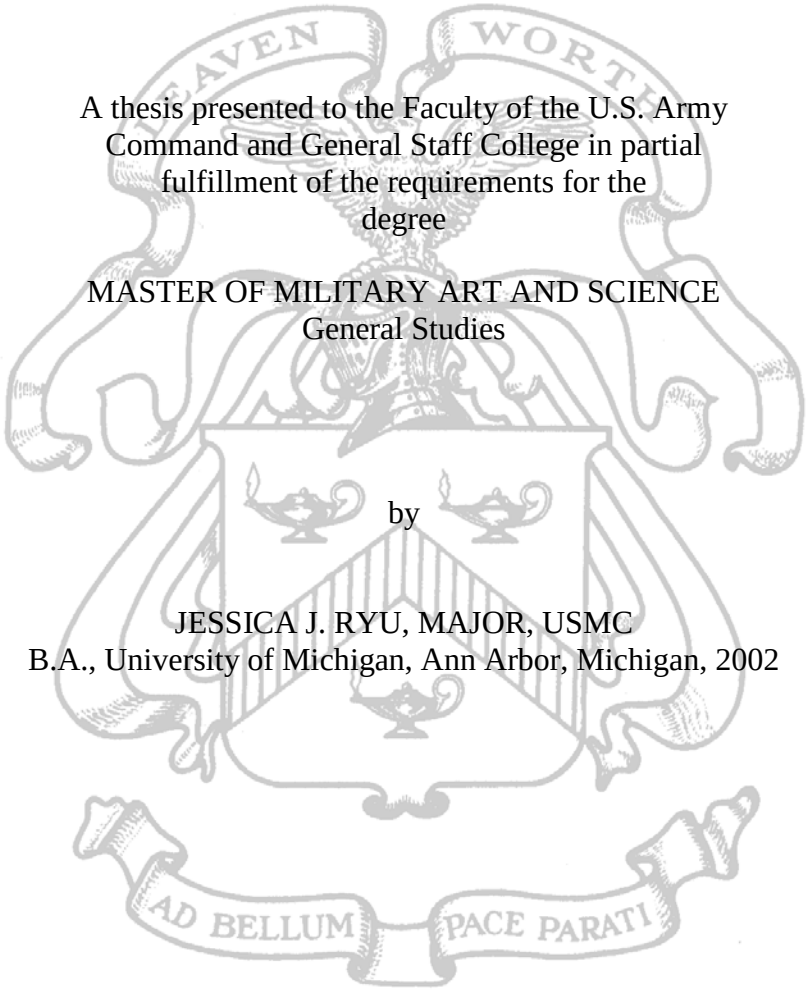
USMC ISR: PREPARING FOR THE A2AD THREAT

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JESSICA J. RYU, MAJOR, USMC
B.A., University of Michigan, Ann Arbor, Michigan, 2002



Fort Leavenworth, Kansas
2014-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-06-2014	Master's Thesis	AUG 2013 – JUNE 2014

4. TITLE AND SUBTITLE

USMC ISR: Preparing for the A2AD Threat

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Jessica J. Ryu

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States Marine Corps continues to rely heavily on uncontested access to the electromagnetic spectrum to conduct intelligence operations. However, with the rise of state and non-state actors seeking to avoid our conventional strength and employ an anti-access and area denial strategy, that uncontested access will potentially be threatened. A host of relatively inexpensive technologies offer present and future adversaries the ability to exploit a real and damaging vulnerability. Such technologies include jammers, anti-satellite weapons and directed energy weapons, which pose a viable threat to the Marine Corps' ability to provide near real-time intelligence support.

While facing this looming threat, simultaneously, the United States Marine Corps faces substantial reductions in budget and manpower. In light of this unfolding reality, in order to maintain dominance throughout the global commons, immediate innovation is necessary. It must be combined with focused training within the framework of refined doctrinal and organizational changes.

15. SUBJECT TERMS

Marine Corps, Intelligence, ISR, A2AD, electromagnetic spectrum, cyberspace, innovation, anti-access, area denial

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	91	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Jessica J. Ryu

Thesis Title: USMC ISR: Preparing for the A2AD Threat

Approved by:

_____, Thesis Committee Chair
Elizabeth Bochtler, M.A.

_____, Member
Joseph G. Babb, Ph.D.

_____, Member
LTC William E. Stebbins Jr., M.S.

Accepted this 13th day of June 2014 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

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

USMC ISR: PREPARING FOR THE A2AD THREAT, by Major Jessica J. Ryu, 91 pages.

The United States Marine Corps continues to rely heavily on uncontested access to the electromagnetic spectrum to conduct intelligence operations. However, with the rise of state and non-state actors seeking to avoid our conventional strength and employ an anti-access and area denial strategy, that uncontested access will potentially be threatened. A host of relatively inexpensive technologies offer present and future adversaries the ability to exploit a real and damaging vulnerability. Such technologies include jammers, anti-satellite weapons and directed energy weapons, which pose a viable threat to the Marine Corps' ability to provide near real-time intelligence support.

While facing this looming threat, simultaneously, the United States Marine Corps faces substantial reductions in budget and manpower. In light of this unfolding reality, in order to maintain dominance throughout the global commons, immediate innovation is necessary. It must be combined with focused training within the framework of refined doctrinal and organizational changes.

ACKNOWLEDGMENTS

I would like to thank my thesis committee, Mrs. Elizabeth Bochtler, Dr. Geoffrey Babb, and LTC William Stebbins Jr., for their support and guidance during this project. Without their assistance and mentorship along the way, I would have been lost. In particular, I would like to thank LTC “Seabass” Stebbins for the countless hours he spent providing feedback and recommendations to my thesis. His passion for learning is infectious and I am grateful for having had the opportunity to work with him.

TABLE OF CONTENTS

Page

ACRONYMS

A2AD	Anti-Access/Area Denial
ASB	Air Sea Battle Concept
CCJO	Capstone Concept for Joint Operations: Joint Force 2020
DOD	Department of Defense
DOTMLPF	Doctrine, organization, training, materiel, leadership and education, personnel, and facilities
EMS	Electromagnetic Spectrum
EW12	Expeditionary Warrior 2012
ISR	Intelligence, Surveillance and Reconnaissance
JOAC	Joint Operational Access Concept
JWICS	Joint Worldwide Intelligence Communications System
NIPRNET	Non-classified Internet Protocol Router Network
NSANET	National Security Agency Network
SATCOM	Satellite communication
SIPRNET	Secret Internet Protocol Router Network
TTP	Tactics, Techniques and Procedures
USMC	United States Marine Corps

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

> Trying to predict the future is a discouraging and hazardous occupation, because the prophet invariably falls between two stalls. If his predictions sound at all reasonable, you can be quite sure that in 20 or at most 50 years the progress of science and technology has made him seem ridiculously conservative. On the other hand, if by some miracle, a prophet could describe the future exactly as it was going to take place, his predictions would sound so absurd, so far-fetched, that everybody would laugh him to scorn.
>
> — Arthur C. Clarke, science fiction writer, inventor, and futurist
> "BBC Horizon, 1964"

The Military Problem

The military is facing an intelligence quandary as operations drawdown in Afghanistan and the Department of Defense budget begins to shrink. Uncertain of the future threat, it must prepare for all possibilities, while simultaneously contracting within the capability's budget. Simultaneously adversarial state and non-state actors are finding it easier to acquire improved technology at declining costs. With an unknown future, strategic guidance continues to advocate the need for global leadership as America works to identify potential threats.

Current guidance from the Secretary of Defense directs the United States military to prepare for operations in an anti-access and area denial (A2AD) environment. Dr. Andrew Krepinevich, Barry Watts and Bob Work first coined the term A2AD in 2003 in a Center for Strategic and Budgetary Assessments' paper, "Meeting the Anti-Access and Area-Denial Challenge." However, the concept of denying an adversary access to a given area (A2) or preventing his freedom of movement in either a specific domain or area of

operation (AD) is not a new concept. This strategic approach to defending one's interests has existed since the early days of conventional warfare.

During World War II, the United States continuously battled an enemy committed to denying them access to specific terrain. Once the military established a foothold, gaining ground against an enemy employing area denial tactics was common. This was the nature of warfare in both the European and Pacific theaters of operation. Critical to the success of these campaigns was the ability of the U.S. military to innovate during the years between World War I and World War II.

The United States Marine Corps (USMC) seized the opportunity during the Interwar Period to carve out a niche that would serve the needs of future wars. Specifically, the Marine Corps identified the future requirement to conduct opposed amphibious landings. Commitment to innovation far exceeded the investment. The leaders of the Marine Corps understood the importance of modifying amphibious doctrine, incorporating that new doctrine into their professional military education, and putting the doctrine into practice through joint service exercises. In terms of testing doctrinal concepts, they conducted day and night landings, experimented with multiple types of weapons from landing crafts, smoke screens for cover, dispersed infiltrations and concentrated assaults, broad-front attacks and subsidiary landings (Millett 1996,74-7). The Service leaders eventually concluded that successful opposed landings were not due to specialized, niche equipment. Rather, specialized equipment, combined with sound, tested doctrine and a professionalized staff would determine the future success of amphibious operations.

While it is not a new concept, the U.S. military will need to transition to defeat the A2AD strategy after the last twelve years of predominantly land-based counterinsurgency operations. “This action comes at an important time as the United States emerges from a significant period of land-centric operations and faces an era of strategic uncertainty and increased challenges to access” (HQMC 2010, 34). This will require a review of current doctrine, an increased emphasis on science and technology and an organizational culture that encourages innovative thinking.

Research Question

This paper seeks to answer the following question: How can the Marine Corps combat emerging threat capabilities that challenge access to the electromagnetic spectrum and cyberspace across the range of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF)? Secondary research questions that arise from the primary question are as follows: With the continued emergence of intelligence, surveillance and reconnaissance systems that are dependent on the electromagnetic spectrum, what emerging adversary technologies will challenge Marine Corps ISR operations in the anti-access/area denial environment? Will future threat technologies contest the heavy reliance on intelligence reach back support upon which the United States Marine Corps has come to rely?

Assumptions

The nature of warfare will change in the future. Since the publishing of the *Joint Operational Access Concept* (JOAC) in 2012 and the follow-on *Air Sea Battle Concept* (ASB), scholars have published a significant amount of literature on combating the

A2AD threat. Organizations such as the Defense Advanced Research Projects Agency, RAND Corporation, Center for New American Security, and Department of Defense (DOD) think tanks, to name a few, have invested time and money to determining what threats already exist and what future threats potentially await joint forces operating in an A2AD environment. However, the preponderance of this work focuses on threats to the physical domains of air, land and sea.

The *Joint Operational Access Concept*, published in 2012, highlights emerging key anti-access capabilities available to potential adversaries. Primarily this list focuses on the emergence of surface-, air-, and submarine-launched ballistic and cruise missiles, long-range reconnaissance and surveillance systems for both intelligence and targeting, and increased submarine force capabilities. While the document does acknowledge the development of improved cyber attack capabilities that could negatively impact command and control, this is left as more of a conceptual idea (JCS 2012, 9).

Insufficient attention is paid to threats that exist to freedom of maneuver in the electromagnetic spectrum and cyber domain. Given the rapid proliferation of technology that empowers growing threats to the space and cyberspace domains, the USMC must transform to operate in these contested environments. With the military's increased dependence on the electromagnetic spectrum for command and control and intelligence operations, it is critical to maintain dominance in this domain. The Secretary of Defense identifies this in the operational access precepts addressed in the 2012 JOAC, "Protect friendly space and cyber assets while attacking the enemy's space and cyber capabilities" (JCS, 26). The precept further states the need to protect access to the electromagnetic spectrum. Given the high cost of acquiring precision munitions and the technology to

employ these weapons, it is expected that future adversaries will be more likely to conduct counterspace and countercyber operations, which are comparatively inexpensive (JCS 2012, 26-7).

In an article published by *Breaking Defense*, Admiral Jonathan Greenert evaluates modern day reliance on the EMS stating,

> The electromagnetic spectrum is an essential–and invisible–part of modern life. We unlock our car and control our television with remote controls, routinely communicate using smart phones, and avoid automobile or aircraft collisions with any number of electronic sensors. EM transmissions and cyberspace are also essential to modern warfare. Our military forces use wireless computer networks to coordinate operations and order supplies, use radars and sensors to locate each other and the enemy, and use electronic jammers to blind enemy radars or disrupt their communications. (Greenert 2013)

As he identified, use of the EMS is an intrinsic part of not only daily life, but also for the conduct of military operations. Adm Greenert goes on to further explain that over the last twenty years the U.S. military has operated in an environment relatively free of challenges within the EMS. However, the emergence of "inexpensive jammers, signal detectors, computer processors and radios make it easier for unfriendly states, terrorists, and criminals to manage their efforts while jamming our own ability to sense and communicate" (Greenert 2013). Further, the number of users operating in the EMS has grown significantly during this same time period and will continue to do so for the foreseeable future.

In November 2012, General James F. Amos, 35th Commandant of the Marine Corps, stated in a *Proceedings* editorial,

> Our nation has a more complex role than it did in the 20th century. The threats to our nation come in different shapes and sizes-many that would be unrecognizable to previous generations of Americans. Wily opponents have adapted to the conventional dominance of U.S. forces, and have demonstrated themselves to be intelligent, cunning, and brutal. (Amos 2012, 19)

As the old saying goes, “The enemy gets a vote.” U.S. adversaries continue to demonstrate the ability to quickly adapt to our strength by leveraging ever-increasing and comparatively-cheaper, yet powerful technologies. This is evident in the challenges faced in both Operations Iraqi Freedom and Enduring Freedom. For example, the simple, very high frequency radio repeater systems employed by the insurgency throughout Afghanistan continues to provide a reliable communications system used for both propaganda and command and control. Difficult to find and target, these repeater systems provide the adversary the ability to communicate effectively against coalition forces.

The threat to freedom of movement in the EMS is not constrained to the A2AD environment. The enemy will continue to attempt to degrade our communications and ISR networks throughout all phases of an operations. However, it is critical to provide accurate and timely intelligence to the maneuver element as they attempt to gain access to a contested area. Once access is gained and forces begin to flow into a theater of operations, communications specialists will focus on building redundant networks to enable ISR operations during follow-on phases.

The Need to Innovate

The *Oxford English Dictionary, second edition,* defines “innovation” as “the introduction of novelties; the alteration of what is established by the introduction of new elements or forms; revolution” (1989, 998). Within a more specific area, scholars in the field and historians debate the single definition of “military innovation.” In the *Journal of Strategic Studies*, “The Future of Military Innovation Studies,” Adam Grissom argues that although individual nuances are debated, the majority of scholars in the field agree on three components of a clear definition:

1. An innovation changes the manner in which military formations function in the field.

2. An innovation is significant in scope and impact.

3. Innovation is tacitly equated with greater military effectiveness (2006, 907).

Therefore, more strict criteria govern the definition of "military innovation." Frequently people tend to think of innovation strictly in terms of technology. Grissom's article broadens the scope of understanding to include the need for doctrinal, organizational, cultural and technological changes.

Dr. Williamson Murray, a former Professor of Military History at the United States Army War College, presented recommendations to guide the process of military innovation in his essay "Innovation: Past and Future." First, it is imperative that the military innovate against an actual opponent who possesses tangible capabilities as well as strategic and political objectives (Murray 1996, 326). This recommendation should not stymie the necessity to understand the future capabilities that technology may bring to bear. Rather, it emphasizes the need to additionally focus on the current capabilities of our adversaries. Second, the military should carefully examine the need to conduct large scale exercises, which are increasingly expensive. Services are better off to conduct fewer exercises and instead focus on understanding the implications of both exercise successes and failures. Furthermore, military professionals must evaluate lessons learned from these exercises without a bias towards validating current processes and doctrine. Third, the services cannot undermine the importance of professional military education throughout a service member's career. True innovation requires a military culture that actively seeks to promote those persons who demonstrate imagination and an intellectual ability to support

innovation. Lastly, the culture of the United States military and resultant mindset are not conducive to innovation (Murray 1996, 326-7). Murray compares today's officer corps to the Luftwaffe's approach to innovation in World War II. He states that modern military professionals think of innovation "in quantitative and qualitative terms of equipment and techniques rather than in conceptual terms" (Murray 1996, 327).

