Understanding the Anti-Access and Area Denial Threat: An Army Perspective

A Monograph

by

MAJ Ben Jackman
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2015-01

Approved for public release; distribution is unlimited.
Understanding the Anti-Access and Area Denial Threat: An Army Perspective

The U.S. Department of Defense has designated newly developed technologies with increased range and lethality, designed to prevent opposing forces from maneuvering to or within an operational area, as “anti-access” and “area denial” threats. These threats represent one of the most significant challenges to U.S. military superiority and could potentially threaten U.S. interests abroad if the U.S. does not take steps to balance those threats with new strategies. Understanding the capabilities referred to by the anti-access and area denial labels, and the ways potential adversaries may employ those capabilities, provides the first key to mitigating their presence, deterring their use, and defeating them in combat if necessary. The Army must recognize its role in overcoming these threats and the implications they will have on the way the Army operates as part of the joint force. Finally, the Army, in coordination with the other services, must organize and train to defeat anti-access and area denial threats both to strategically deter anti-access and area denial capabilities from being used against them, and in anticipation of defeating them operationally in future conflict.
Monograph Approval Page

Name of Candidate: MAJ Benjamin E. Jackman

Monograph Title: Understanding the Anti-Access and Area Denial Threat: An Army Perspective

Approved by:

______________________________, Monograph Director
Peter J. Schifferle, PhD

______________________________, Seminar Leader
James MacGregor, COL

______________________________, Director, School of Advanced Military Studies
Henry A. Arnold III, COL

Accepted this 21st day of May 2015 by:

______________________________, Director, Graduate Degree Programs
Robert F. Baumann, PhD

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)
Abstract


The US Department of Defense has designated newly developed technologies with increased range and lethality, designed to prevent opposing forces from maneuvering to or within an operational area, as “anti-access” and “area denial” threats. These threats represent one of the most significant challenges to US military superiority and could potentially threaten US interests abroad if the US does not take steps to balance those threats with new strategies. Understanding the capabilities referred to by the anti-access and area denial labels, and the ways potential adversaries may employ those capabilities, provides the first key to mitigating their presence, deterring their use, and defeating them in combat if necessary.

Development of AirSea Battle by the US Air Force and US Navy, coupled with the application of capabilities as outlined by existing joint doctrine, may provide a way to accomplish the imperative set forth in the 2012 Defense Strategic Guidance – to project power despite anti-access and area denial challenges. Additionally, operational level planners must consider a critical review of joint doctrine with respect to the new and emerging threats posed by increasingly sophisticated anti-access and area denial weapons, as well as how to integrate the ideas presented by the AirSea Battle concept into existing or newly developed joint doctrine.

In the resource-constrained era of the near future, the joint force will require efficient solutions to difficult problems such as the one caused by anti-access and area denial weapons. The Army must recognize its role in overcoming these threats and the implications they will have on the way the Army operates as part of the joint force. Finally, the Army, in coordination with the other services, must organize and train to defeat anti-access and area denial threats both to strategically deter anti-access and area denial capabilities from being used against them, and in anticipation of defeating them operationally in future conflict.
Introduction

Early in the afternoon on 16 September 1943, a German Dornier Do 217K bomber and its crew of four men reached their cruising altitude of 18,000 feet. They flew far above the maximum ceiling of any effective Allied harassment except perhaps a rare interception by the high altitude capable P-38 Lightning, with its dual engines and formidable twenty millimeter cannons. Keeping a watchful eye out for formations of P-38 fighters rising to meet them, the German crew set course for Allied warships supporting the US Fifth Army’s tenuous position at the Salerno beachhead on mainland Italy. Upon sighting the fleet, the crew targeted the HMS Warspite, a heavily armored super dreadnought with fifteen-inch guns and carrying 5,000 tons of water for the Allied attackers. Bombardier and pilot of the Dornier bomber exchanged final terse radio commands in the high altitude cold as the bombardier released three Fritz-X 1400 bombs, carefully guiding them towards their intended target with radio controls. The new, and at the time highly sophisticated, bomb technology allowed the Dornier crew to score three hits on the Warspite, sending her back to Malta for repairs. Fortunately for the Allies, their naval losses and the 8,659 casualties caused by ferocious German Army counterattacks against the Salerno beachhead were not enough to repel them. They had narrowly succeeded, and had learned much in doing so – as had the enemy, and as would future students of their historic battle.1

Of the many lessons taken from the Allied advance through Italy, the Germans realized that their most significant chance to stop the Allied force came and went with the US Fifth Army’s establishment of a lodgment at Salerno and the German withdrawal to defensive positions at the Viktor Line, the location where they intended to make a final stand across the Italian peninsula. Despite heavy losses, the Americans and their allies inevitably forced their way up the

---

Italian peninsula in the months that followed, making the lesson clear – the Americans may make their enemies pay dearly if allowed to establish a foothold in the operational area. This lesson remains true today. With economic and military strength still difficult to rival, potential adversaries to the United States must consider ways to mitigate those strengths. One of those ways may be through use of strategies reminiscent of the Dornier bomber, by attacking the US force at or before the point of lodgment with weapons difficult to detect or counter. These strategies have been given the label “anti-access and area denial,” and the last decade has seen not only an increase in proliferation of the means to execute these strategies globally, but also an effort to counter anti-access and area denial with new approaches developed by and for the US military. The concept known as Air-Sea Battle remains one of the most significant of these approaches, and even as it continues to evolve, the US military must continue to develop understanding of threats abroad to describe and direct efficient and effective ways to mitigate those threats.

On 08 January 2015, the director of the US Joint Staff released a memorandum that effectively re-named the concept known as Air-Sea Battle to the Joint Concept for Access and Maneuver in the Global Commons. While the details of the new concept remain classified, speculation as to the reason for the new moniker indicates that it has to do with an increased multi-service interest in the problems addressed through the original Air-Sea Battle idea. Originally proposed by teams of think-tank scholars and planners representing the interests of the US Air Force and the US Navy, Air-Sea Battle attempted to resolve a perceived shift towards instability in the Western Pacific Theater of Operations. They assessed Chinese development of

---

2 Director, Joint Staff, Memorandum for Deputy Commanders of the Combatant Commands: Joint Concept for Access and Maneuver in the Global Commons (Washington, DC: Government Printing Office, 8 January 2015), 1.

anti-access and area denial capabilities as the primary driver of this instability. The growing range, sophistication, and proliferation of Chinese systems, to include ballistic and cruise missiles, integrated air defense systems, advanced fighter aircraft, and cyber warfare tools, caused the Secretary of Defense to direct the Air Force and the Navy to develop the ways and means necessary to balance power in the region by countering Chinese military attempts to threaten US power projection. The authors of Air-Sea Battle attempted to do this by mitigating the new threats with proposed changes to the force structure and posture of naval and air forces operating in the Western Pacific region.

Originally proposed in 2010, Air-Sea Battle recommended a strategy with selected initiatives intended to preserve regional military balance and ensure victory in the event of necessary military intervention in the Western Pacific region. However, as indicated by the 2015 memorandum mentioned above, the significance of potential threats in the Western Pacific has gained traction with military audiences beyond those planning for that specific theater. Just as the Chinese People’s Liberation Army has done, other potential adversaries may see the benefits of developing anti-access and area denial strategies. These strategies may aim to undermine the ability of the US to assure its allies that it maintains global freedom of maneuver, reducing US military credibility and causing unfavorable shifts in power. The US military must therefore

---

4Ian Easton, *China’s Military Strategy in the Asia Pacific: Implications for Regional Stability* (Arlington, VA: Project 2049 Institute, September 2013), 3-13. Easton correctly points out that China’s current strategy seeks not only to undermine the military superiority of the US in the western Pacific, but that a successful Chinese military modernization campaign will increase the probability of conflict in the region.


recognize that anti-access and area denial threats are a cause for concern across the globe, not just within 2,000 kilometers of the Chinese coastline.\(^8\)

Additionally, the US military must recognize that strategies to mitigate the asymmetry caused by development of new anti-access and area denial capabilities should not reside in the capabilities of any single military service, so that political leaders and operational planners retain flexibility for their responses to these threats. Effective strategies must account for threats to US power projection across all domains – land, sea, air, space, and cyber – and leverage the strengths of the joint force, as well as provide US political leaders with a range of options that does not force them to employ politically unsuitable means to the situation. In certain cases, such as the one presented by new potential threats in the Western Pacific, some domains will have less relevance than others or play only a minor supporting role. In other cases, the joint force may find itself fully engaged across all domains, whether conducting operations to deter conflict or operations to seize the initiative and dominate the battlefield during open hostilities.\(^9\) In light of the need to maintain joint assured access to deter war or win should the need arise, continued emphasis on development and evolution of regionally focused joint concepts such as the formerly titled Air-Sea Battle provide good mechanisms to this end. However, further exploration and analysis of the common and central problem to assured access may allow the joint force to not


only solve immediate problems of access and regional military balance, but also may permit for
development of a broader planning framework that accounts for anti-access and area denial
threats.

