DEFENDING THE FLEET FROM CHINA’S ANTI-SHIP BALLISTIC MISSILE: 
NAVAL DECEPTION’S ROLES IN SEA-BASED MISSILE DEFENSE

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Security Studies

By

Jonathan F. Solomon, B.A.

Washington, DC
April 15, 2011
DEFENDING THE FLEET FROM CHINA’S ANTI-SHIP BALLISTIC MISSILE: NAVAL DECEPTION’S ROLES IN SEA-BASED MISSILE DEFENSE

Jonathan F. Solomon, B.A.

Thesis Advisor: Dr. Karl Mueller, Ph.D.

ABSTRACT

This thesis project tests the hypothesis that U.S. Navy active missile defenses’ utility against China’s Anti-Ship Ballistic Missile (ASBM) reconnaissance-strike system can be significantly increased when paired with emerging Electronic Warfare (EW) technologies and novel tactical deception concepts. Qualitative open source-based technical, tactical, and doctrinal analyses of China’s ocean surveillance, reconnaissance, and ASBM strike systems are conducted to outline their likely capabilities and limitations. Qualitative process-tracing is next used within a historical case study of how the U.S. Navy employed EW and tactical deception during the Cold War to defend aircraft carrier battle groups against Soviet ocean surveillance, reconnaissance, and strike systems. The case study’s data and conclusions are then used to qualitatively infer the ASBM concept’s inherent technical, tactical, and doctrinal vulnerabilities. Following this, emerging EW technologies are identified that have the theoretical potential to exploit Chinese radars, electro-optical and infrared sensors, radiofrequency direction-finding/Electronic Intelligence (ELINT) systems, satellite communication networks, and decision-making systems. EW’s theoretical influence on a naval surface force’s active missile defenses’ effectiveness against ASBMs is also qualitatively assessed. The case study’s conclusions and the analysis of emerging EW technologies are additionally used to derive potential U.S. Navy tactical deception concepts as well as recognize the prerequisites for their effective use. Lastly, EW and tactical deception’s implications for U.S. maritime strategy and conventional deterrence against Chinese aggression in East Asia are assessed.
This thesis is dedicated to my wife Tracy, who not only put up with my obsessive research and writing efforts during winter and spring 2011 but also graciously contributed her considerable professional editing and formatting skills to helping me with this project.

With deepest love and appreciation,

J. F. Solomon
Table of Contents

Introduction.................................................................................................................................................. 1

Section I: The Operational-Strategic Environment in East Asia................................................................. 6

Section II: The Chinese Ocean Surveillance System .................................................................................. 11

Section III: The ASBM Strike System...................................................................................................... 21


Section V: Assessing the Chinese Ocean Surveillance and ASBM Reconnaissance-Strike Systems ...... 69

Section VI: Promising EW Technologies and Techniques for ASBM Defense ...................................... 79

Section VII: Anti-ASBM EW Implementation Concepts for the U.S. Navy............................................. 107

Conclusion: Implications for U.S. Conventional Deterrence in East Asia ........................................... 126

Bibliography ............................................................................................................................................ 138
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEW</td>
<td>Airborne Early Warning</td>
</tr>
<tr>
<td>AGI</td>
<td>Auxiliary intelligence-gathering ship</td>
</tr>
<tr>
<td>AOU</td>
<td>Area of Uncertainty</td>
</tr>
<tr>
<td>ASBM</td>
<td>Anti-Ship Ballistic Missile</td>
</tr>
<tr>
<td>ASW</td>
<td>Anti-Submarine Warfare</td>
</tr>
<tr>
<td>CAP</td>
<td>Combat Air Patrol</td>
</tr>
<tr>
<td>CCP</td>
<td>Chinese Communist Party</td>
</tr>
<tr>
<td>COSS</td>
<td>Chinese Ocean Surveillance System</td>
</tr>
<tr>
<td>DRFM</td>
<td>Digital Radiofrequency Memory</td>
</tr>
<tr>
<td>ELINT</td>
<td>Electronic Intelligence</td>
</tr>
<tr>
<td>EMCON</td>
<td>Emissions Control</td>
</tr>
<tr>
<td>EORSAT</td>
<td>Electronic Intelligence Ocean Reconnaissance Satellite</td>
</tr>
<tr>
<td>EW</td>
<td>Electronic Warfare</td>
</tr>
<tr>
<td>FLTCORGRU</td>
<td>Fleet Composite Operational Readiness Groups</td>
</tr>
<tr>
<td>FLTDECGRU</td>
<td>Fleet Deception Group</td>
</tr>
<tr>
<td>HALE</td>
<td>High Altitude Long Endurance</td>
</tr>
<tr>
<td>HF</td>
<td>High Frequency</td>
</tr>
<tr>
<td>HULTEC</td>
<td>Hull to Emitter Correlation</td>
</tr>
<tr>
<td>HVU</td>
<td>High Value Unit</td>
</tr>
<tr>
<td>ICADS</td>
<td>Integrated Cover and Deception System</td>
</tr>
<tr>
<td>ISAR</td>
<td>Inverse Synthetic Aperture Radar</td>
</tr>
<tr>
<td>LCS</td>
<td>Littoral Combat Ship</td>
</tr>
<tr>
<td>MRBM</td>
<td>Medium Range Ballistic Missile</td>
</tr>
<tr>
<td>NGJ</td>
<td>Next Generation Jammer</td>
</tr>
<tr>
<td>NIE</td>
<td>National Intelligence Estimate</td>
</tr>
<tr>
<td>ONR</td>
<td>Office of Naval Research</td>
</tr>
<tr>
<td>OTH-B</td>
<td>Over the Horizon-Backscatter</td>
</tr>
<tr>
<td>PLA</td>
<td>People’s Liberation Army</td>
</tr>
<tr>
<td>QDR</td>
<td>Quadrennial Defense Review</td>
</tr>
<tr>
<td>RF</td>
<td>Radiofrequency</td>
</tr>
<tr>
<td>RGPI</td>
<td>Range Gate Pull In</td>
</tr>
<tr>
<td>RGPO</td>
<td>Range Gate Pull Off</td>
</tr>
<tr>
<td>RORSAT</td>
<td>Radar Ocean Reconnaissance Satellite</td>
</tr>
<tr>
<td>SAR</td>
<td>Synthetic Aperture Radar</td>
</tr>
<tr>
<td>SEI</td>
<td>Specific Emitter Identification</td>
</tr>
<tr>
<td>SEWIP</td>
<td>Surface Electronic Warfare Improvement Program</td>
</tr>
<tr>
<td>SOSS</td>
<td>Soviet Ocean Surveillance System</td>
</tr>
<tr>
<td>SRBM</td>
<td>Short Range Ballistic Missile</td>
</tr>
<tr>
<td>TEL</td>
<td>Transportable Erectable Launcher</td>
</tr>
<tr>
<td>UAV</td>
<td>Unmanned Aerial Vehicle</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra-High Frequency</td>
</tr>
<tr>
<td>USV</td>
<td>Unmanned Surface Vehicle</td>
</tr>
<tr>
<td>VHF</td>
<td>Very-High Frequency</td>
</tr>
</tbody>
</table>
Introduction

On 28 December 2010, Admiral Robert Willard, commander of U.S. Pacific Command, startled the international defense analysis community with his public judgment that China had fielded a ballistic missile capable of striking a moving ship over a thousand miles out to sea.\(^1\) Up until his announcement, China’s Anti-Ship Ballistic Missile (ASBM) development program was widely considered a hypothetical effort of uncertain technological maturity.\(^2\) The earliest open source reports in the West regarding China’s ASBM development efforts, in fact, only date back to 2005. Admiral Willard’s announcement represented formal U.S. recognition that China possessed the world’s first operationally-deployed ASBM.\(^3\)

Countering the ASBM is of the greatest importance to U.S. grand strategy for defending American interests in East Asia. Although many in the security studies community point to the Taiwanese sovereignty question as the primary Sino-American fault line in East Asia, it is hardly the only one applicable within the ASBM’s context. China’s recent diplomatic and military provocations aimed at supporting its sovereignty claims over various maritime areas in the East and South China Seas, not to mention Beijing’s continued backing of the North Korean regime, also serve as major sources of East Asian strategic instability. China’s political and military leaders openly profess that conventionally-armed ballistic missiles in general and ASBMs in particular can play decisive roles in blunting America’s military ability and political willingness

---

\(^1\) Kato, “U.S. Commander Says China Aims to be a ‘Global Military’ Power.” Distance measurements in this paper will primarily be in miles in order to aid with visualization. Most military technical analyses of ballistic missile capabilities tend to be in kilometers, however.

\(^2\) In this paper, the term ASBM generally refers to both the current \textit{DF-21D} anti-ship ballistic missile and any notional follow-on Chinese medium or intermediate range anti-ship ballistic missile. A note is made in the text any time that the term is applied solely in the context of the \textit{DF-21D}.

\(^3\) As will be discussed in Section IV, the Soviet Union developed the world’s first ASBM during the early 1970s but never operationally deployed it. See Polmar, “Antiship Ballistic Missiles... Again,” 86-87. Polmar’s article also appears to be the first to mention China’s ASBM development efforts in the English language naval analysis literature.
to intervene in East Asian crises. Indeed, America’s ability to prevent potential Chinese military
faits accompli and reinforce allies and partners in the region relies heavily upon use of the
Western Pacific. Persuading East Asian allies and partners that the ASBM is not a ‘showstopper’
therefore emerges as an important U.S. prerequisite for sustaining strategic influence within the
region. Furthermore, future U.S. conventional deterrence credibility in East Asia will rely in part
on convincing Chinese leaders that their faith in the ASBM’s operational-strategic decisiveness,
never mind tactical utility, may be seriously misguided.

The majority of scholarly articles and monographs addressing this topic focus their
analysis on U.S. Navy active missile defenses’ probable effectiveness against the ASBM and/or
the ASBM’s overall operational-strategic implications in East Asia.\(^4\) A few other researchers
have investigated whether development of longer-ranged strike systems would allow the U.S.
Navy to conduct effective land-attack operations from outside ASBM range.\(^5\) In contrast, ‘non-

\(^4\) The definitive works include: 1. Erickson and Yang, “Using the Land to Control the Sea: Chinese Analysts
Hagt and Durnin, “China’s Antiship Ballistic Missile: Developments and Missing Links.”
\(^5\) See 1. Ehrhard and Work, “Range, Persistence, Stealth, and Networking: The Case for a Carrier-Based Unmanned
Combat Air System;” 2. Hooper and Albon, “Get Off the Fainting Couch.” These other researchers recommend
development of offensive systems such as submarine-launched conventionally-armed intermediate range ballistic
missiles or carrier-based armed unmanned aerial vehicles (UAV). Both of these concepts have merit and could
provide needed operational capabilities as well as military-strategic utility. However, neither concept acknowledges
the fact that at least some U.S. Navy surface forces will likely need to operate within ASBM range during notional
crises and/or a notional war’s early phases. For example, at least a few U.S. Navy large surface combatants will
likely be operating in Ballistic Missile Defense (BMD) patrol stations within the Sea of Japan and near the Ryukyu
Islands at the time of any Chinese surprise first ASBM salvo. Similarly, it is highly likely that U.S. East Asian
conventional deterrence strategy will require that the Navy’s permanently Japan-homeported aircraft carrier and
escorts operate within the ASBM coverage zone as tensions peak, perhaps as a deliberate ‘trip wire’ force. U.S. East
Asian contingency plans for the first few weeks and/or months of a notional war will also likely require that surface
forces be used to restore U.S. control over selected regional sea lines of communication, resupply and reinforce U.S.
and allied theater forces via trans-oceanic convoys, and possibly even conduct amphibious operations—all within
Western Pacific areas likely to still be somewhat-effectively covered by ASBMs. While U.S. long-range land and
sea-based counterstrikes will play a major role in physically neutralizing the PLA’s ASBM targeting capabilities,
U.S. campaign requirements and the overall strategic situation probably will not grant Navy surface forces the
luxury of waiting for anti-ASBM operations to be completed before they must venture into contested waters. It is
important to note that although long-range strikes play critical roles in denying an enemy’s access to a given area as
well as in helping other friendly forces obtain control of an area, they cannot assert control over an area on their
own. Control of physical space at a given moment in time requires a physical presence. This is why active missile
defenses and non-kinetic countermeasures such as electronic warfare and tactical deception are necessary even if
kinetic’ countermeasures are barely examined in the ASBM literature. This paper strives to fill the research gap by investigating how Electronic Warfare (EW) and tactical deception can be employed alongside U.S. Navy battleforces’ active missile defenses to mitigate the emerging Chinese ASBM threat.

In order to establish our strategic framework, Section I provides a brief overview of Chinese political objectives and military doctrine for notional operations in East Asia. Sections II and III follow by technically and tactically analyzing China’s nascent ocean surveillance and ASBM reconnaissance-strike systems in order to gauge the threats they pose as well as identify their potential inherent vulnerabilities to EW and tactical deception.

---

6 The only major works to touch on non-kinetics in any meaningful way are: 1. Culora, “The Strategic Implications of Obscurants: History and the Future;” 2. Hoyler, “China’s Anti-Access Ballistic Missiles and U.S. Active Defense;” 3. Tangredi, “No Game-Changer for China.” All three articles focus their attention on strategic and operational-level issues; none systematically examine the ASBM concept’s theoretical vulnerabilities, investigate EW technologies, or propose deceptive tactical concepts as this paper aims to do.

7 Some definitions for terminology used within this paper: 1. An active missile defense is one that uses BMD interceptor missiles to engage threat ballistic missiles and/or their separating warheads. The U.S. Navy’s active missile defenses are provided by the Aegis BMD system and its Standard Missile (SM)-3 BMD interceptors. 2. Passive missile defenses include warship armor and other damage mitigation measures, dispersed formations, use of EW, and use of deception. 3. A naval battleforce is a group of warships, ship and shore-based maritime aircraft, submarines, unmanned vehicles, and/or logistical support ships under the tactical control of a single commander. Common examples include aircraft carrier strike groups, amphibious ready groups, surface combatant action groups, maritime BMD groups, or various other types of task groups. Surface forces serve as the inherent core of any major battleforce. The term ‘battleforce-level’ describes the tactics, capabilities, operating concepts, and other considerations applicable to operating a naval group as an integrated whole.

8 Some definitions: 1. Surveillance is the act of continuously monitoring the activities within a given area. A ‘ocean surveillance system’ is a networked ‘system of systems’ that fuses data from dispersed surveillance sensors, then uses this data to cue reconnaissance-strike systems. 2. Reconnaissance represents the use of scouts to precisely locate and identify an adversary force, then relay this targeting data to friendly strike units. The line between surveillance and reconnaissance can be blurry in practice, particularly given the advanced capabilities of contemporary sensors and data networks. 3. A ‘reconnaissance-strike complex’ is a Soviet term for a “fully integrated and highly automated system capable of delivering powerful strikes simultaneously against several targets.” In this system of systems, dispersed reconnaissance sensors provide cueing and/or targeting data to dispersed weapons-firing units via a central command and control network. The term was uncritically adopted by the U.S. defense analysis community after the Cold War as a practical example of ‘revolution in military affairs’ theory and the ‘network-centric warfare’ concept. It is more accurate to refer to it as a reconnaissance-strike system. For more information on how maritime reconnaissance-strike systems fit into Soviet naval theory, see Vego, Soviet Naval Tactics, 257-258.
Section IV builds on this analysis by examining the Cold War’s iterative technical and tactical competition between the Soviet Union’s ocean surveillance and reconnaissance-strike systems on one side and the U.S. Navy’s battleforce defenses on the other. This Cold War case marks the only modern historical example of a long-range, predominantly land-based, and theater-wide maritime strike capability being challenged by naval EW and tactical deception. As this competition consisted of multiple moves and countermoves over the course of three decades, it offers numerous insights regarding how a similar competition might unfold between China’s ASBM concept and U.S. Navy battleforce defenses. Section V validates this observation by using comparative analysis to demonstrate that China’s ASBM capabilities are vulnerable to the same EW and tactical deception principles that governed the Cold War case study’s competition.

Section VI identifies emerging EW technologies that appear applicable against China’s maritime surveillance, reconnaissance, and ASBM strike systems. This technical analysis is complicated by the fact that Chinese sensors’ actual designs and capabilities are obviously not available in the open literature. Nevertheless, since the basic physical principles by which these sensors work are widely understood, it is possible to point out general vulnerabilities and the EW technologies that can exploit them while deferring analysis of specific potentially-applicable EW techniques to the classified realm.

Section VII uses this technical analysis to help interpret existing unclassified information about U.S. Navy EW capability development efforts as well as to propose additional near and intermediate-term countermeasures that could be used for ASBM defense and tactical deception. The Cold War case study’s principles are then applied to suggest how these EW and tactical deception capabilities could support U.S. Navy operations in a notional East Asian war. Some important caveats are also examined in order to highlight the operational and policy prerequisites
for effective use of EW and tactical deception. A concluding section examines anti-ASBM EW and tactical deception’s implications for the maritime component of U.S. conventional deterrence in East Asia.

This paper’s analysis qualitatively tests the hypothesis that U.S. Navy active missile defenses’ utility against China’s ASBM reconnaissance-strike system can be significantly increased when paired with emerging EW technologies and novel tactical deception concepts. It is important to note the impossibility of proving this hypothesis’s definitive truth using the data presently available in the public domain. Lack of access to classified analysis regarding Chinese maritime surveillance, reconnaissance, and ASBM strike capabilities as well as U.S. sea-based missile defense capabilities precludes absolute certainty in this paper’s conclusions. Also, as much historical data related to the Cold War case remains classified, it is impossible to definitively prove the U.S. Navy achieved sustained successes using EW and deception against Soviet maritime reconnaissance-strike capabilities. Nevertheless, sufficient unclassified data and circumstantial evidence is available to support rigorous, analytically-defensible partial verification of this paper’s hypothesis. As such, this paper fills a major gap in the existing scholarly literature regarding means for countering future ASBM threats.
I. The Operational-Strategic Environment in East Asia

Recent Trends in China’s Relations with its East Asian Neighbors

China’s reemergence as a great power is defined by a central paradox. On one hand, the Chinese Communist Party’s (CCP) ideologically ironic embracement of market capitalism not only helped elevate millions of Chinese citizens out of abject poverty over the past three decades but also established the ‘Middle Kingdom’ as an integral global supplier of raw resources and commercial goods. On the other, the Chinese people’s newfound economic strength has not translated into widespread popular demands for political liberalization, and the CCP’s leaders have at best seemed ambivalent about their willingness to cooperate with other stakeholder countries on resolving regional questions and global challenges.

Nowhere is China’s ambivalence more apparent than in East Asia. As China’s regional clout rapidly expanded over the past ten years, CCP leaders’ ambitions appear to have grown beyond their multi-decade focus on coercing Taiwan’s political reunification with the mainland. A particularly glaring recent example of this trend is China’s reasserting long-dormant sovereignty claims to other islands and waters outside of its internationally recognized territorial seas. Whereas most such disputes only a few years ago were limited to quiet exchanges of diplomatic notes, they are now punctuated by Chinese policy elites’ vociferous nationalist rhetoric, Beijing’s impositions of unilateral trade embargoes, and vigorous demonstrations of Chinese military power projection capabilities. At the same time, CCP leaders have signaled reluctance to negotiate bilaterally and have expressed adamant opposition to multilateral discussions or third-party mediation. These issues, not to mention China’s solidarity with North Korea despite the latter’s continuous nuclear proliferation brinksmanship and unprovoked 2010
military aggression against South Korea, are driving East Asian countries’ advocacy for the U.S. to maintain its strategic balancer role in the region. The region’s future stability hinges on whether an increasingly self-confident China will be willing to restrain some of its elites’ revisionist urges and instead cooperate with its East Asian neighbors and America in addressing major regional issues, or whether CCP leaders actively covet eventual regional hegemony and a corresponding displacement of America’s strategic influence in the Western Pacific.