In a speech at the Joint Warfighting Conference by General Martin E. Dempsey in 2012, he challenged the audience to focus more on missions and capabilities vice size of the force. With a declining defense budget and the potential rise of state and non-state actors that are capable of threatening U.S. interests, the Services must identify how the nature of warfare will change. Based on analysis and assumptions, the Services then need to develop innovative ways to fight successfully on the battlefield of the future.

Scope and Delimitations

This study will examine the implications of future weapons and tactics that challenge U.S. freedom of maneuver in the electromagnetic spectrum. For purposes of this research, the author used the following definition of the electromagnetic spectrum from Joint Publication 1-02: "The range of frequencies of electromagnetic radiation from zero to infinity" (JCS 2014, 83). This study was intentionally conducted at the unclassified level and does not seek to provide technical solutions to current vulnerabilities.

Through the limited examination of a historical period of successful innovation, the author's aim is to suggest pertinent, feasible changes across the DOTMPLF that will posture the United States Marine Corps to handle these challenges. The purpose of this

research is to provide recommendations to Service-level intelligence professionals on how to effectively prepare for the future nature of warfare in the EMS.

This study will not assess those A2AD threats that challenge operations in the air, land and sea domains. The author conducted research with a specific focus on Marine Corps' intelligence operations and will not address challenges to the joint force in the A2AD environment. While the scope of the paper does include cyber operations, the primary focus will be on cyber defense vice cyber attack capabilities. The definition of the cyberspace domain also comes from Joint Publication 1-02 and is as follows: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems and embedded processors and controllers" (JCS 2014, 64). At the time of publication, there is an ongoing debate regarding whether the EMS should be merged into the cyberspace domain, be classified as its own domain, or if the EMS should continue to remain as just a factor of military operations.

CHAPTER 2

LITERATURE REVIEW

> I see much of what we're going through right now. I don't see any of it waning away. I don't see major theater wars. I see thorny, difficult, challenging, human intensive–not necessarily technology intensive–conflicts.
>
> — Gen James F. Amos, Commandant of the United States Marine Corps
> "Top Marine Sees a Future of Perpetual War"

National and service level intelligence agencies continue to identify the rise of both state and non-state actors that are capable of posing a threat to access. Some of these actors possess weapons systems hinder freedom of maneuver in the cyber domain and the EMS, both of which are critical to the conduct of military operations. The Marine Corps continues to field ISR systems heavily dependent on the EMS and cyberspace. The rise of A2AD capabilities around the world threatens the ability of U.S. Marines to provide accurate, timely and relevant intelligence to the commander. The purpose of this research is to identify recommendations across DOTMLPF to defeat these threats.

A significant amount of published literature regarding emerging threat capabilities and the future of warfare exist. The literature largely falls into three categories: guidance; technology forecasts; and editorials, which include published articles by think tanks and members of the military.

The President of the United States issues the *National Security Strategy*. Based on this guidance the Department of Defense and subordinate Services publish follow-on guidance. This guidance aims to predict areas of future conflict and provide a general overview of how the U.S. will combat these challenges. The United States Marine Corps has published very little guidance that specifically focuses on the A2AD environment.

Therefore, the preponderance of the guidance reviewed comes from the national and joint levels. Researchers and intelligence analysts provide critical input to these documents, including information about emerging threat capabilities and scientific advancements, both military and civilian. Think tanks and military professionals seek to identify what the next technological innovation will be, where it will occur and how the military must prepare to defeat the threat.

Guidance

Strategic and operational guidance provided by the President, the Secretary of Defense, and the Service leads, provides broad commentary on what the future hold and where the military must innovate in order to remain relevant. An overview of the strategic documents provides a foundation for understanding focus areas for the USMC and how they align with national interests. This section provides a synopsis of those documents that shape the future strategy of the Marine Corps. Although the Obama administration is currently working on a draft version of the new *National Security Strategy* (NSS), during the period of research, the most updated version was the NSS published in May 2010.

The *National Security Strategy* provides overall guidance for the protection of U.S. interests, goals and objectives. The NSS overview states,

> At the dawn of the 21st century, the United States of America faces a broad and complex array of challenges to our national security. Just as America helped determine the course of the 20th century, we must now build the sources of American strength and influence, and shape an international order capable of overcoming the challenges of the 21st century. (U.S. President 2010, 1)

According to the National Security Strategy Archive, the *National Security Strategy* "is intended to be a comprehensive statement articulating the worldwide interests, goals, and

objectives of the United States that are important to its security. The 2010 NSS examines the global progress made over the last 20 years in the spread of democracy, a growing economy and international alliances. The strategy also identifies the growing trends of religious, ethnic and tribal identity wars. Additionally, it also recognizes issues of nuclear proliferation, regional economic instability and food shortages. The strategy highlights the importance of our international alliances, military pre-eminence, economy, the strength of our democracy and our citizenship (U.S. President 2010, 1). As it regards likely future threats, it states that, "[I]nstead of a hostile expansionist empire, we now face a diverse array of challenges, from a loose network of violent extremists to states that flout international norms or face internal collapse" (U.S. President 2010, 17). Furthermore, both state and non-state actors continue to threaten U.S. interests in both space and cyberspace. Though the *National Security Strategy* demonstrates an awareness of challenges that require greater defense needs, the current budget fails to acknowledge these needs.

The 2010 NSS promises to confront these challenges, ensuring that the United States will "maintain superior capabilities to deter and defeat adaptive enemies and to ensure the credibility of security partnerships that are so fundamental to regional and global security" (U.S. President 2010, 17-8). This guidance focuses primarily on dismantling Al-Qa'ida and its violent extremist affiliates around the globe. The United States will seek to prevent the spread of nuclear, chemical and biological weapons (U.S. President 2010, 23).

NSS 2010 identifies that United States must place an emphasis on cybersecurity to protect not only military operations but also infrastructure within our continental

borders. National power grids, telecommunications and banking systems rely heavily on the existence of a safe and secure cyber domain. Cyber hackers are continuously looking for vulnerabilities throughout the networks. These include both state and non-state actors. The *National Security Strategy* states, "We will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks" (U.S. President 2010, 27). The U.S. government strives to safeguard military and industry networks by leveraging both government and private sectors to build more comprehensive and secure technology. The relationship between the military industry and private sector is critical to ensuring data preservation. Protection of critical infrastructure and privacy is an inherently difficult task. However, the U.S. must possess a military force capable of responding to threats in the cyber domain (U.S. President 2010, 28).

Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, published in January 2012 by the Secretary of Defense, is the overarching defense strategic guidance supporting the *National Security Strategy*. It "describes the projected security environment and the key military missions for which the Department of Defense (DOD) will prepare." This initial strategic level guidance provides a basic framework for the capabilities required of Joint Force 2020. It includes guidance for making decisions about the shape and size of the force considering program and budget changes.

The Secretary of Defense describes eight principles to guide the military in planning for Joint Force 2020. Three of these principles are important to this research.

1. First, given the uncertainty of the strategic environment, the military must remain flexible, adaptable, and capable of conducting a multitude of operations.

2. Second, the DOD will need to manage a limited budget and determine what investments must be made now and what can wait.
3. Lastly, every effort must be made to continue investing in science and technology as well as maintaining a suitable industrial base (DOD 2012b, 6-8).

It is evident that the services must work together to achieve the above principles and the primary missions listed below. Figure 1 shows the primary missions of the U.S. armed forces are expected to accomplish in the future.

- Counter Terrorism and Irregular Warfare
- Deter and Defeat Aggression
- Project Power Despite Anti-Access/Area Denial Challenges
- Counter Weapons of Mass Destruction
- Operate Effectively in Cyberspace and Space
- Maintain a Safe, Secure, and Effective Nuclear Deterrent
- Defend the Homeland and Provide Support to Civil Authorities
- Provide a Stabilizing Presence
- Conduct Stability and Counterinsurgency
- Conduct Humanitarian, Disaster Relief, and Other Operations

Figure 1. Primary Missions of the U.S. Armed Forces

Source: Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: U.S. Government Printing Office, 2012), 4-5.

In addition to the tasks listed in Figure 1, the guidance from the Secretary of Defense specifies the need to rebalance toward the Asia-Pacific region (DOD 2012b, 2). There are several reasons listed for this rebalance to the Asia-Pacific region - economic, peace, stability, maintaining free flow commerce, and the importance of monitoring China's military growth and strategic intentions. A strong global economy is in the

interest of all nations and contributes to stability around the world. Ensuring free flow of commerce, specifically in the global commons, reinforces the economy. North Korean instability and its pursuit of a nuclear weapons program are key concerns for U.S. interests and threaten regional stability. Although this rebalancing is necessary, it cannot and will not come at a cost to ongoing operations in the Middle East and Afghanistan (DOD 2012b, 2).

Additionally to the guidance published by the Secretary of Defense in January 2012, the Department of Defense also disseminated the *Joint Operational Access Concept* (JOAC). Chairman of the Joint Chiefs of Staff, General Martin E. Dempsey explained, "This framework describes how we will gain entry and maintain access anywhere and in any domain: land, air, space, sea, and cyber" (2012). Joint operations are the future of warfare, and JOAC examines the roles of each service in an A2AD environment.

> The JOAC defined two key terms - anti-access and area denial.
>
> **Anti-access** - those actions and capabilities, usually long-range, designed to prevent an opposing force from entering an operational area. Anti-access actions tend to target forces approaching by air and sea, predominantly, but also can target the cyber, space, and other forces that support them.
> **Area denial** - those actions and capabilities, usually of shorter-range, designed not to keep an opposing force out, but to limit its freedom of action within the operational area. Area denial capabilities target forces in all domains, including land forces. (DOD 2012a, 6)

The DOD published this guidance to address growing concerns about the growth of anti-access and area denial (A2AD) capabilities around the world. As overseas defense posture changes, the DOD identified the need to further develop A2AD strategies to address the potential threats posed by both state and non-state actors.

The JOAC presents the military problem as, “The essential access challenge for future joint forces is to be able to protect military force into an operational area and sustain it in the face of armed opposition by increasingly capable enemies when U.S. overseas defense posture is changing and space and cyberspace are becoming increasing important and contested domains” (DOD 2012a, ii). Several capabilities were identified as needed to combat these future challenges. Though not all of these capabilities directly apply to the United States Marine Corps, it is necessary to discuss them all to understand how the Service integrates with the overall joint force.

JOAC states that ballistic and cruise missiles, capable of being launched from multiple platforms at distances of over 1,000 nautical miles will enable U.S. forces to defeat enemy anti-access long-range weapons systems. Improvements to intelligence, surveillance and reconnaissance (ISR) systems are necessary to increase range, on-station time, and technical capabilities to provide critical targeting information. With the continued emergence of space-based technologies, U.S. force projection will rely on kinetic and non-kinetic anti-satellite weapons that are capable of disabling space systems. Kinetic weapons, both direct and indirect fire, provide the ability to physically destroy a given target. However, situations may sometimes demand the ability to destroy or disrupt a target without causing physical damage through the use of non-kinetic weapons that target an enemy’s use of the electromagnetic spectrum. The United States Navy must invest further in providing a robust submarine force, capable of protecting sea lines of communication in international waters. Cyber defense operations must continue to develop in order to counter the adversary’s attempts to disrupt U.S. command and control

systems (DOD 2012b, 9-10). The development and continued pursuit of these capabilities will assist the DOD in defeating anti-access threats.

Some technologies and capabilities serve as both anti-access and area denial systems. In addition to those capabilities listed above, the U.S. must also seek ways to defeat the proliferation of precision-guided rockets, artillery, missiles, and mortars (G-RAMM). Furthermore, the U.S. must eliminate enemy use of chemical and biological weapons, defeat enemy electronic warfare capabilities, and deny the adversary persistent intelligence collection from unmanned systems (DOD 2012a, 10). The *Joint Operational Access Concept* challenges joint forces to operate synergistically not only across Services, but also across different domains in order to reduce vulnerabilities and present opportunities to establish superiority over adversaries (DOD 2012a, 14). Operations in the A2AD environment will heavily rely on the ability of U.S. forces to gain intelligence, while simultaneously preventing the enemy the same opportunity (DOD 2012a, 29).

The *Capstone Concept for Joint Operations: Joint Force 2020* (CCJO), published in September 2012, builds upon the defense strategic guidance and provides a way forward for the future of joint operations. It addresses challenges facing the United States and the necessary missions that the joint force must be prepared to accomplish. General Martin E. Dempsey stated, “In this concept, Joint Force elements, globally postured, combine quickly with each other and mission partners to integrate capabilities fluidly across domains, echelons, geographic boundaries, and organizational affiliations” (JCS 2012, iii). CCJO identifies a global environment in which threats and crises continue to become more complicated. Specifically, the Secretary of Defense’s guidance highlights, “In a world where fragile critical infrastructure is widely connected to the internet, and in

which sabotage and terrorism have profound effects, adversaries can also more easily escalate a conflict laterally, including to the U.S. homeland" (JCS 2012, 3).

Two force development implications addressed in the CCJO pertain to intelligence. The first implication requires the force to "Develop analytic capabilities that correspond with the wider array of threats and contexts in which they will occur" (JCS 2012, 10). This task predominantly focuses on training the force in intelligence tradecraft. The second task is to "Improve capabilities that better fuse, analyze, and exploit large data sets" (JCS 2012, 10). To accomplish this, the services must first collaborate and determine the correct information technology infrastructure needed to support this requirement.

Each service brings unique capabilities to the fight that are important to mission accomplishment. Interoperability is critical to the future of joint force operations. However, the CCJO identifies a risk in standardization and interoperability. Standardization should not lead to homogeneity, which would diminish the intent of joint operations where unique capabilities complement one another (JCS 2012, 15). Therefore, a balance must be struck between service capability development and the need for joint interoperability.

The force development implications identified in 2012 by the Secretary of Defense demonstrate an understanding of how the battlefield will potentially change in the future. The capstone concept calls for the force to "enhance our ability to operate effectively in a degraded environment" (JCS 2012, 9). This task directly links to the increased ability of U.S. adversaries to disrupt, degrade or destroy both cyberspace and space systems, which are critical to Joint Force operations. Military planners must

identify redundant capabilities within technological systems, thus increasing resiliency of the architecture (JCS 2012, 9). This further acknowledges the anti-access and area denial threats posed against future operations. It is imperative that Joint Force 2020 maintains the ability to gain access and maneuver freely through contested areas. Pursuit of these capabilities will rely on the maturation of fires that are capable of deterring and defeating these threats (JCS 2012, 11).

Building on the above documents and further outlining the future security environment, the United States Navy and the United States Air Force partnered to write *Air Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges* in May 2013. A classified version of *Air Sea Battle* (ASB) exists, but in order to make this research more readily accessible, for the purposes of this study, the unclassified overview will be discussed. With the rebalance towards the Pacific, as discussed above, the DOD identified a requirement to focus developmental efforts on ensuring the ability of the United States to project power throughout the global commons, enabling freedom of maneuver (DOD 2013, 2).

Since World War II, the United States has been able to build up combat power in a desired area, conduct rehearsals and then operate when and wherever necessary. However, this may change in the future. The ASB Office states, "While A2AD ideas are not new – the desire to deny an adversary both access and the ability to maneuver are timeless precepts of warfare – technological advances and proliferation threaten stability by empowering potentially aggressive actors with previously unattainable military capabilities" (DOD 2012, 2). Many assumptions are made in ASB regarding how future adversaries will fight.