This study develops recommendations for land component planners within the joint force
seeking to mitigate the problems caused by anti-access and area denial strategies and their
associated means. The intent is to deliver these recommendations in the context of design and
operational art, constructs understood by joint planners.\textsuperscript{10} To do this requires an argument that
presents several ideas in a logical fashion. The argument must include a description of the terms
“anti-access” and “area denial” to develop an understanding of why the ideas and capabilities
these terms represent may cause problems for future operational level military planners. This
description should account for the means available to potential adversaries, the ways in which
they could employ those means, and the significance of the concepts and terms themselves. The
argument must also address doctrine relevant to the land component’s role in meeting anti-access
and area denial threats. This includes analysis of doctrinal joint concepts for forcible entry
operations, as well as the unclassified published ideas proposed in the Air-Sea battle concept.
Finally, this argument must contain the ideas necessary for planners to consider when developing
a joint forcible entry operation plan, with recommendations as to the steps the US military can
take now to make those plans more efficient and/or effective in their execution.\textsuperscript{11}

The value inherent in making the argument described above stems from the continuous
need for the US military to assess its ability to meet the strategic goals of the country, as well as


efficiency as the ratio of resources expended to the results gained, and defines effectiveness as the
quality of the results it produces. An older document – Headquarters, Department of the Army,
42 – notes that the possibility exists for efficiency and effectiveness to become adversarial
concepts, which will “tear at the moral, operational, and administrative fabric of organizations.”
its impact on actors, norms, and environments across the globe. By contributing to the study of threat weapons and strategies to employ them, this argument enhances understanding of the ability of the US to defeat those threats if necessary to pursue broader strategic or operational goals.\textsuperscript{12} It also enables further discussion about the relationships between those threats and US power, even when the US has not directly engaged those threats in open conflict. Finally, the discussion presented here may allow military planners to identify capability gaps within US formations based on a more detailed or nuanced understanding of enemy strategies and means. Should this occur, the research and analysis presented in this discussion might help to communicate a clearer understanding of the problem to the agencies and institutions that have a role in developing solutions to those problems.

So what has caused the perception that anti-access and area denial threats present a new or increasingly dangerous problem? The US military has a long history of overcoming contested access to its intended operational area, and then fighting effectively to achieve the maneuver space necessary to continue operations and supply new troops and material to the battlefield.\textsuperscript{13} It therefore seems hollow to imply that enemy actions to deny access to key terrain, or actions to prevent freedom of maneuver in that terrain, represent a new problem simply because unique terms have been crafted that mean those very things. However, as discussed in the following pages, these terms do represent something new. They represent not only linear, and therefore predictable, changes in technology; they represent the potential for changes in enemy strategies that could affect warfare during the execution phase, as well as the balance of power between the

\textsuperscript{12} Headquarters, Department of the Army, \textit{Army Doctrine Publication (ADP) 1-02: Operational Terms and Military Symbols} (Washington, DC: Government Printing Office, August 2012), 1-12. Defeat is defined as: a tactical mission task that occurs when an enemy force has temporarily or permanently lost the physical means or the will to fight. The defeated force’s commander is unwilling or unable to pursue his adopted course of action, thereby yielding to the friendly commander’s will, and can no longer interfere to a significant degree with the actions of friendly forces. Defeat can result from the use of force or the threat of its use. Defeat is not defined in JP 1-02, the Joint Dictionary of Military and Associated Terms.

\textsuperscript{13} Matthew E. Davin, \textit{Anti-Access/Area Denial: Time to Ditch the Bumper Sticker?} (Newport, RI: Naval War College, 2013), 1-6.
US and other actors in peacetime.\textsuperscript{14} If not thoroughly understood, planned for, and dealt with promptly, the implications of anti-access and area denial threats could be grave.

The presence and proliferation of anti-access and area denial threats has created some serious concerns for operational planners. The military should continue to develop understanding of these threats in order to ensure superiority across all domains and the ability to seize the initiative against all adversaries. Defeating anti-access and area denial strategies and capabilities in the future requires that the US military understands these threats, understands the strengths and weaknesses of existing plans to meet those threats, and has broad conceptual guidance ready to guide future operational planning in an anti-access and area denial environment. Only by understanding both the capabilities and strategies of potential enemies, along with the strategies and capabilities of the US military, can planners adequately prepare to achieve superiority and operational success on the battlefield. The argument that follows addresses each of these components specifically as they relate to operational level land component planners, while simultaneously attempting to provide an appreciation of the broader concerns relevant to the joint US force as a whole.

What Do Anti-access and Area Denial Mean?

Anti-access and area denial capabilities are those mechanisms that prevent US forces from entering an area of operations or expanding operations from an initial lodgment. Anti-access and area denial capabilities, often referred to simply as “A2AD,” represent more than a linear technological progression towards increasingly sophisticated and long range weapon systems.\textsuperscript{15} While certainly true that the ever-increasing range of missile systems, manned and unmanned

\textsuperscript{14}Van Tol, et al, x.

\textsuperscript{15}Brendan P. Walsh, \textit{Access Denied: Future Military Operations in an Anti-Access Environment} (Newport, RI: Naval War College, 4 May 2011), 5. Walsh makes the argument that the exponential increase in technology development has made or may make US aircraft carriers obsolete, requiring a major shift in how the US thinks about power projection, particularly in the western Pacific.
aircraft, and other technologies play a potentially pivotal role in future warfare, the real threat of anti-access and area denial systems lies in the concept itself. Anti-access and area denial capabilities represent the idea that future adversaries of the United States will attempt to prevent their ground forces from ever engaging with US forces in maneuver engagements. Future adversaries will instead rely on anti-access and area denial capabilities to shape engagements in their favor, using a “silver bullet” at the outset of military conflict. Given their understanding that US forces could quickly seize and maintain the initiative if allowed to plan and execute military operations without the threat of an early and devastating anti-access or area denial attack, the development of anti-access and area denial capabilities makes logical sense for adversaries attempting to mitigate US power projection.16 This thinking highlights that actors across the globe, primarily states, have identified a way to mitigate the asymmetry caused by the overwhelming dominance of US ground forces when engaged in combined arms maneuver at the operational level.

The US military, and the Army specifically, should remain concerned about the increasing proliferation of the anti-access and area denial idea. If the US Army cannot get to the fight, or if it cannot employ capabilities as required to complete missions in support of operational and strategic goals, then it will not fulfil its purpose to fight and win the nation’s wars.17 To address the anti-access and area denial problem, the US military developed a joint

16 Ben Berk, China’s Silver Bullet: A Brief Analysis of the Threat Posed by the PRC’s Anti-ship Ballistic Missile (Chapel Hill, NC: University of North Carolina Printing Office, 2011), 4-5. Berk highlights the Chinese development of the DF-21d ballistic missile as a “silver bullet” response to American Carrier Strike Group power projection in what China considers its territorial waters. He uses “silver bullet” in the colloquial sense – a single point solution assumed to be fail safe.

17 As stated in Headquarters, Department of the Army, Army Doctrine Publication (ADP) 1: The Army (Washington, DC: Government Printing Office, September 2012), 1-1; the Army provides the United States with the landpower to prevent, shape, and win in the land domain. Contrast this with the purposes laid out in Title X of US Code, listed as: “preserving the peace and security, and providing for the defense, of the United States, the Commonwealths and possessions, and any areas occupied by the United States; supporting the national policies; implementing the national objectives; and overcoming any nations responsible for aggressive acts.
concept for entry operations, intending to guide service specific planning by providing a framework for forcible entry operations that accounts for anti-access and area denial threats. However, the Department of the Navy and the Department of the Air Force had already developed a service specific concept prior to publication of the capstone joint concept. Labeled “AirSea Battle,” this concept provides broad solutions useful for air and naval forces in an attempt to redress the change in balance of power in the Pacific region based on China’s development of anti-access and area denial systems. This does not mean that the joint capstone concept and the jointly developed AirSea Battle concept are at odds; it does mean that the Army and Marine Corps must jointly develop a concept for the land component force that addresses anti-access and area denial, nests within the joint capstone concept, and leverages the strengths of AirSea Battle when applicable.

By first describing what constitutes anti-access and area denial threats as a whole, what differentiates anti-access from area denial, and why these threats represent a significant departure from the ways adversaries of the US have operated in the past, the Army can be better prepared to determine how it intends to fight in the future. Because these ideas are not new, a number of published works have already defined anti-access and area denial and described their significance to the joint force of the twenty-first century. Not all of these definitions and analysis appear to agree perfectly, and the argument that follows here attempts to describe each of the predominant schools of thought and reconciles them to a common understanding of anti-access and area denial threats. Additionally, because the terms “anti-access” and “area denial” play such a prominent

---


Richard A. Bitzinger and Michael Raska, The AirSea Battle Debate and the Future of Conflict in East Asia (Singapore: S. Rajaratnam School of International Studies, February 2013), 3-4. While numerous articles describe Air-Sea Battle, this one attempts to describe its conceptual evolution, with particular focus on why Chinese capabilities have become central to the concept.

Davin, 1-6. Davin provides evidence that challenges the idea that anti-access and area denial threats represent a new way of war, but acknowledges the increased risk posed by evolving threats.
role during the development of a joint approach to forcible entry, the importance of the terms themselves also receives analysis.

