggests smaller units and platforms that are rapidly deployable yet lethal. This concept sees deployment and combat as a single evolution of parallel actions rather than as distinct and sequential phases. Each formation will operate in multiple domains as required. While maneuvering independently, they will maintain the ability to concentrate smoothly into larger formations as necessary. While they will be self-contained with respect to the envisioned mission, the joint force will be able to support them quickly with external capabilities as needed—principally additional air, space, electronic, and cyberspace capabilities, which can best mitigate the latency imposed by distance.

Such distributed operations will place a burden on both command and control and sustainment, as Section 9 will discuss.

- ***Exploit advantages in one or more domains to disrupt enemy antiaccess/area-denial capabilities in others.*** Joint forces will attempt to identify and exploit any domain mismatches, seeking to apply relative strength against weakness both within and between those domains in which joint forces enjoy advantages. Gaining superiority in any given domain is not merely a matter of operations in that domain. One of the great asymmetrical advantages of joint forces over most potential enemies is their potential to bring combat power to bear across domains, often in complementary and reinforcing combinations that prevent the enemy from countering effectively. Operating initially in unopposed or lightly opposed domains as described above, joint forces will apply combat power to gain superiority in other contested domains in pursuit of the combination that will provide the overall freedom of action necessary to accomplish the mission.

The decision on which domains to operate in initially will depend on the mission and the enemy's capabilities and vulnerabilities in the various domains; there is no universal sequence. That said, joint force projection almost always will include the early conduct of information operations and operations in space and cyberspace, since freedom of action in those latter domains is increasingly important to all joint operations. Moreover, those operations rarely require the additional risks incurred in deploying forces to the operational area. In fact, information, space, and cyberspace operations generally should commence well before the need for combat, as part of efforts

to shape the operational area.

Low-signature forces in all domains are especially key for early penetration of an enemy's antiaccess/area-denial defenses before they have been degraded. Where geography supports it, the undersea environment is a potentially valuable place to project military force with limited exposure to enemy fires. Undersea forces tend to operate in a dispersed manner and have only limited vulnerability to forces operating in other domains. Undersea warfare is especially valuable in gaining maritime superiority, although undersea forces also could bring naval power to bear against other domains through the use of land-attack missiles or electronic attack. The air is another domain generally suitable for the early focus of effort, again because air forces tend not to operate in massed formations that make them vulnerable to catastrophic loss and because they tend to be broadly effective in bringing power to bear rapidly against other domains. Finally, special operations forces are valuable for locating, targeting, and destroying key enemy capabilities, as well as for cultivating indigenous resistance elements that can help disrupt the antiaccess/area-denial strategy. Like space and cyberspace forces, special operations forces likely will be in position, often operating in denied territory, in advance of the commitment of major forces to set the conditions for the employment of those forces. Operations to maintain or gain access in the maritime commons can build on these low signature operations, avoid high density threat antiaccess weapons, and maneuver to achieve surprise and rapid operations.

In contrast, large land forces generally will be the last to penetrate within range of an enemy's antiaccess and area-denial weapons because of the potential for catastrophic loss. That is not irrevocably true however. Land forces, for example, could be used to seize advanced bases on the outskirts of an enemy's defenses from which to project air and naval power into the heart of those defenses. Moreover, small land or surface naval forces, to include special operations forces, could infiltrate an enemy's antiaccess defenses undetected.

The sequence of expansion into additional domains will depend on a variety of factors. Access to space, cyberspace, and the electromagnetic spectrum generally will not rely on superiority in other domains as a precondition. In contrast, access to the land domain and, to a lesser extent, the surface maritime domain (at least within range of an enemy's antiaccess capabilities) very often will. In almost all cases, air is an important domain in which to expand because airpower generally can be brought to bear responsively to most other domains and air superiority often is a precondition to gaining access to the land and sea within a contested operational area.

- ***Disrupt enemy reconnaissance and surveillance efforts while protecting friendly efforts.*** The reconnaissance/counterreconnaissance fight is a critical multidomain contest in any combat operation to gain operational

access, as each combatant attempts to gain better situational awareness than the other. The joint force likely will start at an intelligence disadvantage as it moves into an enemy's home areas, a situation likely to be exacerbated as the enemy disposes antiaccess and area-denial capabilities from concealed positions, often hidden in complex environments. The disadvantage can be mitigated to some degree through intelligence provided by forward-deployed forces. The joint force will require a major intelligence, reconnaissance, and surveillance effort applied aggressively, to include fighting for information, to overcome those disadvantages. Conversely, it will need to degrade the enemy's situational awareness through a combination of attacking his reconnaissance and surveillance operations and confounding his collection efforts through deception and concealment.

- **Create pockets or corridors of local domain superiority to penetrate the enemy's defenses and maintain them as required to accomplish the mission.** It is not necessary to achieve domain superiority permanently in a given domain throughout the operational area to accomplish the mission. Although joint forces in recent decades usually enjoyed such superiority—or even supremacy—future joint forces often may not. A joint force commander who waits for that condition will likely surrender the initiative and miss opportunities. Rather, by using the asymmetrical advantages and cross-domain synergy described above, future joint forces will open limited pockets or corridors of superiority in the necessary domains and maintain them long enough to accomplish required tasks.

This concept envisions the joint force managing the fluid opening and closing of access corridors over time and space as needed. It is not enough merely to open one of these corridors in the enemy antiaccess/area-denial defenses; the joint force must maintain it as well, although it may not be necessary to maintain it for the entire duration of a mission as long as it can be re-opened as needed. It is important, however, that forces that have penetrated into the depth of the enemy defenses not be left in an unsupportable position.

- **Maneuver directly against key operational objectives from strategic distance.**¹⁵ Some elements of the joint force will operate directly against key objectives from points of origin or other points outside the theater without the need for forward staging.¹⁶ Not being tied to fixed forward bases will increase

¹⁵ Headquarters, Department of the Army, FM 3-0, *Operations* (Washington, DC, 27Feb08), paragraphs. 8-2 through 8-4. *Strategic distance* refers to action originating from outside an operational area, often from home station.

¹⁶ **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." See also origin:

operational flexibility while complicating enemy defensive preparations. The greater the proportion of such elements in the joint force, the less will be the overall burden on such bases and the less vulnerable the joint force will be to a successful attack against those bases. Moreover, avoiding intermediate staging en route can increase tempo by eliminating operational pauses. This is another capability that is especially valuable in initial assault forces.

Not all elements of the force will be able to operate this way, however. Where forward basing is an operational necessity, the joint force may be required to seize and operate temporary or permanent forward operating locations or operate from a seabase. Seizing such bases may be a mission best suited to elements able to maneuver as described above.

- ***Attack enemy antiaccess/area-denial defenses in depth rather than rolling back those defenses from the perimeter.*** This concept envisions that joint forces will attempt to penetrate into the depth of an enemy's antiaccess/area-denial defenses. To do this, they will exploit and expand any domain advantages and maximize cross-domain synergy as described above. Additionally, they naturally will take advantage of any identified gaps in the enemy defenses. The penetration is designed to disrupt the integrity of the enemy defensive system, the preferred defeat mechanism, by striking at critical hostile elements, such as logistics and command and control nodes, long-range firing units, and strategic and operational reserves.¹⁷

The historical alternative to this approach is to attack the perimeter of the enemy's defenses, pushing back those defenses while advancing. Such an approach operates primarily by attrition and does not threaten the integrity of the enemy's defensive system, but rather merely compresses those defenses as they fall back. This may actually play into the enemy's antiaccess/area-denial strategy, which likely will attempt to use space and time to inflict cumulatively unacceptable casualties on an advancing joint force.

While striking enemy antiaccess/area-denial capabilities in depth, a joint force should also attempt to neutralize the enemy's ability to do the same to it, attacking those capabilities the enemy could employ to attack U.S. command and control, sustainment, and lines of communication.

"Beginning point of a deployment where unit or non-unit-related cargo or personnel are located." Dictionary of Military Terms, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 20Apr11].

¹⁷ That said, the potentially escalatory effects of strikes into an adversary's homeland must be carefully weighed against U.S. political objectives and acceptable risk. Such escalation is particularly likely when the conflict is distant from the US homeland, and there has been no corresponding attack on US territory. In these cases, the probability and risk of reprisal attacks against the continental United States must be considered.

- **Maximize surprise through deception, stealth, and ambiguity to complicate enemy targeting.** Surprising the enemy is always a virtue in war. Given the vulnerability of deploying joint forces to increasingly lethal antiaccess and area-denial weapons, surprise arguably is even more valuable—indeed, possibly even essential—in the context of future opposed access, and future commanders should spare no effort to achieve it by any available means. That said, while the desire to surprise may be as great as ever, the ability to surprise rests ultimately on the enemy’s susceptibility to being surprised. This will be problematic in a future operating environment increasingly characterized by pervasive sensors and information transparency. This paper therefore carefully distinguishes among three basic ways to achieve surprise: deception, stealth, and ambiguity.¹⁸

For the purposes of this paper, *deception*¹⁹ means convincing an enemy that the joint force will adopt one course of action while adopting another. Successful deception therefore depends less on one’s own efforts than on the enemy’s inclination to accept misleading evidence. In other words, successful deception tends to be less about creating false expectations than about understanding and exploiting enemy expectations that already exist. Skillful deception therefore will always be an art form that depends on the existence of an alternative course of action that appears likely to the enemy. Successful deception will be difficult in the future opposed access environment, although when achieved deception tends to have the greatest effect among the three methods of surprise. In the context of future opposed access, forms of deception that could prove especially useful include electromagnetic deception²⁰ and cyber deception, which could provide intentionally erroneous information on the location and activities of deploying joint forces to enemy intelligence networks.

Stealth means denying the enemy information about friendly capabilities, intentions, or dispositions. (Stealth in this context should not be confused with “stealth” technology, which is only one means of achieving stealth.) The

¹⁸See Marine Corps Doctrinal Publication (MCDP) 1, *Warfighting* (Washington: HQMC, 1997), pp. 43-44.

¹⁹**Deception:** “Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests.” See also military deception—“Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.” *Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 3Dec10].

²⁰**Electromagnetic deception:** “The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability.” *Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 3Dec10].

enemy is not deceived as to friendly plans, but is ignorant of them. Again, achieving stealth in a transparent operating environment characterized by pervasive sensors and information networks will be extremely challenging, although U.S. forces should continue to pursue technologies and other means that offer potential opportunities to restore stealth to the battlespace.

The third basic method for achieving surprise is through *ambiguity*. Joint forces achieve ambiguity by operating in a way that supports multiple courses of action and therefore forces the enemy to prepare for all of them. In a future opposed access environment characterized by information transparency—indeed often by information overload—ambiguity may be the single method of surprise offering the best potential for success. This concept supports ambiguity in two important ways. First, the idea of operating on multiple, self-contained lines of operations provides multiple options for a joint force and compels an enemy to defend on multiple axes. Second, since reliance on fixed forward bases tends to commit a force to certain lines of operation, the idea of maneuvering against key objectives directly from ports of embarkation without reliance on such bases similarly enables a joint force to appear ambiguous as to its ultimate objectives.