First, the United States will have few indications and warnings that the adversary will begin military operations. Second, adversaries will likely attack U.S. and allied territories, to include the continental United States, aircraft, space assets, ships, networks and people. Lastly, a near-peer threat will be capable of attacking across any domain. Multi-domain attacks will be the most likely course of action in order to create a complex problem for U.S. forces (DOD 2013, 3-4). Given these predictions, the DOD must develop ISR systems capable of defeating A2AD technologies in order to maintain situational awareness. Additionally, the posture of the force around the globe is critical to ensuring swift reaction to any threats to U.S. interests with a force capable of operating in any domain.

Air Sea Battle proposes to defeat the challenge of A2AD by developing a networked, integrated force that is able to attack-in-depth and disrupt, destroy or defeat adversary forces (NIA/D3) (DOD 2013, 4). ASB identifies that integration can no longer be considered a task only for the combatant commander; rather, integration must begin at the Service level (DOD 2013, 6). The ASB concept enables individual Services to protect, develop and maintain unique capabilities, cultures and equities, while collaborating in a more formal manner (DOD 2013, 8).

Four of the primary missions assigned to the DOD in *Sustaining U.S. Global Leadership* relate directly to the A2AD environment: deter and defeat aggression, project power despite anti-access/area denial challenges, operate effectively in cyberspace and space, and provide a stabilizing presence (DOD 2013, 7). Furthermore, this concept supports and complements the *Capstone Concept for Joint Operations: Joint Forces 2020* and the *Joint Operational Access Concept*. Building on tasks assigned by the

Secretary of Defense, ASB seeks to provide a conceptual framework for future operations in contested environments.

Air Sea Battle recommends integrating contested and denied environments into training, both at the Service and joint level. Professional military education provides a venue for incorporation of these concepts, challenging individual service members to begin thinking about potential impacts to operations. ASB specifies that, "Required training focus will include both active measures, such as integrating capabilities to neutralize advanced adversary air defenses, and passive measures, such as comprehensive emissions control training" (DOD 2013, 10-1). Additionally, exercise scenarios must include A2AD challenges across all five domains – air, land, sea, cyberspace and space.

The success of the ASB concept relies on levels of joint and combined integration that have not been reached to date. Joint force development, operations, training, acquisition and modernization must be evaluated and modified as required to prepare Joint Force:2020 for the challenges ahead. As proliferation of more advanced weapons systems continues, NIA/D3 solutions will enable the U.S. military to successfully operate forward and project power around the globe (DOD 2013, 13).

In June 2010, the United States Marine Corps released the third edition of the *Marine Corps Operating Concepts: Assuring Littoral Access…Winning Small Wars*. Although published prior to the *Air Sea Battle Concept*, this document provides guidance to the force in addressing anti-access and area denial environments. Additionally, the operating concept hopes to "inspire discussion, debate, and innovation during the capability identification and solution development process" (HQMC 2010, 11). Highlighting our ties to the United States Navy, the "Marine Corps Operating Concepts"

emphasizes the task of assuring littoral access. The USMC's specific portion of this task is to conduct cross-domain operations, "bridging the difficult seam between operations on sea and on land" (HQMC 2010, 1). The rise of A2AD technologies in the 21st century throughout the global commons presents a threat to these seams.

"The Marine Corps has repeatedly demonstrated its institutional and operational adaptability by effectively bridging the nation's most critical seams between domains. Those seams have always and will always confront a maritime power with global interests" (HQMC 2010, 3). The USMC fights as a Marine Air Ground Task Force (MAGTF), which is comprised of the Command Element, Ground Combat Element, Aviation Combat Element and the Logistics Combat Element. The various sizes of the MAGTF are as follows: Marine Expeditionary Force, Marine Expeditionary Brigade, Marine Expeditionary Unit and the Special Purpose MAGTF. These units are all task organized to accomplish a given mission, providing the geographic combatant commander with a scalable, flexible, adaptable fighting force.

Due to the construct of the MAGTF, Marines are capable of fighting in the air, land, sea and cyber domains. This trans-domain perspective forces the Marine Corps to adapt based on the operational conditions of a given environment (HQMC 2010, 4). Rather than focus solely on one domain, Marines view an adversary holistically, determining the best way to defeat the threat. This approach to warfighting drives the USMC "to develop unique technologies, methods, and organizations suited to the trans-domain edge" (HQMC 2010, 4). With the proliferation of weapons technology, it is evident that the Marine Corps' flexibility and expeditionary qualities are relevant (HQMC 2010, 5).

Technology Forecasts

Predicting how the nature of warfare will change is an exceptionally difficult task. Identifying how non-existent technology will drive those changes is logically impossible. However, many organizations specifically exist just for this purpose. The Defense Advanced Research Projects Agency (DARPA) and the Center for a New American Security (CNAS) are two such organizations.

The mission of the DARPA is to create breakthrough technologies in support of national security. With a budget of nearly three billion dollars, DARPA focuses on emerging capabilities that could assist in securing national interests. Testifying before the House Armed Services Subcommittee on Emerging Threats and Capabilities, Deputy Director DARPA, Kaigham Gabriel, stated, "It may appear that the best way to create strategic surprise is to predict what's next. Predict with great accuracy and as far out as possible. We hunger to know what's next. To predict the future. But our hunger to predict is not matched by our ability to do so" (U.S. House 2014, 1).

DARPA's research and development efforts have contributed to innovations such as precision guidance and navigation, unmanned aerial systems, night vision, stealth, and communications and networking protocol used today (DARPA 2013, 1-2). With an abundance of new weapons and techniques in existence that threaten U.S. interests, DARPA dedicates resources and personnel to identifying those actors that can challenge U.S. global influence in fundamental ways (DARPA 2013, 1). DARPA's mission concentrates on three different critical, interdependent strategic objectives:

1. Demonstrate breakthrough capabilities for national security;

2. Catalyze a differentiated and highly capable U.S. technology base

3. Ensure DARPA itself remains robust and vibrant to deliver on its mission today and in the future (DARPA 2013, 2).

Testimonies, research papers and news articles abound regarding the work DARPA is doing to achieve these objectives.

The Center for a New American Security (CNAS) attempts to develop principled, strong and pragmatic defense and national security policies. CNAS employs its staff and advisors to identify innovative, research-based ideas designed to prepare the national security leaders for today and the future. Their publications provide insight into the needs of the future force.

In the September 2013 CNAS published paper, "Game Changers: Disruptive Technology and U.S. Defense Strategy," the authors focus on the impact of technological change on the defense strategy. In this paper, CNAS argues,

> In contrast to what the acolytes of network-centric warfare proclaimed, technology is not a silver-bullet solution, nor does it "lift the fog of war." What makes a technology "game changing," "revolutionary," "disruptive," or a "killer application" is that it both offers capabilities that were not available – and were in many ways unimaginable – a generation earlier and in so doing provokes deep questions whose answers are not readily available. (Brimley 2013, 4)

With the rise of new powers and the accelerated proliferation of advanced technology around the globe over the next day, the technological dominance the United States military has come to expect may be challenged (Brimley 2013, 7). The threat to technological supremacy compels the U.S. military to identify potential changes to the nature of warfare.

Interestingly, the CNAS paper examined the history of the Department of Defense and subordinate military Services in regards to embracing technological investment. Historically these entities have been resistant to committing money to innovations that

potentially take away from legacy platforms, core competencies and concepts of operation (Brimley 2013, 10). The drawdown of the war in Afghanistan and the impact of the 2011 Budget Control Act on the DOD, combined with an emerging political call to return to a policy of isolationism, will limit the investments made on research and development (Brimley 2013, 9).

In order for a technology to be "game-changing," four primary areas must converge: congruence, perspectives, societal values and organizational culture, and time. Furthermore, the technology itself must exist, an organization must have a concept of employment and it must confront a relevant problem (Brimley 2013, 11).The congruence of these three factors enables new technology to be game-changing. Across the globe, different actors base technological research and development in differing areas. In order for a new technology to truly impact the nature of warfare, the perspective of a given actor must see value in that area of innovation. Not all elements of society or an organization view new technologies as beneficial. Legal implications and human rights concerns can negate the utility of new technology. Lastly, time is a critical factor affecting the potential of technology. Although an invention can take significant time to mature, technology can rapidly advance once it reaches a tipping point (Brimley 2013, 13).

This CNAS study specifically targeted five potential game changing technologies through a program called NeXTech. The NeXTech project, initiated by the Rapid Reaction Technology Office of the Office of the Undersecretary of Defense for Acquisitions, Technology and Logistics, was primarily designed for two purposes. First, to determine how emerging technologies would impact future warfare. Second, to

identify areas in technology that would potentially affect the future strategic environment (Brimley 2013, 8). “During the series of NeXTech war games, participants explored five technology areas with the potential to cause a series of discontinuous shifts in military affairs: additive manufacturing, autonomous systems, directed energy, cyber capabilities and human performance modification” (Brimley 2013, 14). With respect to this thesis, the portions on autonomous system, directed-energy weapons and cyber capabilities are important.

The automation of certain platforms has transformed intelligence, surveillance and reconnaissance operations. Rapid developments in robotics, software, artificial intelligence and wireless networks support these autonomous and semi-autonomous platforms. Additionally, as the electronic components become cheaper to manufacture, the ability to make relatively inexpensive, small ISR platforms is becoming a reality (Brimley 2013, 15).

Directed-energy weapons are another significant advancement in technology. “Directed-energy weapons generate effects through the use of millimeter waves, high-power microwaves, lasers or electromagnetic pulses (Brimley 2013, 15). Replacing modern day munitions, directed-energy weapons are capable of being stealthy and highly accurate. These weapons systems pose a threat to electronic systems within a designated range (Brimley 2013, 16).

Although relatively new to military doctrine and tactics discussions, cyber technologies are advanced enough to cause tangible effects in the physical domain. Evermore connectivity exists between electronic devices via intranets and the Internet.

While this network enables sharing of information in near real-time, it creates a vulnerability to those who rely on constant access.

> For warfighters, this [cyber technology] could create game-changing alterations to current concepts of persistent ISR and enable large-scale management of autonomous systems. However, this same connectivity also provides a means for sophisticated and lethal hacks and for hijacking of large systems, and it furthers a trend of putting technology previously unavailable to governments into the hands of individuals. (Brimley 2013, 17)

Understanding the implications of the cyber domain on military operations will be critical to the success of future operations in the A2AD environment.

The CNAS study concludes with several warnings to policymakers regarding the need to continue making necessary investments in future game-changing technologies (Brimley 2013, 22). The report highlighted the need to potentially reverse the qualitative bias demanding large platforms characterized by persistence, range and stealth. Instead of this traditional mindset, CNAS stresses the opportunities available in the quantitative dimension. That is, pursuing cheaper, expendable systems capable of overwhelming the adversary's advanced defensive systems (Brimley 2013, 20).

Editorials

Military professionals, historians, policymakers and many others continue to publish editorials regarding the future A2AD challenges that the U.S. military will face. While there are far too many to cover in this literature review, there are some specific articles of interest that are worth expounding on in further details.

In his testimony to the U.S. China Economic and Security Review Commission on January 27, 2011, Martin Libicki, from RAND Corporation, presented two scenarios involving the use of cyberwar by the Chinese. In the first scenario, the Chinese employ a

strategic cyber attack against the U.S. power grid in an effort to deter U.S. forces indirectly from entering into a war to defend Taiwan (Libicki 2011, 1). In the second scenario, China conducts an operational cyber attack directly against the U.S. military. As Taiwan seeks independence, the Chinese determine that it is time to take control of the island. In order to delay the intervention of U.S. military forces, China carries out a cyber attack on military information systems, corrupting the time-phased force deployment data (Libicki 2011, 2).

Both of these scenarios are fictitious, but they provide insight to the potential damage that a cyber attack may cause. It is critical that the U.S. military, "determine to what extent its ability to carry out its missions is at risk from any cyber attack, ensure that it has the resiliency to fight through cyber attacks, and make everyone else, not least of which is China, aware of how well it can withstand attack" (Libicki 2011, 4). In addition to protecting U.S. networks and information systems, it is just as important to prepare to operate in the event of a successful cyber attack.

Mr. Libicki concludes two specific things during his testimony:

> First, that the threat of strategic cyberwar is probably overblown. Second that the United States Department of Defense needs to take the prospect of operational cyberwar seriously enough to understand imaginatively and in great detail how it would carry out its mission in the face of a full-fledged attack. (Libicki 2011, 4)

As adversarial state and non-state actors increase their ability to conduct destructive cyber attacks, the U.S. military must prepare effectively.

A second article published in July 2008 by the Association of Old Crows (AOC), "Electronic Warfare: The Changing Face of Combat," provides recommendations to the DOD to prepare more effectively for future threats. According to the organizations

website, “The Association of Old Crows is a not-for-profit international professional association with over 13,000 members and 200+ organizations engaged in science and practice of Electronic Warfare (EW), Information Operations (IO), and related disciplines.” The 2008 paper emphasizes that the technological supremacy the United States has come to expect is rapidly eroding due to the increasing proliferation of information technologies (AOC 2008, 1).

“In the near future, if the U.S. technological edge continues to erode, U.S. forces may not be able to employ their sensors, or use their computers and communication links effectively in combat, exposing the vulnerability of heavy emphasis on such systems in current military doctrine” (AOC 2008, 1). As the technological advantage enjoyed by the U.S. military decreases, the enemy is able to acquire more sophisticated systems. These systems have the ability to modify signal waveforms, frequency hop and utilize an increasing range of the electromagnetic spectrum (AOC 2008, 2). The need to dominate the EMS will be a consistent factor in future military operations (AOC 2008, 3).

AOC provided three areas for change in order to ensure the U.S. military maintains this dominance. First, the highest levels of military leadership must fully understand the importance of controlling the spectrum. Creation of an organization in the Office of the Secretary of Defense responsible for oversight of systems acquisition, planning, coordination and training of joint EW operations is critical. Additionally, each Service should assign a Flag/General Officer to manage and oversee Service-specific EW programs. Second, the paper recommended the creation of an “EW Critical Technologies List,” as well as adequate funding to develop technologies that will meet the future needs of the force, 10 to 15 years out. Finally, the DOD should capitalize on progress made in

the field of EW during ongoing operations in Iraq and Afghanistan. The Joint Staff should establish a joint, services, theater-wide EW coordination cell that would provide support to combatant commands in planning all aspects of EW for future operations.

A more recent article written by Colonel Vincent Alcazar, U.S. Air Force, in *Strategic Studies Quarterly*, "Crisis Management and the Anti-Access/Area Denial Problem" highlights a disturbing trend. Col Alcazar states, "Moreover, to the extent A2AD appears in U.S. defense writings, there is a frantic focus on systems versus systems rather than strategies for success" (2012, 44). Alcazar argues that reliance on connectivity for ISR operations both in theater and for reach back support makes the military more vulnerable to the effects of A2AD information disruption and network attack. A strategist can reasonably assume that the degradation of this connectivity will make it more difficult to provide intelligence support to the commander (Alcazar 2012, 49).

In order to succeed and maintain dominance against A2AD threats, the United States must understand how to operate in a nonpermissive environment. Colonel Alcazar identifies four aims of the A2AD strategy.

1. Strategic Preclusion – The adversary will attempt to discredit the United States' ability to assist allies in terms of the capability to respond to crisis in a timely manner.
2. Operational Exclusion – Deny the U.S. military access to critical networks, preventing forces from gathering and disseminating intelligence to forward deployed forces.

3. Operational Degradation – Prohibit U.S. forces from leveraging the cyber domain and the electromagnetic spectrum for command and control and ISR operations. Additionally, sever the connectivity between forward deployed troops and the senior commanders who control the fight from great distances.
4. Strategic Exhaustion – Targeting the extended logistics lines of U.S. forces, preventing the military from receiving critical resupply and delaying force generation and deployment (Alcazar 2012, 51).