The language used to describe the idea that US forces may face significant challenges when conducting future joint forcible entry operations helps to create immediate understanding for a broad range of audiences. By using the terms “anti-access” and “area denial,” leaders can succinctly describe the most critical part of the problem facing a joint force when conducting a forcible entry operation. While representative of a larger problem – the shift away from the current battlefield asymmetry that favors the US – use of the terms anti-access and area denial focuses the audience’s attention on the systems that present the a significant threat to the US joint force.20 There are actually two different, although related, ideas captured by the terms anti-access and area denial. However, by placing the terms together, and especially by using the abbreviated term “A2AD,” the audience receives the message that these two ideas are not only related, but inseparable. It means that problems with access, traditionally left to naval and air forces to solve, must be looked at in conjunction with a traditionally Army-centric problem, that of how to maneuver once in a given area. The phrase “anti-access and area denial” provides not only a central clue as to a significant problem facing the joint force, it reinforces the idea that no potential exists for future operations conducted by a single service. Future operations will be joint and likely multi-national endeavors, and a problem for one service and one country impacts and requires the support of other services and countries.21

---

20Joel Wuthnow, The Impact of Missile Threats on the Reliability of US Overseas Bases: A Framework for Analysis (Carlisle, PA: US Army War College, January 2005), 6-9. For further discussion of the asymmetry caused through acquisition of cruise and ballistic missiles, see Wuthnow’s excellent analysis of ballistic missile effects as both a conventional and WMD capability.

21Gregory T. Kiley and Nicholas F. Szechenyi, U.S. Force Posture Strategy in the Asia Pacific Region: An Independent Assessment (Washington, DC: CSIS, August 2012), 23-42. Kiley and Szechenyi explore the inter-related needs of militaries specifically in the Asia Pacific region, highlighting the cooperative requirements necessary to balance threats, both in peacetime and in the event of combat.
What is an Anti-access Threat?

The analysis that follows describes what anti-access means and why it may be relevant to Army planners, today and in the future. Anti-access threats include all mechanisms an opposing force might use to prevent US forces from reaching and establishing a lodgment in a given area of operations. In the ends-ways-means framework for strategic analysis, anti-access mechanisms can refer to both means or ways. As means, anti-access capabilities refer primarily to military hardware with sufficient operational reach to interdict US forces outside of the intended operational area.22 As ways, anti-access capabilities refer to a broad spectrum of activities that an opposing force could leverage to prevent a US force from reaching the operational area, including social and political pressures as well as military strategies. For operational planners, understanding the breadth of anti-access mechanisms facilitates development of their understanding of the operational environment by providing a framework that addresses a likely center of gravity during Phase One operations. Therefore, it is worth looking at the ends, ways, and means encompassed by the “anti-access” term.

Given the need for US forces to gain access to an operational area, adversaries would likely begin or continue preparations to deny US forces this access. This starts with the development and execution of strategies, or ways, designed to prevent US forces from moving to the operational area, establishing a foothold, or continuing operations within the operational area to seize the initiative and establish dominance. To accomplish this goal, adversaries would likely focus on executing a strategy to disrupt US troop movement, leveraging political means to weaken international support for the US operation, and exploiting opportunities to reduce the will of the US from continuing the operation.23 To meet strategic goals, US operational level planners

---


must understand each of these ways, determine how the US is most vulnerable to these strategies, and attack the enemy’s anti-access capabilities while mitigating the damage the enemy attempts to inflict.

The first concern for operational planners as they plan a forcible entry operation must be the military operational possibilities available to their adversary that might prevent US forces from gaining access to the operational area. These possibilities are likely to leverage military means, tied in with existing physical barriers and obstacles, to disrupt or prevent US forces attempting to access the operational area. For Army planners this presents a specific difficulty because US Army forces are unlikely to be able to move to the operational area without joint assets. This means that Army planners must engage in a dialogue with their joint service counterparts to describe how Army forces must arrive to the operational area to ensure success in follow on operations. Together, Army planners with the joint planning team must then determine the military means available to the enemy and how the enemy could disrupt the movement of US troops and equipment in the manner required. The specific anti-access tactics the enemy might employ could include attacks against US bases, attacks against shipping and troop transport, denial of specific avenues of approach and lines of communication, or attacks against electronic infrastructure and networks.

As previously mentioned, enemy anti-access threats are not limited to military strategies, despite the dominance of military ways and means. Operational planners must also consider the implications of diplomatic, informational, and economic instruments of power and the reciprocal effects created through military action. The enemy may leverage its ties to the international community, including powerful non-state actors such as the United Nations, to degrade international support for the US led operation. Any forcible entry operation will require US forces to use, and likely violate, the sovereign territory of another state. Operational planners will have

_Forces: An Assessment of Relative Costs and Strategic Benefits_ (Santa Monica, CA: Corporation, 2013), 101-104.
to consider a variety of options for use of airspace, basing, and ground maneuver that consider the political landscape. Even the most tactically sound military option will fail if planners do not consider the enemy’s ability to deny access through political maneuvering. This means that requirements for support from allies and potential partners must be identified early, continually assessed, and protected from enemy attempts to influence the supporting states.

Another significant component of an anti-access strategy is the enemy’s ability to influence operations by degrading US will to continue the operation. In this sense, anti-access strategies overlap with adversarial attempts to deter US intervention in a given region. These strategies may blend threat and use of force with information operations to influence perception of the conflict and US public support for continued intervention. Such a strategy would likely use media coverage of US casualties and other propaganda tools to reduce the perception that the US has a vital interest in the region, forcing political leaders to reconsider the cost of using military force in the region. While not a new concept, technological advances have made this strategy more viable, especially for non-state actors, who will find it increasingly possible to access tools of propaganda and messaging traditionally associated with more powerful state actors.

Understanding the various means available to state and non-state actors for anti-access capabilities helps to illustrate the changing problems associated with this concept. So far, the argument presented has described several options for pursuing anti-access strategies against the US, each of which has attacked combinations of diplomatic, information, and military domains. However, the underlying assumption is that military power makes strategies in other domains possible. Therefore, the following discussion focuses purely on military means, specifically

---

where new or increasingly prolific hardware could make previously unlikely anti-access strategies more effective.

The most significant technological developments relevant to the anti-access problem include long-range precision strike systems, littoral anti-ship capabilities, and high quality air defenses. More traditional means exist for anti-access strategies as well, including special purpose forces conducting long range strikes, intercontinental ballistic missiles, and mines. Traditional in this sense has little to do with whether or not these means have been routinely employed, but merely indicates that they have existed for several decades – they do not represent a new capability, even if their employment would be novel.25

What is an Area Denial Threat?

The concept of an area denial strategy describes how US planners understand a shift in enemy thinking when confronted with a US-led forcible entry operation. This shift occurs as adversaries realize they can no longer pursue only activities to prevent US forces from entering an operational area, but that they must attempt to prevent US forces from expanding operations within the operational area.26 This shift does not imply that adversaries have abandoned anti-access strategies, but it does mean that enemy forces would become more likely to focus on degrading capabilities of US forces already positioned at a lodgment in the operational area. Given a finite amount of resources available to an adversary, this could mean that they would re-task capabilities previously committed to anti-access purposes to area denial roles inside the operational area.

The common conception of area denial systems defines them as capabilities designed to limit freedom of action within an operational area. Specifically, area denial strategies aim to

25Gordon and Matsumura, ix.

prevent an attacking force from expanding their lodgment at the point of penetration in the operational area, preventing them from reaching objectives beyond the lodgment or expanding it to allow follow on forces to arrive and begin operations.\textsuperscript{27} Means for area denial include a wide range of military capabilities, including some already described as anti-access capabilities. This has led some authors to describe the distinction between anti-access means and area denial means primarily through range of the systems. In many cases, adversaries may employ means used for anti-access strategies in an area denial role, if minimum range and collateral damage caused by these systems inside the operational area is not a concern for the force employing them. Conversely, area denial systems have more limited range and ability to affect beyond the operational area without moving or maneuvering them, which would essentially expand the operational area. While adversaries could employ countless tactics to achieve area denial effects, analysis of all of them is not necessary in order to understand the changing nature of the area denial threat. Use of means commonly understood by planners today is not the focus of this argument. Instead, the intent here is to describe threats that may force changes to the way plans are developed and executed in the future.

Long-range artillery and rocket systems present some of the most serious area denial challenges for future planners conducting joint forcible entry operations. Rocket systems likely to be employed by future adversaries will generally consist of multiple rocket launchers (MRLs), useful for delivery of highly destructive fires on an area target. For example, the Russian made 9A52-2 MRL, a platform capable of launching twelve 300mm rockets every thirty-six minutes, has a range of up to ninety kilometers.\textsuperscript{28} This system represents the norm for threats in today’s environment. Future threats will pose greater problems as range and accuracy increases. The

\textsuperscript{27}Van Tol, et al, 9-15.

\textsuperscript{28}US Army TRADOC G-2, Worldwide Equipment Guide: Volume 1: Ground Systems (Fort Leavenworth: United States Army Training and Doctrine Command Intelligence Support Activity, August 2012), 7-49. The warheads fired by this system include approximately 230-260kg fragmentary, fuel-air-explosive, and napalm munitions with electronic timing fuzes.
Chinese are currently developing new families of MRLs, such as the WS-2, with ranges up to 300-350 kilometers.\textsuperscript{29} If used to prevent US forces from seizing and holding terrain, especially port and airfield infrastructures in the lodgment, these weapon systems could have a dramatic effect on the battlefield.