While conceptually distinct, these three methods can tend to blur in practice. And while depending entirely on either deception or stealth for future surprise could prove risky, this concept envisions that some artful combination of the three could be an essential element of future joint operations to gain access in the face of armed opposition.

- ***Protect friendly space and cyber assets while attacking the enemy's space and cyber capabilities.*** Space and cyberspace are now essential to all joint force projection, both for the support they provide to operations in the other domains and as operational domains in their own right when directed. The former provides critical position, navigation, and timing, command and control, missile warning, weather, and intelligence collection. The latter supports an increasing proportion of joint command and control and logistics functions. For just this reason, most enemies adopting an antiaccess/area-denial strategy will attack joint space and cyberspace operations in an attempt to disrupt force projection efforts. In fact, many enemies may try to disrupt U.S. use of space and cyberspace—commercial as well as governmental—well before the onset of lethal combat. The same can be said about the electromagnetic spectrum generally, which is especially critical in the context of force projection given the distances involved—although that is hardly a new phenomenon.

For this reason, efforts to gain and maintain adequate space and cyberspace superiority, as well as ensure use of the electromagnetic spectrum, will be a continuous part of preparing the operational area for access. Both counterspace and counter cyberspace operations are appealing to many

potential enemies because attacks can be comparatively inexpensive and often are difficult to attribute. For these reasons, a joint force conducting force projection must protect its access to space and cyberspace capabilities. That is not to say that losses will not occur. As in any other domain, losses are inevitable, and joint forces projecting military force must be prepared to operate effectively despite such losses.

Similarly, many potential enemies increasingly rely on space and cyber capabilities, both of which are relatively affordable when purchased commercially. In the context of antiaccess and area-denial, both can be critical to an enemy's targeting capability and therefore an important part of an antiaccess/area-denial strategy. Degrading an enemy's cyber and space capabilities therefore can be a critical part of gaining and maintaining operational access. Developing good cyberspace and space situational awareness²¹ will be critical to both protecting friendly and degrading enemy capabilities.

Specific critical tasks include, but are not limited to, protecting friendly satellite communications and ensuring friendly position, navigation, and timing support while denying the enemy the same.

Gaining space and cyberspace superiority when and where needed is not necessarily a symmetrical effort—that is, cyberspace operations to gain cyberspace superiority and space operations to gain space superiority—but often can be achieved more effectively, like superiority in the other domains, through the cross-domain application of combat power.

9. Joint Operational Access and the Joint Functions

This concept has implications for the performance of the various joint functions.²² Attaining cross-domain synergy will require effective application of the joint functions across the five domains and often will require integration with interagency and foreign partners.

²¹ **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.” *Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 24Jan11].

²² **Joint functions:** “Related capabilities and activities grouped together to help joint force commanders synchronize, integrate, and direct joint operations. Functions that are common to joint operations at all levels of war fall into six basic groups - command and control, intelligence, fires, movement and maneuver, protection, and sustainment.” *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 18Nov10].

- **Command and control.** This concept will put a heavy burden on command and control. The command and control system²³ must support forces operating at global distances, deploying and maneuvering independently on multiples lines of operations from multiple points of origin, and concentrating fluidly as required. It must support an operating tempo the enemy cannot match and facilitate integration across multiple domains simultaneously and at lower echelons. The synergy that is central to this concept will require a high degree of integration and synchronization in planning and execution across domains, not only at the component level, but at lower echelons as well. The joint command and control system will have to include techniques, procedures, and technologies that enable commanders to integrate operations across domains in innovative ways.

To support high-tempo distributed operations and to cope with a degraded command and control environment, this concept envisions decentralized command and control to the extent possible in both planning and execution. Such mission command²⁴ enables subordinate commanders to act independently in consonance with the higher commander's intent and effect the necessary cross-domain integration laterally at the required echelon. While distributed-collaboration technologies can facilitate this effort, commanders also must be prepared to operate effectively in a degraded environment. The ability to do so has implications for doctrine, training, and education.

The adversary will deliberately attempt to degrade friendly use of the electromagnetic spectrum, to include disruption of space and cyber systems. Due to heavy joint reliance on advanced communications systems, such an attack will be a central element of any enemy antiaccess/area-denial strategy, requiring a higher degree of protection for friendly command and control systems.

Especially with respect to incorporating space and cyberspace operations in a joint access campaign, new and adaptable relationships and authorities may be required to better integrate the capabilities of geographic and functional combatant commands with overlapping responsibilities. Moreover, combat operations may commence immediately upon deployment and may

²³ **Command and control system:** "The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the missions assigned." *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 14Jan11].

²⁴ **Mission command:** "The conduct of military operations through decentralized execution based upon mission-type orders." See also **mission-type** order: "1. An order issued to a lower unit that includes the accomplishment of the total mission assigned to the higher headquarters. 2. An order to a unit to perform a mission without specifying how it is to be accomplished." *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/dod_dictionary/ [accessed 9Jun11].

span multiple areas of responsibility en route to the operational area, creating the need for a single campaign across traditional boundaries and requiring a re-examination of command relationships and methods and timing for establishing a joint task force.

- **Intelligence.** Given the increased lethality, precision, and accuracy of antiaccess and area-denial systems, the joint force requires the ability to collect, fuse, and share accurate, timely, and detailed intelligence across all domains. Furthermore, this intelligence collection, fusion, and sharing may include interagency and multinational partners. All of this will require a reexamination of the current classification, access, and data sharing protocol restrictions.

Intelligence remains a critical contest in an access/antiaccess battle with each combatant trying to gain necessary intelligence while denying the other. The joint force must be prepared to fight for information rather than expecting uncontested collection and may begin operations at a disadvantage. Characterizing an adversary is a continuous activity, commencing years before hostilities begin and continuing during and after those hostilities. This has implications for steady state sizing, systemic capacity, and analytic technologies of intelligence forces. Specifically, the reconnaissance and surveillance contest is critical to access operations.

This concept's preference for disruption over attrition will require intelligence not only about the location of enemy elements, but also about how those elements work together as a coherent system, including their potential for cross-domain cooperation.

- **Fires.** Defeating opposed access will require lethal and nonlethal fires applied flexibly and responsively between domains. The emphasis on cross-domain synergy that is central to this concept applies first and foremost to fires. Although current capabilities provide some measure of flexibility and responsiveness, this concept envisions a qualitative improvement in these attributes. Achieving this objective increases the need to adopt flexible procedures for requesting, approving, and coordinating fire support among the Services and, possibly, among combatant commands.²⁵ Target acquisition must be rapid and accurate, and procedures must be developed to minimize the latency or delay between identification and engagement of potentially fleeting critical targets.

Gaining operational access against armed opposition will remain a

²⁵ While tactical or operational control of some counterspace and counter cyber "fires" may be delegated to the joint force commander engaged in an operational access mission, some of these fires may be employed by a supporting commander (e.g., Commander, U.S. Strategic Command).

classic fire-and-maneuver problem, albeit often on a large scale. Joint forces must be able to concentrate or distribute fires quickly as the situation requires based on the needs of maneuvering forces. This concept envisions that any element maneuvering independently will have responsive access to the necessary joint fires, regardless of echelon or Service. Such access will depend on the ability to ensure the necessary communications in a potentially degraded information environment.

Although reliance on precision-guided munitions to attack selected targets will increase, the inventory of such munitions will remain finite, and joint forces attacking a prepared antiaccess/area-denial defense often will lack the precise targeting information required to justify their expenditure. Moreover, joint forces will continue to require accurate area fires to neutralize, suppress, and obscure targets to protect friendly forces and facilitate maneuver. While the *Joint Combat Concept* (JCC) emphasizes the need for discrimination, commanders at every echelon will need to reconcile that requirement with the significant threat posed by a capable antiaccess/area-denial system.

This concept envisions that lethal and nonlethal fires in all five domains will be managed within the same targeting and fire support coordination systems. While that is true today for traditional nonlethal fires such as electronic jamming, it may not be true for certain cyber and space capabilities, which today are controlled by supporting functional combatant commands. This concept envisions that control of such capabilities in the future will devolve to lower echelons to make the fires more responsive to the needs of operational commanders. The precise level to which that control can appropriately devolve remains to be determined.

- **Movement and maneuver.** This concept envisions the fluid, adaptive maneuver of joint force elements as they advance on the objective area, operate within it, and conduct retrograde operations in an antiaccess/area-denial environment.

Self-contained joint elements, supported by joint fires, will move independently on multiple lines of operations from multiple ports of embarkation, rerouting as necessary en route, concentrating quickly against key objectives, and dispersing again as the situation requires. These maneuver elements will make maximum use of deception, stealth, and ambiguity to mask their movements and reach their operating areas without unacceptable risk or losses. Air and naval forces will maneuver in simultaneous and complementary movements as they advance. Where geography allows, land forces likewise will maneuver against intermediate land objectives to facilitate the continued advance of those naval and air forces before maneuvering against objectives in the objective area through forcible entry if the mission requires.

Some portion of the joint force will be able to maneuver directly against key objectives from ports of embarkation, without reliance on fixed intermediate or forward bases, identifying and changing those objectives en route. This will put a premium on en route communications for command and control.

Space and cyber forces will “maneuver” as necessary to conduct and support operations in advance, and will maintain or improve their positions as the situation develops. Joint forces likewise will “maneuver” in cyberspace by penetrating hostile digital networks.

- **Protection.** Protecting the joint force will be critical to ultimate success since most enemy antiaccess/area-denial strategies will operate on the principle of attrition. Protection against antiaccess and area-denial capabilities will pose different challenges. While all protection schemes will involve a combination of active and passive measures to defeat enemy attack, protecting against antiaccess weapons will place a greater emphasis on minimizing the exposure of the force during its advance toward the objective area, when many elements of the force are most vulnerable. A joint force will lessen its exposure by a combination of dispersion, multiple lines of operations, speed of movement, agile maneuver that reroutes around threats, deception, masking or other concealment techniques, and disruption of enemy intelligence collection through counterreconnaissance, countersurveillance, and other methods. Once arrived in the objective area, joint force elements can no longer use some techniques to avoid detection and will therefore rely on active and passive defensive measures to defeat actual enemy attack.

Protecting joint force command and control will demand special emphasis because this is a critical function against which many enemies will concentrate their targeting. To protect command and control systems, the joint force must develop systems, technologies, and warfighting techniques to ensure continued freedom of action and access to space, cyberspace, and the electromagnetic spectrum when and where needed.

Protecting logistics will include protecting logistical bases, distribution activities, and logistics networks and associated data. Several options exist for base protection. These include hardening of bases to withstand attack, distributing the functions of a base into smaller, more numerous and temporary installations to mitigate the effects of an attack, and employing mobile seabasing where possible. Any operational solution likely will include some combination of these options.

Of growing concern to future joint forces will be missile defense and defense against sabotage—the former because of the increasing availability of and dramatic improvements in missiles and the latter because many enemies will see it as an inexpensive capability with the potential for disproportionately

large results. In both cases, defense against the capability tends to be much more costly than the capability itself.