A comprehensive understanding of these four A2AD aims will enable military leadership to better prepare for the challenges of the future.

Sam J. Tangredi's recently published book, *Anti-Access Warfare: Countering A2/AD Strategies* is the final editorial that significantly contributed to the author's understanding of the research question. Published by the Naval Institute Press in 2013, Tangredi's book aims to provide historical context to the A2AD concept. He argues that although anti-access/area denial are modern terms, "they constitute an ancient concept – that they are techniques of strategy that have been used throughout military history" (Tangredi 2013, 1). As an example, he discusses the U.S. war with Imperial Japan in the Pacific from 1941 to 1945. The Japanese employed an A2AD strategy in order to retain the conquests achieved, starting with the capture of Manchuria in 1931 (Tangredi 2013, 8).

Adversaries who face an operationally superior force will employ an A2AD strategy to prevent said force from entering the contested region. Five fundamental elements exist in an anti-access and area denial strategy:

1. The perception of the strategic superiority of the attacking force
2. The primacy of geography as the element that most influences time and facilitates attrition of the enemy
3. The general predominance of the maritime domain as conflict space
4. The criticality of information and intelligence, and – conversely – the decisive effects of operational deception
5. The determinative impact of extrinsic events or unrelated events in other regions (Tangredi 2013, 13).

Of importance to this specific paper is the fourth fundamental. An adversary who employs an A2AD strategy will seek to limit the attacker's ability to gather information and intelligence, specifically through the denial of the EMS and deception operations intended to confuse the attacking force. An honest assessment of current military doctrine and recent operations demonstrates the criticality of information and intelligence in the conduct of operations from the tactical to the strategic level.

An enemy does not have to disable an entire network to significantly impact U.S. forces ability to conduct operations. The targeting of a specific node could potentially degrade an entire process (Tangredi 2013, 63). For example, jamming the downlink of an ISR asset could prevent critical targeting information from reaching its intended user. While a weapon can be shot without specific targeting data, this will effectively reduce accuracy and increase the potential for collateral damage. Summarizing, Tangredi says,

> The point is that viewing the anti-access efforts as a network of strategies, techniques, and systems prompts the understanding that defeat of a particular portion of the network could seriously degrade it. Likewise, it points to the need for redundancy in systems and fallback strategies in order to deal with critical damage. (Tangredi 2013, 63)

The vulnerabilities created by the military's reliance on the EMS are driving factors for the future adversaries' strategies.

Tangredi discusses the potential for an adversary to blind U.S. military satellite reconnaissance, surveillance, and communications assets through the use of anti-satellite technology (2013, 163). However, he caveats this thought stating, "To be smart, we have to study anti-access networks seriously from a tactical perspective and not be fixated on the threat (or acquisition) of new technologies" (Tangredi 2013, 233). Technology cannot be the focus on innovation, rather it must be a comprehensive review of equipment, tactics, and enemy intentions.

In the 1990s, strategists began to believe that new information systems would help remove the fog of war (Tangredi 2013, 244). While these systems contribute to the commander's situational understanding of the battlefield, they do not eliminate the unknowns. Additionally, reliance on these systems creates vulnerabilities throughout the operating force. As information systems evolve, adversaries will invariably identify weaknesses. Tangredi recommends, "the creation of a small, relatively low-tech/low-observable counter-anti-access force that can initially penetrate the outer rim of anti-access networks as the rest of the power-projection forces reboot" (2013, 244). This force would be required to operate without the Global Positioning System (GPS) and with very limited communications capabilities. He also posits the need for weapons that are capable of conducting sustained and precision attacks. The U.S. military's focus on high-tech, expensive, precision systems must shift to including robustness, sustainability and survivability (Tangredi 2013, 247).

Methodology

This study will consist of qualitative research, specifically employing the critical research methodology. The study will primarily be conducted through document analysis and interviews. The critical research will initially focus on the intelligence branch within the United States Marine Corps, specifically the current ISR systems and how they leverage the electromagnetic spectrum. Additionally, the research will provide a firm understanding of the anti-access/area denial environment and the future challenges it poses to USMC ISR operations. The study will then seek to identify those emerging threats in the A2AD environment that challenge freedom of operation in the EMS.

In order to better understand the process of innovation, it is necessary to research and identify what made the United States Marine Corps successful during the Interwar Period. The research will predominantly focus on the USMC's development and refinement of amphibious operations and supporting doctrine. Although the challenges to access and freedom of movement are different today, the lessons learned are still relevant to identifying a way forward in developing A2AD doctrine.

As the USMC looks to the future, Marine Expeditionary Brigade level exercises attempt to provide a realistic A2AD threat scenario. This research will attempt to identify those specific things that should be continued as well as making recommendations to further prepare the force for the challenges ahead.

CHAPTER 3

USMC ISR AND THE A2AD ENVIRONMENT

> Essentially, the impact of diminished spectrum access will be a reduction in the effectiveness and overall capability of our military forces. It will impact our capacity to efficiently execute our mission. Losing spectrum is like losing any other resource, it costs.
>
> — Emmett Paige, Jr., Assistant Secretary of Defense for Command, Control, Communications and Intelligence, *Armed Forces Communications Electronics Association Spectrum Management Symposium*

> To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds.
>
> — Mao Tse Tung, *On Protracted War*

The United States Marine Corps does not dominate any specific domain. Rather, "Marines operate in the domain of uncertainty and provide the necessary and critical transition of control at the point that history repeatedly demonstrates requires special and adaptable skills – at the interface between the sea, land, and air domain" (HQMC 2010, 6). In order to operate effectively across this domain, the USMC relies on unchallenged access to the EMS. It is necessary to identify the vulnerabilities that exist in the current communications architecture that supports USMC intelligence operations. Once identified, the Service can then effectively train, implement protection measures and adequately defend the critical access to the EMS.

Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE)

In May 2010, the USMC Director of Intelligence announced the publication of the MCISRE Roadmap, which provides a framework and direction for Service-level

continued development and sustainment of an all-source ISR enterprise to meet specified and implied tasks in the Marine Corps Service Campaign Plan. This document defines "enterprise" to include equipment, personnel and organizations from both the supporting establishment as well as the operating forces that have ISR responsibilities. The enterprise is designed to optimize the operation of USMC ISR capabilities (Paul 2011, 182). The mission of MCISRE is the "synergistic integration of all Service ISR elements into a single capability or system that is networked across all echelons and functional areas including the operating forces, supporting establishment, systems and personnel in order to achieve superior decision making and enhance lethality" (Chudoba 2012, 6).

While the MCISRE Roadmap is classified "For Official Use Only", a significant amount of data has been released through briefings at the unclassified level. Additionally, RAND completed an assessment in 2011 titled "Alert and Ready: An Organizational Design Assessment of Marine Corps Intelligence," providing an explanation of how the roadmap guides the future of USMC intelligence. The analysis forecasts a future where adversaries employ primitive and sophisticated technologies against U.S. forces with both conventional and irregular tactics. Further, the physical environment will be clouded by political considerations. This future will require a continuously operational USMC intelligence organization, ready to meet a variety of challenges during times of both war and peace (Paul 2011, 182).

The operating forces include those intelligence personnel assigned to the Marine Expeditionary Forces, to include the subordinate Marines in the intelligence, radio and reconnaissance battalions and Marine Unmanned Aerial Vehicle (VMU) squadrons, as well as the intelligence personnel assigned to the Marine Forces (MARCENT,

MARFOREUR, etc.). The intelligence supporting establishment consists of the Marine Corps Intelligence Activity (MCIA), Marine Cryptologic Support Battalion (MCSB), elements of Marine Corps Combat Development Center (MCCDC), and the intelligence specific programs under the Marine Corps Systems Command (MCSC). All of these forces and the equipment comprise the enterprise. Figure 2 provides an overview of the United States Marine Corps Intelligence Structure as of 4 September 2013.

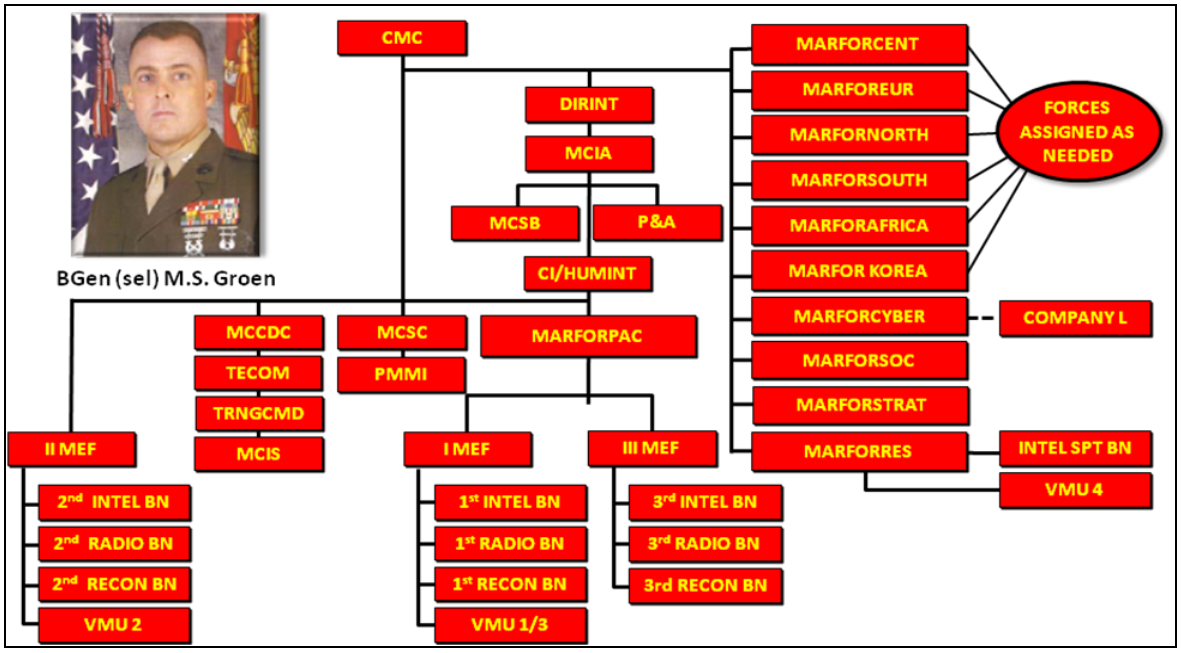


Figure 2. USMC Intelligence Organization, 4 September 2013

Source: Headquarters Marine Corps, Intelligence Department, *eHQMC Intel Team Slide Library* (Washington, DC: HQMC, Intelligence Department, 2012).

The full implementation of the MCISRE Roadmap relies heavily on high-bandwidth, reliable and redundant communications networks. In other words, dominance

of the EMS and the cyber domain in order to ensure access to intelligence information in near real-time around the globe.

The Electromagnetic Spectrum and Cyberspace

Joint Publication 1-02 defines the electromagnetic spectrum as, "the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands" (JCS 2014, 83). LCDR Blake Tornga provides a simpler explanation, "We physically pass information wirelessly through space by transmitting encoded electromagnetic waves at a particular frequency. These waves possess different characteristics depending on the frequency transmitted" (2008, 3). However, these definition do not convey the criticality of the EMS to the conduct of military operations. Without freedom of maneuver in the EMS, command and control, ISR, logistics, and other critical military functions are put at risk.

While it is important to prevent the enemy from freely using the EMS to communicate, gather intelligence, command and control his forces, and conduct targeting, it is equally important to protect U.S. systems from being degraded by an adversary. In *Anti-Access Warfare: Countering A2/AD Strategies*, Tangredi identified the importance of information and intelligence in the A2AD environment. He states, "But few if any of the tactical operations in an anti-access or counter-anti-access campaign can be conducted without very detailed information and intelligence and the resulting targeting information" (Tangredi 2013, 101). He then identifies the potential for an adversary with an anti-satellite capability to deny U.S. forces the ability to leverage satellite communications, surveillance and reconnaissance assets (Tangredi 2013, 163).

Figure 3, the Marine Corps Intelligence, Surveillance and Reconnaissance Enterprise (MCISRE) high-level operational concept graphic, depicts the criticality of the spectrum to USMC intelligence operations.

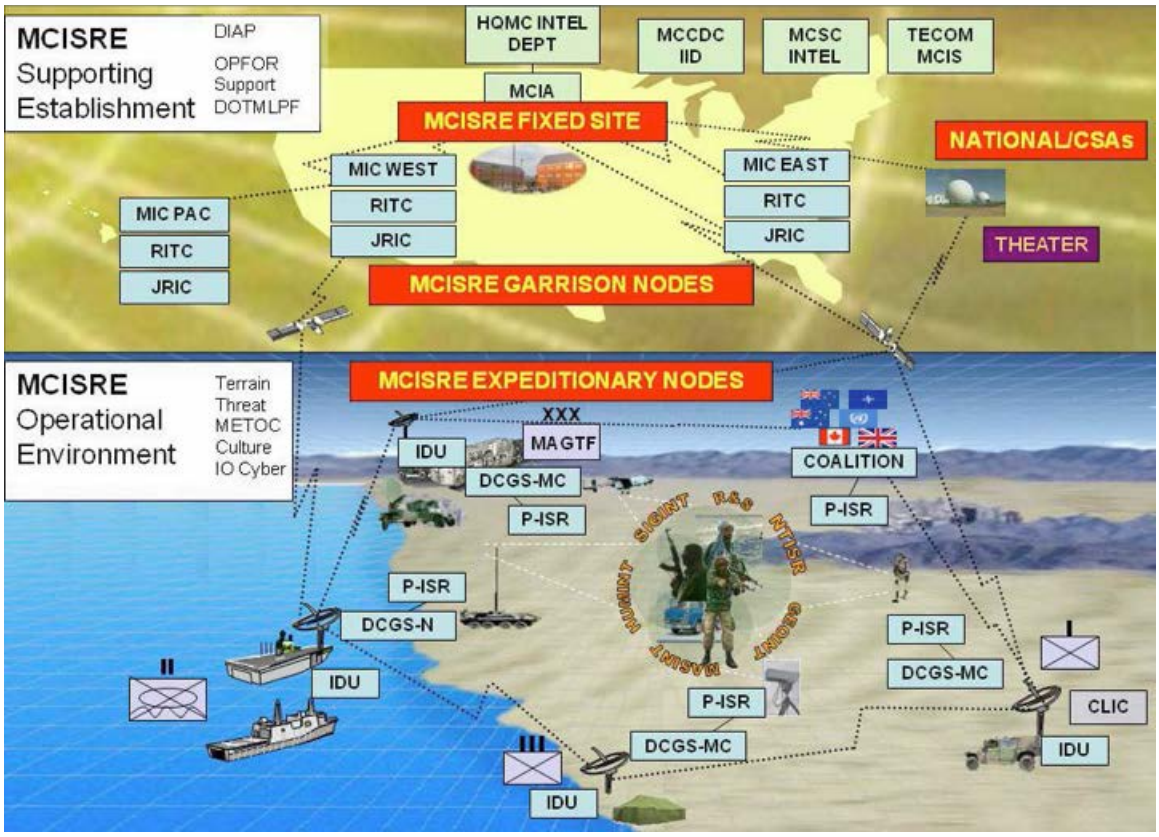


Figure 3. MCISRE High-Level Operational Concept Graphic (OV-1)

Source: Chudoba, Phillip. *USMC Intelligence Innovation* (Washington, DC: HQMC, Intelligence Department, 2012), 3.