The argument presented thus far has described the differences between anti-access systems and area denial systems. The taxonomy used here intentionally represents a hybrid of two schools of thought concerning anti-access and area denial systems. The first school of thought sees the distinction between anti-access strategies and means as one primarily concerned with range. Essentially, this idea focuses on the fact that similar capabilities may be used for anti-access and area denial strategies, and that the main reason to differentiate between anti-access and area denial is to denote the purpose behind the capability being employed. On the other hand, some writers have argued that the difference between the two comes from the capabilities being used. The argument presented in this paper posits that both ideas must be considered when describing adversary capabilities; they can be classified as either anti-access systems or area denial systems based on their range, collateral damage considerations, and whether the system is likely to be used inside the proposed operational area or out of it.\textsuperscript{30}

\textsuperscript{29}Gordon and Matsumura, 17.

\textsuperscript{30}Andrew Krepinevich, Barry Watts, and Robert Work, \textit{Meeting the Anti-Access and Area Denial Challenge} (Washington, DC: Center for Strategic and Budgetary Assessments, 2003), 5-10. Randy Huiss, \textit{Proliferation of Precision Strike: Issues for Congress} (Washington, DC: Congressional Research Service, May 14, 2012), 1-6, 13-28. Krepinevich et al., made significant inroads into describing and differentiating anti-access and area denial threats through their purpose, a theme that later impacted development of Air-Sea Battle, with Krepinevich as a central proponent of the strategy, and with his writing on these subjects primarily published through CSBA. Gordon and Matsumura take a different approach, more specifically identifying systems and classifying them as either anti-access or area denial weapons. Their writing has been published through the RAND Corporation.
Current US Military Orientation on Anti-Access and Area Denial Threats

Enemy anti-access and area denial systems deployed in the defense have the capability to cause mission failure for attacking forces by disrupting movement, inflicting strategically unacceptable losses, denying expansion of the lodgment, and/or preventing effective combined arms coordination. Current and future anti-access and area denial systems provide one of the most, if not the most, significant obstacles for attacking army forces to overcome. A substantive review of the body of doctrinal knowledge that addresses how army forces intend to orient on and defeat these systems can therefore help to ensure that current doctrine remains relevant as anti-access and area denial capabilities become potentially more prevalent and lethal.

Joint Publication 3-18, *Joint Forcible Entry Operations*, lays out a basic construct for planning and executing joint forcible entry operations, providing planners with guidance for defeating contemporary enemy defenses at the point of lodgment to allow operations to expand in the pursuit of follow on objectives. JP 3-18 identifies twelve principles that provide the foundation for operations to gain a lodgment. These principles are: achieve surprise, control of the air, control of space, electromagnetic spectrum management, operations in the information environment, sea control, isolate the lodgment, gain and maintain access, neutralize enemy forces within the lodgment, expand the lodgment, manage the impact of environmental factors, and integrate supporting operations.31 Examination of the principles proposed in JP 3-18 allow the reader to develop a basic understanding of the current doctrinal construct for joint forcible entry operations. This provides understanding as to how US forces plan to defeat anti-access and area denial systems that orient against them enroute to and at the point of lodgment.

JP 3-18 first dictates that planners must achieve operational surprise in joint forcible entry operations. This means that at a minimum, planners must consider information operations,

---
operational security, military deception, and operational tempo.\textsuperscript{32} This requires planners to protect the actual details of the operational plan while simultaneously providing the enemy with information that causes him to think erroneously that he understands the friendly plan. Operational surprise prevents the enemy from targeting friendly forces in a way that would effectively or significantly disrupt the friendly plan.\textsuperscript{33} Future technological changes fail to nullify the importance of surprise as a fundamental planning principle. This should not come as a shock. Surprise remains one of the principles of US joint operations and one of the characteristics of the offense. However, increasing sophisticated weapons and detection systems could make surprise a more difficult principle to achieve, particularly when attacking a prepared defense.

Control of the air and control of the sea during forcible entry operations both have significant bearing on the land component force conducting the assault. Control of the air and sea domains represents a critical concern during operations in an anti-access and area denial threat environment that must be coordinated by the joint planning team. This control enables targeting inland of the objective, allows for rapid movement of ground troops and equipment into the lodgment, and sets the conditions to establish the lines of communication necessary for continued operations in the theater. However critical to the success of the ground operation, control of the air and sea domains relies primarily on the ability of a limited number of joint strike fighter aircraft to suppress anti-access systems long enough to project overwhelming ground and sea-based combat power into the theater and cripple enemy defenses.\textsuperscript{34} Especially considering the

\textsuperscript{32}JP 3-18, 1-2.

\textsuperscript{33}Headquarters, Department of the Army, \textit{Army Doctrine Reference Publication (ADRP) 1-02: Operational Terms and Military Symbols} (Washington, DC: Government Printing Office, August 2012), 1-13. Disrupt, in this sense, uses the definition from ADRP 1-02 to illustrate the difficulty in achieving an operational effect by using “direct and indirect fires, terrain, and obstacles to upset an enemy’s formation or tempo, interrupt his timetable, or cause his forces to commit prematurely or attack in piecemeal fashion,” when surprised.

\textsuperscript{34}Krepinevich, et al, iii. The authors point out that the F-35 aircraft may provide the only means to target SA-10D and SA-20 SAMS, as TLAM cruise missiles and other older or non-stealth technology would be largely ineffective.
imperative to fight in a joint construct, this singular reliance on a specific stealth airframe to ensure the ability of the force to project power into the theater of operations, both in the littorals and on land, may be a significant weakness in the current joint forcible entry construct, when potential adversaries develop countermeasures to those systems.35

Control of space and electromagnetic spectrum management both address the land force component’s reliance on digital information systems to support maneuver. Both provide the means to navigate, communicate, and share intelligence. ADRP 3-0, Unified Land Operations, acknowledges that both cyber and space domains may be increasingly contested in the future, meaning that future plans must address protection of the space and cyber capabilities critical to the mission at hand, redundancy in those capabilities, or the means to rapidly target enemy systems oriented on those capabilities.36 In an anti-access and area denial environment, control of the space and cyber domains equates to control of the effective employment of key weapons systems. Short and medium range ballistic missiles will remain particularly susceptible to electronic attack, as they require electronic systems for fire control and terminal guidance.37

JP 3-18 reiterates several points made earlier under the principle of information operations. It again mentions military deception, operational security, electronic warfare, and cyberspace operations. This principle also identifies the importance of key leader engagements and public affairs operations.38 Overall, the integration of these capabilities into a plan focused on defeating anti-access and area denial threats will assist commanders in controlling the narrative relevant to the situation, but may not have a direct tactical impact on the threat systems at hand.


36ADRP 3-0, 1-10.


38JP 3-1, I-4.
Next, JP 3-18 addresses the most critical components of a joint forcible entry operation, all focused on the initial lodgment. It directs planners to isolate the lodgment, gain and maintain access, neutralize enemy forces within the lodgment, and expand the lodgment. Anti-access and area denial systems play a key role in a unit’s ability to meet those requirements. Two of these tasks, isolation and neutralization, present planners and their units with tasks, clearly focused on the enemy. Isolation of the lodgment requires units at the operational level to prevent enemy units in the lodgment from receiving support from sources external to the lodgment and to restrict their movement within the lodgment. Considering that indirect fire support plays a critical support role to the enemy forces within the lodgment, and that prevalent medium range ballistic missiles (such as Iran’s Shahab-3b) have a range of up to 1,300 kilometers, this requires an attacking force to neutralize missile sites located throughout the threat country, area, or region to secure a lodgment. Using Iran as an example, to isolate a lodgment in any part of the country of Iran would potentially require an attacking force to neutralize every one of the up to 500 Shahab-3b missile sites in the country, which might be scattered, hidden, and defended in an area of over 600,000 square miles. That also assumes that no other actor external to Iran would attempt to prevent the attacker from achieving the lodgment, an assumption that if proved wrong, would only serve to exacerbate the problem.

The authors of the joint publication next direct units to gain and maintain access to the lodgment while expanding it, presumably simultaneously. This simple set of directions requires the effects of anti-access systems to be mitigated to a level at which they could not significantly impact the ability of the attacking force to not only get to the lodgment initially, but also to

continue to supply and reinforce the lodgment. In the face of conventional and anti-ship cruise and ballistic missiles, as well as an integrated air defense with a range of hundreds of kilometers from the border, all based or launched from mutually supporting sites across the theater, such a task becomes daunting. These directions also require units to mitigate the effects of area denial systems oriented on or placed within the lodgment. While expected to impede ground maneuver, these obstacles and weapons systems would require the attacking force to carefully balance requirements for joint support of maneuver forces within the lodgment with requirements for protection of lines of communication and bases outside of the lodgment. Again, in real terms, planners looking to seize a lodgment in Iran would need to balance requirements for air sorties and indirect fires over a division’s maneuver area with requirements to protect US bases and lines of communication from Shahab-3 and Shahab-4 medium range ballistic missiles. With these missiles targeting US bases in Oman, Qatar, Kuwait, and Saudi Arabia, support to forces in the lodgment would have to come from bases and platforms in excess of 2,000 kilometers from the front lines. This argument does not presume to conclude that the construct JP 3-18 lays out lacks feasibility, merely that the process involved in meeting the demands of this construct becomes increasingly complicated and risky as distances and requirements increase.