- **Sustainment.** Because of the logistically intensive nature of force projection, effective sustainment will be critical to future joint force success—and therefore a likely target for enemy attack. Joint forces will require new sustainment concepts that account for adversary capabilities. These innovations may require new platform designs, more robust information networks, and the ability to more rapidly reach distributed combat forces operating in contested areas.

The distributed nature of operations described in this concept will especially strain the distribution system and its command and control. Commanders will require a robust and flexible system that allows them quickly to move, support, and sustain forces that may be in multiple locations with multiple objectives. In support of those units that maneuver directly against operational objectives from strategic distance, this concept envisions a merging of the intertheater and intratheater segments of the global distribution pipeline. Logistics commanders will require full visibility of all requirements, resources, and capabilities throughout the full length of that pipeline to effect the level of coordination required to support the operations described.

This concept envisions a sustainment system comprising a combination of basing options, the prepositioning of equipment and supplies, and a flexible, protected distribution process. Establishing such a system will be a key part of preparing the operational area for access. This concept envisions no breakthrough advancement that will dramatically change the sustainment challenge. Rather, it envisions incremental efficiencies in three areas. First, decrease the logistical appetite of joint forces in all classes of supply, but especially in fossil fuels. Second, improve supply chain management by increasing visibility of both expenditure rates and available inventory levels. Improvements in these areas will support command decision-making (that said, warfare is an especially wasteful and unpredictable activity, and the joint force cannot expect and should not attempt to manage the distribution system with anything approaching the efficiency of the business world). Third, improve the capabilities and capacities of U.S. military airlift and sealift. This may include developing lift assets that would not be perceived as catastrophic losses if destroyed and those that provide options for maneuvering within an area-denial environment. Innovative solutions such as lighter-than-air craft may ease the lift challenge.

In some situations, it may be preferable for joint forces to sustain themselves via seabases, which increases employment options by decreasing reliance on airfields and other ashore sustainment infrastructure. Large-scale distribution from a seabase will require new capabilities and capacities. Ship-to-ship and ship-to-shore connectors will be required for the configuration and

distribution of a broad variety of sustainment packages, under challenging sea states and in support of continuous sustainment demands.

Given limitations in organic logistical resources, operations to gain operational access may have to rely on the contracted use of commercial service providers. Joint forces will require the expeditionary ability to access such support, from identifying support requirements and potential providers to letting contracts and managing the associated contractor personnel. Additionally, commanders must be able to direct contractors, who currently require direction from government contracting officers, furnish support for contractors in their operational areas, and manage risks associated with contractor nonperformance. Moreover, inadvertently awarding contracts to local entities with ties to the enemy is a real concern that requires close attention to contractor vetting. In the event of significant attacks on staging bases, logistics facilities and other locations with significant contracted capabilities, retention and protection of civilian contractors may become a critical challenge.

To meet the challenges of opposed access, the survivability of the joint sustainment system will be critical. For land-based logistics especially, the challenge will be to ensure the survivability of the infrastructure. As noted above, this concept envisions enhanced joint force protection capabilities through some combination of hardening, dispersal, redundancy, and mobility of the infrastructure and the logistics network. This concept further envisions that a greater portion of joint combat power will likely be dedicated to protecting distribution activities—although this will occur at the expense of forces available to attack the enemy’s antiaccess/area-denial defenses and at some point such a shift can imperil the overall mission.

10. Capabilities Required by this Concept

The following capabilities have emerged as essential to the implementation of this concept. They derive logically from the concept itself or from accompanying experimentation. This list is neither all-encompassing nor prioritized. It is designed merely to provide a baseline for follow-on concept development, analysis, and experimentation. Although grouped by joint function for ease of understanding, many of these capabilities apply across multiple joint functions. (While information and engagement are not joint functions, they have been added as categories because several of the capabilities fall within those groupings.) Furthermore, many of these capabilities have implications for DOTMLPF as well as for integration with interagency and foreign partners.

Command and Control

- JOA-001. The ability to maintain reliable connectivity and interoperability among major warfighting headquarters and supported/supporting forces while en route.
- JOA-002. The ability to perform effective command and control in a degraded and/or austere communications environment.
- JOA-003. The ability to create sharable, user-defined operating pictures from a common database to provide situational awareness (including friendly, enemy and neutral situations) across the domains.
- JOA-004. The ability to integrate cross-domain operations, to include at lower echelons, with the full integration of space and cyberspace operations.
- JOA-005. The ability to employ mission command to enable subordinate commanders to act independently in consonance with the higher commander's intent and effect the necessary cross-domain integration laterally at the required echelon.

Intelligence

- JOA-006. The ability of operational forces to detect and respond to hostile computer network attack in an opposed access situation.
- JOA-007. The ability to conduct timely and accurate cross-domain all-source intelligence fusion in an opposed access situation.
- JOA-008. The ability to develop all categories of intelligence in any necessary domain in the context of opposed access.

Fires

- JOA-009. The ability to locate, target, and suppress or neutralize hostile antiaccess and area-denial capabilities in complex terrain with the necessary range, precision, responsiveness and reversible and permanent effects while limiting collateral damage.
- JOA-010. The ability to leverage cross-domain cueing to detect and engage in-depth to delay, disrupt or destroy enemy systems.
- JOA-011. The ability to conduct electronic attack and computer network attack against hostile antiaccess/area-denial capabilities.
- JOA-012. The ability to interdict enemy forces and materiel deploying to an operational area.

Movement and Maneuver

- JOA-013. The ability to conduct and support operational maneuver over strategic distances along multiple axes of advance by air and sea.

- JOA-014. The ability to “maneuver” in cyberspace to gain entry into hostile digital networks.
- JOA-015. The ability to conduct en route command and control, mission planning and rehearsal, and assembly of deploying forces, to include linking up of personnel and prepositioned equipment.
- JOA-016. The ability to conduct forcible entry operations, from raids and other limited-objective operations to the initiation of sustained land operations.
- JOA-017. The ability to mask the approach of joint maneuver elements to enable those forces to penetrate sophisticated antiaccess systems and close within striking range with acceptable risk.

Protection

- JOA-018. The ability to defeat enemy targeting systems, including their precision firing capabilities.
- JOA-019. The ability to provide expeditionary missile defense to counter the increased precision, lethality, and range of enemy antiaccess/area-denial systems.
- JOA-020. The ability to protect and, if necessary, reconstitute bases and other infrastructure required to project military force, to include points of origin, ports of embarkation and debarkation, and intermediate staging bases.
- JOA-021. The ability to protect forces and supplies deploying by sea and air.
- JOA-022. The ability to protect friendly space forces while disrupting enemy space operations.
- JOA-023. The ability to conduct cyber defense in the context of opposed access.

Sustainment

- JOA-024. The ability to deploy, employ, and sustain forces via a global network of fixed and mobile bases to include seabasing.
- JOA-025. The ability to quickly and flexibly establish nonstandard support mechanisms, such as the use of commercial providers and facilities.
- JOA-026. The ability to plan, manage, and integrate contractor support in the context of operations to gain operational access in the face of armed resistance.

Information

JOA-027. The ability to inform and influence selected audiences to facilitate operational access before, during, and after hostilities.

Engagement

JOA-028. The ability to develop relationships and partnership goals and to share capabilities and capacities to ensure access and advance long-term regional stability.

JOA-029. The ability to secure basing, navigation, and overflight rights and support agreements from regional partners.

JOA-030. The ability to provide training, supplies, equipment, and other assistance to regional partners to improve their access capabilities.

11. Risks of Adopting this Concept

Adopting this approach for gaining and maintaining operational access in the face of armed resistance is not without risks.

- ***The most serious of these is that joint forces fail to achieve the synergy that is essential to this concept.*** This concept rests on the premise of cross-domain synergy, but merely combining Service capabilities across domains does not ensure synergy. To mitigate this risk, commanders should be aware of that reality and consciously take steps to create the conditions under which synergy can emerge. That said, commanders should keep in mind that achieving synergy by itself does not guarantee victory.

- ***Likewise, joint forces may not be able to achieve the necessary coordination required to apply combat power effectively across domains, again negating the concept's central premise.*** The cross-domain application of combat power relies on the ability to coordinate between those domains, which may be difficult in a degraded command and control environment. The mitigation to this risk is to maintain the ability to fall back on intradomain and Service-specific capabilities.

- ***Similarly, the concept's emphasis on cross-domain combat power could be misread by resource allocators to suggest significantly less need for organic self-sufficiency.*** Such an outcome would be dangerous if degraded command and control prevents cross-domain integrations, leaving elements to their organic capabilities. Mitigating this risk requires maintaining a sensible balance between organic capabilities and those accessible only through external support, together with robust and redundant means for

requesting and coordinating that support.

- ***The concept's conditional preference for disruption could lead commanders and staffs to waste valuable time and energy in search of precise disruption mechanisms even when the nature of the enemy or the conditions of warfare preclude such a diagnosis.*** This risk, inherited from the JCC, misinterprets the concept, which acknowledges the peril of relying solely on disruption and instead affirms the need for whatever attrition may be required to defeat an enemy's antiaccess/area-denial defense. Commanders must balance these mechanisms based on a sound understanding of the situation.

- ***The concept's call for integrating simultaneous actions across multiple domains on multiple lines of operations could lead to joint operations of debilitating complexity.*** The friction of military conflict urges simplicity and punishes unnecessary complexity, but operations to overcome opposed access are complex by nature. Commanders must be alert to this tension and must continuously strive for the proper balance.

- ***The concept's reliance on deep, precise strikes to neutralize enemy antiaccess and area-denial weapons before they can inflict significant losses may be unrealistic in the time frame of the concept.*** Locating, targeting and defeating such systems effectively from a distance remains a very difficult challenge, from the perspectives of both target intelligence and weaponing. If such hostile systems cannot be neutralized, the successful execution of the concept could be at risk.

- ***The concept could be logistically unsupportable.*** The concept's call for multiple operationally self-contained formations operating independently imposes a logistical burden, but the concept offers no direct remedies other than improved efficiency. To mitigate this risk, commanders must remain aware of the logistical burden imposed by the concept of operations and must be prepared to adjust the concept accordingly. Likewise, force developers must seek to reduce logistical demand throughout the force.

- ***The concept could be economically unsupportable in an era of constrained Defense budgets.*** In its fullest form, this is a resource-intensive concept. The emphasis on cross-domain synergy implies a degree of joint interdependence at relatively low echelons that will demand a robust command and control system and a major investment in frequent and realistic training for those forces. The emphasis on distributed, independent lines of operations will tend to demand greater numbers of smaller, but still capable, platforms, while also increasing lift and sustainment requirements. The very nature of opposed access argues for additional organizational strength to account for higher casualty levels than joint forces have suffered in decades.

