### ABSTRACT

Imagine a large "red bubble" extending beyond the shores of the People's Republic of China with the purpose of deterring any kind of intrusion from outside the region. This paper discusses BMD as a counter to anti-access -- the longer range operational threat. In that regard, imagine IAMD as a "blue bubble" under which a friendly force may operate. A bubble inside a bubble. Decisive operational access provided, in part, by IAMD permits freedom of action to achieve strategic objectives within an A2/AD threat environment. To that end, a comprehensive ballistic missile defense system that communicates through a common architecture, uses command by negation, and pushes the engagement envelope, is essential to air and maritime superiority and therefore critical to operational access.

### SUBJECT TERMS

Ballistic Missile Defense System (BMDS); Integrated Air and Missile Defense (IAMD); PRC; China; anti-access; area-denial; Pacific; Joint Operational Access
1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g., 30-06-1998; xx-08-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F338515-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. 1F665702D1257.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. AFOSR-82-1234.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSOR/MONITOR'S ACRONYM(S). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

Standard Form 298 (Rev. 8-98) Prescribed by ANSI-Std Z38-18
TITLE:
The Ancile of Mars: Establishing Operational Access with Ballistic Missile Defense

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES

AUTHOR:
LIEUTENANT COMMANDER ADAM D. WIEDER, UNITED STATES NAVY

AY 12-13

Mentor: Wray R. Johnson, Ph.D
Approved: [Signature]
Date: [Signature]
DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.
Introduction

Imagine a large “red bubble” extending beyond the shores of the People’s Republic of China with the purpose of deterring any kind of intrusion from outside the region. In the next ten to fifteen years China will possess a fully developed Anti-Access / Area-Denial (A2/AD) capability. On the other hand, the United States will seek to expand its influence in the region. To counter Chinese A2/AD capabilities, U.S. and regional allies continue to develop an Integrated Air and Missile Defense (IAMD) capability, combining traditional air defense against aircraft and missiles alongside ballistic missile defense (BMD). This paper will limit the discussion to aspects of BMD as a counter to anti-access—the longer range operational threat. In that regard, imagine IAMD as a “blue bubble” under which a friendly force may operate.

Decisive operational access provided, in part, by IAMD permits freedom of action to achieve strategic objectives within an A2/AD threat environment. To that end, a comprehensive ballistic missile defense system that communicates through a common architecture, uses command by negation, and pushes the engagement envelope, is essential to air and maritime superiority and therefore critical to operational access.

Definitions

For purposes of clarity and consistency, we must define several important terms that either do not appear in the JP 1-02 joint dictionary or vary in definition between sources. Below are the definitions as they will be used in this paper:

*Anti-Access (A2):* Actions, both political and operational, to prevent forces from deploying to the theater, limit operations within the theater, or compel friendly forces to
operate away from the locus of conflict than desired. In general, anti-access refers to long-range threats.

*Area-Denial (AD)*: “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.”

*Operational Access*: “The ability to project military force into an operational area with sufficient freedom of action to accomplish the mission.” In a strategic context, “operational access is the joint force contribution to assured access, the unhindered national use of the global commons and select sovereign territory, waters, airspace and cyberspace.”

**Geo-Strategic Implications of Operational Access (Ends)**

The recent U.S. “pivot to the Pacific” highlights the strategic importance of maintaining security and stability in the Western Pacific. Reconciling this political objective with prospective means and circumstances requires joint operational access. Operational access depends on in-theater basing and projection of maritime forces. Basing will require friends and allies in the region, including Australia, Japan, the Republic of Korea, and the Republic of the Philippines. Securing other allies and partner nations will be equally important, enabling our ability to forward-base military forces. Such bases would be most likely threatened by short to medium range ballistic missiles.

Also critical to operational access are the network of bases and facilities within the U.S. and its territories. Two prime examples are the bases in Hawaii and Guam. Both are beyond the
First Island Chain (see appendix A) of the Western Pacific but well within the range of medium
to intermediate range ballistic missiles.