Finally, management of environmental factors and integration of supporting operations refer to anticipating and mitigating natural and manmade impediments to maneuver, leveraging special support capabilities for this and other mission critical tasks. Special operations forces, civil-military liaisons, or reconnaissance and surveillance assets could provide these special capabilities. The significance for units conducting a forcible entry operation against significant anti-access and area denial threats comes from the need to protect those assets, when leveraged, with capabilities far beyond that organic to the assets themselves or the units they support.

---


Planners cannot reasonably expect that enemy attempts to deny maneuver space on the ground or in the air will be limited to maneuver forces. They must understand that enemy attempts to degrade the capabilities of US unmanned aerial vehicles, special operations forces, long-range surveillance detachments, and other reconnaissance platforms will be part of the enemy’s plan to deny the US an advantage in battlespace awareness. These capabilities represent critical vulnerabilities that leaders must plan to protect during the conduct of a joint forcible entry operation.

While JP 3-18 has outlined ways to tackle joint forcible entry operations by leveraging the strengths of today’s US military, some analysts have described ways in which the future combat environment may change, potentially making the strengths of today’s military irrelevant in the future. As described in the previous section of this paper, anti-access and area denial threats may represent one of those changes. These threats may challenge US air superiority in ways not experienced since the Second World War, making the successful application of ground combat power both more difficult and more critical to overall operational success. To return superiority in all domains, and specifically in the air domain, to the United States, the military needed a new strategy that accounted for anti-access and area denial threats. This strategy has begun to emerge in the nascent doctrine broadly known as “AirSea Battle,” a concept that may offer a way to ensure continued US military superiority in the face of emerging anti-access and area denial threats.

The US Air Force and US Navy developed the concept of AirSea Battle to balance a perceived shift in military power in the Asia-Pacific region, specifically due to emerging anti-

\[42\] Krepinevich, et al, 75.


\[44\] Erik V. Larson, Assuring Access in Key Strategic Regions: Toward a Long-Term Strategy (Santa Monica, CA: RAND Corporation, 2004), 45-47. Note the US Joint Chiefs of Staff first released the classified version of the AirSea Battle Concept in May 2012, and the implementation plan for that concept in September 2012.
access and area denial threats developed by the Chinese People’s Liberation Army.\textsuperscript{45} While regionally focused and specifically designed for correcting a shift in US-Chinese power back in favor of the United States, the core concepts of AirSea battle provide a useful construct for examining how to defeat anti-access and area denial threats elsewhere in the world. AirSea Battle directs US forces to conduct a two-stage campaign, each with four distinct lines of effort. With the regionally specific verbiage removed, the first stage prescribes action to: withstand any initial enemy attacks, execute a “blinding campaign” against enemy C4ISR systems, suppress long-range strike systems, and to seize and sustain the initiative in air, sea, space, and cyber domains.

In the second stage, the lines of effort include: sustaining and exploiting the initiative across domains, conducting blockades from outside the enemy’s strike range, sustainment operations, and increased industrial production of war materials.\textsuperscript{46} This approach, while absent the ability to project land based combat power, shows the considerations taken for current generation anti-access and area denial threat systems in planning for future US power projection. An argument to consider re-imagination of the AirSea Battle construct for use as a broader, globally applicable construct begins with the two-stage design described above. It must also incorporate land forces, allowing the Army to provide a role during offensive land based operations, instead of assuming that air and sea power will be sufficient to achieve operational objectives.

Given the two primary constructs developed to support US efforts to project force into hostile environments, several gaps appear between the perceived understanding of the significance of the threat and the joint reaction to that threat. To develop a comprehensive argument, the specific implications of those gaps must be considered. Would the US Army and its joint counterparts succeed in an offensive operation directed against anti-access and area denial

\textsuperscript{45}Van Tol, et al, ix. The authors express the intent of the AirSea Battle concept as one to offset China’s rapid increase in A2/AD technology and proliferation of systems that would affect the US ability to project power into the region if left unchecked.

\textsuperscript{46}Van Tol, et al, 52-53. The “two stage” verbiage falls outside normal doctrinal language for the US Army, but has been preserved here to prevent confusion with “phases” as normally used when planning joint operations.
threats if they employed current doctrine? If the answer to that question is no, the changes that need to be made, and the timeline necessary to make them must also be considered, especially when considering that those changes may require more than rearranging operations — they may require changes to basing, materiel solutions, doctrine, or training methods at the operational level.

Implications of Anti-Access and Area Denial Threats

The Army currently deploys around the globe with little concern for potential enemy threats to forces travelling to theaters of operation, despite continued involvement in campaigns against globally organized terror networks.\(^4^7\) Given the nature, proliferation, and capabilities of anti-access and area denial systems as previously described, Army planners cannot assume assured access to a theater of operations against a determined and aggressive adversary. Instead, planners must assume that adversaries will contest the initiative, meaning the ability to control the situation, in every domain from the start of operations.\(^4^8\) The land component force’s ability to seize the initiative in future conflicts could be severely degraded by enemy anti-access and area denial threats if those threats are not properly addressed during ongoing planning and preparation for future combat. While the Navy and Air Force have provided conceptual frameworks for these threats, as well as next generation equipment to match their jointly developed concepts, the Army has paid less attention to anti-access and area denial threats and more attention to the conduct of campaigns once the force achieves access to the theater. If concepts developed by the Navy and Air Force, under the umbrella term “Air-Sea Battle,” can definitively assure access for Army

\(^4^7\)Brendan P. Walsh, Access Denied: Future Military Operations in an Anti-Access Environment (Newport, RI: Naval War College, 4 May 2011), 1. In his opening remarks, Walsh notes that the ability of the US to project power globally has been virtually unchallenged since the end of the Cold War.

forces to any theater under a variety of conditions, then any argument to suggest that the Army must play a bigger role in overcoming anti-access and area denial threats becomes pointless. However, the likelihood of a successful forcible entry operation against a near-peer enemy without the application of land power directly integrated into that operation is small.\textsuperscript{49}

To exacerbate the implications of anti-access and area denial threats during forcible entry operations for the Army, this argument focuses primarily on the Army as the land component force, writing out the Marine Corps and its capabilities, as done throughout this paper. This construct does not intend to imply that Marine capabilities, if applied correctly, could not solve the anti-access and area denial dilemma, it merely allows this argument to focus on an operation or a portion of an operation where Army forces must gain entry into a theater without a Marine force directly preceding or supporting them. Any number of future combat scenarios make this assumption plausible. For example, Marine forces may have been committed elsewhere or the conflict may be large enough that the Marine Corps cannot provide combat power for all of the initial forcible entry operations needed. Perhaps most likely, Marine forces might not be able to leverage their distinct amphibious or vertical envelopment capabilities from the sea because the risk to ships by enemy anti-access and area denial systems has been deemed too great. In this case, the Marines would find themselves in a similar predicament as the Army – they would need to deploy from a land base directly into the theater of operations and either service would need to solve similar problems.\textsuperscript{50}

Another key assumption stems from the need for Army forces to prepare to deal with anti-access and area denial threats in the conduct of future operations. This assumption is that


\textsuperscript{50}Joint Chiefs of Staff, \textit{Joint Concept for Entry Operations} (Washington, DC: Government Printing Office, 7 April 2014), 23-33. This document, signed by General Martin E. Dempsey in the foreword, describes the capabilities required for implementation of the Joint Concept for Forcible Entry Operations, listing these capabilities by warfighting function and making the assumption that both Marines and Army service forces can meet these requirements, albeit with different means, in a land component role.
Army forces have to defeat an enemy center of gravity under the protection of anti-access and area denial systems in order to achieve their broader strategic purpose. This means that situations where friendly forces gain advantage and reach strategically favorable decisions through deterrence or another use of Army forces that does not require them to penetrate an anti-access and area denial defense, do not apply here. While seemingly self-evident, this assumption means that one cannot conclude that Army forces have no business attacking an enemy with a robust and intact anti-access and area denial system. The emphasis is on the need for the Army to deliver the punch that defeats the enemy, because air and naval forces cannot deliver the decisive blow to the enemy center of gravity without the “boots on the ground” that the land component alone supplies.51

The broad range of anti-access and area denial threats available to potential future enemies provide an inexhaustible number of combinations of threats they could employ against a deploying Army force. Furthermore, numerous leaders have remarked on the Army’s inability to predict accurately future warfare scenarios accurately, meaning that commitment to any particular military solution today could very likely be useless tomorrow.52 Given this, the Army must recognize that the ongoing trends towards more capable and prolific anti-access and area denial systems have some real implications for future deployments of Army forces. Leaders, and especially planners at the Corps and Division levels, must recognize that getting to the fight will potentially challenge them as much as achieving a decision once engaged in the fight, that new centers of gravity will develop based on emerging anti-access and area denial threats, and that


52Micah Zenko, “100% Right 0% of the Time: Why the US Military Can’t Predict the Next War,” accessed January 2015, http://foreignpolicy.com/2012/10/16/100-right-0-of-the-time/. Zenko details four separate incidences from 2010 through 2012 where senior US Army officers acknowledged the inability to predict the scope or location of future conflict, usually with tongue-in-cheek comments such as Major General H.R. McMaster’s 2012 quote: "We have a perfect record in predicting future wars — right? … And that record is 0 percent."
Army forces will be required to attack and protect vulnerabilities that may have been assumed away in the past.\textsuperscript{53}

Getting to the fight presents the first of several challenges for operational level planners when confronted with anti-access and area denial threats. While a panacea solution for deploying forces from their starting location into the area of operations cannot be developed here, it would similarly be unwise to concede that planners will be able to simply muddle through the complexities of an anti-access and area denial environment without any prior attention given to the matter. For this reason, this argument attempts to highlight some of the changes that an anti-access and area denial threat environment may have on operational planning, even absent the particular details relevant to the envisioned future conflict.