*China’s Military Strategy, Operational Concepts, and Doctrine for East Asian Contingencies*

Trends in the Chinese People’s Liberation Army’s (PLA) conventional force structure and doctrine over the past 20 years offer little reassurance on this front. Recent PLA modernization efforts are dominated by extensive procurement of advanced tactical aircraft, ‘blue water’ naval forces, and traditional guided munitions such as anti-ship cruise missiles. The PLA, however, is also striving to develop disruptive ‘leap ahead’ armaments technologies that can compensate for the PLA’s qualitative inferiority relative to U.S. forces and systems. The PLA’s already-massive and still rapidly growing arsenal of precision-guided, conventionally-armed Medium Range Ballistic Missiles (MRBM) represents perhaps the most prominent example of this drive for ‘leap ahead’ weapons. The ASBM represents this inclination to an extreme.¹⁰

---

¹⁰ MRBMs are generally defined as ballistic missiles with maximum ranges of no greater than about 3000km (1860 miles). This range-based definition is rather arbitrary and differs from source to source over time, even between U.S. Government documents. Section III contains detailed analysis on the likely size and composition of the PLA’s MRBM arsenal. This arsenal is maintained and operated by the PLA’s Second Artillery Corps, which is a separate PLA service branch that is nominally co-equal with the PLA’s Ground Force, Navy, and Air Force. For simplicity’s sake, though, our analysis will refer to the PLA instead of the Second Artillery Corps when discussing the Chinese ballistic missile arsenal.
As illustrated by Figure 1’s yellow-shaded zone, the PLA ASBM arsenal’s primary purpose is to deter U.S. Navy battleforces from operating within approximately 1240 miles of the Chinese coast during a notional East Asian crisis. This ability to swiftly and massively strike far

---

12 The ASBM’s minimum and maximum effective ranges are currently unknown in the open literature. Like any other ballistic missile, the ASBM will have inherent design limitations that prevent it from striking a target inside some minimum range. As the PLA’s first ASBM appears to be a variant of their DF-21 MRBM, this minimum range is probably no less than a few hundred miles downrange of the launch site. In contrast, there is considerable credible speculation in the open literature regarding this DF-21 ASBM’s maximum effective range. Most Western sources’ maximum range estimates fall between 930-1240 miles. At least one recent PLA source claims the missile can strike as far as 1740 miles. See Erickson, “Global Times Claims Chinese Conventional Ballistic Missile with 4,000 km Range (Sufficient to Strike Guam) “Ready for Service” by 2015 & DF-21D is “Already Deployed in the Army”.”
out into the Western Pacific signifies the ASBM’s relevance to potential East Asian conflicts that do not necessarily involve Taiwan.\textsuperscript{13} Nothing prevents China from threatening to use or actually using ASBMs against U.S. Navy battleforces intervening in notional crises elsewhere along the First Island Chain.\textsuperscript{14} PLA leaders are well aware that America’s conventional military responses to past international crises have depended upon threatening or executing strikes, blockades, amphibious assaults, and/or information operations from the sea to prevent an adversary’s conventional military \textit{fait accompli} while simultaneously commencing massive reinforcement of allies’ defenses via strategic sealift.\textsuperscript{15} The PLA ASBM concept is therefore designed to enable rapid neutralization of forward deployed U.S. naval forces in the region as well as maritime logistical isolation of America’s regional allies and/or partner countries.\textsuperscript{16} It follows that if these

\textsuperscript{13} It is conceivable that the PLA may eventually also develop a smaller ASBM warhead that can be used by Short Range Ballistic Missiles (SRBM). This possibility is not widely discussed in the open literature and would further complicate U.S. and allied tactical planning for East Asian contingencies. An ASBM of this type would have a maximum range of approximately 1000km (621 miles) per the arbitrary general definition of a SRBM. This range would be sufficient to strike battleforces operating in the East and South China Seas, the Sea of Japan, and the Taiwan Straits. Hypothetical SRBM ASBMs would therefore pose a threat in crises involving the Korean Peninsula, Taiwan, the Ryukyus and Senkakus, or the internationally-contested Spratly Islands. This coverage could theoretically free the MRBM ASBM arsenal to be focused on interdicting battleforces and convoys approaching the main Japanese islands or Southeast Asia. China’s historical willingness to export its advanced SRBMs to Iran, Pakistan, and others suggest a particularly-menacing proliferation risk as well. SRBM ASBMs are not specifically examined in this paper due to the absence of open source evidence that they are actually being developed. The maritime surveillance and targeting considerations that govern MRBM ASBM use, however, would also govern SRBM ASBM use. Likewise, the EW and tactical deception technologies, techniques, and concepts explored in Sections VI and VII would probably be extensible against SRBM ASBMs.

\textsuperscript{14} The ‘First Island Chain’ is a Chinese geostrategic concept that describes an arbitrary maritime line stretching from the Kurile Islands through the Japanese archipelago and the Ryukyus and Senkakus, through Taiwan, through the Philippines, to Borneo. While U.S. and allied forcible entry operations such as amphibious assaults are very unlikely to occur in a notional war with China (particularly in a Taiwan scenario) until significant attrition of PLA maritime strike-capable forces have occurred, the possible need to eventually conduct such operations in the First Island Chain cannot be discounted. For instance, China might open a notional war by seizing Japanese islands in the Ryukyu and/or Senkaku chains for use as forward bases or to deny U.S. and Japanese maritime access to the East China Sea. Should this happen, U.S. and Japanese forces might find it necessary to not only neutralize these Chinese bases but also recapture at least some of these islands in order to deny Chinese maritime access to the Western Pacific. See Holmes and Yoshihara, ‘Ryukyu Chain in China’s Island Strategy.’

\textsuperscript{15} A strike is an attack to neutralize or physically destroy a target. Strikes are generally kinetic attacks, such as a missile raid or a bombing sortie. Strikes can arguably also use non-kinetic means such as a cyber attack. However, non-kinetic attacks are generally folded into the category of ‘information operations.’ EW, deception, and psychological operations are also included under information operations.

\textsuperscript{16} It is important to note that the ASBM is but one of many Chinese weapons intended to challenge U.S. maritime access to East Asia. The PLA can also use submarines, large surface combatants, and land-based aircraft to execute sea denial missions within the ocean areas covered by the ASBM. What sets the ASBM apart is that its speed allows
East Asian countries come to believe that the U.S. cannot or will not make good on its extended defense commitments, let alone serve in its declared role as the region’s offshore balancer, China will be able to add the ASBM to the growing PLA arsenal of tools for regional political coercion.

The PLA’s ASBM concept is best understood within the context of Chinese views regarding the use of conventionally-armed MRBMs in general. Numerous articles within publicly available PLA professional journals as well as the contents of publicly released PLA doctrinal documents suggest that Chinese leaders believe precision-guided MRBMs form the core of their conventional deterrent against U.S. intervention in East Asian crises. These writings assert that should Chinese deterrence fail, massed surprise conventionally-armed MRBM strikes against U.S. force concentrations and logistical infrastructure in Japan as well as against U.S. naval forces at sea would contribute to a quick, low-cost decapitation of America’s military ability and political willingness to stand in the way of Chinese objectives. Chinese doctrine further implies extreme PLA confidence that an MRBM first strike’s horizontal and vertical escalation effects could be effectively managed. Chinese MRBM advocates clearly believe early use of these weapons in a deteriorating situation could hand Beijing a swift, decisive victory in a limited campaign against the U.S. and/or its allies individually or together.

---

17 A first strike represents the initial use of offensive weapons against a victim state, thereby opening a war. First strikes are generally aimed at decapitating the victim’s ability to retaliate and/or resist further coercion. First strikes can be against targets on land, at sea, in space, or all three of those domains near-simultaneously. The victim’s national computer network infrastructure may represent an additional domain for first strikes. However, the challenges related to attributing cyber attacks to a specific actor makes it harder to say that a victim state would respond to a first strike limited to the cyber domain in the same ways that it would to first strikes within real-world domains. This paper will specify whenever it discusses a first strike limited to only a single domain. If a domain is not specified, it should be assumed that a first strike being discussed in the text is being conducted near-simultaneously against targets in all three real-world domains and perhaps also the cyber domain.

II. The Chinese Ocean Surveillance System

Extensive maritime surveillance and reconnaissance capabilities are needed to provide ASBM launcher crews with long-range targeting cues. It is believed that these capabilities will eventually include ocean surveillance satellites, land-based Over the Horizon-Backscatter (OTH-B) radar, long-range manned and unmanned reconnaissance aircraft, surface combatants, submarines, and possibly even Chinese nationals serving as satellite phone-equipped observers aboard commercial vessels and boats. All of the above sensor platforms would likely relay their data to a fusion and analysis center.¹⁹ These sensors, the data fusion center, and the communications pathways connecting them constitute the Chinese Ocean Surveillance System (COSS).²⁰ Since effective EW depends upon understanding the nature of the adversary’s sensing and decision-making system, a brief summary of each major COSS element follows.

Space-Based Sensors

COSS’s maritime surveillance satellites are divided into two categories based on their search methods. Actively-searching COSS satellites will employ Synthetic Aperture Radar (SAR).²¹ Passively-searching COSS satellites will carry electro-optical, infrared, and

---

¹⁹ This center might be located within or directly subordinated to the PLA Joint Theater Command in charge of the offensive campaign against U.S. airbases and aircraft carriers in the Western Pacific. The physical location of this center or its alternates is unclear from the open literature. See Stokes, “Conventional Strategic Strike,” 14, 30.
²⁰ COSS is a term invented for this paper. As will be discussed in Section IV, Cold War-era Western defense analysts referred to the Soviets’ maritime surveillance and reconnaissance network as the Soviet Ocean Surveillance System (SOSS). The new term COSS, therefore, builds on the Cold War-era terminology precedent. Most other analysts today refer to China’s ocean surveillance system as being a generic Naval Ocean Surveillance System (NOSS). Needless to say, several countries have NOSSs of varying scale and complexity. It is therefore more precise to call China’s system COSS.
²¹ A SAR uses the velocity of the platform carrying it to achieve far higher cross-range resolution than the laws of physics would otherwise allow. Since radar pulses travel at the speed of light, a traditional short-wavelength radar can generally resolve a contact’s range to within a few hundred feet by measuring the time between the radar’s transmission and its reception of the contact’s radar reflection. The radar’s cross-range resolution, though, is limited by the radar beam’s width at the range of the contact. A radar beam spreads as it propagates in direct proportion to its transmit beamwidth. For example, a radar with a 2 degree beamwidth would have an approximately 14 mile-wide beam at 400 miles from the radar. This means a contact 400 miles away could be located up to 7 miles left or right
radiofrequency (RF) direction-finding/Electronic Intelligence (ELINT) sensors. Although the planned scope of COSS’s space-based sensor architecture is unclear, it is believed that the orbital constellation will be completed during the 2015-2020 timeframe.

China’s satellite naming nomenclature is highly confusing, perhaps deliberately so. While at least two separate maritime surveillance satellite programs appear to be underway, the fact that both share a few common contractors makes it impossible to tell whether the programs are competing, complimentary, or one and the same. The first program, *HJ-1*, appears to take direct advantage of military satellite technology transferred by Russia during the late 1990s. The *HJ-1* series consists of China’s 2008-launched *HJ-1A* and *HJ-1B* electro-optical satellites as well as the never-launched *HJ-1C* SAR satellite. Considerable evidence suggests *HJ-1C*’s debut in orbit has been postponed repeatedly since 2006. Technology cooperation proposals made by *HJ-1C* of the beam’s centerline. Wide beamwidth also means that the radar cannot easily distinguish between multiple contact reflections in the beam at that range, i.e. a single ship as opposed to large swells on the ocean’s surface. The only way for a traditional radar to decrease beamwidth and increase cross-range resolution is to increase the size of the radar’s antenna(s). For high cross-range resolution at distant ranges, the necessary antenna size becomes impractical. A SAR, in contrast, uses a mathematical ‘shortcut’ to attain high cross-range resolution. A SAR knows how far the platform it is mounted on (for instance, a satellite) has travelled laterally in a given amount of time. By taking this lateral motion into account, it can integrate the pulse-to-pulse measurements of the contact’s range along with the relative motion-induced Doppler shifts in the reflected radar pulse’s frequency. This allows the SAR to increase its cross-range resolution as if it had a much larger antenna (hence, a ‘synthetic aperture’) and a correspondingly narrowed beamwidth. With this increased cross-range resolution, a SAR conducting wide-area search can resolve smaller contacts from background ‘clutter’ and/or can discriminate smaller features on a single contact. Furthermore, a highly-sensitive SAR transmitting at a sufficiently short wavelength can be used to ‘image’ a newly-detected contact’s real-world shape. This image, if refined enough, can be used by the SAR’s control processor or a human operator to determine whether the contact is a warship, a merchant ship, a landform, a decoy, etc. A very capable SAR can even distinguish between different warship classes. These discrimination capabilities would obviously make deception much harder for the defender. See Payne, *Principles of Naval Weapon Systems*, 52.

RF direction-finding/ELINT systems are also known euphemistically as ‘Electronic Support Measures’ (ESM) or just plain ‘Electronic Support’ (ES). These systems detect RF transmissions from radars and/or communications radios, then analyze the received signals to identify the emitter and calculate its approximate location. Two or more RF direction-finding/ELINT satellites that detect the same RF transmission can crossfix the emitter’s location.


The Russian Kondor-E military SAR satellite technology that was reportedly transferred to China is a product of the same Russian design bureau that developed the Soviet-era Radar Ocean Reconnaissance Satellite (RORSAT). RORSAT is thoroughly discussed in Section IV. Russian Kondor-E military-grade electro-optical satellite technology may also have been provided. Kondor was originally developed as the ocean surveillance and targeting satellite system for another of the design bureau’s products, the Yakhont anti-ship cruise missile. See 1. Fisher, “New Developments in Russia-China Military Relations: A Report on the August 19-23 2003 Moscow Aerospace Salon (MAKS);” 2. Friedman, *The Naval Institute Guide to World Naval Weapon Systems*, 541.
program engineers to European Union researchers in January 2010 imply the satellite’s SAR might not yet be capable of reliably discriminating ship wakes from other ocean surface phenomena. *HJ-1C* and its -1D partner are presently scheduled for 2011 launches. Four *HJ-1* electro-optical and four *HJ-1* SAR satellites are planned for orbit by 2015.\(^{25}\)

The second satellite development program’s products are designated with the prefix *Yaogan*. This series has already launched six SAR, four electro-optical, and three RF direction-finding/ELINT satellites since 2006. The three RF direction-finding/ELINT satellites, in fact, were launched on the same day in March 2010 and are organized into a co-orbital constellation that appears optimized for crossfixing RF-emitting warships’ positions. Some reports suggest the largest of these three RF direction-finding satellites also carries an electro-optical or infrared sensor for quickly investigating and identifying RF-emitting contacts of interest. Two non-co-orbital *Yaogans* launched within days of each other in December 2009 also appear to allow for coordinated use of their respective SAR and electro-optical sensors. The 2009-2010 *Yaogan* launch rate implies the program enjoys high national-level prioritization. It follows that the *Yaogans* likely serve as COSS’s initial dedicated space-based sensor support for ASBM targeting.\(^{26}\) It is unclear how—or whether—the *HJ-1s* and *Yaogans* relate to each other.\(^{27}\)

\(^{25}\) Data for this portion of the paragraph comes from: 1. Fisher, “Report on the 5th Airshow China: Zhuhai, PRC, November 1-7, 2004;” 2. Erickson, “Satellites Support Growing PLA Maritime Monitoring and Targeting Capabilities;” 3. Huang, “Chinese HJ-1C SAR and Its Wind Mapping Capability,” Slides 3, 4, 6, 7, 18. Of note, the Huang presentation suggests Chinese interest in cooperating with EU researchers on developing algorithms that can use SAR data to ‘map’ wind direction on the ocean’s surface. If the SAR control processor can calculate the wind’s speed and direction in a given area, it can examine the SAR’s imagery to discriminate ocean surface phenomena—such as a ship’s wake (or perhaps the ship, itself)—that do not correlate with the local wind.

\(^{26}\) There is also Chinese-source discussion of yet another ‘separate’ maritime electro-optical and SAR surveillance satellite program dubbed the HY series. Again, it is not clear whether or how this series is separate from the HJ-1s and Yaogans. See 1. Erickson, “PLA Maritime Monitoring and Targeting Capabilities;” 2. Stokes, “Conventional Strategic Strike,” 16-17. Of note, the chief designer of the three RF direction-finding Yaogans was apparently heavily involved in development of the two non-Yaogan ELINT satellites. See Easton, “China’s Secret Co-Orbital Satellites: The Quiet Surge in Space.”

\(^{27}\) Many hypotheses are possible. HJ-1C could represent a foreign technology-capturing front for the Yaogan SAR satellites, a second-generation design meant to be the Yaogan SAR satellite design’s successor, a failed Yaogan
Chinese writers do not believe that COSS’s maritime surveillance satellites will be able to relay real-time data to the COSS data fusion center. At minimum, this delay will drive ASBM warhead sensors’ required field of view. If the delay is extensive, terrestrial COSS scouts would need to be dispatched to redetect a battleforce and provide more timely ASBM targeting data. It is also important to note that infrared and electro-optical satellites are not effective maritime search sensors due to their search swath limitations, inability to peer through clouds and precipitation, and decreased utility when an area is not illuminated by sunlight. Therefore, the electro-optical Yaogans are best understood as contact validation and identification sensors cued by SAR satellites or other COSS assets.

Chinese writers suggest that if a war appeared imminent, the PLA could form a network of up to six electro-optical, ten SAR, and six RF direction-finding/ELINT satellites by surging backup assets into orbit. This would theoretically enable COSS to sweep any given location in East Asian waters at least once every 40 minutes. Some Chinese sources suggest small maritime surveillance satellites with short operational lifetimes are being developed for launch on 12 hours notice in response to rapidly-changing operational-tactical circumstances in a crisis or war.

predecessor, a less-successful competitor, or a complimentary capability. Of note, artistic renderings of the Yaogan SAR satellites look nothing like the Russian Kondor-E SAR satellites that supposedly are the basis for HJ-1C.

See discussion of data relay satellites later in this Section and discussion of ASBM warhead sensors’ fields of view in Section III. Also see Stokes, “Conventional Strategic Strike,” 14.

A Royal Navy analysis from 1963 highlights the search swath coverage issue. The Royal Navy found that a satellite with a 25yd-resolution camera orbiting at a 250 nautical mile altitude yielded a search swath 45 miles in width. At that resolution, ships were barely discernable in the image. A 5yd-resolution camera would have a 7 mile-width swath, which was too narrow to support effective search during the limited time the satellite’s footprint carried over a given area. For global 5yd-resolution coverage within an actionable timeframe, a constellation of 30 satellites would be necessary. Then as now, this would be prohibitively expensive. It therefore makes more sense to cue optical (and infrared) satellite sensors on where to look. See Friedman, Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare, 365-366.

Our analysis assumes that Chinese SAR satellites will automatically image all contacts they detect during routine wide-area search (or at least all contacts whose radar reflections meet certain criteria). If this is not the case and COSS operators must manually order a SAR satellite to image a designated contact, the system becomes incredibly inefficient. This would also present an architectural vulnerability ripe for exploitation.

Small satellites would likely be limited to carrying electro-optical, infrared, or RF direction-finding/ELINT sensors. High resolution maritime surveillance SARs are too big and require too much power for a small satellite.
Other Chinese sources suggest that RF direction-finding/ELINT sensor packages installed on Chinese commercial sector satellites will augment COSS’s capabilities.\textsuperscript{32}

\textit{OTH-B}

OTH-B radars operate in the High Frequency (HF) portion of the RF spectrum. Whereas most radars operate in decimeter or centimeter-wavelength RF bands to precisely locate and track contacts, HF waves are measured in tens of meters. This allows them to be reflected off of the Earth’s ionosphere, and thereby achieve far greater terrestrial propagation ranges than is possible with shorter wavelength RF systems. The tradeoff is that OTH-B radars’ long wavelengths require use of transmit and receive antenna arrays that are each often a mile or more long in order for the OTH-B’s beamwidth to be narrow enough to be tactically useful. Needless to say, this precludes OTH-B radars from being readily mobile and leaves them vulnerable to direct physical attack.\textsuperscript{33}

The PLA OTH-B can reportedly cover a 60° swath of the East China Sea and Western Pacific out to approximately 1860 miles from China’s shores. As the ionosphere’s reflective effect blinds OTH-B to contacts inside a minimum range of about 500 miles, the OTH-B’s separate transmit and receive antennas are located roughly 500 miles west of the Chinese coast.


\textsuperscript{33} Cruise missile-delivered cluster munitions might be particularly useful in wiping out OTH-B antenna elements along a transmit or receive array’s length. Loss of even a small number of an array’s individual elements would negatively affect the OTH-B’s beamforming capabilities and overall sensitivity even if the majority of the array remained intact.
The PLA OTH-B’s coverage area appears to exclude the Sea of Japan, the maritime approaches to the main Japanese islands, and much of the South China Sea.\textsuperscript{34}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig2}
\caption{Estimated PLA OTH-B Coverage Area\textsuperscript{35}}
\end{figure}

Despite OTH-B’s ability to detect ships thousands of miles away, these radars’ relatively-wide beamwidths make them very poor at resolving a contact’s actual position. Chinese writers believe the PLA OTH-B will only be able to localize a contact to a positional error margin of 12-25 miles. Nor can OTH-B identify a contact let alone accurately estimate its course and speed. The task of confirming a specific contact is an adversary’s warship and not a neutral vessel or a decoy will probably fall to space-based sensors, reconnaissance aircraft, or other COSS scouts. Furthermore, OTH-B’s receiver must cope with significant HF background noise from the ambient environment as well as radar reflections from the sea’s surface and other ‘clutter’


\textsuperscript{35} Stokes, “Conventional Strategic Strike,” 19.
sources in order to detect valid contacts’ faint reflections. This is further exacerbated by wide daily variations in ionospheric conditions.\textsuperscript{36}

OTH-B is therefore best understood as a theater-level warning sensor that cues further investigation of a contact or contact grouping by other COSS sensors. Its limited coverage area means COSS must rely on other wide-area sensors for maritime surveillance of the South China Sea and the waters around Japan. Its relative inaccuracy makes it insufficient for use as an ASBM raid targeting sensor. Lastly, its dependence on the ionosphere could make its day-to-day and even hour-to-hour performance capabilities vary considerably.

\textit{Maritime Reconnaissance Aircraft and Unmanned Aerial Vehicles}

The PLA fields several ELINT and maritime scouting variants of its \textit{Y-8} transport aircraft. Effective range appears to be up to 3480 miles, though this may vary considerably between \textit{Y-8} variants depending upon their differing electronic equipment. \textit{Y-8} variants’ sensors’ effective ranges are also unclear, and available imagery does not suggest that any variants have long-range search radars. Likewise, it is unclear whether \textit{Y-8} variants with maritime reconnaissance capabilities have satellite communications systems.\textsuperscript{37} Nevertheless, it is highly probable that future Chinese maritime reconnaissance aircraft will have improved sensor and communications capabilities.

The PLA is also developing a 4350-mile range High Altitude Long Endurance (HALE) UAV called \textit{Xianglong}. Rumored sensor options may include electro-optics, RF direction-

\textsuperscript{36} See 1. Hagt and Durnin, 93-94; 2. Cadirci, “RF Stealth (or Low Observable) and Counter-RF Stealth Technologies: Implications of Counter-RF Stealth Solutions for the Turkish Air Force,” 103-104. Cadirci notes that Digital signal processing techniques have increased OTH-B technology’s contact localization precision considerably over the past two decades. Nevertheless, HF’s long wavelength makes further decreases in OTH-B contact localization error margins extremely difficult if not impossible.