Finally, operational access depends on the power projection of maritime forces. For the U.S., Naval Carrier and Expeditionary Strike Groups, represent the centerpiece of coercive diplomacy in their ability to provide power projection and sea control wherever required. Alliances with regional maritime and military forces will strengthen this capability. Burgeoning technology now presents a threat to these strike groups in the form of a family of anti-ship ballistic missiles (ASBMs).

Anti-Access Threat (Circumstances)

The People’s Republic of China continues to assert itself on the world stage, gaining influence globally and especially consolidating its position in the Western Pacific. The Chinese insist on “historical” rights over most of the waters within the First Island Chain adjacent mainland East Asia. They therefore seek the political and military freedom to influence states in the region through a collection of bilateral agreements. Backing up these agreements, the People’s Liberation Army (PLA) has deployed a range of anti-access systems, aircraft, and other weapons. It is the PLA that maintains the red bubble. Sensors such as the over-the-horizon (OTH) radar located in central China provide both air and maritime situational awareness (see appendix B). Analysts believe that the OTH radar provides cueing for ASBM systems. Indeed, China’s Second Artillery Corps maintains one of the largest ballistic missile inventories in the world, and while the primary emphasis is mobile short and theater range systems, China does possess a nuclear inter-continental ballistic missile (ICBM) capability.
In the next ten to fifteen years, China will develop new technologies, including maneuverable re-entry vehicles and decoys. China will also acquire the ability to engage a moving target at sea employing short and medium range ASBM systems. Given this arsenal, China will be able to attack targets from their coastline out to 5,500 kilometers with some 1,300 missiles. While this represents a significant capability, A2/AD weapons and sensors do not provide perfect coverage. China cannot maintain the red bubble 100 percent of the time across 100 percent of its intended coverage. This leaves open an opportunity for exploitation.

**Ballistic Missile Defense System (Means)**

As it evolves over the next ten to fifteen years, BMD will present the primary means to exploit gaps in an anti-access environment. According to the U.S. Missile Defense Agency (MDA), BMD is “an integrated, ‘layered’ architecture that provides multiple opportunities to destroy missiles and their warheads before they can reach their targets.” BMD has three primary components: sensors, defensive engagement capabilities, and a command and control system. Sensor systems within the Ballistic Missile Defense System (BMDS) include space-based, fixed, mobile, and sea-based capabilities. When placed in a threat region, these sensors detect, localize, and track ballistic missiles. Tracking information cues the defensive engagement capabilities, which are further subdivided into three components. Each component corresponds to the phases of ballistic missile flight: boost, midcourse, and terminal. Working backward, defeating the terminal phase includes the proven Patriot Advanced Capability-3 (PAC-3) anti-missile system, the Navy’s Sea-Based Terminal (SM-T) system, and the emergent Terminal High Altitude Area Defense (THAAD) system. Due to the height at which most ballistic missiles travel during the midcourse phase there are fewer engagement systems and, presently, only one that significantly
facilitates operational access. The U.S. Air Force’s Ground-Based Midcourse Defense (GMD) system consists of fixed sites protecting the U.S. homeland from intermediate and long-range ballistic missile threats. The system does not, however, provide much capability for an overseas fight. Another midcourse engagement system that will be updated within the next ten to fifteen years is the Aegis Ballistic Missile Defense Standard Missile-3 (SM-3). The Aegis Ballistic Missile Defense System, hereafter referred to as Aegis system, resides on U.S. Navy ARLEIGH BURKE-class destroyers as well as TICONDEROGA-class cruisers. Equipped with the SPY-1 phased-array radar, these ships possess the capability to individually detect, localize, track, and destroy ballistic missiles. Based on their inherent mobility and flexibility, the Aegis systems would form the core of the operational commander’s bid to gain operational access. To counter the boost and ascent phase, only the Aegis system is capable of engagement; however, the U.S. continues to develop new technologies that show promise. Probable solutions include using “unmanned aerial vehicles (UAVs) and space assets for pervasive over-the-horizon sensor netting” to extend the SM-3 engagement zone to “the pre-apogee portion of a [ballistic] missile’s trajectory.” Finally, the overarching segment of BMDS is the Command, Control, Battle Management, and Communications (C2BMC) program. C2BMC enables national decision-makers and commanders at the operational levels to plan, monitor, and manage BMDS sensors and weapons systems.