Planning deployment of forces necessitates a starting point for those forces, which for the vast majority of scenarios will be military bases within the United States. In the past, movement of forces from their initial locations in the United States to intermediate staging bases forward has been largely a logistics problem, with little attention paid to threats to the deploying forces to the rear of the designated intermediate staging base. Future scenarios could require planners to revise the assumption that friendly forces are generally free from threats in the US and to the rear of the intermediate staging area, as well as necessitating a revision of the calculus involved in determining the location of the intermediate staging area, if used at all. This not only complicates planning by removing the sanctity of movement to and from rear areas as a purely logistical problem, but also means that commanders may have to consider the combat power required to protect those areas and the lines of communication from them to the theater of operations. Therefore, the new considerations for movement of forces from a starting location to the theater of operations fall into three broad, and potentially overlapping categories – protection of rear areas, security along global lines of communication, and planning for the intermediate staging

area. Looking at each of these areas in turn will facilitate understanding of the problems associated with each.

Rear areas, especially those in the continental US, have often been irrelevant during development of plans for forces operating in foreign theaters. This is not to say that protection for military basing in the United States has never been a concern, but it does imply that protection of those bases has not required commanders to commit significant combat power or resources to protecting those bases that they could otherwise utilize as an operational level maneuver capability in the forward theater of operations. Instead, the major components needed to protect bases and assets in the United States have been incorporated into strategic plans and mechanisms that protect the US as a whole, not military infrastructure specifically. Theater ballistic missile defense infrastructure offers a good example of infrastructure that enables protection of military assets without existing solely for the protection of military personnel, equipment, or basing.

The vulnerability of US bases and stateside infrastructure to attacks does not come from a rapid advance in technology or a game-changing capability projected to be in the hands of potential enemies in the near future. The threat to stateside infrastructure comes from future enemies with the desire to prevent their main combat forces from ever encountering US forces on the battlefield. Future enemies who assess significant asymmetry in major combat forces in favor of the US will conduct anti-access attacks to degrade the ability of US forces to engage them. This could start with attacks against US bases by enemy special operations forces, by

---


56 Mark Stokes, *China’s Evolving Conventional Strategic Strike Capability* (Arlington, VA: Project 2049 Institute, September 14, 2009), i.

ballistic missiles, or by terrorist forces leveraging technically unsophisticated means to disrupt, delay, and degrade the ability of the US to deploy forces to the theater of operations. One could argue that these threats have been present far longer than the term “anti-access” and warrant no special new attention when planning for combat in the future. However, this fails to account for the tending global changes that may make such attacks more likely. Increasing globalization, meaning ease of travel and communication, may make delivery of attacks into the homeland more plausible for future enemies of the United States. Increasing disparity between the capabilities of major combat systems may also make it more favorable for enemy forces to attempt to disrupt US projection of combat power rather than risk meeting US military forces once they have deployed and assumed a posture ready to engage.

For similar reasons, enemy forces may attempt to target US forces enroute to the theater of operations, as opposed to waiting until they have arrived to the theater before targeting them. However, targeting US forces enroute to the theater presents entirely different problems for the enemy than targeting them while still stateside, and this means different considerations for planners as well. Future enemies will have limited capabilities to attack US troop transports, especially given that those troops will likely move by sea or air. Anti-access capabilities that can target and interdict air and naval assets outside of the area of operations, while increasing in global proliferation and decreasing in cost, are still relatively rare, and planners can adjust movement plans to avoid areas where those systems present known threats. Moreover, movement

significance of anti-ship missile attacks to degrade British abilities to generate offensive combat combat power. The assessment concluded with recommendations for increased protection assets to prevent such attacks from being successfully used against US maritime forces – note that this is as early as 1983.

58Alcazar and Lafleur, 82. Alcazar and Lafleur note that adversaries may target US logistics in particular, in every domain, and from the operational area “all the way back to the continental US zip codes.”

59Berteau, 67-71. Berteau’s discussion focuses on the risks that may face future US operations, noting that tomorrow’s environment may present access challenges that are the “polar opposite” of power projection norms the US leverages to its advantage today.
of troops via air and sea assets falls into the realm of their respective planners, who will develop appropriate control measures for the mission. The implications for Army planners begin again once the theater has been reached and the Army must begin to maneuver within the operational area. Here, the threats to mobility are categorized as area denial threats. Two options exist for conducting operations in the overlapping transitory space between where anti-access threats end and area denial threats begin. First, Navy and the Air Force could deliver Army forces into the area of operations, taking steps to mitigate anti-access and area denial threats. This would then require a battle handoff between the services transporting Army forces and the Army forces themselves. Alternately, the transporting services could deliver the Army forces to a staging area outside of the area of operations, relieving the transporting services of the responsibility of mitigating area denial threat systems.

This construct, which leverages the accepted definitions and concepts associated with the terms anti-access and area denial to facilitate division of responsibilities for mitigating various threats, could be misleading. Army planners in particular must understand that the enemy may choose to expand his area of operations at any time, meaning that he may try to deny entry to the area of operations or degrade the ability of US Army forces to maneuver within an area of operations through the same means. Therefore, Army planners should focus less on whether the threat system is an anti-access system or an area denial system and more on the control measures necessary to ensure seamless identification and mitigation of threats. In the case of anti-access and area denial threats, the purpose of the threat systems may matter less than its task. Whether or not the threat intends to prevent access to the theater or movement within it may mean less than the strategic implications of a successful enemy attack against a transportation asset.

Potentially the most significant challenge for Army planners stems from the need to build combat power at an intermediate staging base, or area, prior to the final deployment of forces into the area of operations and against the enemy’s main combat forces. At the tactical level, this problem presents nothing new – only issues that soldiers have identified and dealt with
throughout the history of warfare, such as the impacts of terrain, friendly and enemy capabilities, and the mission on how and where units should assemble the intermediate staging base. However, increasing anti-access and area denial capabilities by potential enemies does have several implications for operational level planners. Since at least the close of World War II, the US military has recognized the need to posture forces forward, with available basing across the globe to support potential contingencies as well as ongoing Phase Zero, or shaping, operations.60 As the US developed facilities worldwide, operational planners recognized threats to those facilities in the form of intercontinental ballistic missiles, attacks by conventional forces, or terrorist attacks. The future likely holds nothing so extravagantly different in the potential forms of attacks against established bases that similar planning techniques could not be used to mitigate those attacks, but it is likely that the feasibility and frequency of those attacks could go up while their cost to enemy forces goes down.61 This means that planners must plan to commit a greater cost in friendly assets to protect both existing bases and the ones they plan to establish in support of a specific contingency, meaning that the overall cost of the mission could increase and challenge the US ability to sustain that cost. If costs become too prohibitive, the US could further drawdown its forward presence and would lose the obvious operational benefits of having forward bases readily available across the globe.62

60Wuthnow, 10-12.

61Anthony H. Cordesman, Challenges and Opportunities in the CENTCOM AOR (Washington, DC: Center for Strategic and International Studies, 2013), 34. Cordesman lays out current perceived air and missile threats to US-allied facilities, with caveats indicating that low near term probability of these threats exists without a clear adversarial strategic goal present.

62Move Forward, “AirSeaLand Battle: Access Assured, Area Un-Denied,” Small Wars Journal (October 2011): 1-15, 2-4. Published under a pseudonym, the author points out not only the current cost associated with maintaining forward presence such as the Bagram, Afghanistan air operations capability (at a cost of $34 billion annually), but also points to the historical examples of drawdown that have occurred following several other major conflicts. Joel Wuthnow, Impact of Missile Threats (Carlisle, PA: US Army War College, 2005), 1. Wuthnow places more direct emphasis on the vulnerability of forward basing, noting that the US has 35 medium or large facilities worldwide, with closures expected as of his 2005 publication.
As Army planners begin to look at developing and refining plans that account for current and future anti-access and area denial threat systems present on the battlefield, potential adversaries will continue to refine their own plans and means to mitigate or bridge the gap between their current capabilities and those of the US military. Much as the AirSea Battle concept attempts to prevent a shift in regional Pacific balance by offsetting Chinese material developments with new operational approaches, the US joint force may need to critically evaluate its ability to project power across all regions of the globe and develop regionally specific approaches to dealing with increasingly prolific anti-access and area denial threats. A coherent and broadly applicable approach to the anti-access and area denial problem may be valuable, as systems and solutions for the problems at hand will have limited value if they only apply to a certain area for a limited time. Broader application becomes even more important in a fiscally constrained environment where material solutions, creation or expansion of bases, and costly training exercises must have the maximum effect per dollar spent.