- ***Current national policy may not support operational requirements.***

This concept advocates attacking the full depth of an enemy's antiaccess/area-denial defenses rather than merely their perimeter. At times, that will require strikes deep into the sovereign territory of other nations. Policy guidance may restrict such strikes, especially if an enemy emplaces antiaccess/area-denial systems in populated areas or possesses nuclear weapons and escalation is a strategic concern. Moreover, this concept calls for early preparatory actions in the space and cyberspace domains. Under current policy, authorization for such actions might not be forthcoming, especially in pre-crisis stages. In any case, the mitigation is to work with policy makers to ensure that operational requirements are clearly understood and accounted for.

- ***Gaining and maintaining operational access in the face of armed resistance is inherently fraught with risk.*** This is the nature of any opposed access mission and not a risk specific to this concept in particular, but it is worth stating nonetheless. The future antiaccess/area-denial environment will demand accepting higher levels of calculated risk. Calculated risk is not reckless; prudent consideration and actions to protect the force are an enduring requirement. When national interests are not at stake, risk calculation rightly favors the expenditure of time and resources to minimize casualties. Ultimately though, war is a dangerous enterprise and a force conditioned to avoid risk develops habits that may leave it disadvantaged against an opportunistic, willful, and risk-accepting adversary. Therefore, the joint force must continuously evaluate risk while simultaneously recognizing and exploiting or creating opportunities inside the adversary's decision cycle. It is just this opportunistic advantage, gained through cross-domain synergy that is proposed for mitigating the risk in the antiaccess/area-denial environment.

12. Conclusion

Joint forces must be able to project military force into any operational area in the face of armed opposition in support of national interests. This is not a new challenge, but it is one that U.S. joint forces have not been called upon to face in recent decades. That condition likely is changing, and the ability to overcome opposed access may prove to be of critical importance in coming years. While the nature of force projection has not changed, three emerging trends will impact its future conduct: dramatic improvement and proliferation of antiaccess/area-denial capabilities, changing U.S. overseas defense posture, and the emergence of space and cyberspace as increasingly important and contested domains.

To meet this challenge, future joint forces will leverage *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—to establish superiority in some combination of domains that will provide the freedom of action required by the mission. The central idea describes in the broadest terms how the joint force will gain operational access in the face of armed opposition. The supporting precepts amplify that basic concept with an additional level of description. Operationalizing this concept will result in implications across the joint functions and will require the development and implementation of essential capabilities. The capability and capacity implications of this approach are potentially profound.

ANNEX A GLOSSARY

Unless otherwise stated, all definitions are from “DOD Dictionary of Military Terms,” http://www.dtic.mil/doctrine/dod_dictionary/.

airborne. In relation to personnel, troops especially trained to effect, following transport by air, an assault debarkation, either by parachuting or touchdown.

air superiority. That degree of dominance in the air battle of one force over another that permits the conduct of 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.

air supremacy. That degree of air superiority wherein the opposing force is incapable of effective interference.

amphibious force. An amphibious task force and a landing force together with other forces that are trained, organized, and equipped for amphibious operations. Also called AF.

antiaccess. Those capabilities, usually long-range, designed to prevent an advancing enemy from entering an operational area. [JOAC]

area-denial. Those capabilities, usually of shorter range, designed not to keep the enemy out but to limit his freedom of action within the operational area. [JOAC]

assured access. The unhindered national use of the global commons and select sovereign territory, waters, airspace and cyberspace, achieved by projecting all the elements of national power. [JOAC]

combat. A category of military activity that aims to defeat an armed enemy through the application of force. [CCJO]

combined arms. More than one tactical branch, arm or specialty of a single Service employed together in operations. [Adapted from AR 310-25, *Dictionary of U.S. Army Terms*]

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

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. [JOAC]

cyber defense. The integrated application of DoD or U.S. Government cyberspace capabilities and processes to synchronize in real-time the ability to detect, analyze and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend designated networks, protect critical missions, and enable U.S. freedom of action. Cyber defense includes:

- Proactive NetOps: (e.g., configuration control, information assurance (IA) measures, physical security and secure architecture design, intrusion detection, firewalls, signature updates, encryption of data at rest);
- Defensive Counter Cyber (DCC): Includes: military deception via honeypots and other operations; and redirection, deactivation, or removal of malware engaged in a hostile act/imminent hostile act;
- Defensive Countermeasures.

[From “Joint Terminology for Cyberspace Operations,” VCJCS memo for the Service chiefs, combatant commanders and directors of Joint Staff directorates, undated.]

cyberspace. 1. A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [JP 1-02] 2. Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. [From “Joint Terminology for Cyberspace Operations,” VCJCS memo for the Service chiefs, combatant commanders and directors of Joint Staff directorates, undated.]

cyberspace operations. The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. [From “Joint Terminology for Cyberspace Operations,” VCJCS memo for the Service chiefs, combatant commanders and directors of Joint Staff directorates, undated.]

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, sea and space forces at a given time and sphere of operations without prohibitive interference by an adversary. [From “Joint Terminology for Cyberspace Operations,” VCJCS memo for the Service chiefs, combatant commanders and directors of Joint Staff directorates, undated.]

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. See also military deception—Actions executed to deliberately mislead adversary military decision makers as to

friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

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. [JOAC]

electromagnetic deception. The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability.

electromagnetic spectrum. The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands.

electronic attack. Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

engagement. A category of military activity that seeks to improve the capabilities of or cooperation with allied and other partners. [CCJO]

fires. The use of weapon systems to create a specific lethal or nonlethal effect on a target.

force projection. The ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations.

forcible entry. Seizing and holding of a military lodgment in the face of armed opposition. (JP 3-18)

forcible entry (JOAC working definition). Projection of land forces onto hostile territory in the face of armed opposition.

freedom of navigation operations. Operations conducted to demonstrate U.S. or international rights to navigate air or sea routes.

global commons. Areas of air, sea, space and cyberspace that belong to no one state. Access to the global commons is vital to U.S. national interests, both as an end in itself and as a means to projecting military force into hostile territory.

information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

information operations. The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

intelligence. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.

joint force. A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander.

joint functions. Related capabilities and activities grouped together to help joint force commanders synchronize, integrate, and direct joint operations. Functions that are common to joint operations at all levels of war fall into six basic groups—command and control, intelligence, fires, movement and maneuver, protection, and sustainment.

joint synergy. The combination of Service capabilities such that each enhances the effectiveness and compensates for the vulnerabilities of the others. [CCJO v3.0]

joint task force (JTF). A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a sub-unified commander, or an existing joint task force commander.

landing force. A Marine Corps or Army task organization formed to conduct amphibious operations. The landing force, together with the amphibious task force and other forces, constitute the amphibious force. Also called LF.

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.

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.

maritime supremacy. That degree of maritime superiority wherein the opposing force is incapable of effective interference.

mission command. The conduct of military operations through decentralized execution based upon mission-type orders.

mission-type order. 1. An order issued to a lower unit that includes the accomplishment of the total mission assigned to the higher headquarters. 2. An order to a unit to perform a mission without specifying how it is to be accomplished.

movement and maneuver. This joint function encompasses disposing joint forces to conduct campaigns, major operations, and other contingencies by securing positional advantages before combat operations commence and by exploiting tactical success to achieve operational and strategic objectives. This function includes moving or deploying forces into an operational area and conducting maneuver to operational depths for offensive and defensive purposes. It also includes assuring the mobility of friendly forces.

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.

operational access. The ability to project military force into an operational area with sufficient freedom of action to accomplish the mission.

operational area. An overarching term encompassing more descriptive terms for geographic areas in which military operations are conducted. Operational areas include, but are not limited to, such descriptors as area of responsibility, theater of war, theater of operations, joint operations area, amphibious objective area, joint special operations area, and area of operations.

port of embarkation. The geographic point in a routing scheme from which cargo or personnel depart. This may be a seaport or aerial port from which personnel and equipment flow to a port of debarkation; for unit and non-unit requirements, it may or may not coincide with the origin.

power projection. The ability of a nation to apply all or some of its elements of national power - political, economic, informational, or military - to rapidly and effectively deploy and sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability.

protection. The preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area.

reachback. The process of obtaining products, services, and applications, or forces, or equipment, or materiel from organizations that are not forward deployed.

relief and reconstruction. A category of military activity that seeks to restore essential civil services in the wake of combat, a breakdown of civil order, or a natural disaster. [CCJO]

seabasing. The deployment, assembly, command, projection, reconstitution, and re-employment of joint power from the sea without reliance on land bases within the operational area.

security. A category of military activity that seeks to protect and control civil populations, territory and resources, whether friendly, hostile or neutral. [CCJO]

space. A medium like the land, sea, and air within which military activities shall be conducted to achieve U.S. national security objectives.

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.

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.

strategic distance. A descriptor for action originating outside the operational area, often from home station. [JOAC]

sustainment. The provision of logistics and personnel services required to maintain and prolong operations until successful mission accomplishment.

unmanned aircraft. An aircraft or balloon that does not carry a human operator and is capable of flight under remote control or autonomous programming. [Note: Includes remotely piloted aircraft, remotely piloted vehicles, unmanned aerial vehicles and unmanned aircraft systems.]

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.

ANNEX B ASSESSMENT PLAN

The development of the JOAC followed a comprehensive *Concept Development Plan* that employed an innovative approach and coordinated campaign to concept development and assessment. The JOAC campaign consisted of four integrated lines of effort: concept development; analysis; experimentation; and engagement/transition. This annex provides a summary of the assessment activity used to develop the JOAC. It concludes with a recommended way ahead that identifies key aspects requiring further assessment that are suitable for inclusion into the annual joint experimentation work plan.

B.1 Concept Development Framework

Figure 3 depicts the JOAC campaign framework with concept development, experimentation, and engagement and transition lines of effort across the project timeline with the analysis line of effort interwoven throughout the project. This framework enabled complete integration of all lines of effort in support of the development of the JOAC.