In the near future, these capabilities will continue to expand. In 2009, President Obama released the U.S. Missile Defense Policy entitled a “Phased, Adaptive Approach” for Missile Defense in Europe. The policy outlines four phases of technology and capability advances, with each successive phase achieving greater range and countermeasures against long-range missiles.
“In the 2020 timeframe...[the Department of Defense will] deploy the SM-3 Block IIB to help better cope with medium-and intermediate-range missiles.” In addition, there will be advances in communication and network capacity that enable greater fidelity and integration both within and between tactical and operational data networks. By the end of the next decade, new systems will be able to track, among others, the Chinese DF-21D anti-ship ballistic missile. Some new weapons systems may come from our allies such as Japan or Australia. Nonetheless, the means by which a commander may achieve operational access will rely on the BMDS in use today.

Creating the “Blue Bubble” (Ways)

In achieving operational access with the means described above, the operational commander will integrate anti-submarine warfare (ASW), cyber warfare, information operations(IO), and IAMD, but BMD will be a crucial enabler. The ability to enter an adversary’s A2/AD bubble enhances the capabilities that can be brought to bear against the enemy. As joint and combined forces create and exploit gaps in the red bubble, BMDS forces will lead the way. BMDS sensors and shooters will gain efficiencies by engaging enemy missiles in the boost / ascent phase. This will expand the coverage of the blue bubble. For example, an Aegis-equipped ship in the East China Sea may be able to defend effectively not only bases in Okinawa but those on the main islands of Japan and even Hawaii. Pushing BMDS assets deeper into the operational area reduces risk to joint and combined forces. Once forces penetrate the red bubble of anti-access to create the blue bubble of operational access, follow-on forces will be able to expand the friendly bubble through IAMD, ASW, IO, etc.

Nevertheless, building air and maritime superiority in an A2/AD environment will present challenges. The phased adaptive approach described earlier may keep U.S. ballistic
missile defense technology on the leading edge and, more importantly, ahead of threat ballistic missile capability, but for now and in the near future there will remain a capability gap. Currently, the PLA fields more ballistic missiles than joint and combined interceptors can handle. So, just like A2/AD systems in the red bubble, state-of-the-art BMDS does not convey a perfect blue bubble (i.e., 100% coverage over 100% of the operational area). The operational commander must still understand the adversary’s strengths and weaknesses, develop an effective plan, and in doing so select where and when to deploy operational access systems within the anti-access bubble. Forethought and design are essential for successful execution at the operational level.

So What? -- Missile Defense Design

The importance of missile defense in achieving operational access requires attention now. Specifically, the U.S. ballistic missile defense system needs a grand design that will guide spending, development of new technologies, and training. The BMDS “grand design” must evolve according to three guiding principles: 1) the BMDS must have a common architecture; 2) it must use the “command by negation” concept; and 3) BMDS technology must persistently advance in capability.

A comprehensive BMD system of the future must have a common architecture across all joint and combined missile defense forces. This common architecture must include integrating technology and common operating concepts in the form of doctrine. While each organization will develop its own contributions to missile defense, there must be standardized integrating technology that permits seamless sharing of information and, when required, engagement hand-over. This should be handled through information networks and communications. A good
example of this type of integrating technologies is the Joint Tactical Information Distribution System (JTIDS)/Multifunctional Information Distribution (MIDS) Link 16 system. JTIDS connects all participating joint and allied forces in “a digital information sharing system for tactical interoperability and situation awareness.” A similar integration system, or the expansion of an existing system, would allow for near-real time data sharing and enhanced engagement cueing.