\textsuperscript{37} “Yun-8 Turboprop Transport Aircraft,” \textit{Sinodefence}. 
finding/ELINT, and/or search radar. Even if Xianglong or its successors have autonomous flight capabilities, they will almost certainly also need satellite communications capabilities in order to relay data to COSS operators. UAVs and maritime reconnaissance aircraft together will likely constitute COSS’s main assets for ‘timely’ verification and identification of ship contacts, particularly when local meteorological conditions or other phenomena make it impossible for satellite sensors to fill this role.

Surface Combatants, Submarines, and Commercial Vessel-Based ‘Observers’

Any surface combatant, submarine, or observer aboard a commercial vessel can serve as a COSS scout. PLA Navy (PLAN) warships and intelligence-gathering ships can use HF or military satellite communications to relay radar, sonar, RF direction-finding, and/or visual contact reports to COSS. Commercial satellite communication systems or handheld satellite phones serve the same purpose for relaying visual reports from commercial vessels. Since neither China nor the U.S. will be able to secure uncontestable control of Western Pacific waters at the start of a notional war, PLAN submarines may be used as scouts in the maritime approaches to Japan and the rest of the First Island Chain. PLAN intelligence-gathering ships might also be deployed in these areas prior to a PLA first strike, but their extreme vulnerability means they would likely not remain forward deployed afterwards. PLAN destroyers and frigates will likely be held back within the East and South China Seas where they can be more effectively supported by land-based tactical air cover. Commercial vessels would remain viable scouts throughout the Western Pacific unless the U.S. and its allies declared and enforced a maritime exclusion area within the combat zone.

COSS Data Relay, Positional Correlation, Fusion, and Decision Systems

The PLA has at least one data relay satellite, Tianlian-1, in geosynchronous orbit to serve as a link between space-based sensors and ground control stations. Tianlian-1 reportedly offers non-real-time relay services, meaning that some additional latency is imposed upon maritime surveillance satellites’ data downlinks. A second Tianlian data relay satellite is scheduled for launch during 2011. It is also possible that China might use commercial data relay satellites to augment the COSS data relay network as well as to prevent any wartime attacks on the Tianlians from compromising connectivity with COSS’s space-based sensor constellations.

Given that COSS sensors will be distributed under, on, and above the Western Pacific, a common navigational system is necessary to provide a geodetic reference point for correlating reports from multiple sensors. China’s Beidou satellite navigational system currently provides this service across much but not all of the Western Pacific. The Beidou coverage area will quickly increase in the coming years, however, as additional satellites are launched to achieve the system’s planned 2020 global coverage capability. It stands to reason that the sensor correlation challenge means that ASBMs cannot be effectively used against targets located by sensors that are insufficiently supported by Beidou.

COSS’s data fusion and decision systems appear designed to plug into a developmental PLA-wide command and control network that will provide decision-makers with situational

---

40 Friedman, Seapower and Space, 312.
41 See 1. Erickson, “PLA Maritime Monitoring and Targeting Capabilities;” 2. “Beidou Navigation System.” Wikipedia. If the locations of each of the sensors supporting ASBM targeting are not known across COSS to a very high degree of precision, then their respective contact data cannot be correlated with high precision. At minimum, this increases the amount of uncertainty regarding a target’s real-world position. At maximum, it makes contact data correlation from multiple sensors impossible. Note that this has nothing to do with whether or not the ASBM warhead uses Beidou for navigational support during its flyout to a target.
awareness and decision-making capabilities at the tactical, theater, and strategic levels of war. The degree of integration between COSS and this network is unclear, but PLA leaders reportedly aim for the network to provide them with a much greater degree of centralized control than is the case within the U.S. military. PLA leaders at the operational and strategic levels of war, in fact, seek to increase the PLA’s combat agility by bypassing subordinate commands and delivering orders directly to tactical-level units and weapon systems. Senior PLA leaders appear to believe that network-centric systems like COSS will provide them with impeccably reliable and accurate operational-tactical situational pictures. This centralized command and control approach is historically consistent with autocratic regimes as well as militaries that favor synchronicity over battlefield initiative. It also presents a severe vulnerability: an adversary in theory only needs to blind or deceive a small group of decision-makers at a high command echelon in order to exploit or collapse a highly centralized fighting system at a critical time.

---

III. The ASBM Strike System

Developmental History

In the 1995-1996 Taiwan Strait crisis’s aftermath, CCP and PLA leaders concluded that Chinese deterrence against U.S. intervention failed because the PLA could not reliably detect and rapidly strike U.S. Navy battleforces at standoff ranges from the Chinese coast. It appears that basic research regarding potential solution technologies was conducted between the late 1990s and the early 2000s. Although it is unclear whether any weapon system alternatives to the ASBM concept were actively considered, a decision to initiate ASBM applied research and development appears to have been made around 2003. Countless Chinese journal articles as well as U.S. Office of Naval Intelligence statements suggest that the ASBM is a new variant of the PLA’s existing **DF-21** MRBM series. One Chinese source in particular claims the ASBM development program has at least two initial phases. The first phase allegedly aimed to develop and field a 1060 to 1240-mile ASBM designated **DF-21D** by the end of 2010. The second phase is supposedly geared towards improving the **DF-21D**’s Maneuvering Reentry vehicle (MaRV) warhead’s design so that it can attain an 1860-mile maximum range as well as better evade Ballistic Missile Defense (BMD) interceptors.

---

43 The PLA conducted a series of major multi-service exercises in the Taiwan Strait between July 1995 and March 1996 aimed at influencing Taiwan’s December 1995 parliamentary election and March 1996 presidential election. As the PLA continued massing combat forces opposite Taiwan well into December 1995, the U.S. dispatched the **Nimitz** carrier battle group on a brief transit through the strait as a demonstration of American interest. This, however, failed to deter China from conducting a ballistic missile exercise in the Strait three months later in which several missiles impacted approximately 20 miles off the coast from major Taiwanese ports. As a result, the U.S. deployed the **Independence** and **Nimitz** carrier battle groups near Taiwan as a deterrent against further Chinese escalation. It is unclear whether these deployments forestalled additional Chinese provocations in 1996, but CCP and PLA decision-makers reportedly concluded that new PLA capabilities were required to hold any future U.S. Navy interventions at risk. See Porch, “The Taiwan Strait Crisis of 1996: Strategic Implications for the United States Navy.”

The first phase apparently delivered on time. As noted previously, in late December 2010 the U.S. Navy publicly announced its judgment that DF-21D had attained an initial operational capability. Since DF-21D has not yet been tested against a target at sea, the implication of the initial operational capability judgment is that the U.S. Navy believes that at least a small number of DF-21Ds are now deployed in PLA road-mobile launcher units and that COSS can provide these units with at least rudimentary targeting support. Without an at-sea test, though, it remains unclear whether the DF-21D MaRV warhead’s sensors and COSS’s sensor, data fusion, and decision support capabilities are effective in an operational environment against a moving ship. Further overt and realistic testing would be necessary to demonstrate that these capabilities can perform under operational conditions.

**Technical Characteristics**

DF-21D incorporates several new technologies that theoretically give it the ability to strike ships far out at sea. It will likely use a new solid rocket motor design as indicated by Chinese media reports and construction of new production facilities at the DF-21 series’ primary manufacturing site. It may also mount a hybrid solid/liquid-fueled post-boost vehicle to enable

---

45 For open-source indications from summer 2010 that ASBM initial operational capability was imminent, see Stokes and Ma, “Second Artillery Anti-Ship Ballistic Missile Brigade Facilities Under Construction in Guangdong?” At least one DF-21D overland test would likely have been necessary for the U.S. Navy to form its judgment. It appears the PLA conducted an overland DF-21 test in July 2010. See Forden, “Hangzhou Light Show.” The PLA reportedly conducted another MRBM test in September 2010, but the test missile’s launch towards a target allegedly 1860 miles away exceeds the range of a DF-21C carrying a full warhead load as well as the DF-21D’s commonly reported maximum reach. One possibility was that the test was of a BMD interceptor derived from the basic DF-21 design. See Gertz, “Chinese Missile Test.” This test may alternatively have been of a DF-21C or D carrying a light payload. If the test was of a DF-21D, it is also possible that the missile’s new solid rocket motor design provides it with greater reach than assumed in open-source estimates.

46 Kato, “U.S. Commander Says China Aims to be a 'Global Military' Power.”


MaRV evasive maneuvers against U.S. BMD interceptor missiles along with trajectory aimpoint adjustments during the exoatmospheric midcourse phase.\textsuperscript{49}

Relatively little is publicly known about the MaRV warhead’s targeting and homing sensors. Some Chinese open sources suggest that the MaRV will conduct an initial target search using a SAR during the midcourse phase. This search would be necessary to correct for COSS’s Area of Uncertainty (AOU) regarding the target’s location at the time of the ASBM’s launch. The MaRV would likely conduct an exoatmospheric maneuver to adjust its aimpoint based on this updated target location.\textsuperscript{50}

The MaRV warhead would have a separate sensor suite for terminal homing. Terminal sensors could include a millimeter-wave radar, an RF direction-finding sensor, an imaging laser, an infrared sensor, and/or an electro-optical sensor.\textsuperscript{51} It is reasonable to believe that any millimeter-wave radar contained within the terminal suite would have a search mode sensitive enough to detect aircraft carriers, amphibious warships, supply ships, cruisers, and destroyers against an ocean background. With sufficiently high resolution, the terminal radar might also be

\textsuperscript{49} A post-boost vehicle, also known as a ‘bus,’ is an assembly that can be mounted as a ‘final stage’ atop a ballistic missile. The missile’s warhead(s) are mounted atop the post-boost vehicle. The post-boost vehicle may contain a small rocket motor and/or thrusters that allow it to conduct preprogrammed exoatmospheric maneuvers. These maneuvers might be used as an evasive measure against inbound BMD interceptor missiles. They might also be used to provide aimpoint adjustment for the warhead(s). The post-boost vehicle may additionally be used to deploy countermeasures against missile defense sensors. See Hagt and Durnin, 89-90.

\textsuperscript{50} Stokes, “Conventional Strategic Strike,” 21, 23-24. An AOU reflects the combination of sensors’ inherent imprecision, any geodetic ambiguity regarding a sensor’s own position, and the time elapsed since the last received sensor report. A satellite’s SAR can theoretically be precise to within a few yards. A crossfix between two RF direction-finding sensors would be less precise. An OTH-B contact’s AOU radius could be several tens of miles. Use of \textit{Beidou} will render geodetic ambiguity negligible in peacetime, but any loss of \textit{Beidou} system fidelity under combat conditions would increase an AOU’s size as a COSS sensor’s position at a given moment would be less certain. Since COSS’s data relay system imposes a time delay of perhaps up to several minutes, a targeted ship will have moved in the interim. It will also take several minutes for COSS operators to interpret the sensor data, decision-makers to issue an attack order, lower-level commands to relay the order to subordinate ASBM units, and ASBM units to accordingly prepare a missile for launch. The longer all this takes, the larger the AOU will grow. Following ASBM launch, several more minutes will tick by as the missile boosts itself outside the atmosphere. All this is why the ASBM warhead will need to conduct its own search for the target, not to mention why the ASBM’s sensors’ sensitivity and field of view sizes will dictate how many missiles need to be fired against a target based upon the size of the AOU at the time of launch. For more on AOU considerations, see Hoyler, 86, 93-94.

\textsuperscript{51} Stokes, “Conventional Strategic Strike,” 23-25.
capable of Inverse Synthetic Aperture Radar (ISAR) imaging to support final aimpoint adjustments as well as discriminate the targeted ship from unsophisticated decoys. The other sensors in the suite would likely help with target discrimination as well as provide a measure of redundancy in the event one or more sensors failed to operate or were effectively jammed. It is important to note that if a RF direction-finding sensor is included in the suite, it might also be able to help support the MaRV warhead’s midcourse phase aimpoint adjustment maneuvers based on the targeted battleforce’s shipboard radar emissions.

---

52 ISAR uses the same relative motion principle as SAR to achieve higher cross-range resolution than the radar antenna’s physical size would otherwise permit. While SAR uses the radar platform’s velocity relative to a contact’s to artificially increase cross-range resolution, ISAR uses the contact’s angular motion relative to the radar for the same purpose. An ISAR-equipped reconnaissance airplane or missile flying towards a contact will only see the contact’s radar reflection grow in intensity as it approaches; this closure will not induce much relative angular motion. Ocean swells, however, will induce a warship to roll slightly from side to side. Since the ISAR knows its transmit wavelength, it can integrate the slight relative angular motion-induced Doppler shifts in its pulses’ reflections off the contact to calculate the contact’s cross-range position with greater precision. If the ISAR uses a suitably short wavelength and has sufficient sensitivity and discrimination capabilities, it can image the contact by integrating the positions of the individual shapes that constitute the contact. See Payne, 53.

53 This illustration is from a 2004 U.S. Office of Naval Intelligence assessment of a notional ASBM MaRV terminal guidance sequence based on then-available information. It therefore should not be considered a definitive illustration. See Stokes, “Conventional Strategic Strike,” 21.
Considering the MaRV warhead’s hypersonic speed upon atmospheric reentry, it will need to slow its descent considerably to provide the terminal sensors the tens of seconds they need to search for, identify, and track the targeted ship. Chinese writers describe a pre-programmed speed control maneuver by the MaRV at a 16-31 mile altitude to support terminal sensors’ search as well as interceptor missile evasion. In addition to the MaRV’s evasive maneuvers, *DF-21D* might employ penetration aids such as faster-burning rocket motors, chaff clouds, active EW systems, decoy objects, and measures aimed at reducing the warhead’s observable signatures. The MaRV’s payload could be a deck-penetrating unitary high explosive, submunitions for destroying carrier aircraft parked on deck or a warship’s topside sensors and communications antennas, or High Power Microwave (HPM) devices for neutralizing unshielded sensors and communications systems.

*DF-21Ds* are carried by Transportable Erectable Launchers (TEL) in order to enhance their prelaunch survivability. The *DF-21D*’s TEL may in fact have off-road driving capabilities. As the U.S. and its allies learned during the 1991 Gulf War when trying to locate and destroy Iraqi *Scud* units, this tactical mobility makes TELs very difficult to target. TEL units can also take advantage of terrain for cover as well as employ camouflage and decoy launchers to prevent from being targeted. This historical experience suggests that the most a counter-TEL campaign can hope for is suppressing the missile launch rate. Also, unlike Iraq during the 1991 counter-*Scud* TEL campaign, China’s robust territorial air defenses provide *DF-21D* TELs with extensive operational sanctuary. A sustained, comprehensive suppression or destruction

---

54 Hagt and Durnin, 91.
56 HPM devices induce massive component-level voltage surges in unshielded voltage-sensitive electronic systems. By ‘burning up’ these systems’ microelectronics, HPM can leave a warship unable to sense, control its defensive weapons, or communicate.
57 “DongFeng 21 (CSS-5) Medium-Range Ballistic Missile.” Sinodefence.
campaign against *DF-21D* TELs likely would not be possible until these air defenses were reduced.\(^5^9\)

**Notional 2020-Timeframe DF-21D Inventory**

In order to further understand the ASBM threat’s scope, it is useful to derive a rough *DF-21D* arsenal size in 2020. As will be discussed in Section VII, 2020 marks the approximate timeframe that U.S. Navy anti-ASBM systems whose formal requirements are defined as late as Fiscal Year 2012 and/or that will rely on technologies currently in the applied research stage would probably begin entering service based upon historical systems development timelines. The U.S. Department of Defense’s (DOD) annual estimates of the PLA’s *DF-21* series arsenal’s overall size from 2005 through 2010 can help with development of the arsenal size and production rate estimates.

<table>
<thead>
<tr>
<th>Year</th>
<th>Estimated Number of <em>DF-21</em> Series Missiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>19-23</td>
</tr>
<tr>
<td>2006</td>
<td>19-50</td>
</tr>
<tr>
<td>2007</td>
<td>40-50</td>
</tr>
<tr>
<td>2008</td>
<td>60-80</td>
</tr>
<tr>
<td>2009</td>
<td>60-80</td>
</tr>
<tr>
<td>2010</td>
<td>85-95</td>
</tr>
</tbody>
</table>

\(^5^9\) A sustained counter-TEL campaign requires either a persistent strike-capable aircraft presence near the area in which TELs are believed to be operating or very high speed long-range strike weapons. This proximity and/or speed of attack is necessary because TEL crews can prepare their missile for launch, execute the launch, and then relocate within a very short amount of time. No amount of stealth can prevent a scout or strike aircraft from eventually being discovered the longer it loiters in a given area without EW and/or kinetic air defense suppression support. Special forces could be used to monitor an area for TEL activity, but the area that they could effectively monitor would be far smaller than the area that could be monitored from the air. Even if *DF-21D* TEL launch rate suppression was all that could be achieved, it could still contribute greatly to battleforce missile defense operations overall. It clearly would not be enough to obviate robust sea-based defenses, though. Nor would counter-TEL operations likely be possible prior to China initiating open hostilities.

\(^6^0\) This data compiled from the 2005, 2006, 2007, 2008, 2009, and 2010 Office of the Secretary of Defense Reports to Congress on the Military Power of the People’s Republic of China. 2005 was the first year this report provided estimates regarding the PLA ballistic missile arsenal’s size and composition. These reports do not describe the DOD’s methodology for making these estimates, however.
Table 1’s data cannot distinguish between the three land-attack \textit{DF-21} variants that were in active service during the 2005-2010 period as the DOD estimates do not provide this amount of specificity. The original \textit{DF-21} served as China’s first operationally-deployed solid-fueled MRBM. Developed from the mid 1970s through the mid 1980s, its relatively low accuracy likely limits it to a theater nuclear deterrence role.\textsuperscript{61} Its immediate successor, \textit{DF-21A}, was developed during the early-to-mid 1990s and produced from the late 1990s into the early 2000s. Although \textit{DF-21A} improves upon the original \textit{DF-21}’s maximum range, it shares its predecessor’s relatively low accuracy and probable nuclear-only role.\textsuperscript{62} The third variant, \textit{DF-21C}, improves significantly upon \textit{DF-21A}’s accuracy and payload capabilities. \textit{DF-21C}, in fact, appears to have been designed to be capable of both nuclear and conventional land-attack missions. \textit{DF-21C} reportedly began production in 2004 or 2005 but may not have been operationally deployed until 2007 or early 2008.\textsuperscript{63} Based on these data points, we can assume the vast majority if not all of the missiles in the 2005-2007 inventory estimates were existing first generation \textit{DF-21s} and newly-produced second generation \textit{DF-21As}. We can also assume the major increase in deployed \textit{DF-21s} during 2008-2010 predominately reflects \textit{DF-21C} deployments. These facts provide a baseline for estimating a normalized \textit{DF-21} generic-variant production rate in Table 2 below:

\textsuperscript{61} Stokes and Easton, “Evolving Aerospace Trends,” 12.


\textsuperscript{63} The 2004-2005 production start is claimed in “Dong Feng 21C (CSS-5 Mod-3) Medium-Range Ballistic Missile.” \textit{Sinodefence}. However, the 2005-2007 DOD Reports to Congress’ PLA ballistic missile inventory tables specifically describe the first generation \textit{DF-21} and second generation \textit{DF-21A} as the variants counted as in service during those years. This distinction is dropped in the 2008-2010 DOD Reports to Congress. See 1. “Annual Report to Congress: Military Power of the People’s Republic of China 2008,” 42; 2. “Annual Report to Congress: Military Power of the People’s Republic of China 2008,” 56. This suggests that increases in the DOD’s \textit{DF-21} inventory estimates during 2005-2007 reflect production of additional \textit{DF-21As}. 
Table 2: Derived DF-21 Inventory Data

<table>
<thead>
<tr>
<th>Year</th>
<th>Mean Number of Estimated DF-21s in Inventory</th>
<th>Mean Year over Year Growth in DF-21 Generic Variant Inventory</th>
<th>Year over Year Growth: High-Range of DOD Estimated Inventory</th>
<th>Year over Year Growth: Low-Range of DOD Estimated Inventory</th>
<th>Range of Year over Year Inventory Growth Uncertainty</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>21</td>
<td>+13.5</td>
<td>+27</td>
<td>0</td>
<td>+0 to +31</td>
</tr>
<tr>
<td>2006</td>
<td>34.5</td>
<td>+10.5</td>
<td>0</td>
<td>+21</td>
<td>+0 to +31</td>
</tr>
<tr>
<td>2007</td>
<td>45</td>
<td>+10.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2008</td>
<td>70</td>
<td>+25</td>
<td>+30</td>
<td>+20</td>
<td>+10 to +40</td>
</tr>
<tr>
<td>2009</td>
<td>70</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2010</td>
<td>90</td>
<td>+20</td>
<td>+15</td>
<td>+25</td>
<td>+5 to +35</td>
</tr>
<tr>
<td>Average</td>
<td>+13.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

While the DOD annual high and low-end production estimates vary 20-30 DF-21s from one year to the next, average growth is roughly 14 missiles per year.\(^64\) Since DF-21D’s late 2010 initial operational capability suggests that its initial field deployments began during the second half of 2010, and since the DOD inventory estimates only count operationally deployed DF-21s, it is reasonable to assume that DF-21Ds are not yet included in the DOD estimates. Also, as noted earlier, DF-21D has separate production facilities from earlier DF-21 variants. This suggests DF-21D production will not compete with DF-21C production for factory space.