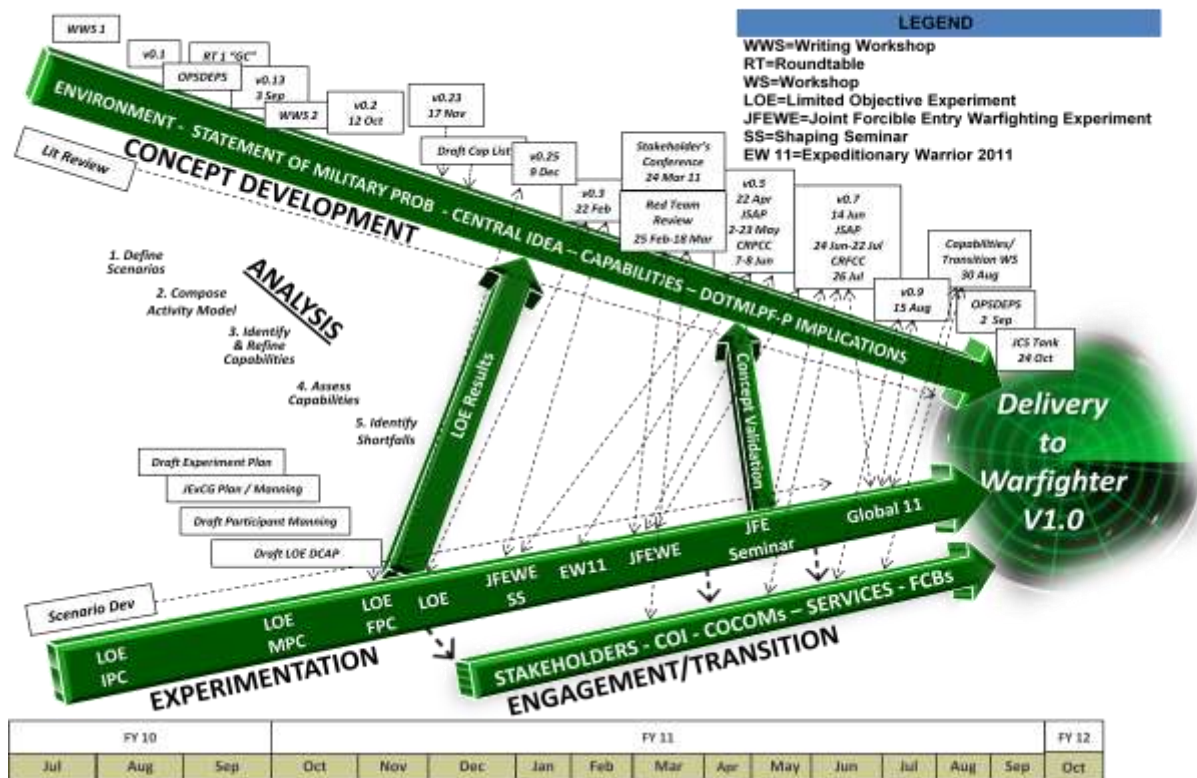


Figure 3. JOAC Project Framework

Based on an approved warfighter challenge and guided by CJCSI 3010, the JOAC Project Team adapted the Statement of the Military Problem, Outcomes,

Objectives, Products, and Activities (SOOPA) model shown in Figure 4, which was updated as understanding of the JOA problem and solution improved.

S	Statement of the Military Problem	<p>The essential problem for future joint forces is to be able to project military force into an operational area and sustain it in the face of armed opposition in light of the following three trends:</p> <ul style="list-style-type: none"> • Future enemies are acquiring dramatically improved antiaccess and area-denial capabilities. • U.S. overseas defense posture is declining, increasing the requirement for force projection from the U.S. Homeland. • Space and cyberspace are becoming increasingly important and contested domains. <p>Meeting that challenge increasingly will require defeating integrated antiaccess/area-denial systems of growing lethality and sophistication.</p>
O	Outcomes	<ol style="list-style-type: none"> 1) Concept that describes how a future Joint Force Commander (JFC) will fight for freedom of action within the global commons and select sovereign territory across the range of expeditionary operations in an opposed access environment. 2) Required joint force capabilities identified / transitioned to the appropriate capability development sponsors.
O	Objectives	<ol style="list-style-type: none"> 1) Establish a common intellectual framework for military professionals, policymakers, and others interested in the challenge of opposed access. 2) Invigorate interest in, and the study of, an operational challenge that a generation of military leaders, focused on other missions, has not had to consider in recent years. 3) Establish a basis for subsequent joint and Service concepts and doctrine. 4) Identify the broad capabilities required to gain operational access in the face of armed opposition. 5) Inform study, evaluation, wargaming, and experimentation that will result in changes to DOTMLPF.
P	Products	<p><i>JOAC</i> that serves as the Chairman’s vision for the joint force’s ability to <u>gain and maintain operational access across all domains.</u></p>
A	Activities	<p>Complete all Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3010 Concept Development activities as required, including but not limited to:</p> <ol style="list-style-type: none"> 1) Initial Stakeholder Conference 2) Writing Workshops 3) Writing activities of outlines, drafts, and final products 4) Planning Conferences 5) Capabilities Limited Objective Experiment 6) Leveraging other combatant command and Service events 7) Red Team Review and Red Team Comments Resolution 8) Joint Staff Action Process (JSAP) Staffing 9) In-progress reviews (IPR) to Operational Deputies (OPSDEPS) 10) Joint Chiefs of Staff (JCS) Tank Presentation 11) Transition “Off Ramps”

Figure 4. JOAC SOOPA Model

This SOOPA model resulted in an initial draft of the *JOAC* that included an identification of the scope and purpose of the concept as well as an overview of the threat environment.

Figure 5 provides an overview of the concept development architecture for the JOAC project. Highlights of this architecture include a breakout of each line of effort and the interrelationships between key supporting activities. This approach recognizes Joint Experimentation as an integral part of the full cycle of concept development, assessment, and transition. Joint Experimentation design experts and analysts were included from the outset in the concept development process.

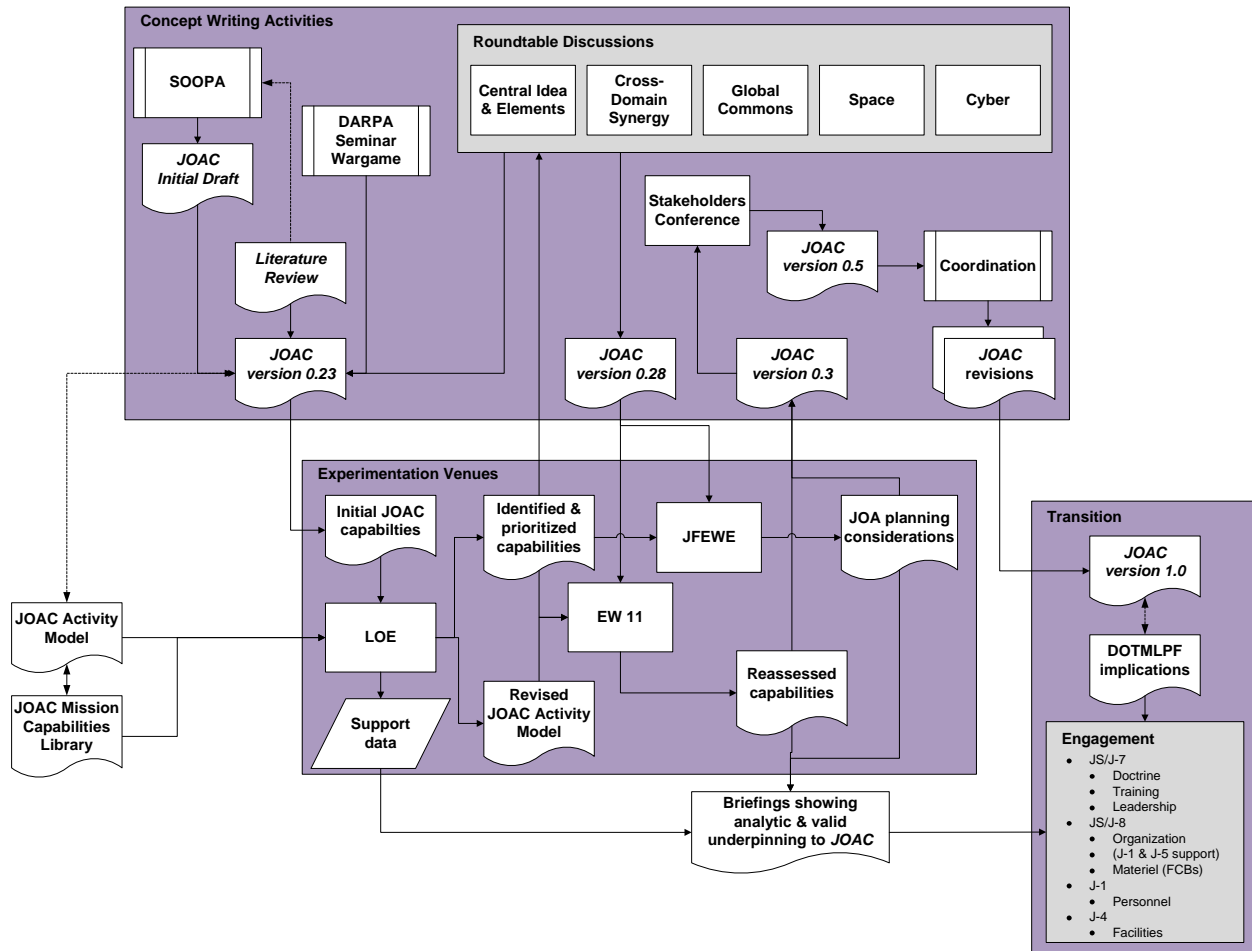


Figure 5. JOAC Development Architecture

Summaries of the major JOAC development activities by line of effort follow in the sections below.

B.2 Concept Development Line of Effort

The JOAC Core Writing Team (CWT) consisted of subject matter experts (SME) from each of the four Services, JS J7, a space SME from OSD AT&L, and a

USJFCOM concept development team. Each of the combatant commands also had the opportunity to assign a SME to the CWT. Throughout the development process, the CWT participated in an extensive literature review, a series of SME round table discussions, and the CJCSI 3010 defined concept development process. The CWT also participated in and leveraged findings from the experimentation and analytic support efforts. The following subsections summarize these activities.

B.2.1 Literature Summary and Data Review

Development of the *JOAC* began with an extensive literature summary and data review to identify leading thought among academics and military leaders on the issues surrounding opposed operational access and the potential solutions to combating these issues. The summary of the literature and data reviews provided a front-end analysis of JOA and a comprehensive body of knowledge that provides support to the concepts found in the *JOAC*. The review also examined past, ongoing, and future concept development activities that could contribute to the JOA Concept project.

The review contains a summary of key facts, assumptions, implications, conditions, and issues related to JOA. The activity centers on identification of ideas that supported the CWT's development of each section of the paper. The review enabled development of an initial list of tasks and capabilities related to JOA that were vetted and refined through experimentation. Key findings from the literature survey, as found in its executive summary, are excerpted as quotes below.