In figure 3, reliance on the EMS is evident to support not only expeditionary nodes, but also the fixed site and garrison nodes of the intelligence enterprise. Satellite and tactical communications provide a robust network from the operator on the ground and a multitude of collection platforms, both ground-based and aerial, to intelligence

analysts around the world. Admiral Jonathan Greenert, Chief of Naval Operations, aptly states, “Our dependency on the spectrum and computer networks could become an Achilles’ heel – for us as well as our adversaries. We must therefore make a concerted effort to harness them to our advantage” (Greenert 2012).

Figure 3 does not convey reliance on uncontested access to the cyberspace domain as clearly as it does with the EMS. Intelligence operations and analysis rely on access to high bandwidth communications over multiple computer networks, to include the Non-classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIRPNet), the Joint Worldwide Intelligence Communications System (JWICS), the National Security Agency Network (NSANet) and multi-national networks established for specific operations. A multitude of databases exist to consolidate collected information, enabling analysts around the world to process and exploit information and disseminate intelligence products to commanders in support of ongoing operations.

Distributed Common Ground System-Marine Corps

The Distributed Common Ground System-Marine Corps (DCGS-MC) is one of three core pillars that supports MAGTF intelligence. Under Section 6 of the “USMC Concepts and Programs 2013” publication, which covers intelligence, surveillance and reconnaissance, DCGS-MC is a “service-level effort to migrate select Marine Corps ISR capabilities into a single, integrated, net-centric baseline” (HQMC 2013, 217). DCGS-MC is a systems component of the intelligence cycle and serves as an element of the processing, exploitation, analysis and production phases. According to this same publication, “DCGS-MC provides the foundation to expose and discover data from a multitude of geospatial intelligence (GEOINT), human intelligence (HUMINT), signals

intelligence (SIGINT), and other sources to provide all-source intelligence production" (HQMC 2013, 126-7).

DCGS-MC is part of a larger family of systems that was initially originated from the DCGS Mission Area Initial Capabilities Document (ICD) Joint Requirements Oversight Council Memorandum (JROCM) 001-03, which was published 6 January 2003. JROCM-001-03 "established the overarching requirements for a collection of net-centric capable systems that will contribute to joint and combined Warfighter needs for ISR support" (HQMC 2013, 127). In 2009, JROCM-041-09, DCGS Enterprise ICD, superceded JROCM-001-03, which defined and expanded "the DoD level vision for making ISR data more readily available to users" (HQMC 2013, 127). This initiative directed the USMC to coordinate across the joint force to establish common enterprise services that supported a net-centric vision.

The DCGS architecture is heavily reliant on the electromagnetic spectrum for operations. Figure 4 displays the system's communication architecture, which relies heavily on both the EMS and cyberspace. While this is an overview of the larger DCGS program, it is still indicative of how critical uncontested access will be for the success of DCGS-MC in support of operations.

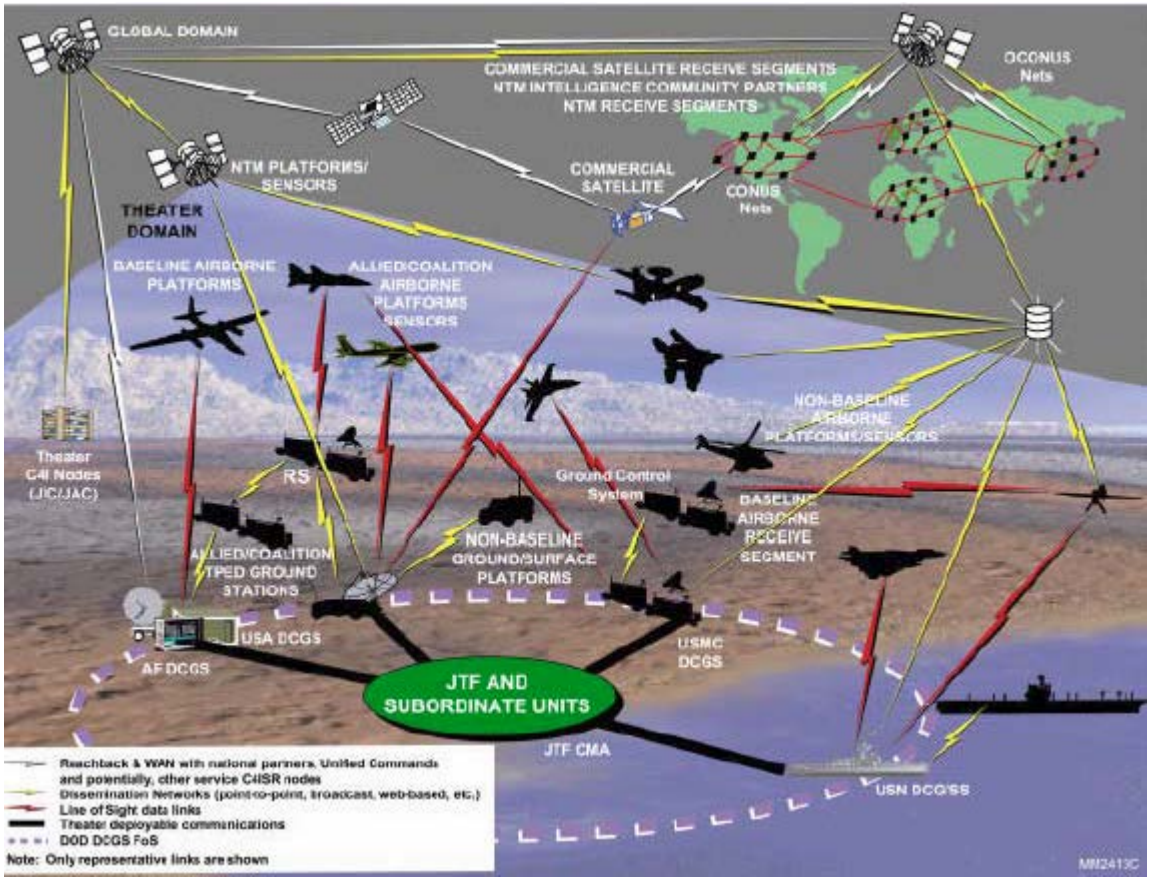


Figure 4. DoD DCGS High-level Operational Concept (OV-1)

Source: Scott E. Corsano, *Joint Fires Network ISR Interoperability Requirements within a Joint Force Architecture* (Monterey, CA: Naval Postgraduate School, 2003), 17.

In figure 4 satellite communication links, terrestrial based networks, and radio waves connect theater ground/surface and airborne platforms to ground stations around the world. All of the links depicted in yellow, white and red are vulnerable to the effects of jamming or denial of service.

Persistent-ISR

"USMC Concepts and Programs 2013" states that Persistent-ISR (P-ISR) "provides the means for intelligence planning, directing, and collecting" (126). This how

the MCISRE "sees" the battlefield. It is more of a strategy than a system, linking joint and national ISR assets to expand the organic capabilities of the MAGTF. P-ISR seeks to develop "sensors, analytic and predictive technologies, designed to enhance situational awareness and understanding to enable real time tactical decision making while lightening the warfighter's load" (Kruger 2012, 1).

P-ISR includes development of unmanned aerial systems (UAS) such as the RQ-7B Shadow, RQ-21A Integrator and the RQ-11B Raven. "USMC Concepts and Programs 2013" listed these three UASs as requirements for future Marine Corps operations. While these three platforms provide somewhat different capabilities, they all have one common factor. They require EMS-resident data links to operate effectively, including transmitting information back to the ground controller.

According to the DOD's "Unmanned Systems Integrated Roadmap: FY2011-2036," these data links are a critical component of UAS operations. Specifically, it states

> Communications: Unmanned systems rely on communications for command and control (C2) and dissemination of information. DoD must continue to address frequency and bandwidth availability, link security, link ranges, and network infrastructure to ensure availability for operational/mission support of unmanned systems. Planning and budgeting for UAS Operations must take into account realistic assessments of projected SATCOM [satellite communication] bandwidth, and the community must move toward onboard pre-processing to pass only critical information. (DOD 2011, vi)

The roadmap addresses the need to protect communications through multiple efforts to include low probability of intercept (LPI), low probability of detection (LPD) and anti-jamming (AJ) techniques. LPI techniques are technical modifications to waveforms, which make them more difficult to intercept. LPD aims to prevent the enemy from seeing specific mission activity and "involves techniques such as low power, spread spectrum, pulsed transmissions and/or directional antennas" (DOD 2011, 70). Lastly, AJ techniques

incorporate frequency hopping and randomization at the protocol level, as well as other waveform modifications (DOD 2011, 70).

The A2AD Environment

With an understanding of the MCISRE and how both DCGS and P-ISR rely on the EMS and cyberspace, it becomes clear how certain elements of the A2AD environment present a viable threat to Marine Corps' ISR operations. In 2010 Dr. Andrew Krepinevich, who is credited with coining the A2AD concept, drafted a paper for the Center for Strategic and Budgetary Assessments titled *Why AirSea Battle?*. Krepinevich argued that since the end of the Cold War, the "U.S. military's power-projection capabilities in defense of the nation's interests were effectively unchallenged" (2010, vii). However, he quickly followed this argument with recognition that proliferation of advanced military technologies to both state and non-state actors was rapidly and fundamentally changing this paradigm.

The U.S. seeks to project power for many reasons, one of which is economic globalization. Economic strength is closely tied to global supply chains, which provide access to goods and services (Krepinevich 2010, 5). U.S. global access will be challenged in the future.

> Specifically , several states, notably China and Iran, are strenuously working to raise precipitously over time – and perhaps prohibitively – the cost to the United States of projecting power into two areas of vital interest: the Western Pacific and the Persian Gulf. Their efforts present US leaders with a strategic choice of the first magnitude: either acquiesce in the advent of a new world order in which the United States can no longer freely access areas crucial to its economic well-being, or effectively assist key allies and partners in those areas in defending themselves from aggression or coercion. (Krepinevich 2010, 7)

Krepinevich identifies weapons, such as anti-ship cruise missiles, integrated air defenses, and medium-range artillery, rockets and missiles, that threaten the air, land and sea domains, as well as anti-satellite (ASAT) and cyber weapons. ASAT weapons are capable of disabling satellites either kinetically or non-kinetically. Therefore, an A2AD threat will also pose challenges to the EMS and cyber domain.

Electronic Jammers

In his article, "Command and Control Vulnerabilities to Communications Jamming" that was published in *Joint Forces Quarterly*, RDML Ronald C. Wilgenbusch, USN (Ret.) explained that the "way we command and control our forces is highly vulnerable to disastrous disruption. Modern operations have become dependent on high-capacity communications, and this vulnerability could cause our forces to sustain a serious mauling or, perhaps, not to prevail" (2013, 56). Electronic jammers are weapons that seek to deny an adversary use of the EMS to command and control, collect and disseminate intelligence, or communicate. Potential adversaries around the world are aware of the military's reliance on the EMS after studying U.S. operations over the past two decades (Wilgenbusch 2013, 58).

Wilgenbusch and co-author, CAPT Alan Heisig, USN (Ret.), define *jamming* as "electronically rendering a circuit or network unusable by disrupting it so it cannot be effectively used as a means of communication for purposes of command and control" (2013, 56). Intelligent and cunning use of jamming weapons makes it difficult to identify whether a system or frequency is experiencing interference or being targeted deliberately. Communications specialists and signals intelligence personnel are critical to determining how friendly systems are targeted by enemy electronic attack weapons.

The U.S. military relies on space-enabled communications to support operations. These communications largely travel over commercial broadcast satellite systems. Specifically, the article identifies that "[i]ntelligence, surveillance, and reconnaissance systems reflect how dependent U.S. forces have become on access to the orbital and cyber dimensions of the global commons" (Wilgenbusch 2013, 57). Wilgenbusch and Hesig stated that these systems lack comprehensive protection against jamming, "which is probably the cheapest, most readily available, and most likely form of denying or degrading the reliability of information flow" (2013, 57). In addition to communications over satellite systems, the military relies on space-based platforms to provide precision navigation and timing to a multitude of systems. Manned and unmanned aircraft, radio communications, precision munitions and a host of other military platforms require reliable access to GPS in order to function properly.

Dan Parsons, a staff writer for *National Defense Magazine*, published "Simple, Inexpensive Jammers Threaten GPS" in September 2013. He explained that inexpensive jammers made in China are as small as a cigarette pack and are capable of scrambling GPS signals in a small radius (Parsons 2013, 10). "GPS jamming is the act of interfering with the ability of receivers to lock onto the GPS signal, eliminating the ability to determine 3D positioning or calculate other information such as time, speed, bearing, track, trip distance and distance to destination" (Parsons 2013, 10). While the military operates on GPS signals that are harder to jam than civilian GPS, it is still vulnerable.

When GPS was first considered, it was primarily intended to be used as a navigational aid, not to control communication timing or direct weapons to their targets. "Jamming of GPS might be either unintentional or intentional. Johns Hopkins University

Applied Physics Laboratory has carried out an independent assessment of the system and concluded that accidental jamming is not a major risk. Intentional jamming poses a major threat, however" (Price 2001, 261). A Russian company, Aviaconversiya, currently produces a mobile, low-powered GPS jamming system with an advertised range of several hundred kilometers as long as it is operated within line-of-sight of the targeted receiver (Price 2001, 261). Given the reliance of a multitude of military systems on GPS, the potential threat of GPS jamming is critical to understand and combat.

Anti-Satellite Weapons

The People's Republic of China (PRC) and the People's Liberation Army (PLA) developed a kinetic ASAT capability and demonstrated this when they shot down an inoperative Chinese weather satellite on January 11, 2007 (Saunders 2007, 39). However, kinetic ASAT weapons are only a portion of the PLA's effort to deny the U.S. access to satellite communications. "The PLA has also developed ground-based ASAT laser systems that have reportedly been employed to 'dazzle' US satellites" (Saunders 2007, 39). A report from the Office of Threat Assessment published in 1995 defined *dazzling* as, "the temporary blinding of a sensor by overloading it with an intense signal of electromagnetic radiation, e.g., from a laser or a nuclear explosion" (Karas, vii). It is currently estimated that nine countries currently have lasers that are potentially capable of blinding or damaging satellites.

In addition to China, Russia also possesses satellite jamming capabilities. Further, "the proliferation of jamming technology has led to an increasing utilization of strategic and tactical jamming" (Wilgenbusch 2013, 58). One of the reasons jamming technology

is appealing to adversaries is that not only is it relatively inexpensive compared to more conventional weapons, but it is also incredibly effective way to disrupt a superior force.

In 2010, the Defense Intelligence Agency hosted a wargame that included more than 60 active duty service members and civilians from every branch. The specific focus of the wargame was how services would handle contested satellite communications access during future operations. During the conduct of the wargame, participants identified that the loss of assured satellite communications would create a significant risk to current military tactics. Further, older infrastructure and doctrine to potentially overcome a lack of assured long-distance satellite communications did not exist, which frustrated the service members and civilians. “Essentially, the entire spectrum of warfighting capability beyond preplanned initial insertion and organic logistics was significantly adversely affected” (Wilgenbusch 2013, 61).

Cyber Attacks

Beyond jammers and ASAT weapons, potential adversaries employing an A2AD strategy are also actively seeking to deny the U.S. military free use of the cyber domain. It is difficult to understand the cyber capabilities of our adversaries, especially through unclassified research, because these are well-kept secrets. However, Krepinevich states, “China’s cyber weapons are generally believed to be formidable, and the United States, as well as many other countries, has long been subjected to persistent cyber probes and attacks emanating from China” (2010, 16).

In *21st Century Chinese Cyberwarfare* authored by William T. Hagestad II in 2012, he explains that the “motivation of the People’s Republic of China to conduct cyber-warfare is comprised of fear, self-preservation and hegemony” (Hagestad 2012, 5).