---

\(^64\) Actual production rates may have varied from year to year due to PLA resource allocation decisions. As a result, peak production during any one year of the 2005-2010 period may have been higher than 14 new missiles. It follows that even the actual peak production rate might not have made use of DF-21 production lines’ maximum capabilities. These surge production capabilities might be tapped if regional tensions increased Sino-American hostility to the point that the political possibility of a direct conflict notably increased. Interestingly, the difference between the DOD’s highest estimate for the DF-21 inventory’s size in a given year tends to be no less than 30 missiles more than the DOD’s lowest estimate for the inventory’s size in the immediately preceding year. This might suggest the DOD’s estimate for the maximum DF-21 production rate. The 2010 DOD report to Congress on PLA developments suggests that the DF-21 production lines’ output could double under surge conditions; a surge rate of 30 new missiles per year is just over double Table 2’s calculated mean of 14. See “Military and Security Developments Involving the People’s Republic of China 2010,” 44. The production rate estimate also relies on the assumption that the PLA did not replace some of its nuclear-only older DF-21 variants with dual-capable DF-21Cs. If this occurred, it would make overall DF-21 production rates appear lower than they actually were. There is some evidence that this may be happening. See Stokes and Easton, “Evolving Aerospace Trends,” 12.
Assuming that DF-21D enters full-rate production during 2011 at Table 2’s DF-21 generic-variant production rate, the PLA could have roughly 140 DF-21Ds by 2020.65

**ASBM Target Prioritization and Possible Employment Approaches**

PLA doctrine suggests that U.S. Navy aircraft carriers’ land-attack capabilities make them the ASBM’s highest-priority targets. They might not be the only U.S. naval targets, however. Chinese writings note that carriers’ dependence on at-sea logistical replenishment make supply ships desirable targets, and that strikes conducted during underway replenishment operations offers the chance of neutralizing carriers and supply ships simultaneously.66 PLA doctrine also highlights the importance of preventing adversaries from deploying new forces into the East Asian theater or resupplying forces already in the theater. This could imply potential ASBM use against the U.S. armed services’ Western Pacific-based Maritime Prepositioning Ships.67 This could also imply potential ASBM use against notional trans-Pacific convoys carrying reinforcements and materiel to Japan, or notional intra-theater logistical convoys from the main Japanese islands down the First Island Chain or to South Korea.68 Chinese strategists additionally observe that the U.S. Navy’s Aegis BMD-capable cruisers and destroyers could potentially reduce the effectiveness of PLA land-attack MRBM strikes in East Asia.69 It follows

---

65 A 2020-timeframe DF-21D inventory of approximately 140 missiles appears consistent with unverified Chinese open source reporting that the PLA anticipates deploying six DF-21D TEL battalions with 17 TELs in each battalion. See Stokes, “Conventional Strategic Strike,” 29. This TEL inventory would result in the ability to simultaneously field up to 102 DF-21Ds and have up to approximately 38 missiles in stored reserve, less any used for tests or demonstrations.

66 Supply ships are used to refuel, rearm, and provide food and other stores to naval battleforces at sea.

67 Forward-stationed Maritime Prepositioning Ships offer the operational-strategic capability of quickly delivering a month’s worth of combat materiel to help reinforce U.S. and allied defenses and/or support counteroffensives. The Western Pacific Maritime Prepositioning Ships are based in Guam and Saipan in the Marianas. They would have to cross the ASBM coverage zone in order to deliver materiel to Japan, South Korea, or elsewhere in East Asia. See “Maritime Prepositioning Ship,” Wikipedia.

68 Cliff, “Anti-Access Measures in Chinese Defense Strategy,” 5-6. Note that the DF-21D’s estimated range covers the oceanic approaches to the main Japanese islands, the First Island Chain, and most of Southeast Asia.

69 Yoshihara, 45.
that sea-based missile defense patrol stations might be ASBM targets early in a war, if only to force these U.S. Navy combatants to expend their BMD interceptor missile inventories.

A PLA doctrinal textbook implies some potential ASBM raid tactics. In addition to high explosive, submunition, and/or HPM strikes on carriers’ and other warships, an ‘intimidation’ strike is described in which ASBMs are fired near but not directly at a battleforce as a means of coercing its withdrawal from Chinese “territorial waters.” This might imply the PLA expects to have an abundance of ASBMs to support their use in such a manner. It is more likely, however, that this means the PLA would launch unarmed **DF-21As** or perhaps land-attack **DF-21Cs** into the waters near a battleforce prior to the outbreak of open hostilities as a deterrent demonstration. It follows that the PLA might use this ‘intimidation’ tactic immediately prior to an actual ASBM strike in order to compel a battleforce to activate its missile defense-capable radars and thereby provide additional cues for ASBM targeting. If the ‘intimidation’ strike looked enough like an actual ASBM strike, the battleforce might launch BMD interceptor missiles against it. This would reduce the number of interceptors available for use against a subsequent actual ASBM raid.\(^70\)

Should an ‘intimidation’ strike or actual ASBM raid be coordinated with nearby PLAN units at the start of a war, it could potentially focus a battleforce’s attention on the ballistic missile threat and/or stress the battleforce’s air and missile defense resources in such a way that it takes longer to detect and react to an inbound PLAN anti-ship cruise missile raid. This kind of multi-service, multi-unit, multi-axis, multi-weapon type raid would be incredibly difficult for

\(^{70}\) Erickson and Yang, 61-62, 75.
theater-level commanders to coordinate and COSS to support, but it likely represents the PLA’s ideal for use of ASBMs in a war-opening first salvo.\textsuperscript{71}

The number of DF-21D ASBMs that the PLA would fire in a raid will depend upon a number of factors. The target’s AOU size at the desired time of launch and the size of MaRV warhead sensors’ effective fields of view will dictate how many missiles must be launched just to cover the AOU.\textsuperscript{72} Other variables include the number of ASBM warheads needed to effectively damage the target, the anticipated total system reliability of a launched DF-21D, the probability that a single ASBM warhead’s sensors will successfully detect and identify the correct target as well as guide the warhead to endgame, the anticipated probability that a single ASBM will be able to evade all BMD interceptors fired against it through use of decoys and/or MaRV maneuvers, and the targeted battleforce’s anticipated number of BMD interceptors. These calculations are incredibly complicated and will not be attempted here.

A thought experiment might nonetheless be useful for illustrating the raid-sizing implications of these variables. If we arbitrarily assume that the DF-21D system’s reliability and a U.S. Navy battleforce’s multi-layered active defense’s effectiveness combine to give a single ASBM a 50% chance of its warhead making it to endgame at all times in the absence of EW, that the warhead’s sensors can effectively cover an AOU whose size is equal to the distance a battleforce can travel at maximum speed in a half hour, and that it takes three ASBM warheads

\textsuperscript{71} A first salvo as defined in this paper represents the first maritime strike in a war. An especially effective first salvo could cripple the victim’s war effort from inception if the victim’s military strategy relies upon naval power. A first salvo also has operational and tactical implications in that a massive first salvo could devastate the victim fleet’s ability to execute its planned initial campaign and/or defend itself against follow-on attacks. A first salvo could be conducted at the theater level against all of the victim’s naval forces in a given region, or at the global level against all of the victim’s naval forces operating in regions of interest to the attacker.

\textsuperscript{72} Hoyler, 93-94.
to render an aircraft carrier incapable of flight operations for a tactically meaningful amount of
time, then a minimum of six ASBMs would need to be fired against the carrier alone.\textsuperscript{73}

It is unlikely that the PLA would not also strive to strike the large surface combatants
escorting the carrier, as these warships serve as the battleforce’s primary active missile defense
protection and can also provide robust area air defense during a period in which the carrier
cannot launch defensive aircraft.\textsuperscript{74} Furthermore, U.S. Navy large surface combatants often carry
long-range land-attack cruise missiles. If we assume it takes only one ASBM warhead to knock a
large surface combatant out of action and we also assume there are six of these warships in the
battleforce, then twelve additional ASBMs would be needed in the raid. Recall the earlier rough
estimate that the PLA could field 140 $DF-21Ds$ by 2020. If we assume that U.S. Navy
battleforces always carried the necessary number of BMD interceptors to sustain our arbitrary
effectiveness assumption, we see that the PLA could conduct up to seven ‘full-sized’ raids of
eighteen ASBMs and one additional raid of fourteen ASBMs before expending its inventory.

These raid counts, of course, are unrealistic as a battleforce that successfully fended off one raid

\textsuperscript{73} Several U.S. analysts believe that it would likely take a minimum of 32-35 minutes for space-based sensors’
contact data to be received and analyzed by COSS, a firing order to be received by an ASBM launcher crew, and the
ASBM to fly out to the point of its trajectory in which it begins its terminal phase. The AOU in the above example is
sized accordingly. See Ibid, 93-94. U.S. Navy aircraft carriers are designed with extraordinary inherent damage
control capabilities, so it might not be possible for a conventional ASBM raid sized like the one in the above thought
experiment to sink a carrier. A carrier could be temporarily incapacitated, however, by widespread damage to its
flight deck and topside sensor and communications systems along with destruction of aircraft parked on the flight
deck. The carrier crew’s damage control efforts might be able to restore flight operations capability for surviving
aircraft within a few hours if damage to the armored flight deck is mostly superficial, which is what one might
expect from submunitions-releasing warheads. More severe damage, such as what might be expected from deck-
penetrating unitary high explosive warheads, might require that the carrier leave the combat zone for repairs in a rear
area. Either of these two situations would leave the carrier’s air wing unable to support battleforce defense for some
length of time. Other PLA forces might use this period to conduct follow-on attacks using anti-ship cruise missiles.

\textsuperscript{74} Contemporary U.S. Navy cruisers and destroyers are considered ‘large surface combatants’ as they tend to have
displacements above approximately 8000 tons. It is worth noting that from the 1930s up until the early 1970s, U.S.
Navy destroyer classes were generally designed with 2000-4000 ton displacements and accordingly were considered
small surface combatants. The need for more robust shipboard area air defenses drove the post-1970 growth in U.S.
Navy destroyer classes’ displacements. The U.S. Navy compensated for destroyer size growth by constructing
several classes of single or dual-mission frigates with displacements of 2000-4000 tons from the early 1960s through
the late 1980s. Since then, frigates as well as mine countermeasures ships have served as the U.S. Navy’s small
surface combatants.
by expending most of its BMD interceptors would have few left to counter a follow-up raid launched a short time afterward. A follow-up ASBM raid against a recently-struck battleforce would, however, reduce the number of ASBMs available for later use against other battleforces.

All of the above assumptions are highly generous, and real-world factors as well as actual system capabilities would likely increase the numbers of ASBMs required per raid beyond the arbitrary numbers used here. All the same, this thought experiment has two important implications. First, a naval battleforce cannot physically destroy inbound ASBMs once its BMD interceptor inventory is expended. While a battleforce can opt to leave the combat zone to replenish its interceptor missiles, this may come at the cost of the tactical and perhaps even operational initiative. A depleted defensive inventory also risks leaving a battleforce unable to withstand an especially large ASBM salvo or a quick succession of salvos. A battleforce therefore needs defensive capabilities that are depleted at a much slower rate than interceptor missiles. Ideally, these additional capabilities should complement interceptor missiles so that they combine to increase the battleforce’s defensive depth and effectiveness. This is where EW can play a role.

Second, the ASBM’s complete dependence on effective long-range surveillance and targeting appears to risk it becoming a ‘wasting asset’ in combat. This raises the possibility that U.S. Navy EW and deception could render the first ASBM salvo only partially successful and then render any immediate follow-on raids unsuccessful. If this were to occur, the resultant depletion of the PLA ASBM inventory might induce hesitation to expend further ASBMs without greater confidence in COSS’s operational-tactical picture. Particularly effective U.S. tactical deception following the first salvo might even induce PLA decision-makers to hesitate to conduct any follow-on raids. The longer the hesitation persisted, the more time U.S. forces
would gain to erode COSS to the point that it could no longer effectively support ASBM targeting. As the next Section will show, this approach is very similar to what the U.S. Navy ultimately developed during the Cold War for potential use against Soviet maritime surveillance, targeting, and strike capabilities.

Setting the Stage: Naval Targeting and Countertargeting Before 1958

In order to properly appreciate the nature and scope of Soviet maritime surveillance, reconnaissance, and strike capabilities, it is first useful to understand how warships and coastal defenders dealt with the challenges of these tasks prior to the electronic age. Up until the late 1930s, the human eye served as the primary naval sensor. Successful maritime surveillance depended upon stationing scout ships in waters that adversaries were expected to traverse. Maritime reconnaissance was similarly executed by scouts patrolling over the horizon as ‘early warning’ pickets for the main battleforce or coastal defenses they supported. Scouts could either physically convey their detection reports by making best speed back to friendly forces, or they could pass them to the force commander via signals relayed by intermediary ships. Otherwise, warships could not be maneuvered into battle or coastal fortifications readied for action until the enemy’s ships either poked above the horizon or became visible through darkness or weather.

This sensory limitation was a steady naval principle for millennia, and as such was independent of whether warships were propelled by oar, sail, or steam. The principle likewise impacted warships’ and shore fortifications’ abilities to engage adversaries at the maximum weapons ranges available in a given era, as the only sensors accurate enough for aiming these weapons were the weapons crews’ own eyes. Neither the radio nor airplane upended this principle during the late 19th and first decades of the 20th Centuries. These technologies only affected the distance that scouts could be positioned ahead of friendly forces and the speed by which they could relay their reports back to commanders. Radio-equipped scouts on, above, and
eventually under the ocean could not report on or direct fire at what they could not see themselves. From classical antiquity through the First World War, therefore, naval countersurveillance and countertargeting centered on avoiding enemy scouts when possible, visually deceiving scouts with respect to one’s force composition and scheme of maneuver when evasion was impossible, and using night and weather as well as man-made visual obscurants and decoys to handicap the accuracy of enemy weapons fire.\textsuperscript{75}

The technologies that finally toppled the sensory limitation principle were radar and RF direction-finding. With radar, naval battleforces as well as shore fortifications could now precisely locate enemy ships, aircraft, and surfaced submarines well before they came within visual range. RF direction-finding, while unable to locate enemy forces with radar’s precision, nevertheless provided actionable cues of an adversary’s presence nearby. Both technologies could be used to reposition scouts, launch long-range air strikes against an opponent’s battleforce, or reorient one’s own defenses in preparation for an opponent’s inbound strike.

The story of how radar and RF direction-finding led to the rapid evolution of naval tactics during the Second World War is fairly well known and will not be recounted here.\textsuperscript{76} In contrast, much less has been written about the development of initial naval EW countertargeting measures against those first radars and RF direction-finders. For instance, the Kriegsmarine developed

\textsuperscript{75} These countertargeting practices remained valid during the Second World War. Obscurant smokelaying was the most common countertargeting tactic when in contact with the enemy, but even more elaborate tactics were also used. On one occasion, Allied navies disguised high value tankers being convoyed to Murmansk to look like regular surface combatants, thereby preventing the Luftwaffe from singling them out for attack. On another occasion, an obsolescent Royal Navy battleship escorting a convoy to Malta was disguised to look like a newer battleship in order to attract Luftwaffe attention away from the merchant ships. The Allies also employed a device called Water Snowflake that, at a preset time up to six hours after being tossed in the ocean, would launch an illumination flare skyward. The flare was similar to those used at night by convoys to support visual detection of U-Boats approaching on the surface. Water Snowflake was intended to convince U-Boat commanders who saw the flare from a distance that a convoy’s main body lay just over the horizon. It was hoped that this would lead them to commit their slow U-Boats in a direction away from the main body’s actual location. For additional examples see Holt, \textit{The Deceivers: Allied Military Deception in the Second World War}, 83-84.

\textsuperscript{76} For the definitive analytical summary of this tactical evolution, see Hughes, \textit{Fleet Tactics and Coastal Combat}, 120-140.
tinfoil streamer decoys that could be towed behind U-Boats while at periscope depth. As the streamers’ radar cross sections were larger than that of the periscope or other sea-protruding portions of the U-Boat’s sail, an Allied radar operator’s mistaking the decoy’s radar reflection for the U-Boat’s might offset the manual-aiming of Allied anti-submarine weapons. The Kriegsmarine also developed rudimentary radar detectors that could warn U-Boat crews when an Allied radar-equipped anti-submarine warship or aircraft was nearby. Allied Anti-Submarine warfare (ASW) forces overcame these German RF countermeasures by training radar operators in decoy discrimination and developing ASW radars that transmitted at a different band of the RF spectrum.\textsuperscript{77} Later in the war, the U.S. Navy rapidly developed and fielded a series of RF noise jammers that could sever the radio-control link between Luftwaffe bombers and the Germans’ revolutionary Fritz-X guided anti-ship bomb.\textsuperscript{78} What is perhaps most remarkable about these example countermeasures is the speed at which they were developed and fielded in response to an adversary’s emerging RF technologies.

Despite these revolutionary sensor and countermeasure advances, three key factors involving the nature of maritime surveillance, reconnaissance, and strike did not change. First, during the Second World War and well into the 1950s, the dominant terminal homing sensor for naval weapon systems remained the human eye. Naval radar’s electrical power requirements, relative bulk, and inability to automatically discriminate valid contacts from background clutter

\textsuperscript{77} Roscoe, \textit{United States Submarine Operations in World War II}, 247.
\textsuperscript{78} “How Radio-Controlled Bombs Were Jammed.” \textit{Lone Sentry} (blog). RF noise jamming is the oldest and most straightforward EW technique against an adversary’s radar. It involves broadcasting intense random RF ‘noise’ to saturate the adversary radar’s receiver, thereby preventing the adversary radar from detecting its pulses’ reflections off of a defended warship. An unsophisticated radar cannot overcome this unless it travels close enough to the defended warship such that the strength of the pulse reflections off the warship begin to exceed the jamming noise. A sophisticated radar can overcome this by transmitting on or receiving multiple frequencies near-simultaneously, thereby making it harder for the defender to effectively jam all of them at once. A sophisticated radar can also increase its transmission power such that received reflections exceed the defender’s jamming noise. Lastly, a sophisticated radar can use receiver ‘filters’ and various signal processing techniques to suppress or cancel out jamming noise. For more on RF noise jamming 1. Adamy, “EW Against Modern Radars-Part 2: Radar Jamming Techniques,” 44-45; 2. Payne, 87-90.
at the time meant that self-guided bombs and missiles remained a futuristic concept. Considering that a human observer was still necessary to remotely control Fritz-X and other similarly advanced guided munitions of this period, visual countersurveillance and countertargeting techniques remained just as important as EW techniques.

This led to the second factor: in order to employ its weapons, an attack had to steam or fly within visual range of its targets. This meant that an attacker could not ‘stand off’ and fire his weapons from outside a battleforce’s inner defensive screen. The defending battleforce could therefore mass its screening warships and aircraft in a relatively small area. This, too, lasted well into the 1950s.

The third and most important factor involved the speed at which a long-range attack could be delivered. With fully-laden speeds below 400 miles an hour, it took precious time for propeller-driven maritime bombers to arrive at a distant enemy naval battleforce. In theory, the attacker’s scouts could maintain steady contact with the enemy battleforce while periodically relaying positional updates to guide the inbound raid’s approach. This was virtually impossible in practice, however, as scouts either lacked the speed or fuel needed to maintain contact for such a long duration, or had to flee when threatened by the enemy’s defensive air cover or surface escorts. As a result, raids often had to redetect an enemy battleforce on their own. This involved searching an ever-expanding AOU centered on the battleforce’s last reported position. All this, combined with the attackers’ own speed and fuel limitations, meant that effective air strikes could only be conducted within a few hundred miles of bombers’ home airfields or carriers unless the enemy battleforce either gave away its position via periodic HF radio transmissions or otherwise took station in a known and relatively fixed location. As we will see, the jet age increased the distance at which an effective strike could be delivered while an AOU’s size was
still manageable for the attacker. It did not, however, render the relationship between distance, time, and an AOU obsolete. This relationship became the new key to naval countersurveillance and countertargeting.