- Strategic guidance and doctrine support the development of a concept for JOA. The *National Security Strategy* (NSS) concludes the nation must prepare for "...increasingly sophisticated adversaries, [and] deterring and defeating aggression in anti-access environments." Additionally, the *Quadrennial Defense Review* (QDR) acknowledges a challenging operational landscape that includes:
 - Increasingly multidimensional conflicts ("hybrid" threats)
 - Threats to the global commons and expansion into space and cyberspace
 - Growing anti-access (A2) / area denial (AD) capabilities, including ballistic missile threats
- While the challenges inherent in access are not new, the Joint Force requires a concept for JOA now because of significant changes in the operational environment. Emergent concerns include:
 - Weak and failing states, rising nations, and non-state actors
 - Proliferation of technology and weapons of mass destruction (WMD) combined with the effects of globalization, which will bring the homeland into reach – U.S. bases are not immune

- More widely available longer-range, more precise weapons
 - Protection of “homeland” will include elements of space and cyberspace
 - Hybrid challenges and tactics
 - Air and sea dominance are not assured
 - U.S. dependence on space and cyberspace
- The development of longer range intelligence, surveillance, and reconnaissance (ISR) capabilities by potential anti-access opponent[s] suggests that the assumed near-immunity of U.S. forces in the post-Cold War era is eroding and maritime vulnerability is returning to the late-Soviet period.
 - The open nature of the World Wide Web and the diffusion of related technical knowledge throughout the world have created an environment with major threats to the freedom of cyberspace. Threats to cyberspace subsequently increase vulnerabilities for militaries that rely on cyberspace technologies. Space has become the primary location for global and regional reconnaissance assets used for nuclear weapons monitoring, intelligence gathering, and support of combat operations on the earth's surface. A logical opening operation to any anti-access campaign is to neutralize U.S. space assets.
 - Understanding the strategic and operational implications of the A2/AD challenge requires an examination of the following aspects of the future environment:
 - Rising regional powers adapting strategies and capabilities to deny US access and freedom of action as a strategy.
 - Increasingly capable future enemies will see the adoption of an antiaccess/area-denial strategy against the United States as a viable course of action.
 - The ability to ensure operational access in the future is being challenged—and may well be the most difficult operational challenge U.S. forces will face over the coming decades.
 - While the need for access is not new, changes in the strategic and operational environment, proliferation of technology, emergence of non-state actors with state-like power, and widening abilities to disrupt the space and cyber domains dramatically alter the military equation. Challenges exist in all five domains (air, cyber, land, sea, and space). Hence, solutions mandate development of cross-domain capabilities. These capabilities do not reside in a single Service, and therefore, require a joint concept to effectively gain and maintain JOA.

The *JOAC Literature Summary and Data Review* is available at the link below:
<https://us.jcom.mil/sites/J9/CG/OA/Shared%20Documents/Forms/AllItem>

[s.aspx?RootFolder=%2fsites%2fJ9%2fCG%2fOA%2fShared%20Documents%2fJOAC%20Deliverables%2f3%2e3%20Summary%20of%20Literature%5fData%20Review&FolderCTID=&View=%7bFC439951%2d2D0F%2d4237%2dAFD8%2d16097158B7DF%7d](https://us.jfcom.mil/sites/J9/CG/OA/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fJ9%2fCG%2fOA%2fShared%20Documents%2fJOAC%20Deliverables%2f3%2e3%20Summary%20of%20Literature%5fData%20Review&FolderCTID=&View=%7bFC439951%2d2D0F%2d4237%2dAFD8%2d16097158B7DF%7d)).

B.2.2 Seminar Wargames and Round Table Discussions

Beginning in July 2010, using the literature survey as the starting point, the CWT participated in a series of seminar wargames and held a series of round table discussions with groups of Highly Qualified Experts (HQE) to elicit perspectives on access challenges. The approach targeted events to inform the purpose and scope of the concept, understanding the nature of the challenge and evolving threat, identifying the statement of the military problem, and exploring solutions to that problem. Additionally, the CWT met on a regular basis throughout this process to refine the paper. The CWT developed key terms and working definitions to support the concept. Events that supported them included:

- Joint Operational Environment Seminar Wargame on Challenges to the Global Commons
- National Defense University SME panel discussion on the emerging Antiaccess/Area-denial Threat
- Round table discussion on the statement of the military problem
- Access Challenges to Space round table discussion
- Access Challenges in the Cyberspace Domain round table discussion
- Domain Synergy round table discussion
- Defense Advanced Research Projects Agency (DARPA)/Center for Strategic and Budgetary Assessments (CSBA) Seminar Wargame on A2/AD and Guided Rockets, Artillery, Missiles, and Mortars (G-RAMM)

Executive summaries and results of these events can be found at:

<https://us.jfcom.mil/sites/J9/CG/OA/Shared%20Documents/Forms/AllItems.aspx>.

Key to success was the CWT's ability to participate in and leverage other related Service experimentation efforts including the U.S. Army's Joint Forcible Entry Warfighter Experiment (JFEWE) and the USMC Expeditionary Warrior 2011 (EW 11) to both validate and further enrich the JOAC development process. The effects that these activities had on the progression of thought in the development of the JOAC are discussed within the Experimentation Line of Effort.

B.2.3 Review Activities

Additionally, the JOAC paper has been thoroughly reviewed by subject matter experts both within and outside the Department of Defense.

- The Joint Staff J7 sponsored a Red Team Review consisting of both retired flag and general officers and senior civilians to review *JOAC v0.3*. Over a period of three weeks from 25 Feb to 18 Mar 11, the Red Team analyzed the draft concept, challenging its ideas and assertions to identify defeat mechanisms within it and inform the *JOAC v0.5*
- The Joint Staff J7 conducted an initial coordination review of *JOAC v0.5* via the Joint Staff Action Process (JSAP). Those comments were adjudicated by the CWT to inform *JOAC v0.7*
- The Joint Staff J7 conducted a final coordination review of *JOAC v0.7*. Those comments were adjudicated by the CWT to inform *JOAC v0.9*

B.3 Experimentation Line of Effort

The *JOAC* campaign framework included a line of experimentation used to support the development of the *JOAC*. These activities included: the *JOAC Capabilities Limited Objective Experiment (LOE)*; the United States Marine Corps, Title 10 experiment, EW 11; and the United States Army, JFEWE. Details about these events, the *JOAC* Project experimentation approach, and findings and insights from these events can be found in the *JOAC Capabilities Limited Objective Experiment (LOE) Final Report*, the *JOAC Capabilities Limited Objective Experiment (LOE) Final Report Supplement III – EW 11*, and the *JOAC Capabilities Limited Objective Experiment (LOE) Final Report Supplement IV - JFEWE*, respectively. The *JOAC* Team leveraged two additional events, the United States Air Force Global Mobility Wargame, and the United States Navy Global 11. While these activities provided valuable insight into *JOAC* development and validation, the level of *JOAC* involvement did not warrant formal supplements to the *JOAC* LOE Final Report. The following subsections summarize the events and the key findings for the *JOAC* Project.

B.3.1 Global Mobility Wargame: 7-11 Jun 10

The *JOAC* Project leveraged the USAF Global Mobility Wargame to shape the team's nascent understanding of the antiaccess/area-denial challenge. The purpose of the Global Mobility Wargame was to address air mobility and logistics issues in preparation for Unified Endeavor 2010, the Air Force's biennial Title 10 wargame.

Participation in the Global Mobility Wargame enabled the *JOAC* Project Team to better understand the following four key issues:

- The advantages and disadvantages of future precision delivery systems in geographically challenging environments
- The manner by which joint future theater lift might be employed in concert with the rest of the Mobility Air Forces
- The manner by which antiaccess/area-denial challenges impact the

Pacific en route strategy

- The manner by which the Seabasing Joint Integrating Concept impacts the USAF contribution to theater distribution and sustainment

These findings helped shape the team's initial thoughts pertaining to the operational access challenge and assisted in the development of ideas pertaining to force projection in an antiaccess/area-denial environment.

B.3.2 Limited Objective Experiment: 5-10 Dec 10

The JOAC LOE examined the future challenges the joint force may face gaining operational access while overcoming future A2/AD capabilities in the face of armed opposition by a variety of potential enemies and under a variety of conditions. To enable a sufficient depth of conversation, the JOAC LOE was a classified event, using approved Defense Planning Scenarios (DPS) and Multi-Service Force Deployment (MSFD)-based vignettes to ensure a broad spectrum of enemy challenges and capabilities was captured. Three operational vignettes (near-peer, regional hegemony, hybrid high / low insurgency) were developed and examined spanning a wide range of military operations representing three distinct portions of the future environment.

The objectives for the JOAC LOE were as follows:

- Provide a prioritized list of operational capability requirements needed to conduct JOA across a broad threat spectrum
- Provide insights to the JOAC
- Provide a structure to better understand the JOA challenge

This was accomplished by studying the activities required to conduct JOA. These activities were represented through a JOAC Activity Model (AM) as the backbone of the analytic framework that describes the high level operational activities necessary for JOA. Each of these activities was directly related to doctrinal or Department of Defense (DOD) definitions as well as Universal Joint Task List (UJTL) tasks and Joint Capability Areas (JCA) as applicable. This JOAC AM provided the functional context for the JOAC LOE assessment.

The JOAC LOE was conducted in a single plenary group over the course of six days in a facilitator-led discussion aimed to explore key elements of interest for identifying and then prioritizing the operational capabilities required for JOA. Participants included members of the community of interest, SMEs in the three MSFD threats, and members of the writing team. The facilitator used guiding questions to get at data of interest through the operational context provided by the vignettes. Participants were able to document any additional thoughts or discussion using threaded discussion in FacilitatePro[®], a collaborative tool that

allows participants to contribute to conversations as they occur.

JOAC v0.23 was the current version of the *JOAC* at the time of the event. The results of the experiment were related to this version of the paper. LOE results led to the development of the *JOAC* precepts, underscored many capabilities already found in *JOAC v0.23*, and highlighted additional capabilities required. The *JOAC* LOE provided valuable insights needed for the future joint force to operate against an adversary posing an A2/AD strategy circa 2028. Thirty-six initial capability requirements resulted from the LOE. Significant findings that impacted the revision of *JOAC* included:

- The importance of ISR requirements as a means to understanding intentions through precursor surveillance reinforced the need identified in the *JOAC* to apply information in a precise and effective manner to locate and understand enemy A2/AD capabilities. These ISR capabilities apply to both collection and analysis
- Identification of engagement activities necessary to prepare the operational area for facilitating access. This need for engagement affects other capability areas such as requirements in logistics to build a multitude of dispersed bases and enhancing survivability of pre-positioned materiel
- The importance of a more adaptable and mobile force, which is reflected in the LOE logistics requirements, calling for smaller, autonomous entities that have the ability to move over long ranges with reduced sustainment requirements
- The protection of space and cyber assets and the ability to attack the enemy's space and cyber capabilities. This requirement led to a recommended organizational improvement of a cyber cell within the Joint Task Force (JTF) Headquarters
- The need for cross-domain synergy, the ability to create advantage in one domain (or more) that provides opportunity or advantage in another domain, is emphasized by the *JOAC* as an important requirement for operating in the future environment in order to fragment an adversary's A2/AD capabilities
- Emphasized the need for camouflage, concealment, and deception (CCD), calling for training pertinent to CCD as well as the ability to counter or conceal information
- Identification of the need for better understanding of multi-combatant-command leadership structure, cross-domain synchronization and awareness

B.3.3 Expeditionary Warrior 2011 (EW 11): 31 Jan - 4 Feb 11

The *JOAC* Project leveraged the USMC EW 11, an important component of the USMC Title 10 wargaming program, to vet the ideas contained in the *JOAC v0.28* with the community of interest. The purpose of EW 11 was to explore

the USMC's role in a JOA environment and further develop the Enhanced Marine Air-Ground Task Force (MAGTF) Operations (EMO) concept at the operational and tactical levels in an unclassified seminar-style wargame. The event was co-sponsored by Headquarters USMC, Marine Corps Combat Development Command (MCCDC) G3/5 and the Marine Corps Warfighting Laboratory (MCWL). Representatives from the Services, combatant commands, foreign military officers, and NATO Allied Command Transformation (NATO ACT) participated in the wargame.