The Communist Party of China, PLA, hacktivists and State Owned Enterprises work together to coordinate China's cyber warfare capability. Their computer network attacks (CNA) and computer network exploits (CNE) span a wide range of targets in foreign governments, militaries, and commercial enterprises to acquire sensitive information (Hagestad 2012, 7). The DOD continuously defends against Chinese incursions against their networks. Meanwhile, the "Critical Infrastructure surface and gaps exploitation is a key element of the Chinese Cyber and Information Warfare initiative; specifically the energy industry, which includes the oil, gas and electricity market segments" (Hagestad 2012, 37).

In January 2014, Dr. Roger Cliff, a senior fellow at the Atlantic Council researching East Asian security issues, briefed the U.S.-China Economic and Security Review Commission during a panel on China's military modernization. He identified a potential conflict arising over Taiwan, the East China Sea or the South China Sea. The primary threats that the U.S. military would face in a future conflict with China are "cyber-attacks on U.S. and allied information systems, the use of jammers and lasers to disrupt or blind U.S. and allied radar, surveillance, satellite and other sensors" (U.S. Congress 2014).

CNA and CNE threaten critical military information systems for not only forward deployed forces, but also for garrison commands that provide necessary support to operations. Through his research, Hagestad estimates that 10 to 20 terabytes of data from NIPRNET have been downloaded by the Chinese. The Chinese gather this data through approximately three million daily scans of the Global Information Grid, the main network artery of the DOD (Hagestad 2012, 44).

Potential enemies of the U.S. who cannot survive a head-to-head military conflict will employ an A2AD strategy. This will include both kinetic and non-kinetic attacks. The USMC deploys around the world to rapidly respond to crises and conflicts. Marines depend on having access to near real-time intelligence in support of these operations. In order to continue providing this support USMC ISR must be aware of potential threats to the EMS and cyberspace.

CHAPTER 4

THE NEED TO INNOVATE

> [E]ven the most sympathetic onlooker is likely to sense that the Pentagon lives in a sea of slogans, briefings using elaborate electronic graphics, and a self-satisfied belief that new platforms will solve the tactical and operational problems of the future.
>
> —Williamson Murray, "Thinking about Innovation"

U.S. forces faced enemies in Iraq and Afghanistan that possessed limited technical weapons systems. However, despite this fact, the USMC was unprepared for the threat of remote-controlled improvised explosive devices (RCIED) emplaced by this unsophisticated enemy. During both wars, the USMC, in concert with the rest of the DOD and private sector industries, focused efforts to counter the effects of deadly RCIEDs. Ground forces modified tactics, techniques and procedures (TTP) for patrolling. Engineers employed newly designed counter-RCIED electronic warfare systems. Intelligence analysts refocused their efforts to "attack the network," identifying financiers and builders of the RCIED cells. Essentially, the presence of RCIEDs forced the USMC to innovate.

During this decade of fighting in support of Operations Iraqi Freedom and Enduring Freedom, the USMC has enjoyed uncontested access to the EMS and cyberspace domain. The Marine Corps conducted ISR operations at will, collecting, processing and disseminating intelligence without challenge. However, with the certain proliferation of inexpensive jammers, ASAT weapons and cyber attack capabilities - weapons associated with an A2AD strategy - will the USMC need to innovate ISR TTPs?

Historical Case Study: Amphibious Warfare in the Interwar Period

History demonstrates that the Marine Corps innovated successfully during the Interwar Period and a study of what made their approach successful provides a potential path for future innovation. The senior leadership of the USMC identified a capability gap and approached innovation primarily through training and doctrine, which shaped technological development. Although the problem sets are different, it is useful to review lessons from history to help understand how to approach the process of innovation. This case study demonstrates that fancy new equipment alone cannot fix the ability to conduct ISR operations without the EMS and cyberspace. Rather, a comprehensive approach is necessary that reviews all areas of DOTMLPF.

Through the signing of the "Five Powers Treaty" in 1922, the U.S. and other signatories members agreed not to establish any new bases in Asia and the western Pacific. As a result of this, the U.S. would need the ability to forcibly occupy territory and establish bases for operations in the future (Millett 1996, 51). During the Interwar Period, Japan was the primary enemy the U.S. expected to fight, and that was divined to occur across the central Pacific Ocean. Japan was viewed as a threat because of expansionist international politics and the U.S' commitment to defend the Philippines and Guam (Millett 1996, 56-7). In 1919, the Joint Army-Navy Board's military planning committee began drafting War Plan ORANGE, "the strategic conception for a conflict with Japan" (Millett 1996, 57), which identified the need to seize advanced naval bases in the event of war with Japan.

While Britain and Japan recognized the need for conducting amphibious operations, the U.S. alone identified the requirement to conduct opposed landings. The

task to develop this capability fell to the United States Marine Corps (Millett 1996, 59, 71). With senior politicians questioning the necessity to have an independent Marine Corps, the USMC saw War Plan ORANGE as a way to fill a strategically vital niche capability and simultaneously secure recognition of its service necessity.

Doctrine Development

British failure at Gallipoli in 1916 "convinced the majority of military leadership in the world that joint naval and ground operations - Amphibious Operations - were inefficient and impractical" (Gillum 1967, 42). However, one organization saw a plethora of lessons learned in the fiasco at Gallipoli, the United States Marine Corps. Major General John A. Lejeune, the Commandant in 1920, realized the strategic significance of the amphibious assault mission. Accordingly he tasked Major Earl H. Ellis to conduct a study to determine the requirements for amphibious operations, focusing on the central Pacific. Over the next seven months, Ellis drafted Operations Plan 712, "Advanced Base Force Operations in Micronesia," which became the foundation for future training and planning in the Marine Corps (Millett 1996, 72).

In the early 1930s, the Navy and Marine Corps decided to produce formalize doctrine for amphibious operations. Staff and students assigned to the Senior Course at the Marine Corps Schools began drafting a manual for landing operations. Since there was a dearth of historical examples of successful amphibious operations, the USMC instead focused on the failures of Gallipoli (Gillum 1967, 42). They also reviewed the British tactics and principles, both good and bad. The lessons they drew from their studies provided the foundation for the "Tentative Manual for Landing Operations,"

published in January 1934. By 1938, the Navy accepted it as official doctrine renaming it "Fleet Training Publication #167" (Gillum 1967, 42-3).

While doctrine was being developed, there was also an on-going debate about amphibious operations in professional military and civilian journals. The debates brought to light the challenges associated with conducting opposed landings and helped continue the refinement of doctrine. Additionally, Congress remained aware of the discussions and progress on amphibious operations through annual reports from the service secretaries and congressional hearings.

The Navy and Marine Corps used "Fleet Training Publication 167" as its basis for conducting amphibious operations in the Pacific campaigns. Admittedly imperfect, it nevertheless provided a strong foundation upon which could be built training and real world experience (Gillum 1967, 43). As the USMC learned valuable lessons through training and amphibious operations, they updated and refined their doctrine.

Training

Amphibious landing operations training first began in 1924. By 1930, the Navy and USMC were actively testing their amphibious doctrine through annual exercises. "The Naval War College made its exercise a grand production that included navy and marine faculty and student officers from Newport and Quantico" (Millett 1996, 74). Putting doctrine into practice helped the Marine Corps identify one basic problem - "moving combat troops to landing boats from transports was too slow and disorganized" (Millett 1996, 75). Additionally, the existing landing craft precluded artillery and tanks from being transported to the beach. Further still, close air support, naval gunfire and assault engineering were inadequate to support the assault force.

With the USMC operating overseas from 1927 to 1935, the service had few opportunities to train. However, in 1935, the 1st and 2d Marine Brigades provided the landing force for the Navy's Fleet Landing Exercises (FLEX) (Millett 1996, 76). The Army joined FLEX during its third iteration in 1937. By 1940, the USMC was able to provide a force that was nearly representative of a wartime expeditionary force both in numbers and armament. These exercises helped the USMC make necessary revisions to the concepts put forth in the "Fleet Training Publication 167" (Millett 1996, 76).

Additionally, the exercises shaped refinements to USMC mobilization concepts and training. Primarily, the USMC based training around the concepts set forth in War Plan ORANGE. The FLEXs allowed the Navy and Marine Corps to experiment

> with about every imaginable amphibious technique and tactical approach allowed by their equipment. They tried day and night landings, smokescreens, varieties of air and naval gunfire support, concentrated assaults and dispersed infiltrations, the firing of all sorts of weapons from landing craft, and an array of demonstrations, feints, subsidiary landings, and broad-front attacks. (Millett 1996, 77)

During these exercises, USMC planners identified critical tasks such as the need to combat load equipment, ensuring initially required equipment, weapons, ammunition and rations were positioned to be offloaded first (Shaw 1992, 2). Training continued to shape the USMC's TTPs for amphibious landings and doctrine refinement until the U.S. entered World War II.

In addition to training the landing forces, the USMC understood the importance of aviation in support of amphibious landings. While the Navy was responsible for training the Marine Corps' pilots, those pilots were still subject to tasking by the Commandant of the Marine Corps. In the 1930s, the Commandant tasked the senior aviator stated at Headquarters Marine Corps to focus on understanding how aviation could best support

opposed landings (Millett 1996, 85). The senior aviators of the service saw their role in amphibious operations as providing aerial defense for established and advanced naval bases (Millett 1996, 86). Aviation assets also provided critical reconnaissance prior to an opposed landing. Pilots trained to observe targets and relay information to naval gunfire support.

The process of launching a shipborne landing force against a defended coastline presented a multitude of problems. Naval gunfire support needed to be carefully timed to destroy as much of the enemy's defense as possible while allowing the landing force to move from ship to shore. At the last moment, naval gunfire would cease to prevent friendly fire incidents, at which time Marine aviators would provide aerial defense to enable the force to land (Isley 1951, 38). USMC planners understood the inherent limitations of naval gunfire, "but their general conclusion was that many of these handicaps could be at least partially overcome with practice and experimentation, and that effective employment of ships' guns in lieu of artillery was well within the realm of practical possibility" (Isley 1951, 38).

Initially, the USMC's training exercises experienced similar deficiencies that the British faced during the Gallipoli landings. In 1924, the Marines conducted a force on force amphibious operations exercise on Culebra Island. During the exercise, the Marines identified that the transport ship was ineffectively loaded, leaving the Marines without food on the first night. Certain Naval boat officers landed out of sequence and on the wrong beaches (Diana 2013, 27). The Marines learned from the chaos of the initial amphibious exercises, modifying their doctrine as they learned new lessons and prepared for a future campaign against Japan.

Results

The USMC's first opposed landing occurred in 1942 on Guadalcanal, where intelligence identified that the Japanese had constructed an airfield. This amphibious landing, named Operation Watchtower, came earlier than senior leaders of the Marine Corps expected. 1st Marine Division composed the landing force for the invasion. Henry I. Shaw, Jr., a Marine Corps historian, described the Marines as "confident, certainly, and sure that they could not be defeated," but the majority of these men had never seen combat (Shaw 1992, 6). The campaign, which lasted six months, was costly. "The total cost of the Guadalcanal campaign to the American ground combat forces was 1,598 officers and men killed, 1,152 of them Marines" (Shaw 1992, 51). However, the Japanese forces defending the island lost 25,000, approximately fifty percent of whom were killed in action (Shaw 1992, 52).

While 1st Marine Division sustained heavy losses on Guadalcanal, this was the first opportunity for the Marine Corps to apply doctrine and lessons learned from training against a real world enemy. A week prior to the landing, B-17 bombardments and naval gunfire prepped the landing beaches, driving the occupying force to the west (Shaw 1992, 7). However, the landing force still faced significant enemy opposition upon landing, Japanese forces were hiding in secure caves. The Japanese provided fierce resistance to the landing force. Although the Marines had trained to conduct an opposed landing for over a decade, this first amphibious landing provided yet another learning experience.

Nearly two and a half years later, the Marines found themselves assaulting the shores of Iwo Jima. Major General Harry Schmidt commanded V Amphibious Corps, the designated landing force comprised of three Marine divisions (Alexander 1994, 3). Over

half of this force were veterans of fighting in the Pacific and it was noted that "[t]he troops assaulting Iwo Jima were arguably the most proficient amphibious forces the world had seen" (Alexander 1994, 3). By February 11, 1945 Lieutenant General Tadamichi Kuribayashi's defense force was heavily fortified and dug in to defend Iwo Jima from the Americans. Having learned the importance of sustained naval bombardment to prepare the beachhead for landing, MajGen Schmidt requested ten days of preparatory fires from Vice Admiral Kelly Turner, commander of the Expeditionary Forces. However, due to strategic, tactical and logistical reasons, the Navy would only provide three days of bombardment. (Alexander 1994, 8). Based on training during the Interwar Period and previous amphibious operations in the Pacific, Lieutenant Colonel Donald M. Weller, the Task Force 51 naval gunfire officer, devised a "modified form of the 'rolling barrage' for use by the bombarding gunships against beachfront targets just before H-Hour" (Alexander 1994, 11). The intent of the rolling barrage was to keep naval gunfire support in action while the troops moved towards the beach.

While the application of naval gunfire on Iwo Jima is only one aspect of the amphibious landing, it is exemplary of how the Marines' training in the Interwar Period and ability to learn from pervious experiences in the Pacific benefitted the amphibious force. "Iwo Jima represented at once the supreme test and the pinnacle of American amphibious capabilities in the Pacific War" (Alexander 1994, 49). Lacking the element of surprise, MajGen Schmidt used speed and aggression to overwhelm the Japanese defenders. Colonel Wornham of the 27th Marines stated, "The landing on Iwo was the epitome of everything we'd learned over the years about amphibious assaults" (Alexander 1994, 49). The USMC demonstrated the ability to identify a threat, to train to

defeat that threat, to modify or create doctrine to support new TTPs and to continue learning throughout the Pacific campaign.

Center of Gravity Analysis

Marine Corps Doctrinal Publication (MCDP) 1, *Warfighting*, provides critical questions that military planners must ask about an enemy force. “Which factors are critical to the enemy? Which can the enemy not do without? Which, if eliminated, will bend him most quickly to our will?” (HQMC 1997, 46). We can also use this line of reasoning to analyze ourselves.

A center of gravity is a characteristic, capability or source of power from which a military force derives its freedom of action, physical strength or will to fight (Strange 2004, 7). For the USMC, the physical source of strength is the Marine Air Ground Task Force, or MAGTF. MCDP 1 states, “MAGTFs are task organizations consisting of ground, aviation, combat service support, and command elements. The MAGTF provides a single commander a combined arms force that can be tailored to the situation faced” (HQMC 1997, 55). The USMC’s ability to task organize a force for a geographic combatant commander and a specific mission is a critical to mission accomplishment.

Every center of gravity has critical capabilities, which are those primary abilities that a center of gravity can accomplish (Strange 2004, 7). Critical capabilities generate force of persuasion. The MAGTF’s critical capabilities include power projection, amphibious operations, stability operations and humanitarian and disaster relief operations. Because of the forward positioning of the MAGTF assigned to each Marine Expeditionary Unit, the USMC’s center of gravity can rapidly respond to any type of crisis around the world.

In order for a center of gravity to accomplish critical capabilities, they have critical requirements, those conditions, resources and means that are essential for a critical capability to be fully operational (Strange 2004, 7). The MAGTF's critical requirements include aviation assets, command and control systems, intelligence and the electromagnetic spectrum. Aviation assets can provide critical support to ground forces, assist with logistic operations and conduct reconnaissance. Command and control systems enable the MAGTF commander to direct subordinate elements in mutually supporting operations. Additionally, these systems provide a means for subordinate commanders to relay information to higher headquarters to keep them apprised of the situation on the ground. The MAGTF requires intelligence to prepare effectively for operations, to target enemy forces and to plan for future campaigns. The EMS is a critical requirement for any MAGTF operation. From basic communication to relaying information collected by a UAS, the EMS is an element of the operational environment that permits the very functioning of our highly-technological, digitally-empowered Corps.