During the Cold War’s first decade, the naval competition between the U.S. and Soviet Union was overwhelmingly biased in favor of the former. The 1950s-era Soviet Navy was at best a coastal defense force with extremely limited over-the-horizon search, targeting, and strike capabilities. The Second World War’s devastation, still fresh in Soviet leaders’ minds, played an important role in driving their efforts to counter the U.S. Navy’s then-new aircraft carrier-based nuclear strike capabilities as well as war-demonstrated conventional amphibious assault capabilities. Having captured German guided anti-ship weapons such as the Fritz-X after the war, the Soviets moved to develop new munitions that could be fired from outside a defending battleforce’s inner screen so that attackers would not need to approach within visual range of a targeted warship. This not only required that radar technology be further miniaturized for installation within a missile, but also called for a greater reliance on radar and RF direction-finding for wide-area ocean surveillance and reconnaissance.79

The Soviets tackled the miniaturization hurdle by successfully fielding the world’s first operational air-launched, radar-homing anti-ship missile, *KS* (NATO designation: *AS-1 Kennel*), in 1958 aboard their *Tu-16KS* (NATO designation: *Badger-B*) medium jet bomber.80 The *Badger-B/Kennel* combination was a far from optimal solution, though. Although *Badger-B*

---

79 Friedman, *Seapower and Space*, 132-133.
80 NATO designations were the unclassified codenames by which Soviet warships, aircraft, submarines, and weapons were known in the West. This was primarily to make it easier for NATO militaries to recognize and communicate amongst themselves about these systems. In cases where the actual Soviet names for certain systems were not known in the West, the NATO designations often became those systems’ ‘publicly-popularized’ names.
could strike naval battleforces up to 2000 miles from the Soviet coast and could fire *Kennel* from 35-45 nautical miles away from a targeted warship, the bomber had to continue closing with the target for several critical minutes in order to steadily ‘illuminate’ its prey with a radar beam. The *Kennel* rode this beam until it was close enough for its onboard radar receiver to detect the beam’s reflection off the target, at which point it could terminally home until impact. Needless to say, U.S. Navy Combat Air Patrols (CAP) over carrier battle groups could pounce on the inbound *Badger-Bs* and either shoot them down or force them to cut off their radar illumination support to the *Kennels*. Either would effectively defeat an inbound *Kennel*. Furthermore, the *Kennel*’s weight reduced the *Badger-B*’s maximum cruising speed from approximately 650 miles per hour to approximately 520 miles per hour. This meant it could take nearly four hours for a raid to fly out and strike a battleforce operating at the edge of the *Badger-Bs*’ combat radius. The targeting AOU would be enormous after this length of time if the battleforce was not being continuously tracked by Soviet surveillance capabilities or reconnaissance scouts. Without this targeting support, the *Badger-Bs* would have to burn even more of their precious fuel attempting to redetect the battleforce. This would have cut their effective combat radius even further.\(^{81}\)

The Soviets quickly addressed their anti-ship missile range and homing limitations as well as the raid scouting problem. Their *K-10S* (NATO designation: *AS-2 Kipper*) and *KSR-2* (NATO designation: *AS-5 Kelt*) anti-ship missile systems of the early 1960s allowed a new *Tu-16* variant dubbed *Badger-C* to fire from a stand-off distance of approximately 145 miles. While the *Badger-C* still had to provide a midcourse guidance reference radar beam for the *Kippers* and *Kelts*, these missiles now carried onboard active terminal homing radars that allowed the *Badger-C* to break off once the missiles closed to within approximately 25 miles of their targets. These *Badger-Cs* were also supported by specially-outfitted, unarmed reconnaissance *Badgers* whose

---

\(^{81}\) Ibid, 134, 136-137, 143.
mission was to cue their missile-armed brethren. The ‘pathfinder’ Badgers used RF direction-finding to silently localize an enemy battleforce, then lit off their onboard radars to provide the missile-armed bombers some distance behind them with precise targeting data. This way, Kipper and Kelt-armed Badger-Cs could fire from far beyond the U.S. Navy’s then-current CAP coverage. The trade-off was that these larger and heavier missiles cut Badger-C’s combat radius to approximately 1200 miles.\textsuperscript{82}

The ocean wide-area surveillance problem presented the Soviets with a more complex challenge. In order to take full advantage of the Badger’s combat radius, the Soviets developed a shored-based radio direction-finding network that exploited a naval battleforce’s HF radio transmissions.\textsuperscript{83} Known to the Soviets as Krug, this national-asset system networked multiple HF radio direction-finding stations to crossfix the battleforce’s approximate position up to 8000 nautical miles away. Multiple HF transmission intercepts over time yielded the battleforce’s approximate course and speed. Crossfix precision decreased the further the transmitting contact was from the Krug receivers, but was nevertheless more than adequate to cue bomber raids against U.S. battleforces if they steamed within pathfinder Badger range.\textsuperscript{84}

The U.S. Navy did not become aware of Krug until 1964. That year, Soviet maritime reconnaissance aircraft began flying long distance direct intercepts of U.S. naval battleforces without conducting large-AOU redetection searches as they entered the battleforce’s operating areas. These aircraft and other similar ‘second layer’ surveillance and reconnaissance assets such

\textsuperscript{82} Ibid, 143-147.
\textsuperscript{83} In the pre-satellite era, naval beyond line-of-sight communications could only be accomplished using HF radio. Since an HF radio’s range was often a function of its transmit power, communications with shore-based commanders or other distant battleforces required very high power transmissions. This allowed HF waves to successfully bounce off the Earth’s ionosphere and reach receivers hundreds or even thousands of miles away. Unfortunately, the omnidirectional nature of these transmissions meant that enemy direction-finders were just as capable of detecting them.
\textsuperscript{84} Friedman, Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars, 217, 335.
as Soviet picket-station surface combatants, submarines, and ELINT-gathering auxiliary ships (also known as AGI) could also cue or be cued by Krug. Detection reports from Krug, picket ships, and scout aircraft were fused into actionable targeting data by a central entity that Western military analysts dubbed the Soviet Ocean Surveillance System (SOSS). SOSS further demonstrated its effective peacetime reach in 1968 when its operators guided a Soviet November-class nuclear-powered submarine on a high speed, long distance intercept of U.S. Navy aircraft carrier crossing the Western Pacific. The implication was that Western battleforces could no longer afford lax HF communications discipline if they wanted to sustain their open ocean sanctuary.

*The First Countermove: Rebirth of U.S. EW and Deception (1958-1968)*

The two most obvious defensive measures against these Soviet capabilities were to reduce reliance on HF communications and to push CAP stations further out from the center of the battleforce. Radar-equipped Airborne Early Warning (AEW) aircraft and longer-ranged jet fighters implemented the latter of these two measures by providing U.S. carrier battle groups with greater defense-in-depth. U.S. Navy use of restrictive RF Emissions Control (EMCON) measures delivered the other half of the solution. In 1963, a U.S. Navy carrier battle group steaming east of Japan avoided discovery by second-layer SOSS assets when it completely

---

85Ibid, 217-219, 335.
86 The U.S. Navy initially did this using its then-new E-1 Tracer AEW aircraft and the F-4 Phantom missile-armed fighter. To defend against Badger-Cs armed with the longer ranged AS-2 and AS-5 anti-ship missiles, the Navy established requirements for a more capable future AEW and fighter pair. These requirements also provided for a new large air-to-air missile the fighter could use to shoot down a bomber from a hundred miles away. This development effort produced the famous E-2 Hawkeye, F-14 Tomcat, and AIM-54 Phoenix missile CAP system of the 1970s and 1980s.
87 The U.S. Navy had conducted extensive RF EMCON experiments during the Haystack exercise series of the late 1950s. The Haystack series also trialed various deceptive battleforce formations as well as decoy group concepts. See Angevine, “Hiding in Plain Sight: The U.S. Navy and Dispersed Operations Under EMCON, 1956-1972,” 80-84.
refrained from making HF radio transmissions. The next year, a carrier battle group crossing the North Atlantic split itself into a large decoy group that transmitted HF freely and a small HF EMCON group centered on the carrier. Only the decoy group was intercepted by Soviet maritime reconnaissance aircraft. Most impressively, in 1968 a carrier in the Mediterranean avoided SOSS detection for five weeks by maintaining near-constant HF EMCON. Its short HF transmission periods were primarily conducted at night so that it could use deceptive lighting schemes and high speed sprints once it restored EMCON to prevent redetection by second-layer SOSS assets. Throughout the 1960s, the U.S. Navy found that battleforces using EMCON could only be detected if they encountered a second-layer asset by chance.\textsuperscript{88} That chance could be readily reduced by intercepting these SOSS scouts far from the battleforce’s inner screen in the event of a shooting war.

U.S. Navy planners nevertheless understood that although neutering Krug made efficient surveillance and reconnaissance by second-layer SOSS assets harder, it did not neutralize those assets’ abilities to methodically search for and target U.S. battleforces on their own. This was especially true whenever U.S. battleforces’ steamed in confined seas such as the Mediterranean or maintained relatively-fixed operating stations off the Vietnamese coast. EW and the deception tactics it enabled emerged as a significant part of the American solution.

U.S. Navy tactical deception philosophy from the Second World War onward was predicated on the principle that any warship could mimic at least a few elements of a higher-value warship’s electronic, acoustic, and visual signatures. Since High Value Units (HVU) such as aircraft carriers and amphibious warships never emitted all of their telltale long-range-detectable signatures simultaneously, selective simulation of a few HVU telltales by a non-HVU could greatly confuse an attacker’s targeting picture. To this end, the U.S. Navy developed the

\textsuperscript{88} Friedman. \textit{Network-Centric Warfare}, 233-234.
AN/ULQ-5 and AN/ULQ-6 blip-enhancers and installed them on minesweepers and destroyers.\(^89\) These small surface combatants also broadcasted bogus air traffic control communications and radio-navigation beacon signals to make them look even more like aircraft carriers. These decoy ships allowed actual carriers to evade Soviet scouts so long as the carriers curtailed use of their telltale emitters. When used during U.S. Navy nuclear warfare exercises of this era, the above deception approach demonstrated the theoretical possibility of concealing a carrier long enough for it to get close enough to the Soviet coast so that its air wing could execute a land-attack nuclear strike.\(^90\) Even when the actual carrier battle group was located by the Soviets, the U.S. Navy found that pathfinder Badgers and other Soviet reconnaissance and targeting platforms could not distinguish between the carrier and the decoys from beyond visual range.\(^91\) Without accurate targeting cues from pathfinders, Badgers could neither launch their missiles from outside the reach of battleforce CAP nor even be sure of what they had launched their missiles at.

If EMCON or deception had failed to prevent the Soviets from locating and targeting a U.S. Navy battleforce, EW ‘softkill’ systems backed up the battleforce’s air defense interceptor missiles. Just as small surface combatants’ RF noise jammers had been used to sever the Fritz-X’s radio-control link during the Second World War, similar techniques were developed for use against Badger radars’ missile guidance beams. If neutralizing the guidance beams proved ineffective, the jammers could be reset to seduce the missiles’ terminal homing radars away from HVUs. Unfortunately, this meant the missiles would instead lock onto the escort warships employing the jammers. Losing a few escorts, though, was deemed preferable to losing a

\(^{89}\) Blip enhancers amplify enemy radar pulses. A small ship equipped with a blip enhancer can make its radar reflection indistinguishable in size from a large ship’s radar reflection. Blip enhancers can be mechanical; i.e. objects with shapes and edges designed to reflect much more of a radar pulse’s energy than the ship carrying the objects would do naturally. They can also be electronic, i.e. amplify and rebroadcast a pulse as the AN/ULQ-5 and 6 did. An enemy can defeat a blip enhancer, though, by using more complicated waveform designs and signal processing techniques. The Soviets were eventually able to do so against the AN/ULQ-5 and 6.


\(^{91}\) Friedman, *Seapower and Space*, 148.
carrier.\textsuperscript{92} Chaff decoys that released large clouds of radar-reflecting metallic strips in the air near a targeted warship provided a less-sacrificial alternative for seducing inbound missiles.\textsuperscript{93}


In the late 1960s, the Soviets introduced a second generation maritime reconnaissance-strike system intended to offer greater tactical responsiveness and flexibility than the \textit{Badger-Kipper/Kelt} system. The new system consisted of the supersonic \textit{Tu-22K} (NATO Designation: \textit{Blinder-B}) bomber and the \textit{Kh-22} (NATO Designation: \textit{AS-4 Kitchen}) anti-ship missile. \textit{Kitchen} appeared far more menacing than its predecessors as it offered a maximum stand-off range of about 250 miles, was capable of top speeds of at least Mach 2.5, and carried a powerful terminal radar seeker that allowed it to autonomously home on its target from the moment of a high altitude launch. The Soviets believed \textit{Blinder-B} could sprint to the \textit{Kitchen}’s maximum range, fire its single \textit{Kitchen} off of the tactical picture relayed by pathfinders, and then retire from the scene before being intercepted by U.S. Navy CAP. \textit{Blinder-B}, however, had not been designed from inception to carry \textit{Kitchen} and could only fly approximately 600 miles at supersonic speed when armed with the missile. Also, the U.S. Navy’s newly-debuted CAP team of \textit{E-2 Hawkeye} AEW radar aircraft and long-range \textit{F-14 Tomcat} fighters made it theoretically possible to break up bomber raids by shooting down pathfinder aircraft long before the pathfinders’ radars could

\textsuperscript{92} Dwyer, 102.

\textsuperscript{93} If an RF-reflective metal is cut into a thin strip the length of half of the threat radar’s wavelength, it will resonate when exposed to the threat radar’s pulse. A ‘cloud’ of these chaff filaments will therefore have a massive radar reflection. The cloud can be used to deceive adversary radars as long as prevailing air currents keep it intact and in place relative to the defended warship. Even if the adversary’s radar can discriminate chaff clouds from valid targets as most modern radars can, a chaff cloud placed in the radar’s line-of-sight to the defended warship can delay or prevent the radar’s direct detection of the warship. Of course, the adversary will conclude that there is something behind the chaff cloud that needs to be investigated further. See Payne, 93.
detect U.S. battleforces. Any missile-armed bombers that wandered towards the CAP’s ambush stations would likely fare no better.\(^94\)

The Soviets’ initial solution to the CAP problem was employing destroyers and pathfinder bombers as sacrificial peacetime ‘tattletale’ scouts. Tattletales’ sole mission was to visually identify which warships in a battleforce were HVUs, then provide that targeting data to SOSS. In the event of a war, SOSS could use this information to cue a massive first missile salvo against the battleforces being tracked. U.S. peacetime rules of engagement allowed the tattletales to routinely steam or fly to the centers of battleforces, then loiter there until they either left of their own accord or could be evaded. In doing so, tattletales negated the U.S. Navy’s decoy ship concept. The Soviets accepted that tattletales would likely not survive the first minutes of a war, but considered their loss a small price to pay for the crippling first salvo they could theoretically enable.\(^95\)

The Soviets no doubt understood, though, that their tattletale concept would not work following the first salvo. U.S. Navy warships that survived the first salvo and battleforces that had successfully evaded detection prior to it would thereafter destroy any Soviet scout well before the scout could visually identify new prey. Without tattletales, the Soviets could not counter U.S. Navy decoy ships and deception groups for the duration of a war. As NATO’s

\(^94\) Soviet submarines and surface combatants armed with early-generation long-range anti-ship missiles also depended on the tactical picture relayed by specially-modified pathfinder bombers. Killing the pathfinders meant that the submarines and surface combatants could not effectively target and fire missiles at a naval battleforce from over the horizon. Friedman, *Seapower and Space*, 142, 149-152, 154-157, 343.

\(^95\) Friedman, *Network-Centric Warfare*, 222-223. Soviet tattletale destroyers were generally armed with short range anti-ship missiles. Soviet first salvo tactics likely called for the armed tattletales to launch these missiles against any aircraft carriers they held in visual track as the opening move of a notional war. See Polmar, *The Naval Institute Guide to the Soviet Navy*, 29. If the tattletales could inflict sufficient damage on the carriers, the carriers might be unable to launch their full fighter complements to augment their CAP stations’ defenses against inbound maritime bomber raids. The more Soviet bombers that survived the unaugmented CAP, the more anti-ship missiles could be launched against the battleforces. The more anti-ship missiles launched, the more likely that the raid would succeed in crippling or sinking the carriers and any other HVUs present. The short-range anti-ship missile threat posed by armed tattletale destroyers helped prompt U.S. Navy investment in point defenses such as the basic *Sea Sparrow* missile system and its NATO *Sea Sparrow* successor. For an overview of U.S. Navy point defense missile system development, see Friedman, *U.S. Destroyers: An Illustrated History*, 225-226, 361.
remaining fleets would also cease use of HF communications after hostilities broke out, *Krug* would become useless. This drove the second element of SOSS improvements for the 1970s: space-based maritime surveillance and targeting.

The Soviets developed two types of satellites for this mission. The first, known as *US-A* by the Soviets and the Radar Ocean Reconnaissance Satellite (RORSAT) by NATO, used a SAR to scan the ocean’s surface for large ships. Following eight and a half tumultuous years of development and testing, the Soviets launched their first operational RORSAT in 1974. RORSAT was designed to download its contacts’ coordinates only on command from the SOSS ground control station in Moscow, and it could execute the download only for the few minutes per orbit it flew within the station’s line of sight. In theory, SOSS operators could use the data received from RORSAT pairs whose orbits allowed them to scan the same waterspace 20-30 minutes apart to calculate detected ships’ approximate courses and speeds. After the two RORSATs revisited the same area 90 minutes after their respective initial passes, SOSS operators could confirm their tactical picture’s accuracy. Specially-equipped surface combatants, submarines, and bombers could also receive direct downlinks from RORSATs, but to do so the Moscow ground station had to instruct the RORSATs to transmit a ‘download in the blind’ when they passed over a designated ocean area at a designated time. This meant an equipped ‘shooter’ had to be guided by SOSS controllers into the designated area on time—hardly a simple coordination task amidst the friction of war. While two-hour time-latency RORSAT contact coordinates were considered acceptable by SOSS controllers, it is important to understand that a warship steaming at 30 knots could mathematically be anywhere within a 11300 square nautical mile AOU after

---

96 As will be discussed later in this section, evidence from the 1980s strongly suggests that RORSAT’s SAR lacked the sensitivity and discrimination capabilities needed to image its contacts.
that length of time.\textsuperscript{97} RORSAT, therefore, could provide cueing to help second-layer SOSS assets redetect a battleforce but could not provide targeting-quality data for ‘shooters’ except under ideal circumstances.\textsuperscript{98} The Soviets did not maintain constant RORSAT presence in orbit, but rather launched one or two at a time in response to Western naval activity.\textsuperscript{99}

The second satellite type, known as \textit{US-P} by the Soviets and the ELINT Ocean Reconnaissance Satellite (EORSAT) by NATO, employed RF direction-finding/ELINT sensors. Although the Soviets launched several general-purpose ELINT satellites during the 1960s, most were incapable of detecting U.S. Navy radars’ emissions. EORSAT was designed to fill this specific Soviet capability gap.\textsuperscript{100} First launched in 1975, EORSAT could localize a radar-transmitting U.S. warship within a 1.3 nautical mile AOU. If this or another EORSAT later redetected the same warship, SOSS operators could use the fix history to estimate the warship’s approximate course and speed. More importantly, SOSS operators could correlate EORSAT data with RORSAT contacts. This in turn informed their decisions on where to dispatch second-layer SOSS assets. Like RORSAT, EORSAT stored its data until the Moscow ground station directed a download to either the SOSS fusion center or a waiting missile-shooter at sea.\textsuperscript{101} This delayed reporting problem was amplified by the hours-long gaps between EORSAT revisits of a given area. Revisit gaps of 6-14 hours were common for waters bordering the Soviets’ northern periphery, and gaps of over a day were not uncommon closer to the equator. Although the

\textsuperscript{97} A warship will advance 60 nautical miles in two hours when steaming at 30 knots. Since the 60 nautical miles represent the circular AOU’s radius, we can use the formula for calculating a circle’s area to find the AOU’s area.


\textsuperscript{99} RORSAT orbits tended to have very low orbital altitudes (about 160 miles) compared to other reconnaissance satellites. The low orbit probably was a compensatory measure for the RORSAT SAR’s poor sensitivity. Since its orbital altitude was within the upper atmosphere’s bounds, drag-induced orbital decay resulted in short RORSAT operational lifetimes. These satellites’ expense probably made the Soviets hesitate to launch them until a Western naval battleforce either approached the Soviet maritime periphery or Western naval activity in general increased above a particular threshold. See Grahn, “The US-A program (Radar Ocean Reconnaissance Satellites - RORSAT) and radio observations thereof.”

\textsuperscript{100} Friedman, \textit{Network-Centric Warfare}, 221, 339.

\textsuperscript{101} Friedman, \textit{World Naval Weapon Systems}, 16.
Soviets were expected to surge additional RORSATs and EORSATs into orbit if a NATO-Warsaw Pact war seemed imminent, the Soviets’ lack of a global data relay satellite constellation nevertheless meant even an expanded space-based maritime surveillance network could not have provided SOSS with consistently timely contact data.\textsuperscript{102}

One additional 1970s-era Soviet maritime strike system bears mentioning as it foreshadows much of the emerging Chinese ASBM threat. Unsatisfied by the length of time it took a bomber raid to reach a targeted battleforce, the Soviets strove throughout the 1960s to develop an anti-ship variant of their then-new R-27 (NATO designation: SS-N-6 Serb) submarine-launched ballistic missile. This first ASBM, designated by Western intelligence as SS-NX-13, homed on targets using a radar direction-finding sensor tuned to detect only specific U.S. Navy radars. Since this approach could not offer the homing precision of a terminal radar seeker, SS-NX-13 carried a megaton-class nuclear warhead. This way, the warhead could miss the targeted warships by few tenths of a mile and still annihilate it along with any nearby escorts. SS-NX-13 was to be carried aboard Soviet Project 667A (NATO designation: Yankee) nuclear-powered ballistic missile submarines, and a fire control system was developed that would have allowed a Yankee’s crew to target the missile against warships up to 600 nautical miles away using downloaded RORSAT/EORSAT contact data. The Soviets never operationally deployed SS-NX-13, however, as the first Strategic Arms Limitation Talks (SALT) treaty counted submarines’ ballistic missile tubes against the treaty’s strategic missile inventory limits. The Soviets were apparently unwilling to trade away any part of their strategic nuclear arsenal for a tactical ASBM capability.\textsuperscript{103}


49
The contemporary Chinese ASBM threat is foreshadowed in another interesting way. Several early-1970s statements by the Soviets’ then-Minister of Defense Andrei Grechko and Admiral of the Fleet Sergei Gorshkov implied possible use of land-based nuclear-armed MRBMs against U.S. carrier battle groups steaming near the Soviet periphery at the start of a nuclear war.\textsuperscript{104} No other open source evidence appears to exist supporting their claims. It is therefore impossible to tell whether their statements were misinterpreted, amounted to deterrent posturing, or reflected war plans that were rendered obsolescent by later Soviet maritime bomber and conventional anti-ship missile capabilities.


The 1970s marked tactical deception’s formal integration within U.S. Navy concepts of operations. Innocuous-sounding Fleet Composite Operational Readiness Groups (FLTCORGRU) were established in the Atlantic and Pacific Fleets with the mission of training U.S. Navy crews and commanders in cover and deception. FLTCORGRUs also provided forward deployed battleforces with special systems and personnel to augment warships’ inherent deception capabilities.\textsuperscript{105} The most important of these FLTCORGRU systems, the AN/SSQ-74 Integrated Cover and Deception System (ICADS), allowed a ship to simulate other warships’ telltale signatures. ICADS consisted of a ‘trailer’ that could be temporarily installed on a ship’s flight deck or even on an amphibious landing craft.\textsuperscript{106} Early ICADS variants could simulate an aircraft carrier’s unique radars and radio communications. Later ICADS variants added a RF false target generator designed to specifically spoof pathfinder bombers’ radars and RORSAT, as well as a towed element designed to spoof submarines’ sonars by transmitting a carrier’s acoustic

\textsuperscript{104} McCGwire, \textit{Military Objectives in Soviet Foreign Policy}, 507-508.
\textsuperscript{105} Dwyer, 127.
\textsuperscript{106} “NWP 3-02.12: Employment of Landing Craft Air Cushion (LCAC),” 7-13 - 7-14.
signature into the water.\textsuperscript{107} The U.S. Navy viewed ICADS as a critical countermeasure against SS-NX-13.\textsuperscript{108}

Other EW measures proved equally useful. First-generation Ultra-High Frequency (UHF) communications satellites and highly-directional shipboard satellite radio antennas granted the U.S. Navy an alternative to HF radio, thereby denying Krug the signals it needed to work.\textsuperscript{109} Building upon existing HF EMCON procedures, the U.S. Navy also developed tactics for employing ‘middleman’ aircraft as long-range line of sight radio relays between warships. These radios used the Very-High Frequency (VHF) and UHF bands, neither of which could be reflected by the ionosphere. A radio direction-finding sensor therefore had to be within direct line of sight of a transmitting warship or aircraft to intercept these signals. Taking advantage of this fact, E-2 Hawkeye AEW aircraft were used to handle carriers’ air traffic control duties so that the carriers could remain at EMCON.\textsuperscript{110}

\textsuperscript{107} A false target generator is the next deceptive countermeasure technology beyond a blip enhancer. A false target generator records and analyzes the enemy’s complicated radar pulses. It inserts slight frequency shifts or amplitude variations into the recorded enemy pulse, and then transmits it towards the enemy sensor. Depending on the enemy sensor’s vulnerabilities and the false target generator’s selected EW techniques, it can either fulfill the blip enhancer role of making a ship or decoy ‘look’ like a different type of object or it can project ‘phantom’ false targets at various distances around itself. This is obviously useful both for counter-targeting as well as for defeating an inbound missile’s homing radar.