EW 11 discussions provided a means to determine credibility of the overarching concept of domain synergy, the underlying precepts, and identified capabilities embedded within the *JOAC v0.28*. Facilitated discussions during EW 11 explicitly addressed the utility of the *JOAC* in addressing the JOA problem. The *JOAC* Project Team supported the execution of EW 11 by supplying facilitators, analysts, and rapporteurs to two of the *JOAC* cells: the JTF and Combined JTF (CJTF). EW 11 *JOAC* results supported the development of *JOAC v0.3* and *JOAC v0.5*. Detailed information on EW 11 and the EW 11 Final Report may be obtained by contacting Maj Michael Tirone, Wargaming Division, MCWL, (703) 784-6882, michael.tirone@usmc.mil.

While the EW 11 results indirectly reinforced, and in some cases indicated, areas for refinement in the capabilities required for JOA, the identification of areas requiring expansion, clarification, or inclusion within the *JOAC* was the primary outcome from the wargame. Significant findings that impacted the revision of *JOAC* included:

- The need to create stronger linkages to other current concepts
- The need to add capabilities that enable integration of our multi-national partners
- The need to better articulate the emerging importance of space and cyberspace

B.3.4 Joint Forcible Entry Warfighter Experiment (JFEWE): 19-21 Jan 11, 7-17 Mar 11

The *JOAC* Project leveraged the USA JFEWE 2011 by sending analysts and observers to the JFEWE experiment to identify and record insights to support the development of the *JOAC*. The primary focus for the *JOAC* Project Team was on the JFEWE Shaping Seminar (SS), hosted by the Mission Command Battle Lab (MCBL) at Ft. Leavenworth, KS, 19-21 Jan 11, given its focus on operational access at the planning level. The focus at the tactical level of the JFEWE Simulation Exercise (SIMEX), hosted by the Maneuver Battle Lab (MBL) at Fort Benning, GA, 7-17 Mar 11, was less conducive to the identification of JOA capability requirements at the operational level. The overall approach for JFEWE SS was designed to view Joint Operational Access (JOA) capabilities through the lens of Joint Publication 3-18, Joint Forcible Entry Operations.

JFEWE SIMEX was designed to address the operational access issues of a significant tactical force. JFEWE SIMEX was primarily concerned with area denial issues as defined by the JOAC. The JFEWE SS supported the JFEWE SIMEX and provided limited support to JOAC development.

The design of the JFEWE SS and its primary nature as a JFEWE SIMEX planning effort did not allow direct data collection by the JOAC team. However, the JOAC Project Team indirectly collected data on a revised JOA question set developed following the JOAC LOE. This JFEWE SS data was derived from the event discussions and comments made by the participants in FacilitatePro®. Although open discussion was greatly limited, survey responses collected during the event provided some evidence that reinforced JOA capabilities identified in the JOAC LOE. Similarly, the design and focus of the JFEWE SIMEX limited JOAC insights. However, the survey responses for this event also reinforced JOA capabilities identified during the JOAC LOE. Detailed information on the JFEWE may be obtained by contacting the following points of contact:

JFEWE SS: Mr. Duane Riddle, duane.riddle@us.army.mil

JFEWE SIMEX: Mr. Bob Kruger, bob.kruger@us.army.mil

JFEWE: Mr. Jason Rakocy, jason.rakocy@us.army.mil

JFEWE significant findings that impacted the revision of JOAC included:

- The requirement to operate in a degraded C2 environment and reconstitute supporting space assets once lost
- The requirement to overcome the A2/AD environment and strategy posed by adversaries' closed communities and propensity to operate within and among civilian populations. To do so, the joint force requires the capabilities of: strong HUMINT; trust building activities as part of setting conditions and establishing forward presence; and teams trained to operate within and among the populations of interest
- The requirement for cross-domain synergy and synchronization across the five domains (air, maritime, land, space, and cyberspace)
- The ability to operate in austere and degraded environments
- The criticality of time and space when trying to synchronize the physical domains with operations in the space and cyberspace domains
- Many capabilities identified during the JOAC LOE were underscored by both the JFEWE SS and the JFEWE SIMEX

B.3.5 Global 11 Wargame: 15-22 Jul 11

The JOAC Project leveraged the USN Global 11 Wargame to serve as another validation event, to support revision of the JOAC v0.7, and to inform follow-on

conceptual work and transition efforts. The purpose of the Global 11 Wargame was to investigate the USN's ability to exercise sea control as necessary to support joint ground combat operations via seabasing.

During Global 11, the JOAC Team found that although the term "cross-domain synergy" (the central idea of the *JOAC*) was not a term of art for the players, as planning began it became readily apparent that synchronization of domain capabilities would be required to set conditions to successfully execute the Joint Task Force mission. Additionally, the participants employed many tenets of the *JOAC* precepts during the design, planning, and execution of the wargame.

By the event's conclusion, it appeared that all participants clearly understood the difficulties associated with the future antiaccess/area-denial fight. Discussions during the planning and out brief indicated that the *JOAC* problem statement, central idea, precepts, and required capabilities are correct.

Participation in the event's follow-on DOTMLPF workshop facilitated an implications crosswalk between the wargame's results and the *JOAC*, resulting in a refinement of the concept's identified capabilities.

B.4 Synthesis Activities

The JOAC Project Team compared the results from the experimentation efforts to the material resident in *JOAC v0.3* to provide an analytic assessment of content that the writing team should address in its v0.5 revision. This analysis identified where and how findings from the experimentation efforts were addressed and identified any potential inconsistencies and deficiencies in coverage. It included an *Analysis Crosswalk* between the experimentation analysis products and *JOAC v0.3* and an evaluation of the expression of the capabilities within *JOAC v0.3* in terms of resolution (i.e., operational level) and fidelity (i.e., specificity of the expressed capability). The *Analysis Crosswalk* also contains a combined summary of implications from both of these analyses. The writing team used this holistic evaluation as part of their revision assessments.

The analysis included an assessment of the manner in which the findings and JOA capabilities identified during the JOAC LOE are captured within the *JOAC v0.3*. The analysis also assessed the changes to *JOAC v0.3* resulting from the EW11 and JFEWE experimental findings. The assumptions used to evaluate whether the *JOAC v0.3* capabilities were at the operational level and appropriate for a concept formed criteria and constraints for *JOAC v0.5*. These criteria and constraints are given below:

Criterion 1: The capabilities identified in the *JOAC v0.3* need to be at the operational level

- Criterion 2: The capabilities identified in the *JOAC v0.3* need to be solution agnostic
- Criterion 3: The capabilities identified in the *JOAC v0.3* need to be identifiable as potentially having a solution within the purview of a specific FCB (Battlespace Awareness, Logistics, Force Application, Protection, Building Partnerships, Command and Control, Net-Centric Operations)
- Criterion 4: The capabilities identified in the *JOAC v0.3* need to address those capabilities required to enable cross-domain synergy
- Criterion 5: The capabilities identified in the *JOAC v0.3* need to address those capabilities required to meet antiaccess challenges
- Criterion 6: The capabilities identified in the *JOAC v0.3* need to address those capabilities required to meet area-denial challenges
- Constraint 1: Capabilities must all satisfy criteria one, two, and three as well as at least one of criteria four, five, or six
- Constraint 2: Discussion within the body of the *JOAC* needs to clearly lead the reader to the conclusion that the list of capabilities is required to meet the A2/AD challenge and support the overarching concept of cross-domain synergy. That is, the discussion must support the list of required capabilities

Detailed findings and recommendations from this analysis can be found in the *Analysis Crosswalk* at:

<https://us.jfcom.mil/sites/J9/CG/OA/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fJ9%2fCG%2fOA%2fShared%20Documents%2fJOAC%20Deliverables%2f3%2e17%20Concept%20Draft%20v0%2e5&FolderCTID=0x0120009776195D76ADCB4BB0479D46A3CD069E&View=%7bFC439951%2d2D0F%2d4237%2dAFD8%2d16097158B7DF%7d>.

B.5 Way Ahead

The *JOAC* conceptual and experimental work used in the development of the *JOAC* underscores the importance of overcoming A2/AD challenges across the joint force. Further highlighting the need to continue this work is the fact that the nature of the access problem will likely change and evolve over time, as will the geopolitical environment. Solutions to the access problem lie within the purview of Service capabilities, but must be continually informed by the joint community. Considering the size and scope of the issue, the *JOAC* cannot solve every A2/AD challenge, nor does it provide a detailed capabilities list that will immediately result in DOTMLPF solutions. The *JOAC* should serve as the Joint Force conceptual foundation for addressing the A2/AD challenge. The path to generating solutions starts with a more in-depth examination of the underlying conceptual implications of the *JOAC* to include:

- Integration and development of supporting concepts to operationalize the *JOAC*. These supporting concepts will provide a greater degree of fidelity to key portions of the *JOAC*
- Follow-on analysis, identification and transitioning of the DOTMLPF implications of adopting the *JOAC*
- Further investigation at the joint and Service level of the required capabilities identified in the *JOAC*

The Department of Defense should leverage the Joint Capability Integration Development System as a pathway for this follow-on work to proceed.

ANNEX C BIBLIOGRAPHY

- Ambrose, Stephen E. "Eisenhower, the Intelligence Community, and the D-Day Invasion." *Wisconsin Magazine of History*, (Summer 1981): 261-277.
- Barber, Arthur H. III and Delwyn L. Gilmore. "Maritime Access: Do Defenders Hold All the Cards?" *Defense Horizons* 4, (Oct01): 1-8.
- Boling, James L. "Rapid Decisive Operations: The Emperor's New Clothes in Modern Warfare." *Essays 2002: Chairman of the Joint Chiefs of Staff Essay Competition*. Washington, DC: NDU Press, 2002: 41-62.
- Bosone, John. "Airpower and the Establishment of Sea Control in an Antiaccess Environment." *Naval War College*. Newport, RI: 23April08.
- Bowdish, Randall G. and Bruce Woodyard. "A Naval Concepts-Based Vision for Space," *U.S. Naval Institute Proceedings* 125, no.1 (Jan99): 50-53.
- Bracken, Paul. *Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age*. New York: HarperCollins, 1999.
- Bruger, Steven J. "Not Ready for the First Space War: What About the Second?" *Naval War College Review* 48, no. 1 (Winter 1995): 73-83
- Capstone Concept for Joint Operations, Version 3.0*. CCJO v3.0. United States Department of Defense, January 15, 2009.
http://www.dtic.mil/futurejointwarfare/concepts/approved_ccjov3.pdf.
- China's Active Defense Strategy and Its Regional Implications: Testimony Before The U.S.-China Economic And Security Review Commission*, 27Jan11,
http://www.uscc.gov/hearings/2011hearings/written_testimonies/11_01_27_wrt/11_1_27_thomas_testimony.pdf
- Cliff, Roger, Mark Burles, Michael S. Chase, Derek Eaton, and Kevin L. Pollpeter. *Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States*. Santa Monica, CA: RAND Corporation, 2007.
- "Cooperation and Conflict in the Commons, Conference Report," 29Jul10. (Not yet publicly available.)
- Davis, Paul K., Jimmie McEver, Barry Wilson. *Measuring Interdiction Capabilities in the Presence of Anti Access Strategies*. Santa Monica, CA: RAND Corporation, 2002.
- The DCDC Strategic Trends Programme 2007-2036*, Her Majesty's Government, Ministry of Defence, Development, Concepts, and Doctrine Center, Jan07: 66.
- Denmark, Abraham M., and James Mulvenon. *Contested Commons: The Future of American Power in a Multipolar World*. Washington, DC: Center for a New American Security, Jan10.