Colonel Melvin G. Carter, who is currently serving as the Executive Assistant, to the Associate Director of Military Affairs at Central Intelligence Agency and at the time of this writing has 25 years of experience in USMC intelligence and electronic warfare, said, "you can't really separate what we do in the Marine Corps intelligence community without touching into the electromagnetic spectrum" (2014). He added that cyberspace is just as integral to intelligence operations as the EMS. He further elaborated saying, "everything we do, whether it's people, logistics, command and control, putting munitions and ordnance on target, all rely on the cyber domain" (Carter 2014).

Some of the MAGTF's critical requirements may be vulnerable to neutralization, attack or interdiction, providing a decisive advantage to an adversary. These are known as critical vulnerabilities (Strange 2004, 8). MCDP 1 states,

> Center of gravity and critical vulnerability are complementary concepts. The former looks at the problem of how to attack the enemy system from the perspective of seeking a source of strength, the latter from the perspective of seeking weakness. A critical vulnerability is a pathway to attacking a center of gravity. Both have the same underlying purpose: to target our actions in such a way as to have the greatest effect on the enemy. (HQMC 1997, 47)

Among the critical requirements listed, the EMS is a critical vulnerability to the MAGTF. The Marine Corps relies on technological systems, connected by either the EMS, cyberspace or both, to conduct all major warfighting functions.

An adversary who lacks the combat power force ratio to defeat an enemy's center of gravity directly can alternatively use an indirect approach to achieve the same goal. This indirect approach targets the critical vulnerability (or vulnerabilities) of an enemy force, pitting strength against weakness. In the A2AD environment, an adversary could potentially seek to disrupt the EMS in order to prevent the MAGTF from collecting intelligence, communicating and conducting command and control functions. Rather than targeting the MAGTF directly, an adversary targeting a critical vulnerability can still hope to defeat or delay the MAGTF by limiting their use of a critical resource, in this case the EMS.

Lessons from the Past

As described above, the Interwar Period provides critical lessons to today's Marine Corps as to how to prepare for the challenges and threats of tomorrow. The clear identification of a threat, which was Japan post World War I, is necessary to plan

effectively for future conflicts. The determination of a clear enemy provides the intelligence enterprise a focus for collecting and analyzing information against a specific threat. Conducting realistic training that prepares the Marines for what they will face in combat is critical to ensuring future success.

"Expeditionary Warrior 2012" (EW12) is the USMC most recent Title 10 wargame. Additionally, the Marine Corps currently conducts two major exercises on an annual basis to incorporate the concepts in *AirSea Battle*, "Dawn Blitz" for 1st Marine Expeditionary Brigade (MEB) and "Bold Alligator" for 2d MEB. Due to the similar nature of both exercises, this paper will only discuss Bold Alligator 2013 (BA 13). In a report on the exercise published by *Second Line of Defense,* the author describes the exercise as "starting with a significant anti-access, area denial capability and then working through that challenge to put forces ashore" (*Single Naval Battle* 2013, 2).

Expeditionary Warrior 2012

Conducted in March 2012, EW12 presented a fictional scenario based in 2024 Africa. The intent of this exercise was "to serve as a means to identify potential gaps and opportunities for enabling joint force access and entry against capable adversaries in an anti-access, area-denial environment" (HQMC 2012, i). The EW12 final report identified that opponents employing an A2AD strategy will likely have electronic warfare capability and cyber weapons. Due to the unclassified nature of the report, HQMC did not include specifics on classified excursions conducted at the secret level. Subject matter experts gathered to discuss A2AD threats against command and control systems and the EMS, cyber and information operations, as well as ISR operations (HQMC 2012, 6).

Of note from the discussions on cyber operations, it was identified that while "[t]he fire support construct used to conduct planning for non-kinetic effects is a better fit for some lines of operation such as information operations, but continually evolving, complex capabilities like cyber may require a new framework" (HQMC 2012, 14). The participants also recognized that the potential ability of an A2AD threat to possess the ability to conduct electronic attacks and GPS-denial complicate the ability for elements of the amphibious force to communicate and coordinate efforts. Further, they understood that it was necessary to ensure "limited bandwidth remains intact and that the enemy force does not hamper the transmission of information or introduce malicious code into the combined joint task force networks" (HQMC 2012, 19). One key determination that leadership made was the need to ensure policy, capability and capacity issues related to cyber operations are further researched. Additionally, it is critical that senior military leaders are familiar with U.S. cyber capabilities.

Bold Alligator 2013

According to guidance published for the exercise, BA 13 was

> a synthetic, scenario-driven exercise designed to improve naval amphibious core competency through focusing on the single naval battle concept and refining Expeditionary Strike Group TWO, 2d Marine Expeditionary Brigade, and Carrier Strike Group TWELVE staffs' ability to plan, coordinate and execute MEB-sized amphibious operations from a sea-base operating in a medium threat anti-access/area-denial environment. (*Single Naval Battle* 2013, 8)

Additionally, the focus of BA 13 included command and control relationships, examination of current command, control, communications, computers, combat systems and intelligence (C5I, naval staff integration, force apportionment and employment, and assessment of naval amphibious capabilities, doctrine and TTPs (*Single Naval Battle*

2013, 8). BA 13 was a synthetic exercise, rather than a live exercise, which means that "key combat assets were networked and operated together interactively in response to 'events' generated by the scenarios and challenges set by the exercise" (*Single Naval Battle* 2013, 13). BA 12 was a live exercise, just as BA 14 will be.

As a joint exercise, the USMC worked closely with the Navy during BA 13. The commander of Expeditionary Strike Group (ESG) 2, Read Admiral Ann C. Phillips, explained that the surface fleet went beyond the traditional role of naval surface fire support and also incorporated new weapons and the Navy's ability to respond quickly to cyber activities and other challenges. She also discussed the ability of the Navy to combat air and missile defense threats. Further, the ESG provided the ground force a sea base that assists with intelligence, logistics, fire support, command and control and air support, creating a more effective force (*Single Naval Battle* 2013, 2-3).

The ESG 2 deputy, Colonel Bradley Weisz, explained that the simulated exercise presented a mix and match of threats against the force, specifically those threats that arise in an A2AD environment. The notional adversary possessed coastal defense cruise missiles, anti-ship cruise missiles, surface-to-air missiles and sea mine capabilities. A host of conventional threats in the air, surface and sub-surface domain existed to challenge the entire amphibious force. As the landing force, 2d MEB, moved ashore, they faced both conventional and asymmetric threats from violent extremist organizations (*Single Naval Battle* 2013, 30). Speaking about potential objectives for BA 14, Col Weisz stated, "we need to continue working on and refining our communications strategy. It is clear that in this type of operation, the littoral version of the three-block war,

communications strategy is absolutely crucial for the success of the force" (*Single Naval Battle* 2013, 30).

Just as Marine leaders of the Interwar Period conducted large scale training exercises to prepare for the seizure of advanced naval bases in the Pacific, today's leadership is training to defeat an adversary who employs an A2AD strategy. The USMC conducts both live and simulated exercises on an annual basis to test new systems, TTPs and doctrine. However, missing from the BA 13 enemy scenario is any threat to the EMS or cyberspace domain.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Success is a poor teacher.

— General (Ret) James Mattis,
former Commander, U.S. Central Command

Over the past decade, the United States Marine Corps has experienced freedom of action throughout the EMS and cyberspace. Although being continuously engaged across the full range of military operations around the globe, no adversary has truly presented a threat to the manner in which the USMC leverages the EMS and cyberspace to conduct operations. USMC ISR continues to employ systems that accurately track enemy movements and provide critical information to ground commanders in a timely manner because of this uncontested access. However, it would be unwise to expect that this will be the norm for the future.

With the rise of potential adversaries, both state and non-state actors, who are adopting an A2AD strategy, freedom of action in the EMS and cyberspace will be contested. Electronic jammers, ASAT weapons and cyber threats will challenge USMC ISR operations. Intelligence provides insight into these different weapons systems and which adversaries may possess them, but it is up to the senior leadership of the Marine Corps intelligence division to effectively prepare to face these challenges.

Conclusions

Current guidance from the DOD and individual services presented earlier indicates that senior military leaders and DOD officials understand that adversaries who employ an A2AD strategy will possess weapons to counter use of the EMS and cyber

domain. However, intelligence programs of record at Marine Corps Systems Command continue to research, fund and deliver intelligence systems that are heavily reliant on both the EMS and cyberspace and exceedingly vulnerable.

As the USMC concludes major operations in Afghanistan, and simultaneously faces a drawdown in personnel and budget cuts, it is necessary to prioritize efforts effectively to meet the requirements set forth in the *National Security Strategy*. In the April 16, 2014 edition of the "Marine Corps Communications Playbook," senior leaders depict where the Corps is going. Recognizing the ongoing fiscal crisis, the playbook states that "the Marine Corps is responsibly building a relevant, lean, and prudent force for the 21st century" (HQMC 2014, 4). Committed to maintaining an expeditionary, consistently ready maritime force capable of rapidly responding to crisis, senior leaders understand the need to maintain an innovative spirit to meet tomorrow's threats.

If reliance on the EMS and cyber is a critical vulnerability, then the USMC must expect an adversary to target it. Therefore, it is imperative that the USMC prepare to operate in a contested EMS and cyberspace domain prior to encountering it in a conflict, or there will be severe repercussions. Marine intelligence operators who have come to rely on technology that provides them the ability to provide near real-time support to ground combat units will be unable to effectively operate. An adversary capable of denying the USMC use of the EMS and cyberspace could leave ISR operators blind and deaf.

Recommendations

The DOTMLPF construct provides a method to evaluate the USMC in order to determine future changes that may be necessary to maintain force readiness. Based on an

analysis of the A2AD environment and potential threats to freedom of operation in the EMS and cyber domain, potential changes to USMC training, and leadership and education could better prepare the Marine Corps intelligence branch for the future. Simulating a contested EMS and cyber domain is an initial step to prepare Marines for future scenarios. Additionally, educating Marine Non-commissioned officers and officers about the vulnerabilities involved in relying on the EMS and cyberspace for communications will provide cost effective solutions to preparing the USMC. Materiel solutions may exist, but will not be addressed in this paper.

Training

The USMC conducts three major training operations on an annual basis that focus on combatting an A2AD threat—Expeditionary Warrior, Dawn Blitz and Bold Alligator. Units consistently rotate through Marine Corps Air Ground Combat Center (MCAGCC) in Twentynine Palms, CA to participate in the Integrated Training Exercise (ITX). Multiple exercises are held aboard Marine Corps Air Station Yuma in Arizona. Additionally, Marines around the world conduct regular training exercises at home station. However, due to restrictions on conducting electronic attack, this is not a common component of training exercises.

Marine Corps Warfighting Publication 2-22, *Signals Intelligence*, electronic attack is the "division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability" (HQMC 2004, F-8). While USMC electronic warfare units conduct electronic attack against an adversary, there is potential for bleed over interference against friendly communications.

Many factors affect the range of an electronic attack, such as terrain, power output and frequency ranges. An electronic jammer cannot target a specific emitter. Rather, it produces a radio wave in a designated area that is stronger than the enemy's communications. Because the radio waves cannot be completely controlled, there is potential for electronic attack training to negatively affect civilian communications systems.

For example, in January 2007, during a naval exercise off of the coast of San Diego, California, air traffic controllers, emergency medical personnel with pagers and harbor control officials began having problems with their communications and radar equipment. People in the city lost cellphone service and automated teller machines could no longer connect to their banks. After several days, officials determined that the cause of the electronic interference was naval technicians conducting electronic jamming during an exercise. The objective of the electronic attack was to test their procedures for operating when communications are lost (Hambling 2011, 44). Due to the potential effects of electronic jamming on civilian infrastructure, there are strict limits placed on frequency ranges, power output and location of jamming emitters. Given these restrictions, opportunities to train against a contested EMS environment are very limited.

Additionally, very few units in the Marine Corps possess electronic jamming equipment on their tables of equipment. The three radio battalions, four Marine tactical electronic warfare squadrons and a few of the Marine attack squadrons are outfitted with the capability to conduct electronic attack. Operational commitments of these units limits their ability to participate in every exercise.

In order to overcome these restraints, it is possible for electronic jamming to be simulated. Many exercises incorporate modeling and simulation to train towards specific objectives. For example, the Infantry Immersion Trainer (IIT) in Camp Pendleton, California provides a simulated village based on data gathered from Iraq and Afghanistan. Units using the IIT conduct missions in the village to prepare for squad and platoon sized exercises. The intent of this facility is to provide infantry units with the sights, smells, and sounds of the environment they will see in combat. In addition to creating a realistic environment for training, the IIT uses videography to populate the village with both civilians and insurgents.

Infantry units patrol through the IIT with training ammunition loaded in their weapons. As different images appear, Marines train to react appropriately given the scenario. The digital avatars respond based on the actions of the Marines, providing a training environment that attempts to introduce the confusion of battle.

The intelligence community can significantly benefit from simulation training as well. Given the restrictions on conducing electronic attack, simulating the effects of a contested EMS environment provides a realistic training environment to challenge intelligence operators in the field without risking any unintentional interference. Additionally, this can be done at almost no cost. Unit leaders must look for creative solutions that are readily available to them to challenge their Marines and prepare them to operate in a contested EMS environment.

Training to operate in an A2AD environment where the enemy denies us freedom of action in the EMS can be as simple as eliminating radios and other equipment that relies on radio waves from the scenario. This is the cheapest method to train Marines to

operate effectively without the use of the EMS. Without the ability to disseminate intelligence via the EMS, intelligence operators will devise new ways to pass information across the battlefield. Understanding the consequences of an adversary's jamming system will allow Marine leaders to effectively replicate the loss of communications in a training environment. This will enable Marines to develop TTPs to handle these situations in combat.

However, every jamming system has limitations. Therefore, it is important for Marine leaders to understand how electronic attacks work and attempt to provide realism to the training event. Very rarely is it possible to provide continuous jamming against a specific frequency range. Therefore, during a scenario based exercise it is appropriate to provide periods of communications denial. The periods of simulated jamming should be intermittent and random to provide as much realism as possible. This training technique requires a significant amount of oversight and planning.

Exercise control staff must produce a detailed timeline for simulated jamming and ensure that communications do not occur during these communication “blackout” windows. The USMC operates with centralized command and control and decentralized operations. Essentially, the commander provides intent and subordinate units carry out the mission. Therefore, during an exercise, numerous personnel would be required to supervise small units and implement the simulated jamming scenario. While this may be a hindrance to running an exercise, the benefit to training in a contested EMS environment will effectively prepare Marines for potential challenges in the A2AD environment.

Training to Marines how to handle the loss of cyberspace is more difficult than denying the use of service. Cyber attacks are similar in nature to electronic attacks in that they can affect more than the targeted systems. However, the major difference is in how an attack against the EMS can be limited to a geographic area, whereas a cyber attack has potential to affect systems around the globe.

Marine Corps intelligence operators use programs on NIPRNET, SIPRNET, JWICS and NSANET. The most vulnerable network is NIPRNET, but all four networks have some vulnerabilities. Conducting training that incorporates cyber attacks against any live network has potential to negatively affect operational systems that are supporting real world operations. Therefore, it is difficult to conduct scenario based training that includes an opposing force with the ability to attack USMC networks.

Rather than using live networks, the USMC would significantly benefit from building closed networks for training purposes. These intranet systems would mirror the same functionality of the internet systems, but would never physically touch them, which would negate the potential for taking down a live system. A closed system would provide Marines an opportunity to learn how to operate in an environment where the cyber domain is contested. However, a closed system would require funding.

During an exercise, the exercise control staff would possess the ability to attack the closed network. Marine who operate intelligence systems would train to protect the networks while intelligence analysts and operators determine TTPs to overcome network outages. Similar to a pilot using a simulator for training in various scenarios, a closed network simulator would prepare intelligence operators to handle A2AD cyber threats.