U.S. Navy acoustic deception tactics were developed and tested during the Uptide exercise series of the late 1960s and early 1970s. Pre-ICADS acoustic deception devices demonstrated during Uptide were able to repeatedly lure the exercises’ Opposition Force submarines away from defended aircraft carriers. See Angevine, 84-88.

\textsuperscript{108} Friedman, \textit{Network-Centric Warfare}, 237, 343.

\textsuperscript{109} Directional antenna technology enables extremely-narrow radio beams for line of sight communications systems. This means an ELINT sensor can only intercept a highly-directional radio transmission if it is lucky enough to fly through the beam.

\textsuperscript{110} Friedman, \textit{Network-Centric Warfare}, 237-238. A major side effect of these EMCON tactics was that battleforce commanders found it more difficult to quickly communicate with their subordinate units and vice versa. This placed a high premium on the battleforce commander developing and disseminating his tactical intentions, including explicit delegation of local decision-making authority to unit-level commanders as well as preplanned unit-level and battleforce-level responses to changes in the tactical situation, well in advance of a given operation. This also drove development of simple ‘brevity’ code systems that allowed units to efficiently coordinate their tactical actions as well as relay the battleforce commander’s orders via VHF and UHF line of sight radio. While these measures allowed battleforces to conduct decentralized, dispersed, high tempo operations, it came at the price of the entire battleforce sharing a verbally-disseminated, common, and timely tactical picture. See Angevine, 89-91. The common tactical picture problem was partially addressed beginning in the 1960s by fielding automated battleforce-level tactical datalinks. These datalinks allowed any participating U.S. Navy or allied navy unit to see the positions,
Warship crews also learned to periodically reconfigure their radios and radars as a means of complicating any Soviet attempts to correlate specific RF transmitter systems with specific warships. As an additional countermeasure, U.S. Navy EA-6B Prowler electronic attack aircraft gained the ability to jam pathfinders’ radars. Prowlers and shipboard EW systems could also presumably use their existing communications jamming capabilities against pathfinders’ and tattletales’ radios. This could prevent or disrupt the scouts from relaying their targeting reports to bomber raids or other ‘shooters.’

Some U.S. Navy EW and deception efforts specifically targeted EORSAT. One such countermeasure was to install the then-new AN/SPS-49 long-range air search radar on HVUs as well as on surface combatants. Prior to this, the U.S. had installed different air search radars on different warship types to make it harder for the Soviets to simultaneously jam all of them during bomber raids. By standardizing on a single air search radar model, the U.S. made it impossible for SOSS operators to tell whether an EORSAT-detected AN/SPS-49 signified the presence of a

---

111 Warship crews also learned to periodically reconfigure their radios and radars as a means of complicating any Soviet attempts to correlate specific RF transmitter systems with specific warships. As an additional countermeasure, U.S. Navy EA-6B Prowler electronic attack aircraft gained the ability to jam pathfinders’ radars. Prowlers and shipboard EW systems could also presumably use their existing communications jamming capabilities against pathfinders’ and tattletales’ radios. This could prevent or disrupt the scouts from relaying their targeting reports to bomber raids or other ‘shooters.’

112 Friedman, World Naval Weapon Systems, 408.

113 Vego, Soviet Naval Tactics, 219.
carrier or a frigate. Since the U.S. tracked Soviet satellites in orbit, U.S. Navy battleforces could also schedule EMCON periods timed to coincide with EORSAT passes overhead.\textsuperscript{114}

These EW technologies and tactics could not be easily countered. One U.S. carrier in 1969 operated at EMCON during three days of simulated air strikes in the Yellow Sea and Sea of Japan before being detected by Soviet pathfinders’ radars. Two years later, another carrier operating in the Norwegian Sea avoided detection for almost two days by maintaining HF EMCON while a deception group consisting of several surface combatants and a separate battleforce-simulating inport deception unit distracted Soviet attention. A third carrier remained undetected for over half a month during a 1972 transit from Florida to the Indian Ocean by employing radar EMCON when Soviet ELINT satellites were within line of sight. In the Mediterranean, battleforces that employed EMCON after shaking the tattletales following them often avoided redetection by new tattletales or other scouts.\textsuperscript{115}

Terminal EW defenses against Soviet anti-ship missiles were also proven in combat during this period, albeit not by the U.S. Despite its otherwise overwhelming victory in the 1967 Six-Day War, a month after the ceasefire Israel lost one of its Second World War-vintage destroyers to several Egyptian Soviet-made P-15 (NATO designation: SS-N-2 Styx) anti-ship missiles. In the aftermath, Israel rushed to develop EW tactics and technologies for defending against Styx. Six years later during the Yom Kippur War, the Israeli Navy used these countermeasures to defeat up to 54 Syrian and Egyptian Styx over the course of several night battles. By using low-flying helicopters and warship-launched chaff clouds to decoy the Styxs’

\textsuperscript{114} Friedman, \textit{Network-Centric Warfare}, 237-238.
\textsuperscript{115} Ibid, 234-235.
radars, the Israelis were able to decisively employ their shorter-ranged Gabriel anti-ship missiles against the Syrian and Egyptian flotillas.\textsuperscript{116}

The Final Move: Soviet Maritime Reconnaissance-Strike Capabilities at Their Peak (1979-1991)

1981 witnessed Soviet introduction of their final and most capable maritime bomber, the Tu-22M3 (NATO designation: Backfire-C). Backfire-C, unlike Blinder-B, was designed from inception to employ an improved variant of the Kitchen missile. Estimates still vary for Backfire-C’s unrefueled attack radius. Credible sources suggest the combat-loaded Backfire-C could reach anywhere between 2300 and 2900 miles when flying at high altitudes and subsonic speeds. Backfire-C’s endurance declined, however, when it flew at supersonic speeds and/or low altitudes. All the same, Backfire-C’s impressive reach made it the first Soviet maritime bomber capable of indirectly approaching a targeted battleforce. Whereas Blinder-B’s relatively short range meant it could only attack a battleforce from its initial axis of approach, Backfire-C raids could encircle a battleforce and then attack it simultaneously or sequentially from multiple axes. As an added survivability measure, Backfire-Cs could approach from beneath a battleforce’s radar horizon, quickly climb to high altitude to launch its missiles, and then retire at supersonic speed.\textsuperscript{117}

The Soviets’ initial Backfire-C concept of operations may not have included a need for pathfinder support. At least one credible source claims Backfire-C carried a RORSAT downlink receiver to support over-the-horizon targeting of a battleforce’s major warships without the need

\textsuperscript{116} See 1. Friedman, Seapower and Space, 167, 169-170, 345; 2. Kopp, “Tupolev Tu-22M3 Backfire C Bomber - Missile Carrier.”
to sacrifice manned scouts.\footnote{Ibid} A second source claims SOSS controllers could radio any Soviet maritime bomber that was already in the air with RORSAT/EORSAT-derived targeting data.\footnote{Friedman, \textit{Seapower and Space}, 171.}

Nevertheless, significant circumstantial evidence suggests that pathfinders ultimately remained necessary due to RORSAT’s and EORSAT’s aforementioned capability limitations. For one thing, the Soviets introduced specially-modified pathfinder \textit{Backfires} in 1984.\footnote{Ibid, 171.} In fact, Soviet doctrinal sources published as late as 1990 implied routine pathfinder use in support of all Soviet maritime bombers even in situations where space-based targeting data was available.\footnote{Vego, \textit{Soviet Naval Tactics}, 212-214, 217.} It is unlikely the Soviets would have taken these steps if RORSAT and EORSAT had rendered pathfinders totally obsolete.

Another piece of evidence regarding the Soviets’ continued need for pathfinders comes from declassified early 1980s-vintage U.S. intelligence analyses. The U.S. had concluded by this time that while RORSAT could detect large ships such as aircraft carriers in good weather and small ships such as destroyers in perfect weather, heavy seas and rain effectively blinded the satellite’s SAR.\footnote{RORSAT’s radar operated using the X-band of the RF spectrum. While X-band’s short wavelength gives it very high range resolution, it has difficulty dealing with the radar reflections from RF-scatterers such as water droplets in the air or heavy swells on the ocean’s surface. Any modern radar needs to use sophisticated signal processing techniques to discriminate valid contacts from ‘clutter’ sources such as these, and the shorter the radar’s wavelength the more this becomes necessary. RORSAT’s clutter suppression capabilities were evidently inadequate for its use of the X-band.} Considering the North Atlantic’s typical weather conditions for much of any given year, this did not bode well for complete Soviet reliance on space-based sensors for maritime targeting.\footnote{Grahn. “The US-A program.”} Although the U.S/ intelligence community respected RORSAT’s weather-permitting ability to detect carriers operating near the Soviet Union’s northern maritime periphery, they judged RORSAT incapable of positively identifying contacts on its own. They
also judged that the low number of RORSATs in orbit during peacetime made them incapable of routinely tracking or targeting U.S. battleforces elsewhere in the world. While these analyses incorrectly describe RORSAT and EORSAT as capable of directly providing ‘shooters’ with real-time tactical pictures, they do interestingly note that both satellite types were susceptible to countermeasures and that EMCON was very effective against EORSAT.124

A third form of evidence comes from a ‘sea story’ published online in 2006 by a retired U.S. Navy E-2 Hawkeye officer. In his 1981 anecdote, the officer recounts Soviet use of pathfinders to support a simulated Badger raid against his carrier battle group when it steamed significantly closer to the Kola Peninsula than any other U.S. Navy surface force had in many years.125 One of the pathfinders, in fact, performed the ‘tattletale’ visual targeting role by overflying the officer’s aircraft carrier prior to the Badgers’ arrival at missile-firing range. While no Backfire-Cs apparently participated in this simulated raid, SOSS controllers in theory still could have radioed the Badgers with Moscow-downloaded RORSAT/EORSAT data.126 Given that the warships in the officer’s battle group were operating at EMCON prior to encountering the pathfinders, EORSAT could not have been used to guide the Badgers’ approach let alone provide them with targeting-quality data.127 The lack of EORSAT data also means that SOSS operators could not have remotely distinguished the carrier from the battle group’s other ships since there were no shipboard radar emissions to correlate with individual RORSAT contacts.

125 The sea story appears to take place during the “Ocean Safari/Magic Sword North” exercises of September 1981. Though the blogger does not give a specific date for his story, the name of his carrier and the scheme of maneuver in an operations chart he posted on his blog to illustrate his story correlate to that exercise. This is a key detail, as at least one RORSAT was in orbit during that exercise. Magic Sword North’s importance will be discussed in this paper’s next subsection. See 1. Steeljaw Scribe, “Badgers and Buccaneers and Bears…(Pt 1);” 2. Grahn, “The US-A program.”
126 Recall that Backfire-Cs were supposedly the only type of Soviet maritime bomber equipped with RORSAT/EORSAT direct downlink receivers.
127 Steeljaw Scribe, “Badgers and Buccaneers and Bears…(Pt 3).”
The only other way SOSS could have directly provided the Badgers with space-based targeting-quality data as opposed to general location-cueing data was if SOSS operators had received a RORSAT download, derived a tactical picture from it, and radioed this picture to the Badgers before the data became too old and the battle group’s AOU grew too large. Soviet use of tattletale pathfinders in the above vignette strongly suggests that this was not what happened.  

It is reasonable to conclude that RORSAT/EORSAT data could not substitute for pathfinders and tattletales during the early 1980s at minimum, even when a U.S. battleforce steamed only a few hundred miles off the Soviet coast.

Although Backfire-C certainly posed a far more stressing threat to U.S. Navy battleforces’ active defense schemes and resources than did earlier Soviet maritime bombers, the Backfire-C’s apparent continued reliance on pathfinders meant that U.S. Navy CAP could continue to break up raids if the pathfinders were neutralized before their radars detected the battleforce’s ships. While the U.S. Navy developed and demonstrated new tactics and concepts of operations to do just this, some of these measures risked pressuring carrier battle groups’ air defense resources to their limits. This served to further increase EW’s and tactical deception’s importance.

---

128 Even if the Soviets had extremely low time-latency RORSAT contact data, the lack of EORSAT data handicapped their ability to aim anti-ship missiles using space-based sensors alone. The only way the Soviets could know with some measure of confidence which RORSAT contacts represented valid high-priority targets was if tattletale pathfinders were dispatched to penetrate the carrier battle group, visually identify contacts, and report this targeting-quality information to the inbound raid and/or SOSS controllers. Otherwise, maritime bomber crews would have to fire their missiles somewhat blindly at a U.S. battle group without knowing whether the targets they had selected were HVUs or false targets. While this would still pose a severe threat to the battle group, the raid would face a lower probability of incapacitating or sinking U.S. HVUs at a high cost in expended missiles than if those missiles had been concentrated against contacts definitively known to be HVUs. In any event, a raid without pathfinder support would need to follow a very strict flight timeline in order to be close enough to the battleforce for any RORSAT data radioed by SOSS to be timely enough for targeting purposes. Any bomber delays taking off, forming up, and flying out towards the battle group would result in increased RORSAT contact AOU sizes. These contact identification and flight timeline challenges offer a compelling explanation of why the Badgers in the anecdote were supported by pathfinders despite the possible availability of RORSAT data.

129 For a discussion of the U.S. Navy’s Outer Air Battle tactics of the 1980s, see Friedman, Seapower and Space, 234-239.
One additional Soviet maritime surveillance capability of this era bears mention. At some point during the 1980s, the Soviets allegedly discovered that the non-directional downlink from the U.S. Navy’s UHF communications satellites could be exploited to localize the warships transmitting via those satellites. This provided SOSS with a new, *Krug*-like radio direction-finding capability that could be used to cue searches by second-layer SOSS assets. As the U.S. Navy apparently did not recognize and correct for this vulnerability until after the 1991 Gulf War, any warship using UHF satellite communications potentially disclosed its approximate location to SOSS even if the warship was otherwise practicing EMCON. The location estimate was insufficiently precise for targeting purposes, though, so second-layer SOSS assets were needed as before to redetect and target the warship.\(^{130}\)


Other than renaming the two FLTCORGRUs’ as Fleet Deception Groups (FLTDECGRU) in 1986, U.S. Navy EW and tactical deception against SOSS during the 1980s largely built upon the systems and techniques developed over the course of the previous decade.\(^{131}\) One of these systems, the then-new *AN/SLQ-32* series EW suite, provided U.S. Navy warships with automated threat radar detection and identification capabilities for the first time.\(^{132}\) The *AN/SLQ-32* suite variant installed in HVUs and cruisers included active EW capabilities that reacted automatically to the threat radar detected.\(^{133}\)

---

\(^{130}\) Even though these communications satellites were in geostationary orbit, their orbits were not truly ‘stationary.’ Since the satellites functioned as communications relays, their slight motion relative to the Earth below induced small Doppler shifts into the uplinked signals they rebroadcast. Soviet ELINT stations located within the satellite’s downlink footprint could analyze the signal’s Doppler shift. The shift’s size corresponded to the position of the transmitting warship relative to the satellite. As the Soviets could track the satellite’s position, they could use measurements of the shifts to estimate the transmitting warship’s location. See Friedman, *Network-Centric Warfare*, 238-239.

\(^{131}\) Dwyer, 127-130.


\(^{133}\) Lewis, “*AN/SLQ-32(V) Operator’s Handbook: Volume 1,*” 2.
Anti-RORSAT EW and deception also hit its stride during the 1980s. Destroyer-mounted ICADS units as well as naval aircraft-laid chaff clouds made it extremely difficult for RORSAT to distinguish large warships from false targets. The then-new *Ticonderoga*-class guided missile cruiser’s Aegis area air defense system granted U.S. Navy surface combatants the ability to reliably defend themselves and HVUs against mass raids of *Kitchens* and other Soviet long-range anti-ship missiles for the first time. This gave the *Hawkeye/Tomcat* CAP combination greater flexibility to focus on distant engagement of inbound pathfinders and bombers. In turn, the increased defense-in-depth enabled use of dispersed warship formations that from space looked nothing like the traditional ‘bullseye’ formations centered on a carrier or other HVU.  

With knowledge of RORSATs’ orbital parameters, large warships such as carriers could maneuver to present their lowest radar cross section profiles to the satellites as they passed overhead. By doing so, they made it much harder for RORSAT’s sensitivity-limited SAR to discriminate the warship from background clutter. Weather and sea state, too, provided the U.S. Navy with opportunities for cover from RORSAT.

The U.S. Navy also selectively publicized some of its anti-SOSS deception capabilities as a form of deliberate psychological warfare. This campaign sought to coerce Soviet military decision-makers and SOSS operators into routinely second-guessing radar contacts, U.S. radar emissions detections, and radio direction-finding reports sent by remote sensors to the SOSS fusion center. Over time, the U.S. Navy hoped that Soviet military decision-makers and/or SOSS operators could be conditioned into hesitating to commit scouts or combatants at crucial times unless a higher ‘burden of evidence’ was first met.

---

134 Friedman, *Network-Centric Warfare*, 238.
135 Friedman, *Seapower and Space*, 195.
136 Friedman, *Network-Centric Warfare*, 238.
Selective U.S. Navy use of EW and deception against SOSS during exercises and deployments no doubt reinforced this psychological campaign. Unlike operational data from the 1960s and early-to-mid 1970s, much of the relevant material from the 1980s remains classified or otherwise undiscovered in the U.S. Navy’s various archives. Some anecdotal reporting exists, though, that suggests extensive U.S. Navy use of EW and tactical deception against SOSS in at least one major exercise during the early 1980s. A 1997 monograph published by a historian at the U.S. Central Intelligence Agency’s (CIA) Center for the Study of Intelligence cites an investigative journalist’s account of the August-September 1981 Ocean Safari/Magic Sword North exercises as the basis for describing the nature of early 1980s U.S. Navy operations along the Soviets’ maritime periphery. While noting several reporting mistakes, the CIA historian otherwise observed that the journalist’s account of the exercises “appears to be accurate.” Although it is understood that the monograph represents the historian’s personal views and does not constitute CIA or U.S. Government endorsement of the data he presents, his citing these pieces of evidence lends circumstantial weight to their general credibility by implicit virtue of his position.\textsuperscript{137}

According to the journalist’s account, U.S. Navy leaders decided immediately prior to Ocean Safari/Magic Sword North that the exercise plans would not be disseminated via radio teletype to the participating U.S. and NATO units. Instead, as a hedge against the risk that the U.S. Navy’s encryption protocols had been compromised by Soviet intelligence, the plans were hand-delivered to each participating unit. Since the Soviets in fact had obtained the U.S. Navy’s encryption codes via the Walker spy ring, the U.S. Navy’s stringent operational security

measures prior to these exercises serve as a counterintelligence test of whether Soviet reactions to the exercises were genuine.  

Once underway, the battleforce set EMCON and transited northward using a passing North Atlantic hurricane for cover. An ICADS-equipped destroyer was tasked to steam away from the actual battleforce while simulating a ‘phantom’ carrier battle group. Upon entering the Norwegian Sea, the battleforce dispersed into formations designed to prevent SOSS operators from using RORSAT data to recognize contact location patterns consistent with traditional carrier battle group formations. An unidentified EW system aboard one of the carriers was also used to jam the one RORSAT in orbit at that time. No pathfinders or other Soviet maritime reconnaissance aircraft intercepted the battleforce until it began simulating offensive operations against Soviet military targets from the northern reaches of the Norwegian Sea.

According to the U.S. Navy Second Fleet’s declassified 1981 command history report, the events during and immediately after Magic Sword North “elicited probably the most extensive reaction from Soviet naval forces in almost a decade” and provided “an ideal opportunity to…assess the Soviet capability to conduct surveillance and target allied maritime forces.” The command history also notes second-layer SOSS assets’ extensive attempts to search for the combined U.S. and NATO battleforce as it steamed northward before the exercises,

138 Vistica, *Fall From Glory: The Men Who Sank the U.S. Navy*, 106-109. The ideological bent of Vistica’s book is quite apparent from its inflammatory title. Vistica’s work suffers from glaring misinterpretations of the U.S. Navy’s 1980s Maritime Strategy and Soviet naval capabilities as well as more subtle misinterpretations regarding the nature of Soviet naval strategy. His accounts of Ocean Safari/Magic Sword North ‘81, however, are based on his personal interviews with the Admirals who led U.S. Navy forces in those exercises. The evidence specifically sourced from these interviews are what makes Vistica’s account of the exercises credible. The interview-sourced evidence is the only material from Vistica presented in this paper.

139 Vistica’s account does not mention whether any SOSS assets were dispatched to investigate this decoy. It is therefore unclear whether the ICADS destroyer drew Soviet scouting resources away from the actual battleforce. Since relevant Soviet archival material is unavailable, it is also impossible to tell what if any effect the ICADS destroyer had on SOSS operators’ North Atlantic maritime situational picture.