Using AirSea Battle as a starting point offers a way to develop an operational approach to overcoming the challenges presented by enemy anti-access and area denial systems. As previously noted, this approach does have several drawbacks, most notably that it is designed as a specific solution designed to redress the balance of military power in a particular region (the western Pacific) and also that it does not leverage the capabilities of the land component force. AirSea Battle, by necessity, assumes the land component force out of the concept, except to acknowledge that in some situations the Army as the land component would be required to seize the initiative in the land domain and provide support to other services.\(^6\) However narrow the focus of the AirSea Battle concept, it highlights the centers of gravity that may be more broadly applicable to any fight involving forcible entry against a modern anti-access and area denial capability. AirSea Battle directs the joint force to conduct four operations in parallel, each of

which either attacks an enemy critical vulnerability or defends a friendly vulnerability. In abbreviated form, the tasks associated with attacking and defending vulnerabilities under this concept include: withstand initial attacks, attack enemy networks, suppress enemy long-range strike capabilities, and seize the initiative.\(^\text{64}\)

Analysis of each of these tasks as it may relate to centers of gravity for combatants engaged in joint, multi-domain modern warfare provides an idea of how these concepts could be adapted to the land component force and applied across a broad range of different conditions, so long as the presence of adversary anti-access and area denial systems remains constant. The first task, referred to in the concept brief as a line of operation, is to “withstand initial attacks and limit damage to US and allied forces.”\(^\text{65}\) This wording implies that several relevant assumptions have been made. It implies that the attacks against US and allied forces were conducted first by the attacker, as well as that US and allied forces were within range of the systems that attacked them. As noted in the argument presented in this paper, enemy forces could use such an attack to prevent, disrupt, or delay US forces while still positioned in bases stateside or forward. As an anti-access measure, this type of attack could have serious immediate consequences for US forces, although the ability of enemy forces to target enough US combat power to prevent the US permanently from projecting combat power into the area of operations is unlikely.\(^\text{66}\) The key takeaway for planners is the requirement to routinely assess the impact threat systems are likely to have on existing basing and infrastructure, the impacts threat systems could have on planned infrastructure, and the cost to the mission if protection for that infrastructure increases.

\(^{64}\)Van Tol, et al, 28-36. This assumption rests on the idea that adversaries may not have the capacity to prevent military power projection; it does not imply that the adversary could not degrade US social or political will to continue the fight.


\(^{66}\)Eric V. Larson, Derek Eaton, Paul Elrick, Theodore Karasik, Robert Klein, Sherrill Lingel, Brian Nichiporuk, Robert Uy, John Zavadil, Assuring Access in Key Strategic Regions: Toward a Long-Term Strategy (Santa Monica, CA: RAND Corporation, 2004), 19-38. The authors’ discussion of Iraq in particular highlights the difficulties future adversaries may face in targeting US power projection over the long term.
Conversely, planners must be able to provide an assessment of the impact to the mission if infrastructure does not have adequate protection, particularly if the infrastructure provides a unique or critical capability for friendly forces.

The next AirSea Battle task, “execute a blinding campaign against enemy battle networks and Information, Surveillance, and Reconnaissance (ISR) systems,” directs US forces to leverage electronic warfare and conventional attacks against key vulnerabilities in the enemy anti-access and area denial system. The goal here is to destroy the enemy’s capability to see targets and communicate instructions to subordinates through deliberate targeting of network nodes that contribute to the enemy’s ability to visualize, understand, and act on the battlefield. Army planners may be able to use similar techniques against near peer adversaries, but this does imply that the enemy force being attacked relies heavily enough on integrated digital communications and computer networks that such an attack would have an effect. For a low-tech enemy force attempting to disrupt US forcible entry with minefields at likely landing sites or improvised explosive devices placed on likely avenues of approach, warfare tools designed to target advanced technology may have limited utility. In all cases, however, the goal driving planner’s actions should be the same – to design a plan that degrades the enemy’s ability to conduct reconnaissance and communicate. Regardless of the level of technology used as an anti-access or area denial system, it cannot have its intended effect if it cannot be oriented on an appropriate target as part of a synchronized plan.

The third task, “execute a missile suppression campaign against long range strike systems,” intends to degrade the enemy’s ability to project force towards the edge of the operations area. In theory, this should allow deploying US forces to establish an intermediate staging base with increasing freedom of movement and the ability to build combat power as enemy long-range missile sites are targeted and rendered combat ineffective. For a campaign

---

centered on land component forces conducting forcible entry operations, this approach maintains its relevance but requires the predominant effort to come from fixed wing ground attack aircraft with stealth capabilities, which the Army does not currently have. However, the Army can integrate into the approach by providing special purpose forces to infiltrate enemy defenses and destroy missile launch sites, by providing reconnaissance assets to identify mobile sites, and by conducting ground assessment of friendly force attacks as Army forces begin to exploit the effects of missile suppression operations.69 Also, as Army planners design a lodgment and follow on basing, they must consider the sustainable rate at which those bases can be protected by missile suppression operations. It would be unwise to plan to use terrain without an appreciation of Navy and Air Force capabilities to suppress area denial systems operating from beyond the operational reach of Army systems.

Finally, the AirSea Battle concept calls for “seizing the initiative,” which provides little more than broad guidance to continue to execute the first three tasks mentioned above while exploiting the growing freedom of maneuver and degraded enemy capabilities that these operations have caused.70 Thinking forward to this step allows Army planners to determine the details relevant to the first three tasks. For example, against a near peer adversary, planners may quickly realize that broad suppression of enemy anti-access and area denial defenses is not possible. However, penetration of those defenses along a narrow front may be possible, and by determining where and when the forcible entry operation should penetrate those defenses to generate the greatest number of options or deliver the most significant shock to the enemy may provide a useful tool to guide the detailed planning of the operation.

---


70Air-Sea Battle Office. *Air-Sea Battle: Service Collaboration to Address Anti-Access and Area Denial Challenges* (n.p.: Offices of the Joint Chiefs of Staff. May 2013), 3-4. In addition to Van Tol’s explanation of the Air-Sea Battle concept, this Joint White Paper describes how attacks in one or several domains may create additional freedom of action in other domains.
Future operational level Army planners will likely be required to understand anti-access and area denial threats and their implications to land component planning. They may be required to design operations that integrate with existing frameworks from other service components, such as AirSea Battle, and they will certainly be required to design campaigns that target multi-domain enemy capabilities. To accomplish this, Army planners must remember that the presence and proliferation of future anti-access and area denial threats may mean that they must plan to protect rear areas, secure lines of communication by a jointly operating force, and address centers of gravity relative to anti-access and area denial operations.

Conclusion and Recommendations

The problems posed by anti-access and area denial strategies and systems require the immediate attention of US military commanders and their staff. Waiting until presented with these strategies and physical capabilities by a future adversary in the execution phase of a forcible entry operation can only serve to undermine advantages the US military has long maintained in military capabilities. Furthermore, failure to address these concerns now may allow a balance of power shift in ways not favorable to the US if regional hegemons develop anti-access and area denial means that the US cannot mitigate. This is not to say that US planners or leaders at the operational and strategic levels have allowed such a shift to begin, nor does this argument indicate that anti-access and area denial ways and means have been ignored by the US military. On the contrary, this argument merely contributes to the ongoing discourse that has recognized the anti-access and area denial problem, in the hope that this discourse will result in adoption of viable solutions in the form of new strategies and support for increasingly sophisticated military means. In support of this goal, this argument concludes with three recommendations. The US military must continue to train as part of a joint and combined arms team, it must account for anti-access and area denial threats in both simulated and live exercises, and it must retain a technological edge against potential adversaries.
Numerous challenges face the US Army and no shortage of problems will confront tomorrow’s leaders and operational planners. With problems and situations as complex as disease prevention on the African continent, competing ideologies in the Middle East, and the growing power of China, it may become easy to overlook the threats presented by actors with anti-access and area denial capabilities. Army planners in particular may find themselves tempted to allow another service to deal with the challenge of assuring access for troops from their point of origin to the area of operations. They may be tempted to allow the immense task of defeating area denial challenges to be delegated to tactical units without further thought. These mistakes could be costly, and the best way to prevent them from happening is to routinize the process of identifying and addressing anti-access and area denial threats now in joint, interagency, and multi-national training environments.