When asked about the benefits of simulated training, Col Carter said

> Yes, I'm a firm believer in things of that nature. So, with simulation training, as you know, we've developed the Jedis in the aviation world at WTI. We've now come on board with MCTOG to train ground intel folks and so, we make our money by going to the Twentynine Palms and Yumas of the world, bringing ourselves together as MAGTF planners, action officers, to kind of help us see and understand ourselves better and get ahead of the enemy. So I'm a big fan of these simulated environments, where you can actually, virtually walk through a scenario, stop at a certain point in the scenario, talk about the challenges and lessons learned, reset, go back through it, rehearse, rehearse, rehearse...I think that just makes us better MAGTF officers. (Carter 2014).

Building a simulated training environment comes at a cost. While the DOD faces a shrinking budget, military leaders are forced to prioritize multiple programs to prepare for a multitude of threats. It is important for senior intelligence officials to understand the potential for an A2AD threat to employ electronic and cyber attacks against U.S. forces and prioritize effectively to prepare to operate in these conditions.

Leadership and Education

As discussed in chapter 4, Marine Corps leaders heavily invested in the study of amphibious warfare during the Interwar Period in order to prepare for a potential campaign against Japan in the Pacific theater. The Naval War College and the Marine Corps' Senior Course revised their curriculum to incorporate the study of amphibious operations and current doctrine. Senior Marine leaders, spurred on by the work of Maj Earl “Pete” Ellis, acknowledged the threat posed by Japan and formed the schoolhouse curriculum around those skills necessary to be successful in an amphibious war.

Today's leaders understand the emerging A2AD threat and are developing strategies to counter that threat. However, the schoolhouse has not caught up to educate Marine officers about the potential threat that adversaries who employ an A2AD threat

pose to the EMS and cyberspace. For example, the curriculum at Marine Corps Command and Staff College includes only 13 hours of instruction on cyber planning. The students focus on the following learning objectives: capabilities and limitations of U.S. military cyber operations, current guidance related to cyber strategy, emerging concepts, the integration of information operations and cyberspace operations, roles of the combatant commanders and staff in planning cyber operations, and opportunities and vulnerabilities created in operations by the reliance on networks and information technology in cyberspace (Melchior 2013, 2-3).

The U.S. Army Command and General Staff College's core curriculum and advanced operations course include no specific courses on cyber planning or non-kinetic fires. The CGSC 14-01 course curriculum included one guest speaker from the Army Capabilities Integration Center who addressed the challenges of the cyber domain. While the practical application exercises attempted to incorporate an opposing force with a capability to conduct electronic and cyber attack, this was a negligible attempt to prepare field grade officers for dealing with the A2AD threat to the EMS and cyberspace.

In order to prepare future military leaders for planning and operating in a contested EMS or cyberspace environment, the military education system must evaluate the current curriculums to teach officers and staff non-commissioned officers about this threat. Military planners need to understand current capabilities and limitations of organic equipment and where they are potentially vulnerable to enemy activity. Additionally, planners need to be aware of adversaries who have the capability to conduct electronic and cyber attack. In order to prepare to defeat an A2AD threat, it is imperative that

military leaders understand both the vulnerabilities of their own equipment and TTPs as well as the forces that can threaten how we operate.

Military educators must devise a way to provide students of all occupational specialties with a better understanding of the EMS and cyber domain. The main reason for not incorporating lessons on the EMS and cyberspace into the military schoolhouse relates to the level of classification on these subjects. However, even at the unclassified level a significant amount of information can help students understand the nature of the threat and how to counter it. Incorporating an opposing force who can challenge our access to the EMS and cyberspace for all exercises will force military planners to develop TTPs to operate effectively without constant access.

Small changes to the way we train and educate Marines can have vast benefits for the future of Marine Corps ISR operations. If the USMC continues to expect to operate freely in the EMS and cyberspace, it will be unprepared to face the challenges of the future. An adversary who uses an A2AD strategy to prevent the USMC from accessing the global commons will challenge the method in which ISR operations have been conducted for the past decade. Marines who have come to rely on near real-time access to intelligence will need to operate blindly if we cannot prepare for this threat.

Future Research Topics

During the conduct of research for this thesis, I identified three related topics of interest that would lend themselves to future research. These future research topics are as follows: alternative communications methods, swarming ISR assets, and cyber operations limitations. Subsequent issues that need further research are included in the following paragraphs.

As to the first potential research topic, alternative communications methods, the USMC must envision how it would operate in a contested EMS and cyberspace environment. Rather than focusing on how an adversary can deny the USMC's ability to leverage the EMS and cyberspace, it is relevant to research alternative communication methods that can be leveraged to pass information. For example, aviation assets could provide an alternate method for passing orders if the enemy denies use of the EMS and cyberspace. Another option would be to study an increase in the use of high frequency communications. They are more difficult to jam that very high frequency or ultra high frequency communications and provide users with the ability to pass both voice and data communications over long distances. A review of current doctrine and TTPs for intelligence collection and dissemination could provide insight for new methods to overcome a contested EMS and cyberspace environment. This research should include an assessment of the current table of equipment and whether legacy systems that provide alternative communications methods still exist.

A second topic of interest is the idea of swarming ISR assets in order to defeat A2AD defenses. Currently the USMC has a limited number of expensive UASs that provide intelligence collection and targeting for ground forces. The swarming approach consists of using a multitude of low cost UASs over the targeted area to gather information with the assumption that some will be targeted by enemy systems and others will successfully penetrate the defenses.

Lastly, the third potential research topic is cyber operations limitation. A significant amount of research exists on cyber operations. The data focuses on what an enemy can potentially do via cyber exploitation and attack, but it does not evaluate the

limitations of cyber attacks. Understanding the limitations of an enemy capability can provide insight as to how to protect our systems. Identification of portions of the network that can be protected from adversary cyber operations will provide the USMC with opportunities to continue operations despite potential attacks.

REFERENCE LIST

Alcazar, Vincent. 2012. Crisis management and the anti-access/area denial problem. *Strategic Studies Quarterly* 6, no. 4 (Winter): 42-70. http://search.proquest.com/docview/1240323761?accountid=28992 (accessed February 16, 2014).

Amos, James F. 2012. Who we are. *Proceedings Magazine* 138, no. 11 (November 11). http://www.usni.org/magazines/proceedings/2012-11/who-we-are (accessed February 3, 2014).

The AOC the Electronic Warfare and Information Operations Association. 2008. *Electronic warfare: The changing face of combat*. The Association of Old Crows. https://www.myaoc.org/EWEB/images/aoc_library/Government_Affairs/AOC%20report.pdf (accessed February 16, 2014).

Brimley, Shawn, Ben FitzGerald, and Kelley Sayler. 2013. *Game changers: Disruptive technology and U.S. defense strategy*. Center for New American Security. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Gamechangers_BrimleyFitzGeraldSayler.pdf (accessed February 11, 2014).

Carter, Melvin G. 2014. Interview by author. Fort Leavenworth, KS. April 15.

Chudoba, Phillip. 2012. USMC intelligence innovation. Headquarters, US Marine Corps, Department of Intelligence, Washington, DC. Armed Forces Communications and Electronics Association. http://www.afcea.org/events/tnlf/southwest/documents/ADIRINTPlugFestInnovationBrieffinalChudoba.pdf (accessed March 1, 2014).

Defense Advanced Research Projects Agency. 2013. *Driving technological surprise: DARPA's mission in a changing world*. www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2147486475 (accessed February 11, 2014).

Dempsey, Martin E. 2012. *Release of the joint operational access concept*. DoD Live. http://www.dodlive.mil/index.php/2012/01/release-of-the-joint-operational-access-concept-joac/ (accessed February 3, 2014).

Diana, Gabriel L. 2013. Vision, education, and experimentation: Marine corps organizational behavior and innovation during the interwar period. Master's thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS. http://cgsc.contentdm.oclc.org/cdm/ref/collection/p4013coll2/id/3010 (accessed March 18, 2014).

Gillum, Donald E. 1967. Gallipoli: Its influence on amphibious doctrine. *Marine Corps Gazette* 51, no. 11 (November): 41-46.

Greenert, Jonathan W. 2012. Imminent domain. *Proceedings Magazine* 138, no 12 (December): 16-21. http://search.proquest.com/docview/1239453355?accountid=28992 (accessed February 18, 2014).

———. 2013. Wireless cyberwar, the EM spectrum, and the changing Navy. Breaking Defense. http://breakingdefense.com/author/adm-jonathan-greenert/ (accessed January 28, 2014).

Grissom, Adam. 2006. The future of military innovation studies. *The Journal of Strategic Studies* 29, no. 5 (October 1): 905-934.

Hagestad II, William T. 2012. *21st century Chinese cyberwarfare*. Cambridgeshire: IT Governance Publishing.

Hambling, David. 2011. GPS signals now help you call your mother, power your home, and even land your plane. *New Scientist* 209, no. 2803 (March): 44-47. *Academic Search Complete* EBSCO*host* (accessed April 29, 2014).

Headquarters, U.S. Marine Corps (HQMC). 1997. Marine Corps Doctrinal Publication 1, *Warfighting*. http://www.marines.mil/Portals/59/Publications/MCDP%201%20Warfighting.pdf (accessed January 10, 2014).

———. 2004. Marine Corps Warfighting Publication 2-22, *Signals Intelligence*. http://www.marines.mil/Portals/59/Publications/MCWP%202-22%20Signals%20Intelligence.pdf (accessed April 29, 2014).

———. 2010. *Marine Corps operating concept: Assuring littoral access…proven crisis response, third ed.* Marine Corps Base Quantico. http://www.quantico.usmc.mil/uploads/files/MOC%20July%2013%20update%202010_Final.pdf (accessed January 27, 2014).

———. 2012. *Expeditionary warrior 2012 final report*. Washington, DC. http://www.mcwl.marines.mil/Portals/34/Documents/EW13%20Final%20Report_FINAL.pdf (accessed March 15, 2014).

———. 2013. *USMC concepts and programs 2013*. The Official Website of the U.S. Marine Corps. http://www.hqmc.marines.mil/pandr/ConceptsandPrograms/ConceptsandPrograms2013.aspx (accessed October 3, 2013).

———. 2014. *Marine Corps communication playbook.* Washington, DC. April 16.

Isely, Jeter A., and Philip A. Crowl. 1951. *The U.S. marines and amphibious war: Its theory, and its practice in the pacific*. Princeton, NJ: Princeton University Press.

Joint Chiefs of Staff (JCS). 2012. *Capstone concept for joint operations: Joint force 2020*. Washington, DC: US Government Printing Office. http://www.dtic.mil/futurejointwarfare/concepts/ccjo_2012.pdf (accessed October 3, 2013).

———. 2014. Joint Publication 1-02, *Department of Defense dictionary of military and associated terms*. Washington, DC: US Government Printing Office.

Karas, Thomas H., M. Callaham, R. DalBello, and G. Epstein. 1995. *Anti-satellite weapons, countermeasures, and arms control*. Washington, DC: Office of Technology Assessment.

Krepinevich, Andrew F. 2010. *Why airsea battle?*. Washington, DC: Center for Strategic and Budgetary Assessments.

Krepinevich, Andrew F., Barry Watts, and Robert Work. 2003. *Meeting the anti-access and area-denial challenge*. Washington, DC: Center for Strategic and Budgetary Assessments.

Kruger, Martin. 2012. *Persistent intelligence, surveillance and reconnaissance*. Arlington, VA: Office of Naval Research.

Libicki, Martin C. 2011. *Chinese use of cyberwar as an anti-access strategy*. Santa Monica, CA: RAND Corporation. http://www.uscc.gov/sites/default/files/1.27.11Libicki.pdf (accessed February 12, 2014).

Melchior, P. M. 2013. *Warfighting/strategic communications: Cyber strategy*. Quantico, VA: Marine Corps University Command and Staff College.

Millett, Allan R. 1996. Assault from the sea: The development of amphibious warfare between the years-the American, British, and Japanese experiences. In Mi*litary innovation in the interwar period*, ed. Williamson Murray and Allan R. Millett, 50-95. Cambridge: Cambridge University Press.

Murray, Williamson. 1996. Innovation: Past and future. In *Military innovation in the interwar period*, ed. Williamson Murray and Allan R. Millett, 300-329. Cambridge: Cambridge University Press.

Parsons, Dan. 2013. Simple, inexpensive jammers threaten GPS. *National Defense Magazine* 98, no. 718 (September): 10. http://search.proquest.com/docview/1441429245 (accessed March 7, 2014).

Paul, Christopher, Harry J. Thie, and Katharine Watkins Webb. 2011. *Alert and ready: An organizational design assessment of marine corps intelligence*. Santa Monica, CA: RAND Corporation.

Price, Alfred. 2001. *War in the fourth dimension: U.S. electronic warfare, from Vietnam to the present*. Mechanicsburg, PA: Stackpole Books.

Saunders, Phillip C., and Charles D. Lutes. 2007. China's ASAT test: Motivations and implications. *Joint Forces Quarterly* 46 (3rd quarter): 39-45.

Shaping the single naval battle: Bold alligator 2013 and the way ahead. 2013. *Second Line of Defense* (June). http://www.sldinfo.com/wp-content/uploads/2013/06/Bold-Alligator-2013-Special-Report.pdf (accessed March 15, 2014).

Shaw Jr., Henry I. 1992. *First offensive: The marine campaign for Guadalcanal*. Washington, DC: United States Marine Corps History and Museums Division. http://babel.hathitrust.org/cgi/pt?id=mdp.39015020745652#view=1up;seq=1 (accessed March 18, 2014).

Strange, Joseph L., and Richard Iron. 2004. Center of gravity: Part II The CG-CC-CR-CV construct: A useful tool to understand and analyze the relationship between centers of gravity and their critical vulnerabilities. The Air University. http://www.au.af.mil/au/awc/awcgate/usmc/cog2.pdf (accessed April 15, 2014).

Tangredi, Sam J. 2013. *Anti-access warfare: Countering A2/AD strategies*. Annapolis, MD: Naval Institute Press.

Tornga, Blake J. 2008. U.S. military operations within the electromagnetic spectrum: Operational critical weakness?. Master's thesis, Naval War College, Newport, RI. http://www.dtic.mil/docs/citations/ADA484326 (accessed March 3, 2014).

U.S. Congress. House. House Armed Services Subcommittee on Emerging Threats and Capabilities. 2012. *Department of Defense FY2013 Science and Technology Programs*. 112th Cong., 2nd sess., February 29.

———. 2014. U.S.-China Economic and Security Review Commission. *Hearing on China's Military Modernization and its Implications for the United States*. 113th Cong., 2nd sess., January 30.

U.S. Department of Defense (DOD). 2011. *Unmanned systems integrated roadmap FY2011-2036*. http://www.defenseinnovationmarketplace.mil/resources/UnmannedSystemsIntegratedRoadmapFY2011.pdf (accessed March 3, 2014).

———. 2012a. *Joint operational access concept, Version 1.0*. http://www.defense.gov/pubs/pdfs/JOAC_Jan%202012_Signed.pdf (accessed January 14, 2014).

———. 2012b. *Sustaining U.S. global leadership: Priorities for 21st century defense*. Washington, DC: US Government Printing Office.

———. 2013. *Air-sea battle: Service collaboration to address anti-access and area denial challenges*. Washington, DC: Air-Sea Battle Office. http://www.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf (accessed January 15, 2014).

U.S. President. 2010. *National security strategy*. Washington, DC: US Government Printing Office.

Wilgenbusch, Ronald C., and Alan Heisig. 2013. Command and control vulnerabilities to communications jamming. *Joint Forces Quarterly* no. 69 (April): 56-63. http://search.proquest.com/docview/1429689573 (accessed March 7, 2014).