Deterrence Operations Joint Operating Concept (Version 2.0). United States Department of Defense, Dec06,
http://www.dtic.mil/futurejointwarfare/concepts/do_joc_v20.doc.

Dossel, Will. "Ballistic Missile Defense." *Securing Freedom in the Global Commons*. Stanford, CA: Stanford University Press, 2010: 115-130.

Ebner, Kimberley. "Amnesty Uses Commercial Sat Imagery to Monitor Darfur," *Jane's International Defense Review*, 13Jun07.

Erickson, Andrew and David D. Yang. "Using the Land to Control the Sea? Chinese Analysts Consider the Antiship Ballistic Missile." *Naval War College Review* 62, no. 4 (Autumn 2009): 53-86.

Flournoy, Michele and Shawn Brimley. "The Contested Commons," *U.S. Naval Institute Proceeding* 135, no. 7 (Jul09): 17.

Friedman, Norman. "Globalization of Antiaccess Strategies?" *Globalization and Maritime Power*, edited by Sam J. Tangredi. Washington, DC: National Defense University Press, 2002: 487-502,
<https://digitalndulibrary.ndu.edu/u/?ndupress,27526>.

Gatchell, Theodore L. *At the Water's Edge: Defending Against the Modern Amphibious Assault*. Annapolis, MD: Naval Institute Press, 1996.

Global Strike Joint Integrating Concept (Version 1.0), United States Department of Defense, 10Jan05,
http://www.dtic.mil/futurejointwarfare/concepts/gjic_v1.doc.

Gruselle, Bruno. "Cruise Missiles & Anti-Access Strategies." *Foundation Pour La Recherche Stratégique*. Jun06,
http://www.frstrategie.org/barreFRS/publications/rd/RD_20060601_eng.pdf

Halpin, Tony. "Russia Warns of War within a Decade over Arctic Oil and Gas Riches." *The Times*, 14May09,
<http://www.timesonline.co.uk/tol/news/environment/article6283130.ece>.

Henry, Ryan. "Transforming the U.S. Global Defense Posture." *Naval War College Review* 59, no. 2 (2006): 13-28.

Hresko, Eric. "Effects-based Operations—A Valid Concept for Operations in an Anti-Access Environment." *Naval War College*. Newport, RI: 4May08.

Hyten, John E. "A Sea of Peace or a Theater of War: Dealing with the Inevitable Conflict in Space," *ACDIS Occasional Paper*. Champaign, IL: University of Illinois at Urbana-Champaign, Apr00.

Jasper, Scott, editor. *Securing Freedom in the Global Commons*. Palo Alto: Stanford University Press, 2010.

Joint Combat Concept (JCC), v0.5, 19May10 (Not Approved for Public Release)

Joint Concept for Cyberspace (JCC), v0.1, 1Oct10. (Not Approved For Public Release)

Joint Logistics (Distribution) Joint Integrating Concept (Version 1.0). Joint Chiefs of Staff, Washington, DC: 7Feb06, http://www.dtic.mil/futurejointwarfare/concepts/jld_jic.pdf.

The Joint Operating Environment 2010. Suffolk, VA: USJFCOM, February 18, 2010. http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_0.pdf.

Joint Publication 3-0 Joint Operations (Incorporating Change 2). JP 3-0. Joint Chiefs of Staff, March 22, 2010, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

Joint Publication 3-01, Countering Air and Missile Threats. JP 3-01. Joint Chiefs of Staff, 5Feb07, http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf.

Joint Publication 3-15, Barriers, Obstacles, and Mine Warfare for Joint Operations. JP 3-15. Joint Chiefs of Staff, 26April07, http://www.dtic.mil/doctrine/new_pubs/jp3_15.pdf.

Joint Publication 3-18 Joint Forcible Entry Operations. JP 3-18. Joint Chiefs of Staff, 16June 08, http://www.dtic.mil/doctrine/new_pubs/jp3_18.pdf.

Kaplan, Robert. "The Geography of Chinese Power." *Foreign Affairs*, (May/June10): 22-41.

Kauderer, Dr. H. Todd. *Analytic Support to the QDR... and Beyond*, OSD Policy-Strategy, March 3, 2010. (Not publicly available).

Krepinevich, Andrew, Barry Watts and Robert Work. *Meeting the Anti-Access and Area-Denial Challenge*. Washington, DC: Center for Strategic and Budgetary Assessments, 2003.

———. *Why AirSea Battle?* Washington, DC: Center for Strategic and Budgetary Assessments, 2010.

Larson, Eric V., Derek Eaton, Paul Elrick, Theodore Karasik, Robert Klein, Sherrill Lingel, Brian Nichiporuk, Robert Uy, and John Zavadil. *Assuring Access in Key Strategic Regions: Toward a Long-Term Strategy*. Santa Monica, CA: RAND Corporation (Arroyo Center), 2004.

Major Combat Operations Joint Operating Concept (Version 2.0). United States Department of Defense, Dec06, http://www.dtic.mil/futurejointwarfare/concepts/mco_joc_v20.doc.

Manor, Mike and Kurt Neuman. "Space Assurance." *Securing Freedom in the Global Commons*. Stanford, CA: Stanford University Press, 2010: 99-114.

Mattis, General James N., *Statement of General James N. Mattis, USMC, Commander, United States Joint Forces Command, Before the Senate Armed Services Committee*. Committee on Senate Armed Services, 111th Congress, sess. 2, 9Mar10, <http://www.jfcom.mil/newslink/storyarchive/2010/sp030910.html>.

McKenzie, Kenneth F. Jr. "The Revenge of the Melian: Asymmetric Threats and the Next QDR." *McNair Paper* 62. Washington, DC: National Defense University Press, 2000.

Military Contribution to Cooperative Security (CS) Joint Operating Concept (Version 1.0). United States Department of Defense, 19Sep08, http://www.dtic.mil/futurejointwarfare/concepts/cs_jocv1.pdf.

Myers, Gene. "Getting To The Fight: Aerospace Forces and Anti-Access Strategies." *Air & Space Power Journal* (27Mar01), <http://www.airpower.maxwell.af.mil/airchronicles/cc/myers01.html>

National Defense Strategy. United States Department of Defense, Jun08, <http://www.defense.gov/news/2008%20national%20defense%20strategy.pdf>.

The National Military Strategy of the United States. Chairman of the Joint Chiefs of Staff, Feb11, http://www.jcs.mil/content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf.

National Security Space Strategy, Unclassified Summary, Jan11 http://www.dni.gov/reports/2011_nationalsecurityspacestrategy.pdf

National Security Strategy. The United States White House, Washington, DC: May10, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

New World Coming. United States Commission on National Security/21st Century, 15 Sep99, 143.

Ochmanek, David. "The Air Force: The Next Round." In Hans Binnendijk, *Transforming America's Military*. Washington, DC: NDU Press: 159-192.

O'Rourke, Ronald. *Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress*. Washington, DC: Congressional Research Service, 17Jul09.

Petraeus, General David H. *Statement of General David H. Petraeus, U.S. Army Commander U.S. Central Command Before the Senate Armed Services Committee on the Posture of U.S. Central Command*. Committee on Senate Armed Services, 111th Congress, sess. 2, 16Mar10. <http://armed-services.senate.gov/statemnt/2010/03%20March/Petraeus%2003-16-10.pdf>

Posen, Barry R. "Command of the Commons: The Military Foundation of U.S. Hegemony." *International Security* 28, no. 1 (Summer 2003): 5-46.

Quadrennial Defense Review Report. United States Department of Defense, Washington, DC: 12Feb10, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.

- Seabasing for the Range of Military Options*. United States Marine Corps, 26Mar09.http://www.quantico.usmc.mil/MCBQ%20PAO%20Press%20Releases/090430%20CDI%20Docs%20CDI_SeabasingMilOps.pdf.
- Seabasing Functional Solution Analysis (FSA) #2 Operational Speed, Final Report (Version 1.3)*. United States Joint Force Command J9 Capabilities Solutions Group. Suffolk, VA: 25May10.
- Seabasing Joint Integrating Concept (Version 1.0)*. United States Department of Defense, 1Au05,
http://www.dtic.mil/futurejointwarfare/concepts/jic_seabasing.doc.
- Spacey, William L. “*Does the United States Need Space-Based Weapons?*” Cadre Paper 4. Maxwell AFB, AL: Air University Press, 1999: 1-7, 109.
- Stavridis, Admiral James G. *Testimony of Admiral James G. Stavridis, United States Navy Commander, United States European Command Before the 111th Congress 2010*. House and Senate Armed Services Committee. 111th Congress, sess. 2, 2010,
<http://www.eucom.mil/documents/EUCOposture-statement-03-09-10.pdf>.
- Talmadge, Eric. “Chinese Missile Could Shift Pacific Power Balance,” *Associated Press*, 5August10,
http://news.yahoo.com/s/ap/20100805/ap_on_re_as/as_china_us_carrier_killer.
- Tangredi, Sam J. *Futures of War: Toward a Consensus View of the Future Security Environment, 2010-2035*. Newport, RI: Alidade Press, 2008.
- . “Beyond the Sea and Jointness.” *U.S. Naval Institute Proceedings* 127, no. 9 (Sep01): 60-63.
- Unified Quest 2010, Initial Findings. U.S. Army Future Warfare Study, (Available on Army Knowledge Online).
- U.S. Congress. Department of Defense Annual Report. *Military Power of the People’s Republic of China 2009*. 111th Cong., 1st sess., 2009.http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf
- van Tol, Jan with Mark Gunzinger, Andrew Krepinevich, and Jim Thomas. *AirSea Battle: A Point-of Departure Operational Concept*. Washington, DC: Center for Strategic and Budgetary Assessments, 2010.
- Ward, General William E., *Statement of General William E. Ward, Commander, United States Africa Command Before the Senate Armed Services Committee*. Committee on Senate Armed Services, 111th Congress, sess. 2, 9March10, <http://www.africom.mil/getArticle.asp?art=4133&lang=0>
- Widnall, Sheila E. “The Space and Air Force of the Next Century,” address to the National Security Forum, Maxwell Air Force Base, AL, 29May97.
- Yoshihara, Toshi. “Chinese Missile Strategy and the U.S. Naval Presence in Japan.” *Naval War College Review* 63, no. 3 (Summer 2010): 39-62.

THIS PAGE INTENTIONALLY LEFT BLANK