Simply stating that future training needs to incorporate forces operating as a joint team provides little if any real utility to planners or commanders. The US military has been training in combined arms warfare for over a century and the idea to include joint mechanisms in training is certainly nothing new. To provide value, this training must include ideas for how to defeat or mitigate the effects of anti-access and area denial threats at the operational level. This kind of specificity may help planners to not only think through solving problems associated with anti-access and area denial threats, but should also provide a lens through which operational level training can be addressed as well.\textsuperscript{71} A critical component of this training strategy must be the involvement of joint forces at an operational level, not just a tactical one. Operational level training involves joint forces with at least a US Army corps worth of combat power – at least 50,000 troops. The distinction is important because this would provide the minimum complement

\textsuperscript{71}Peter J. Schifferle, \textit{America’s School for War: Fort Leavenworth, Officer Education, and Victory in World War II} (Lawrence, KS: University Press of Kansas, 2010), 68-73. Schifferle uses the education received by US Army officers at Fort Leavenworth in the interwar period to demonstrate the importance of using education to train staff officers through exercises that increased in difficulty over the course of the curriculum. The interwar exercises forced the students to plan joint operations and account for the most modern changes to the battlefield, a tradition that the US officer education system should (and generally does) employ today.
necessary to conduct a forcible entry operation, and therefore an operation to defeat anti-access and area denial threats.\textsuperscript{72}

This force meets the likely minimum requirement for forcible entry due to the capabilities of the headquarters, the number of troops available, and the capabilities of the force as a whole. The corps has the ability to task organize its headquarters as a joint task force headquarters, making it capable of directing theater operations for a multi-service force. It has enough combat power to conduct forcible entry at multiple locations by one of multiple means, such as airborne, air assault, or amphibious landing; it can attack in depth against a defending division and be reasonably expected to succeed.\textsuperscript{73} One could argue that a US Army or US Marine division has similar capabilities, with only a reduced number of troops. While correct, only a limited set of circumstances would cause deployment of a division sized force to conduct a forcible entry operation. The most likely future battlefields, facing hybrid threats with anti-access and area denial capabilities, would require corps sized formations with joint capabilities. For these reasons, the corps provides both an adequate operational level force as well as the size of force necessary to examine for training to defeat anti-access and area denial threats.

A way to conduct training that accounts for anti-access and area denial threats involves deploying corps sized formations in coordinated attacks across long distances. Including joint support, especially movement assets, would allow planners to identify the real constraints and frictions associated with coordinated execution of plans involving large formations and threats to

\textsuperscript{72}Siegel, Adam B. \textit{The U.S. Experience in Forcible Entry, Sustained Land Operations, and Sustained Land Combat Since World War II} (Alexandria, VA: Center for Naval Analyses, May 1995), 4-10. The size force necessary to conduct a forcible entry operation could provide a significant area for contention. Siegel demonstrates that the use of a division has been necessary for major forcible entry operations, but notes that forcible entry operations would generally be part of a larger operational scheme.

\textsuperscript{73}While no US corps or division formation can leverage all of the capabilities listed, development of unique capabilities has helped to ensure options for movement and employment of force against unknowable future adversaries, particularly in “the era pf persistent conflict.” Jennifer A. Munro, \textit{Transforming the Army Division in an Era of Persistent Conflict} (Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College, 2009), 12.
those formations from the point of embarkation into the proposed operational area. This would of course require both training areas large enough to accommodate the forces proposed for the operation, as well as an opposing force structure that has the capability to replicate threats to the friendly force outside of the training area itself. Generally speaking, the established training areas used by Army forces at Fort Polk, Louisiana; Fort Irwin, California; and Hohenfels, Germany can each support direct action training for brigade and division-sized forces. This means that the Army could facilitate corps level training by using all three training sites in coordination with one another as part of the same exercise. It could also involve using other service or multinational training areas, but examining the use of the three Army training sites provides an idea of how linkage of multiple training sites into one exercise could be beneficial.

Deploying to defeat or mitigate anti-access and area denial threats may involve leveraging military principles of mass, synchronization of forces, and depth to overwhelm the enemy’s ability to target friendly forces. To accomplish this, US forces might deploy near simultaneously along multiple avenues of approach from their points of origin into the operational area, arriving at several key lodgments with decisive force. These lodgments may be adjacent to one another, or more likely, they may be separated by significant distances or terrain features. This makes use of widely separated objectives at multiple training centers not only feasible, but quite practical for developing understanding of the challenges posed to forces operating in a synchronized but disparate manner.

The opposing force has a critical role to play in training to meet anti-access and area denial threats, especially anti-access threats directed at forces still outside the operational area, replicated in this case by the training centers mentioned above. To meet a stated objective of

defeating or mitigating anti-access threats, the threats must be presented in such a manner that the force undergoing training can orient on them and receive timely and accurate feedback as to how their actions interact with the threats being presented in the exercise. This may be especially problematic for Army forces conducting ground movement to the operational area or for forces under threat while still at home station. Restrictions on use of simulated force or military maneuver outside of established training areas could be problematic for meeting this training goal. While exercise controllers could take some measures to adjudicate effects on friendly and enemy forces during movement to the operational area, digital simulation may have to account for much of this action.

Digital training exercises will play an important role in developing understanding of anti-access and area denial threats, particularly at the operational level. Through this mechanism, planners and units can receive feedback quickly and at relatively lower cost than they could through exercises with live troops. Staff formations can conduct digital exercises with numerous iterations of critical events, as digital systems can reset these events much faster than live formations attempting to reposition, unload, or reload troop carriers to achieve the same effect. They may also conduct digital exercises from training sites across the breadth of Army basing, with small teams of trainers deployed to the stations involved in the exercise to facilitate observation, control, and review of the scenario. The Army also possesses facilities to bring together large staff formations to conduct exercise in one location. Most notably, the Mission Command Training Program at Fort Leavenworth has the ability to bring the staff of an entire division together for one exercise. When utilized in conjunction with other services’ digital training centers, this could provide a more than adequate means for studying tactics, techniques,

75John Richmeier, Fort Leavenworth Host to Warfighter Events, accessed January 2015, http://www.leavenworthtimes.com/article/20140607/NEWS/140609481/. The Leavenworth facility has over 20 buildings on 50 acres of ground, and is designed to house Warfighter exercises for Division staffs. The 2014 Warfighter for the 42nd Infantry Division was the largest Warfighter exercise on record, with larger exercises planned for 2015 and beyond.
and procedures necessary for joint corps sized formations to defeat or mitigate threats in an anti-access and area denial environment.

Combinations involving not only multiple digital training centers from multiple services, but also including live formations could enhance training by leveraging the strengths of both means of training. Acknowledging that digital training involves significantly less in terms of financial costs, time, and quantities of personnel and equipment, it is not without its own drawbacks. Effective digital training relies heavily on the quality of the computer simulation incorporated into the exercise design. The simulation may or may not contain all of the parameters needed to meet training objectives, especially if participants conduct the simulated exercise as part of a rapid response to an emerging crisis. It may also not be possible to involve personnel and equipment in the same structure as they would have in a live exercise; the physical setup of the simulation center may constrain the activities of the exercise participants.76 For these reasons, it makes sense to leverage both live and simulated training to address the concerns presented by anti-access and area denial threats.

Training alone cannot provide all the answers to the problems presented by anti-access and area denial threats. As ordered by the most recent Defense Strategic Guidance, the US military must invest in technology to successfully defeat and mitigate these threats. While acknowledging that hardware solutions will not provide all the answers, the US must always retain a technological edge against anti-access and area denial threats by continually assessing the capabilities of potential adversaries and developing means to outperform them at the tactical level. When specifically considering anti-access and area denial capabilities, this statement has several implications. By analyzing these implications through the lens of the four anti-access and

---

76 Claude A. Lambert, “Operationalizing the Mission Command Network for Joint Forcible Entry Operations,” *Infantry* (April-June 2014): 12-15, 15. Lambert’s excellent discussion highlights the need to understand that austere conditions will constrain the physical network infrastructure available to commanders, noting that training environments should attempt to replicate this, instead of relying on ideal network situations.
area denial capabilities, it becomes possible to develop understanding as to how advancements in US technology could help defeat anti-access and area denial threats.

The link between operational art, training, and technological research and development provides the key to decisively defeating anti-access and area denial threats in the future. By developing plans through creative application of Army doctrine in coordination with other services, the Army can set conditions for effective joint training. By then training the force at an operational level using a combination of live and virtual methods, the joint force can determine the strengths and weaknesses of both the joint plan and the physical capabilities available to the combatants. This data must then be leveraged to drive recommendations for changes to functional capabilities, especially with regards to new or improved equipment that may provide better tactical overmatch against known and anticipated anti-access and area denial threats.
Bibliography


45


Gunzinger, Mark. *Outside-In Operating from Range to Defeat Iran’s Anti-Access and Area-Denial Threats*. Washington, DC: Center for Strategic and Budgetary Assessments. 2011.


Hernandez, Daryle J. *Standing Combined Arms for the Heavy Brigade*. Fort Leavenworth: School of Advanced Military Studies, United States Army Command and General Staff College. 2002.


Knox, Sidney A. *Division Restructuring to Support the Joint Operational Access Concept*. Fort Leavenworth: School of Advanced Military Studies, United States Army Command and General Staff College. 2013.


Munro, Jennifer A. *Transforming the Army Division in an Era of Persistent Conflict*. Fort Leavenworth: School of Advanced Military Studies, United States Army Command and General Staff College. 2009.


Murphy, Robert A. *Russia and Beyond – A Case for European Missile Defense*. Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College. 2009.


Olsen, Paul A. *Operation Corporate: Operational Art and Implications for the Joint Operational Access Concept*. Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College. 2012.


Strategic Initiative Group. *Imagining Defeat in 2030: Mitigating Strategic Surprise to the US Army by Envisioning the Worst.* Fort Leavenworth, KS: School of Advanced Military Studies. 2014.


Weinstein, Cliff J. *Sink or Swim: The Marine Corps Capacity to Conduct a Marine Expeditionary Brigade Amphibious Assault Using Expeditionary Maneuver Warfare.* Fort Leavenworth: School of Advanced Military Studies, United States Army Command and General Staff College. 2010.