140 Vistica describes this jamming as bombarding the RORSAT with “dumb data.” It is therefore unclear whether the carrier’s electronic attack was noise jamming, deceptive jamming, or some form of exploitation of the RORSAT’s uplink/downlink communications system.

141 Ibid, 117, 129-134.
followed by “scores” of Soviet pathfinder flights and simulated bomber raids against the battleforce sometime after it entered the Norwegian Sea. As the U.S. Navy conducted a similarly audacious exercise within the Soviets’ Pacific periphery four years later, it is reasonable to conclude that the U.S. Navy’s leadership possessed ample faith in their fleet’s EW and deception capabilities.

Indeed, major fleet exercises of the 1980s were routinely used as proving grounds for new countertargeting tactics and concepts. A veteran analyst from the U.S. Navy’s dedicated Federally-Funded Research and Development Center, the Center for Naval Analyses, went so far to declare in 1981 that EW and deception capabilities could arguably be “the most important or most effective of all our defensive systems.”

Case Study Conclusions

As noted earlier, a Western navy’s EW defenses defeated Soviet anti-ship missiles the only time both types of systems faced off during the Cold War. This is, of course, a statistically useless sample set that solely reflects the offense-defense balance as it existed between the Israeli, Syrian, and Egyptian Navies at the time of the Yom Kippur War. The Soviets learned from these engagements and improved its subsequent anti-ship missiles’ counter-EW capabilities. In turn, the U.S. Navy and its allies did their best to collect information on these counter-EW techniques and develop new countermeasures to exploit or otherwise work around them.

---

142 “Commander Second Fleet Calendar Year 1981 Command History.”
143 Vistica, 216-218.
146 “Russian-Source Naval Anti-Ship Missiles in Action,” 57.
147 The only other widely-known use of Soviet anti-ship missiles in naval combat during the Cold War was by India against the then-Western equipped but hardly modern Pakistani Navy in 1971. All other Cold War-era anti-ship
It remains difficult to definitively judge the U.S. Navy’s effectiveness in deceiving and blinding SOSS using only open sources. The doctrinal and technical information regarding U.S. and Soviet capabilities largely comes from the work of a single analyst, Norman Friedman. Friedman is perhaps the only researcher to publish comprehensive English language technical studies of the Soviet-American naval competition using archival materials made available by both sides after the end of the Cold War. While Friedman is widely regarded in the U.S. naval analytical community as highly knowledgeable and credible, the possibility cannot be discounted that some of the archival materials he used in his research excluded key pieces of information that might have otherwise led him to different conclusions. It is extremely unlikely that the official sources he used were written to be deliberately misleading to researchers, but the sensitivity of any past deception effort against technologies and operational concepts still used by the involved parties makes it a remote possibility.

The case study’s operational evidence taps multiple anecdotal sources and makes a credible circumstantial case that U.S. Navy efforts successfully countered SOSS’s primary remote sensing assets, namely Krug, RORSAT, and EORSAT, on at least several distinct occasions. Furthermore, the anecdotal evidence suggests other U.S. Navy successes evading detection by second-layer SOSS assets such as pathfinders and tattletales. The evidence is insufficient to determine the U.S. Navy’s apparent success rate, however, as data indicating the number of times EW and tactical deception were employed against SOSS as well as the outcomes of each usage over the course of the three decade competition is not publicly available.

missile engagements against Western navies used Western anti-ship missiles: French Exocets by Argentina against the Royal Navy during the 1982 Falklands War, Exocets by Iraq against the frigate USS Stark in 1987, and an American Harpoon by the Iranians against a U.S. Navy battleforce during Operation Praying Mantis in 1988. See Hughes, 151.
Deeper analysis will become possible once data from the mid 1970s onward is declassified over the next decade or so, and researchers can comb through U.S. Navy archives accordingly.

Soviet archival information attesting to the effectiveness of U.S. Navy EW and deception similarly remains classified or otherwise unlocated. The Soviets were intelligent adversaries and most likely learned from each U.S. Navy use of EW and deception against SOSS. The historical record is unclear as to whether they were able to develop tactics, techniques, and technologies of their own to defeat U.S. Navy anti-SOSS countermeasures. Therefore, the possibility that the Soviets possessed ‘war reserve’ anti-deception capabilities or were practicing a grand counter-deception campaign of their own cannot be completely discounted. During the span of the case study, the Soviets regularly dispatched second-layer SOSS assets against U.S. Navy battleforces that did not practice EMCON or that otherwise stumbled across other Soviet scouts. Friedman alludes to possible situational Soviet restraint in dispatching these assets against U.S. battleforces during the 1980s as a means of limiting U.S. Navy insight into SOSS capabilities. He does not, however, cite his basis for this opinion. He observes that the former chief of Soviet naval intelligence once remarked that the Soviet Navy had at least one submarine trailing each deployed U.S. Navy carrier as a tattletale.\footnote{Friedman, \textit{Network-Centric Warfare}, 238-239.} Without access to the Soviet archives, this claim is impossible to prove. While Soviet submarines no doubt trailed U.S. battleforces whenever possible, once they revealed their presence by transmitting a contact report or were otherwise detected they could be shaken off like any other tattletale. Soviet submarines were also subject to deception by systems such as the ICADS acoustic decoy. The Soviets’ experiences with ocean surveillance and targeting represent an important area for future Cold War naval research.

Ultimately, the chief metric for judging a military force’s probable combat efficacy is by observing its peacetime operations. It is axiomatic that a military force can only effectively
execute in war what it routinely practiced during the peace. Existing systems’ ‘war reserve’ modes are one thing, as these modes’ capabilities are generally transparent to the operator and do not necessarily require modifications of existing doctrine and tactics. ‘War reserve’ doctrine and tactics are harder to employ, as an operator cannot easily and confidently execute what he or she has never routinely practiced. This means the doctrine, tactics, and overall capabilities displayed by the Soviets when searching for and reacting to U.S. battleforces are very likely indicative of how they would have operated as well as the constraints they would have faced at the start of a general war. It is highly unlikely the Soviets would have operated during peacetime in ways that jeopardized their readiness for achieving a decisive first salvo at the start of a war—their primary doctrinal objective. It is especially improbable that they would have done so when U.S. Navy battleforces were operating only a few hundred miles off the Soviet coast during a period of increased political tensions, such as was the case during Ocean Safari/Magic Sword North ‘81.

From this dataset, we can derive several principles that can guide our search for potentially-exploitable vulnerabilities in the Chinese ocean surveillance and ASBM reconnaissance-strike systems.

- First, wide-area remote sensing is not a maritime surveillance panacea by any means. Long-range RF direction-finding/ELINT systems only work if a target cooperatively operates its radios or radars. EMCON denies passive sensors this information, and deception systems can make decoy units indistinguishable from real battleforces. The defender may also be able to use natural phenomena for cover depending on the nature of the attacker’s sensors’ vulnerabilities.

- Second, if long-range active sensors such as radar lack sufficient sensitivity and/or discrimination, they can be deceived using actively-emitting and passively-reflecting false
targets. These false targets often must be specially configured to defeat specific sensors’ unique exploitable vulnerabilities.

- Third, both sides are in a perpetual, iterative race to develop countermeasures against and counter-countermeasures for these sensors. The defender can therefore only effectively employ false targets and naturally-occurring cover phenomena against his adversary’s active sensors if he has adequate intelligence regarding those sensors’ current vulnerabilities. This intelligence is either gained through repeated operational exposure to the sensors or clandestine technical collection against them. Without this intelligence, the defender cannot have high confidence in his cover and deception tactics and techniques.

- Fourth, contact identification can be more important than contact detection. High technology weapons are expensive and can take a long time to manufacture. Their numbers are therefore often limited, and successful campaigns can hinge on whether enough of these weapons remain in a force’s inventory following sustained combat action. Force commanders must often decide whether targeting information is sufficient to launch a high technology weapon given the risk of wasting it against an invalid target. If defenders can prevent attackers from confidently determining the identity of a given contact from a distance, then the attacker may not be willing to waste long-range weapons without first sending scouts further forward to identify valid targets. This can simplify the defender’s screening problem greatly as well as impose increased risks on the attacker.

- Fifth, tactical deception’s effectiveness declines rapidly once an actual battleforce reveals itself upon passing through confined waters or commencing strike operations. It may take some time for the adversary to reevaluate his operational and tactical-level pictures to determine the approximate location of the actual battleforce, and the battleforce may be able
to travel far enough in that time to avoid redetection. However, in ‘announcing’ its presence, the actual battleforce will draw the adversary’s attention and as a result will need to prepare for the adversary’s counterstrike attempts.

- Sixth, a tactical deception capability can only be judged effective when it is periodically tested in peacetime against an adversary’s real-world sensors and decision-makers. This not only requires the defender to disclose some of his deception capabilities to his adversary, but also requires the defender’s use of counterintelligence methods to determine whether the adversary’s reaction to the deception is in fact genuine. Real-world testing also perpetuates the iterative countermeasure/counter-countermeasure competition between the two sides.

- Seventh and most significantly, the defender’s periodic peacetime disclosure of real and/or fabricated tactical deception capabilities to an adversary can be used as for psychological operations against the adversary’s commanders. By routinely denying information to, deceiving, or plausibly threatening to deceive the adversary’s surveillance and reconnaissance sensors, EW and tactical deception can cause the adversary’s operational and tactical-level commanders to lose faith in their ability to obtain reliable situational pictures. Periodically saturating the adversary commanders’ pictures with false contacts during peacetime may force them to sortie scarce scouts and weapons-carrying assets against decoy groups, thereby diluting the resources available for use against actual forces. This may condition adversary commanders to be more hesitant to commit reconnaissance-strike assets into the field, which in wartime can translate into increased maneuvering room for the defender to seize and/or retain the operational and/or tactical-level initiative. Conversely, when conducted periodically during peacetime, these kinds of psychological operations can condition the adversary’s commanders into expecting to see the defender conduct certain
types of operations or use certain tactics in the event of actual combat. If decoy groups simulate these same operations and tactics to the adversary in war, the adversary’s attention and/or long-range fire might be drawn away from actual forces.

There are two important corollaries to these principles. The first is that SOSS was a highly centralized system that denied tactical initiative to field commanders. These types of operational-tactical command and control systems may be the most politically reliable, but they generally are also the most exploitable by the other side.

Second, the SOSS case study suggests that centralized surveillance, reconnaissance, and strike systems are not very survivable once a general war breaks out between peer or near-peer states. Once the Soviets took their first and only ‘semi-free’ shot, surviving U.S. Navy battleforces would have been authorized to seek out and destroy any second-layer SOSS assets they came across. These U.S. Navy forces could have done so far from protected HVUs. In addition to employing ‘war reserve’ EW techniques and deception tactics, U.S. forces could also physically destroy SOSS’s land-based sensors and data fusion center with conventional weapons. Furthermore, the U.S. developed aircraft-launched anti-satellite missiles during the 1980s with RORSAT and EORSAT in mind as targets. Systems like SOSS are therefore best understood as optimized for coordinating the delivery of a single massive salvo against naval battleforces within their reach at the start of a war. Robust EW and tactical deception can increase the attacker’s uncertainty by increasing the number of variables he must overcome for his first salvo to succeed. The attacker’s centralized surveillance, reconnaissance, and strike systems’ combat viability wastes away rapidly and not necessarily gracefully from that point forward.\textsuperscript{149}

V. Assessing the Chinese Ocean Surveillance and ASBM Reconnaissance-Strike Systems

Comparisons with SOSS and the Soviet Maritime Reconnaissance-Strike System

There are a number of important similarities and differences between COSS and SOSS, just as there are a number of important similarities and differences between the Chinese ASBM reconnaissance-strike system and the Soviet maritime bomber reconnaissance-strike system. On the similarity side, it appears that COSS will use many of the same types of sensors as SOSS once did. COSS’s SAR and RF direction-finding/ELINT satellites parallel RORSAT and EORSAT. COSS’s current maritime reconnaissance aircraft and forecasted HALE UAVs parallel SOSS’s pathfinders. Eventual Chinese autonomous unmanned systems might someday be used as sacrificial tattletales. The OTH-B radar in some ways parallels Krug as a shore-based theater-wide surveillance and cueing sensor. The DF-21D ASBM parallels the Backfire-C/Kitchen tandem in tactical reach, lethality, and speed relative to its target. DF-21D also achieves the degree of tactical responsiveness and accuracy the Soviets could not with their SS-NX-13. Most significantly, COSS’s architecture and doctrine appears just as centralized—and by extension just as theoretically vulnerable to electronic neutralization, physical destruction, and tactical deception—as SOSS’s.\(^{150}\)

The most obvious difference is that the flight time of a DF-21D fired at maximum range will be about fifteen minutes, whereas the flight time for a Backfire-C raid at maximum unfueled range was measured in hours. Chinese SAR satellites also will not suffer from the sensitivity and operational lifetime shortcomings that plagued Soviet RORSATs. Unlike

---

\(^{150}\) Redundant systems and communications pathways can improve a centralized command and control architecture’s resiliency during intense and/or prolonged combat. However, these technical measures cannot deflect effective tactical deception.
RORSAT, Chinese SAR satellites may even possess a target-imaging capability that can be used as a countermeasure against unsophisticated RF decoys.

COSS will have other capabilities that the Soviets never enjoyed. For one thing, COSS may be able to cue electro-optical satellites for remote visual examination of contacts originally detected by other sensors. Thanks to the *Tianlian* data relay satellite constellation, COSS’s data fusion center will also be able to receive space-based sensor reports at times other than when a given surveillance satellite passes within a ground control station’s line of sight. Lastly, COSS will be able to augment its passive RF direction-finding/ELINT sensors with the actively-transmitting OTH-B. This will give COSS a peacetime wide-area surveillance capability that can provide actionable cues to higher-resolution active sensors carried by satellites and second-layer scouts.

*Combat Survivability of COSS and the ASBM Reconnaissance-Strike System*

The greatest question regarding COSS and its associated ASBM reconnaissance-strike system is how long they can retain their combat utility beyond China’s first salvo at the start of a war. The Chinese ASBM concept, after all, cannot be properly analyzed if it is examined outside of the overall operational, strategic, and political factors that would almost certainly shape any notional Sino-American crisis or conventional war in East Asia. Recall that if a Warsaw Pact-NATO or Soviet-American war had erupted, the Soviets would have received one ‘semi-free shot’ at crippling the U.S. Navy battleforces SOSS held in track at the outbreak of hostilities. Following this first salvo, U.S. wartime rules of engagement and deceptive countermeasures would have vastly complicated SOSS’s surveillance and scouting operations. Furthermore, a Warsaw Pact-initiated general conventional war in Central Europe almost certainly would have
allowed the U.S. to invoke the North Atlantic Treaty’s Article Five as justification for direct physical attacks against SOSS infrastructure located on Soviet soil. U.S. and NATO restraint in conducting an anti-SOSS campaign therefore depended on how limited a notional Warsaw Pact war was in scope.

This highlights the Chinese ASBM concept’s core strategic-level weakness. While no regional collective security alliance similar to NATO exists in East Asia, the U.S does have bilateral defense treaties with Japan and South Korea. If CCP leaders’ political objectives ever drive them to unleash a ‘limited’ PLA campaign against either of those two countries, the U.S. would be treaty-bound to intervene. Similarly and as noted earlier, key elements of PLA doctrine are predicated on the fanciful belief that precision land-attack missile strikes against U.S. military forces stationed on China’s East Asian neighbors’ territories would not be regarded by those host countries as intolerable acts of war. It is by no means clear that South Korean or Japanese citizens and political decision-makers would be willing to embrace this distinction, let alone refrain from invoking the bilateral defense treaties. It also goes without saying that PLA strikes against Guam or Hawaii at the opening of what CCP leaders intended as a ‘limited’ East Asian campaign would constitute direct attacks on U.S. soil. Chinese cyber attacks and/or active EW against U.S. military networks and sensor systems as hostilities broke out would additionally contribute to setting the initial ‘escalatory precedent.’

151 In fact, the North Atlantic Treaty’s Article 6 states that an armed attack conducted in the Atlantic at latitudes north of the Tropic of Cancer or in the Mediterranean Sea against the forces, vessels, or aircraft of a treaty party can be used to invoke Article 5. See North Atlantic Treaty.

152 From CCP leaders’ perspectives, notional PLA offensive operations in East Asia for limited political objectives might include rapid forcible seizure of the Senkakus, Spratlys, or other potentially contested lesser islands along the First Island Chain. Notional PLA seizure of Taiwan’s lesser islands such as the Pescadores, Quemoy, or Matsu archipelagoes might also constitute offensive operations for limited Chinese political objectives. A notional PLA invasion of Taiwan proper would hardly represent a Chinese limited political objective. CCP leaders might, however, consider an air and maritime blockade of Taiwan or a coercive SRBM bombardment campaign against Taiwan as operations for limited political objectives even if the Taiwanese people (and probably U.S. leaders) disagreed with that characterization.
Any one of the above land-attack scenarios, and more likely a combination of them, would provide the U.S. with sufficient political justification to begin a comprehensive and physically destructive campaign against COSS, the ASBM reconnaissance-strike system, and other PLA theater access-denial forces located on Chinese territory, at sea, in the air, and in space. This campaign’s nature, scope, and escalatory tolerance would be restrained only by U.S. and allied political objectives for and passions in this now far-less-limited notional war.

It is possible but unlikely that the Chinese might opt to open a limited regional campaign by only striking U.S. Navy battleforces at sea. CCP leaders might consider this approach if they believed that they could successfully manage escalation by not conducting land-attack first strikes against U.S. and/or U.S. allies’ sovereign territories. CCP leaders might conclude that limiting their first strikes to the maritime domain would make their U.S. counterparts fear setting the war’s escalatory precedent in the form of authorizing counterstrikes against COSS sites and other PLA targets on Chinese sovereign territory. Chinese restraint along these lines, however, would prevent them from accomplishing their articulated primary military-strategic objective: summarily blocking the U.S. from using forces already in theater to disrupt or defeat PLA offensives. Once the Chinese launched their first ASBM at a single U.S. warship, U.S. and allied air and ground forces could take combat readiness-enhancing steps such as dispersing and/or sheltering vulnerable land-based aircraft and materiel. This would dramatically erode the

---

153 Since the data fusion center could be located deep underground or in politically-sensitive areas, and since command, control, and communications systems could be rerouted to any number of alternate locations, under some circumstances it might make more strategic as well as tactical sense to attack the data fusion center(s) ‘virtually’ through EW, tactical deception, and possibly cyber means as opposed to physical strikes.

154 Both sheltering and dispersion would require significant peacetime investment. Many more shelter hangars than currently exist would need to be built at regional airbases to protect U.S. and allied tactical aircraft. Dispersed operations would require more maintenance manpower than likely exists in current forward deployed force structures, fielding of a distributed air operations command and control/mission planning system, and construction/reconfiguration of outlying secondary airbases and/or highway stretches long enough for use as military runways. Dispersed operations would also require extensive use of cover and deception in order to delay or prevent Chinese discovery of the secondary/ad hoc airbases in use during a conflict. Lastly, dispersed operations would
effectiveness of any PLA land-attack missile strikes deemed necessary against those units and resources later in the campaign. Nor would there be any guarantee that U.S. political leaders would refrain from vertically escalatory counterstrikes against PLA assets on land and/or in space.\textsuperscript{155} The key to a first strike is to neutralize or destroy as much of the defender’s combat potential as possible before he can effectively react, thereby foreclosing the defender’s self-defense and retaliatory options in ways that decisively grant the strategic and operational initiative to the attacker. Chinese leaders’ initial political objectives would have to be very limited and their restraint very disciplined, indeed, for them to forego theater-wide first strikes

---

\textsuperscript{155} There is no precedent in modern U.S. history for a response to a near-peer state’s peacetime attack on a U.S. HVU at sea. In terms of war-opening attacks on major U.S. Navy combatants, the closest historical analogies would be the 1898 sinking of the battleship USS \textit{Maine} in Havana harbor (widely believed then as now to be the result of mining) and the 1941 Pearl Harbor raid. While the latter incident directly and the former incident indirectly led to U.S. declarations of war against Japan and Spain respectively, neither occurred when the involved U.S. warships were at sea. The trendline is even less clear when examining attacks by near-peer and non-peer states on smaller U.S. Navy combatants. German submarine attacks on U.S. Navy destroyers in the North Atlantic during summer and fall 1941 did not result in a U.S. declaration of war or U.S. military retaliation. Nor did the 1987 Iraqi anti-ship missile attack against the frigate USS \textit{Stark} in the Persian Gulf. Conversely, the 1964 North Vietnamese torpedo boat attacks on the destroyer USS \textit{Maddox} in the Tonkin Gulf served as the trigger for direct U.S. intervention in Vietnam, and the U.S. broadly retaliated against Iranian maritime forces in 1988’s Operation Praying Mantis following the frigate USS \textit{Samuel B. Roberts}’ striking an Iranian-laid mine in the Persian Gulf.

These data points suggest that U.S. retaliation for attacks on its warships by another state depend on several factors. Since both historical attacks on U.S. Navy HVUs led to war whereas only a few of the attacks on smaller combatants did, the attacked warship’s size, Fleet role, and corresponding national symbolism may be determining factors. In this light, it is worth noting that large surface combatants such as Aegis destroyers are today considered major Fleet assets whose roles and corresponding symbolism are more similar to pre-1940s battleships and cruisers than they are to pre-1970s destroyers. The more important variables, though, appear to be U.S. relations with and political interests relative to the aggressor at the time of an attack. U.S. interests in Cuba, East Asia, South Vietnam, and the Persian Gulf region were deep and publicly articulated at the times of each of the attacks that led to wars or otherwise U.S. military retaliation. Tensions were also already high with Spain, Japan, North Vietnam, and Iran when those incidents occurred. It is highly likely, therefore, that any Chinese East Asian campaign-opening attack(s) conducted at a time of high Sino-American tensions solely against U.S. Navy aircraft carriers, amphibious warships, and/or large surface combatants would not deter the U.S. from retaliating via vertical escalation. These political-strategic factors, combined with images of a damaged symbol of American power and American servicemembers’ casualties, would likely trigger the very response China sought to deter. Regardless, in the unlikely event that a Chinese maritime first salvo did deter American vertical escalation, it would not be vertically escalatory for U.S. Joint forces to initiate a comprehensive campaign against PLA maritime forces, seaborne logistics, and COSS maritime airborne and sea-based scouts.
against American and allied forces on land and at sea at the beginning of an East Asian campaign.