BMDS must also include a common doctrine. Just like a professional sports team requires a playbook, BMDS units require common operating and communication procedures to ensure unity of effort and reduce inefficiencies. Once the joint IAMD community approves the standardized doctrine, each unit must train to the standard.

Command and control (C2) of a multilayer BMD system requires a not only responsive architecture, but also a comprehensive concept; that is, BMDS must use “command by negation.” Command by negation involves centralized planning and decentralized execution. Specifically, a subordinate commander reports his or her intention to take action within higher commander’s intent. The same subordinate commander may then proceed with that action unless the higher headquarters disallows it. This concept “permit[s] component and functional commanders to react effectively even [within] extremely compressed timelines.” The speed of ballistic missiles provides only fleeting opportunity for successful engagement. A tactical commander must often make decisions in an instant or risk failing to engage the threatening ballistic missile.

Another crucial factor for the commander to consider is rules of engagement. They must be clear and understood by all. Recent Taepo-Dong 2 launches from North Korea come to mind.
Does the operational commander shoot down a potential space vehicle just because its failing trajectory looks like a ballistic missile? Command by negation gives the concerned commander the option to accept risk to shoot down the missile or not. Retired Vice Admiral J.D. Williams, one-time Combatant Commander and Deputy Chief of Naval Operations for Naval Warfare, pushed for command by negation in relation to BMD: “Command by negation,” he noted, “will allow the chain of command to adapt to a particular situation in accordance with the supported commander’s stated objectives.”

However, command decision-making is only part of the equation. Another challenge lies in communicating decisions. C2BMC is a good beginning but it is only as adequate as the command, control communications, and intelligence (C3I) networks employed. “A truly effective command and control system... for the long term depends on obtaining a survivable and redundant C3I network that gives the commander flexibility to organize and employ assigned forces in a manner suitable to the operation.” BMDS requires both C3I improvements and command doctrine improvements.

Finally, development of a comprehensive BMDS must constantly push the engagement envelope. Threat characteristics will continue to evolve as new technologies arise. BMD research and development must either keep pace or outpace threat technologies. As discussed earlier, there are defensive efficiencies in developing an earlier engagement capability. BMDS technologies must improve to exploit these efficiencies. In September 2011 the DoD Defense Science Board submitted a report on the feasibility of early intercepts. They found that “it is the forward basing of interceptor assets and high interceptor speeds that facilitate large defended areas.” All of the above entails improved sensors and sensor-to-weapon networks.
The key to successful employment of early engagement hinges on operational access—getting the sensor and BMD shooter closer to the launch point. If an operational commander can exploit technological advantages and anti-access gaps, then there is an opportunity to create the blue bubble. Pushing BMD assets underneath that bubble deeper into the enemy’s anti-access bubble will gain further defensive efficiencies for attacking forces as well as bases further back in the battle space. In essence, a small technological advantage properly exploited will turn the anti-access problem into an access problem for the adversary.

Conclusion

In the next ten to fifteen years, ballistic missile defense will enable decisive operational access and provide the operational commander with the capability to achieve mission success despite the A2/AD threat. Although this paper highlights the importance of BMD, a comprehensive BMDS in and of itself is not the complete solution. Nevertheless, while it may not be the “silver bullet” or “assassin’s mace”, a future force will not gain operational access without BMD. In the 21st Century, BMD must be part of the larger joint and combined arsenal that includes IAMD, anti-submarine warfare, cyber warfare, information operations, etc. All of these capabilities will aid the operational commander in gaining operational access. At the time of this writing, China represents the most capable adversary employing A2/AD assets. That said, the concepts discussed here apply to other potential adversaries, such as North Korea and Iran. In the end, BMD is no longer merely an enabling feature of warfighting but arguably the key feature in gaining operational access.


5 Although this paper addresses the Chinese A2/AD threat, several other nations (e.g. Iran or North Korea) develop and maintain their own A2/AD capabilities.


16 J.D. Williams, 2.

17 J.D. Williams, 5.


Appendix B - Over-The-Horizon Radar Coverage

Bibliography