Based upon all these considerations, COSS’s vulnerability to kinetic and non-kinetic attacks in a notional Sino-American war appears to represent the operational-level key to unraveling the PLA’s overall ASBM capability.\textsuperscript{156} This might be expected to present Chinese leaders with a use-or-lose proposition. Even if the highly-mobile \textit{DF-21D} TELs cannot be routinely located and destroyed by long-range U.S. aerospace forces, COSS would likely be fair game for physical attacks and almost certainly fair game for EW and other non-kinetic attacks. The more centralized that COSS and the ASBM reconnaissance-strike architecture is, the more likely that systematic deception against and/or neutralization and destruction of COSS will make it extraordinarily difficult if not impossible to effectively target U.S. Navy battleforces with ASBMs the longer a notional war lasts.

If CCP and PLA leaders come to believe that COSS is a wasting asset in war, they might find themselves under immense pressure to conduct ASBM strikes against as many major U.S. warships and battleforces as possible as quickly as possible at the beginning of a notional conflict. Notwithstanding the ASBM arsenal’s role in PLA strategy and PLA leaders’ apparent confidence in the COSS maritime picture’s accuracy, the fear of rapidly losing the ability to effectively employ ASBMs will theoretically further heighten the PLA’s incentives for using them early and often. It seems likely that the PLA would size each of these early salvoes to give them the highest reasonable probability of penetrating targeted U.S. Navy battleforces’ defenses. It follows that a few poorly-aimed or decoyed salvos during a notional war’s first days or weeks

\textsuperscript{156} Ironically, many Chinese defense analysts agree with this logic as applied to the U.S. military’s integrated surveillance, reconnaissance, and strike systems’ critical roles in supporting sustained U.S. combat operations in the Western Pacific. See 1. Ross, “Navigating the Taiwan Strait: Deterrence, Escalation Dominance, and U.S.-China Relations,” 72; 2. Cliff, “Entering the Dragon’s Lair,” 37-38, 51-60. It is not clear whether any Chinese defense analysts have acknowledged this in their writings about the ASBM concept.
would impose a meaningful dent in the ASBM inventory at a precarious point in the PLA’s offensive campaign.

Conversely, if CCP and PLA leaders come to distrust the COSS maritime picture’s accuracy in peacetime, then they might hesitate to expend ASBMs in wartime. This hardly means there would be no ASBM first salvo or follow-on salvoes of opportunity. It does mean that a higher threshold of picture confidence might be required before a raid would be authorized, and that this could buy U.S. Navy battleforces time and space for conducting initial theater operations.

As will be discussed in Section VI and VII, these two PLA decision-making scenarios offer numerous opportunities for exploitation via tactical deception. Even though the two scenarios’ decision-making rationales contradict each other on the surface, there is no reason why the associated impulses cannot simultaneously arise in the minds of key Chinese leaders. Should this occur and some measure of Chinese decision-making paralysis result, tactical deception could provide U.S. forces with significant assistance in capturing the tactical and operational initiative.

*Conceptual Alignment of EW and Deception with Anti-ASBM Active Defenses*

The above factors suggest that the primary ASBM scenario the U.S. Navy must prepare for is defense against the first few salvos during the opening days and weeks of a notional East Asian war. The more U.S. Navy warships that survive these first few salvos, the more combat power the U.S. will retain in theater to blunt PLA offensives, protect flows of reinforcements and materiel to U.S. allies, and prevent China from achieving its war objectives.
Since the first ASBM salvo would likely mark the transition from peace to war, peacetime rules of engagement would likely constrain U.S. military forces’ options for actively degrading COSS’s ability to provide targeting support for that first salvo. The tactical focus during the peace-to-war transition would be on cover from and deception against COSS, as well as defensive EW against the first salvo ASBM warheads’ homing sensors. Following rules of engagement relaxation, the subsequent phase would add offensive anti-COSS EW to the mix. Both phases’ EW and deception capabilities would be in addition to and complementary with U.S. Navy active defenses against ASBMs and COSS assets, such as anti-ASBM interceptor missiles and area air defenses against reconnaissance aircraft.

U.S. Navy EW and tactical deception systems would also dovetail with U.S. Joint forces’ kinetic strikes against shore-based COSS sensors, satellite ground stations, and data fusion facilities. It follows that the more that EW and deception tools can contribute to disabling COSS and neutering the ASBM non-kinetically, the more options that U.S. military leaders will have should initial U.S. political objectives make escalation management a priority. The ASBM threat will not evaporate entirely once COSS is fundamentally disabled or compromised, and U.S. Navy battleforces will require ASBM defenses throughout a notional war. Nevertheless, without effective COSS targeting support the remaining ASBM inventory would be far less of a hindrance to the conduct of U.S. Navy combat operations along the First Island Chain.

---

157 Defensive EW constitutes countermeasures employed only upon detecting enemy use of an active targeting sensor (as opposed to a surveillance sensor), enemy weapons launch, and/or the attacking weapons’ homing sensors. The purpose of defensive EW is exclusively to defeat the inbound threat. In practice, defensive EW’s definitional lines can be blurry as many modern surveillance sensors double as targeting sensors and a defender may not be sure whether an active sensor is being used for surveillance or for targeting. A commander’s decision regarding when to employ defensive EW is based on his or her reading of the tactical situation, intelligence in-hand, delegated authority, and legal right of inherent self defense.

158 Offensive EW constitutes countermeasures employed with the intention of actively blinding, disabling, or even destroying enemy surveillance sensors and communications pathways. The purpose of offensive EW is to neutralize and/or roll up the enemy’s surveillance network. Some forms of tactical deception can also fall under offensive EW (i.e. deceptive jamming of a surveillance radar), and an adversary may not even realize his sensors were subjected to a deceptive offensive EW attack until much later. Use of offensive EW does not necessarily require a state of war to be in effect, but its peacetime use is typically subject to higher-level approval as it can be interpreted as a hostile act.
EW and Deception Capabilities Needed

The Cold War case’s principles allow us to derive several key technical questions which need to be answered before an appropriate mix of EW and tactical deception capabilities can be tailored for use against COSS and the ASBM warhead. For instance, countermeasure developers need to understand Chinese sensors’ sensitivity and discrimination capabilities. They also need to understand a variety of other technical details about these sensors such as scan patterns, transmit and/or receive beam patterns and frequency spectrums, transmit waveform designs, signal processing methods, and counter-EW techniques.

Countermeasure developers also need to understand COSS’s communications and data fusion architecture. They need to understand how long it takes the data fusion center to receive downloads from remote sensors. They also need to understand whether any technical constraints or organizational barriers exist that can be exploited to further delay this data. They may even need to understand the basic processing methodology that COSS track management systems will use to fuse sensor data into an integrated situational picture.

Lastly, countermeasure developers need to understand COSS operators’ data analysis skills and routines as well as decision-making preferences and tendencies. Since modern computer systems can manage an incredibly high number of contacts, saturating an ocean surveillance system depends upon psychologically stressing the system’s human operators beyond their mental limits. These psychological attacks can take advantage of apparent gaps in the operators’ training. Apparent operating procedures can also be exploited. As noted previously, a long term deceptive-conditioning campaign can incrementally attack operators’ and decision-makers’ confidence in their operational or tactical pictures by occasionally inducing them to waste surveillance and reconnaissance resources against especially alluring decoys,
presenting them with too many ‘valid-looking’ contacts that require direct investigation by scouts, or using easily-discriminated EW techniques and deception tactics to make them incorrectly tag actual battleforces and warships as decoys. It follows that countermeasure developers must understand what COSS operators and decision-makers expect their sensors and data fusion processors will show them, how they expect these systems will perform under combat conditions, and most importantly what they think U.S. Navy battleforces will do tactically and operationally in a war.

With these intelligence collection requirements in mind, we can next examine several EW technologies with potential applications against critical COSS nodes and/or the ASBM’s own homing sensors. While the limited unclassified information about COSS and the ASBM makes it impossible to detail specific technical solutions against those threats, we can nevertheless use the physical principles behind modern EW as well as the Cold War case’s principles to identify promising technical and tactical concepts for further U.S. Navy research.
VI. Promising EW Technologies and Techniques for ASBM defense

**EW Systems’ Basic Roles in Naval Battleforce Defense**

In order to apply the Cold War case’s principles against COSS and the ASBM reconnaissance-strike system, it is important to visualize how different EW technologies and techniques fit into overall defense-in-depth of a naval battleforce. Figure 4 below illustrates the EW countermeasures used at various points in an attacker’s generic ‘detect-to-engage’ sequence.

![Figure 4: EW-Based Layered Defense](image)

First, cover and deception (C&D devices in the diagram) countermeasures blind or deceive the attacker’s surveillance and reconnaissance sensors on, under, and above the sea over the course of several hours, days, and perhaps even weeks. Assuming the attacker is able to localize the battleforce, active EW (AECM in the diagram) transmissions from shipboard EW systems, active offboard decoys, and passive ‘reflecting’ offboard decoys are used to blind or deceive the

---

attacker so that he cannot easily detect and identify the battleforce’s warships. These same systems can also be used to degrade the attacker’s tactical picture accuracy and coherency such that it complicates his decisions regarding whether or not to launch missiles. If he chooses to launch missiles, then the same systems can be used to influence his decisions regarding when, where, and how many missiles should be fired.

Once missiles have been launched, shipboard EW systems and offboard decoys are used to blind and/or deceive the missiles’ midcourse guidance sensors with the objective of ‘distracting’ them away from the defended battleforce. Should this fail, other ‘distraction’ countermeasure techniques are used to present multiple valid-looking targets to an inbound missile’s terminal homing sensors. If these homing sensors can be fooled into locking onto one of the distraction targets, the raid’s strength will be decreased and more defensive interceptor missile and EW resources can be allocated against the surviving threats. Blinding techniques may also continue to be used at this stage. In the event that a missile’s homing sensors lock onto one of the defended warships, ‘seduction’ countermeasure techniques are employed to break the lock and cause the missile to miss. The EW defense sequence against a launched missile transpires in anywhere between 15 minutes for an ASBM fired from its maximum range to under a minute for a sea-skimming supersonic anti-ship cruise missile first detected as it crosses the defender’s radar horizon.

Most EW systems serve multiple roles in a layered defense. The number of roles that a given EW system can fill depends upon how many adversary sensor types it can influence, and

---

160 ‘Blinding’ by an active EW system involves broadcasting electromagnetic ‘noise’ in the direction of an attacker’s sensor. RF noise jamming is a form of blinding. Intense infrared or visible-band light can also be used to blind an adversary’s infrared and electro-optical sensors. Sophisticated infrared and electro-optics can overcome this to some extent by receiving multiple frequencies near-simultaneously and/or using receiver ‘filters’ and various signal processing techniques to suppress or cancel out the blinding effect.
161 The Israeli Navy’s use of helicopters and chaff clouds as false targets against Styx missiles during the Yom Kippur War represent examples of distraction and perhaps also seduction countermeasures.
the means by which it can influence those sensors. For instance, ICADS performed
countersurveillance and countertargeting missions by generating false RF and acoustic targets.
ICADS’s ability to simulate other warships’ telltale RF emissions may also have been capable of
fooling certain types of missiles’ midcourse guidance systems, and its RF false target generator
may have provided terminal phase distraction capabilities. Shipboard EW systems such as the
1960s-era AN/ULQ-5s and 6s and the post-1980s AN/SLQ-32 were designed to perform
countertargeting, counter-midcourse guidance, distraction, and seduction functions.

COSS and ASBM warhead sensors are far more complex and almost certainly far more
capable than their Soviet ancestors. As a result, a wide variety of time-tested countermeasures
must be combined with several key emerging EW technologies.

*Passive Offboard Countermeasures against COSS and ASBM Warhead Radars*

Shipboard EW systems are necessarily augmented by offboard EW countermeasures. In
the absence of offboard countermeasures, an adversary can adapt his weapons’ sensors to
recognize and home on actively-transmitting shipboard EW systems’ emissions. Offboard
countermeasures are divided into two categories: passive and active. As their name implies,
passive offboard countermeasures reflect, absorb, or obscure the electromagnetic radiation that
adversary sensors use to detect defended warships. Balloons and chaff/RF-obsuring aerosols are
the two main types of anti-radar passive offboard countermeasures.

Rapidly-inflated balloons that float on the ocean’s surface have supported naval
countersurveillance and countertargeting efforts for decades. These balloons are shaped to have
disproportionately-large radar cross sections as compared to their physical sizes. They are often
used as distraction and seduction false targets when their use is coordinated with other EW systems and techniques under appropriate circumstances. \footnote{162}{“AN/SLQ-49 Chaff Buoy Decoy System,” Federation of American Scientists.}

Chaff decoys are perhaps the most common passive offboard countermeasure against an adversary’s centimeter-wavelength search and targeting radars, and RF-obscuring aerosols perform the same role against millimeter-wavelength radars. \footnote{163}{Chaff’s reflective effects against centimeter and even meter-wavelength radars are made possible by the fact that metallic strips can be readily cut to lengths that are half these radars’ wavelengths. It follows that aerosolized sub-millimeter length reflective fibers or particles are necessary to achieve the same effect against millimeter-wavelength radars. See Culora, 73-84.}

Warships create chaff clouds by using mortar-like launcher tubes to propel chaff-dispersing canisters into the air. The chaff system, as controlled by the warship’s EW control system, is designed to automatically launch canisters in preset patterns around the warship depending on the type of inbound missile and the local meteorological conditions. Older distraction chaff techniques involved creating clouds whose large radar cross sections were more attractive to unsophisticated missiles’ homing radars than the actual warships. Similarly, older seduction chaff techniques involved positioning clouds close enough to a defended warship so that their individual radar reflections merged into what would seem to be a single contact to an unsophisticated missile’s homing radar. Since the apparent center of this single large radar reflection would by the cloud pattern’s design not be located on the defended warship, the missile’s ‘locked-on’ aimpoint would be seduced towards one of the clouds. Modern anti-ship missiles’ homing radars are far less susceptible to these particular techniques. \footnote{164}{Friedman, World Naval Weapon Systems, xxii, 357, 422.} However, a properly-placed and periodically-reseeded chaff or RF-obscuring aerosol cloud can still generally conceal a defended warship from overhead radars. The problem is that if the only chaff or obscurant clouds in a given area are those concealing warships, missiles can be programmed to aim for the clouds. If unitary high explosive airbursts, a
release of submunitions, or HPM detonations allow the missiles’ warheads to affect a large enough area, they could still knock a chaff or obscurant-concealed warship out of the fight at least temporarily.

The key, therefore, is to create multiple chaff or obscurant clouds in relatively close proximity to the one cloaking a defended warship. If cloud patterns are laid appropriately, the various radars used by SAR satellites, maritime reconnaissance aircraft and UAVs, or ASBM warheads in theory might not be able to tell based on the targeted warship’s previous motion which cloud conceals that warship. Warships can lay these clouds today, and unmanned vehicles might be able to assist them with increasing the complexity of this ‘shell game’ in the future.

**Active Offboard Decoys against COSS and ASBM Warhead Radars**

Since the late 1990s, active offboard decoys such as the hovering, warship-launched *Nulka* system have emerged as the preferred tools for distraction and seduction of modern anti-ship missiles’ homing radars. While older radars could not automatically discriminate chaff from valid contacts and had difficulty overcoming active EW, post-1970s radars use a wide variety of counter-EW measures to recognize and filter out unsophisticated EW techniques and decoys. For instance, shipboard active EW systems’ use of noise jamming and certain deception jamming techniques increase the RF emissions from the defended warship. As noted earlier, this can draw the attention of search and targeting sensors as well as provide additional homing options for missiles’ guidance sensors. Active offboard decoys are therefore necessary to provide tactical separation between a defended warship and systems employing active EW.

---


167 Kimbrell, 85. This problem was recognized as early as 1971. A Center for Naval Analyses study published that year for the U.S. Navy predicted that offboard active EW would be necessary to counter the then-forecasted next
Another important contribution from active offboard decoys is their ability to employ EW techniques that shipboard active EW systems cannot routinely perform on their own. Two of the most basic active EW techniques against radars are range deception and angular deception. While older, unsophisticated radars were very susceptible to these jamming techniques, post-1970s radars employ randomized pulse-to-pulse characteristics and scan patterns as well as other deception suppression techniques. These counter-EW measures make it virtually impossible
for a shipboard active EW system to project false targets between the adversary’s radar and the
defended ship, as this form of range deception depends on precise predictions of the adversary
radar’s pulse characteristics. They also make angular deception as well as projection of false
targets further away from the adversary’s radar than the defended warship much more difficult to
accomplish without more sophisticated means for quickly analyzing and modifying the adversary
radar’s pulse. 170 Throughout the Cold War, computing technologies with the required processing
receiver is ‘watching’ for reflections). AM and FM are used for a number of technical and tactical reasons such as
improving the radar’s range resolution, making the radar’s waveforms appear ‘random’ so that they can be
camouflaged within the ambient RF noise in the environment, using Doppler shift measurements in a contact’s radar
reflection to discriminate valid contacts from false contacts, and making it harder for an active EW system to
precisely copy and rebroadcast the waveform for deception purposes. Without understanding how a given modern
radar employs these techniques, deceptively jamming it becomes extremely difficult if not impossible. See Denk,
“Detection and Jamming Low Probability of Intercept (LPI) Radars,” 87. Also see Payne, 95-97.

170 Range deception works by copying an adversary radar’s pulse and retransmitting it either slightly after or slightly
before the pulse reflects naturally off of an active offboard decoy or a warship using an active EW system. This
retransmission results in the projection of a false radar contact either behind or in front of the active decoy or the
active EW-equipped warship. Common forms of range deception work against the ‘range gates’ that a radar’s
control processor uses to track contacts. The control processor places a range gate over a newly-detected contact as a
means of isolating the contact’s radar reflection from other apparent radar reflections detected in the contact’s
immediate vicinity. An active EW system can attack this range gate logic by recording and retransmitting a copy of
the adversary’s radar’s pulse with a slight time delay and slightly more energy than the valid contact’s actual radar
reflection. With each enemy radar pulse transmitted at the valid contact, the deception transmission’s rebroadcast
delay is gradually increased until the enemy radar control processor concludes the false ‘reflection’ is actually the
valid contact’s reflection and accordingly ‘locks’ the range gate onto the false reflection. This is called ‘Range Gate
Pull Off’ (RGPO) since it draws the range gate towards a false contact that is further away from the radar than the
valid contact. RGPO was often used to fool an inbound missile’s unsophisticated homing radar into breaking ‘lock’
on the defended warship. The technique then either prevented the radar from locking back onto the defended
warship, or drew the radar’s range gate towards a nearby chaff cloud or other passive offboard decoy. The radar’s
range gate would then lock onto the chaff or decoy, and the missile would miss the defended warship.

A similar range deception technique called ‘Range Gate Pull In’ (RGPI) can be used if the active EW system can
predict precisely when the adversary radar will transmit a pulse at the valid contact as well as the pulse’s specific
characteristics. If successful, RGPI draws the range gate towards a false contact that is closer to the radar than the
valid contact. Modern radars can easily defeat this technique, though, by making their pulse-to-pulse characteristics
very hard if not impossible to predict.

In contrast, angular deception involves recording and retransmitting a copy of the adversary’s radar pulse when the
active EW system judges the adversary radar to be looking slightly away from the valid contact. It is a
misconception that a radar transmits only a single beam towards a contact. While most of a radar’s transmitted
energy is contained within a primary beam called the ‘main lobe,’ all radars also form undesirable lower energy
beams to the sides of the main lobe. These ‘sidelobes’ are unavoidable consequences of the radar’s transmit antenna
design. If an active EW system simulates a false reflection when it believes one of these sidelobes is pointed in its
direction, an adversary’s unsophisticated radar will incorrectly interpret the false reflection’s angular position as
being within the main lobe. This will generate a false contact that is located down the centerline bearing of the main
lobe, not the sidelobe. When combined with range deception, this can be used to surround a defended warship or a
decoy with many false contacts. However, modern radars design their radar antennas to have the smallest and
speed were too bulky for use in lightweight, expendable active offboard decoys. Nulka and other similar systems became possible after early 1990s advances in computer miniaturization supplied the digital memory capabilities and high processing speeds needed for radar pulse analysis and modification within a small expendable decoy.

Active offboard decoys provided naval battleforces with new tactical options. For one thing, they gave battleforce warships greater flexibility in selecting when to operate shipboard active EW systems. By delaying or refraining from use of these shipboard systems, defenders could limit the types and amounts of shipboard RF emissions available for adversary exploitation. Active offboard decoys placed between the adversary’s radar and the defended warship also restored the defense’s ability to generate false targets in this zone. Placement of active offboard decoys at various azimuths from the defended warship similarly helped compensate for modern radars’ counter-angular deception techniques.171

The coming generation of maritime search, targeting, and terminal homing radars feature significantly improved counter-EW capabilities, though. Space-based, aircraft, and missile warheads’ advanced radars will use incredibly complicated pulse designs and transmission patterns as a means of complicating an active EW system’s ability to predict let alone rapidly and precisely duplicate received pulses. Advanced radars’ signal processors can also integrate the data received during multiple successive pulses to help with discriminating and cancelling out unsophisticated false contacts.172 SAR imaging technology is better able now to discriminate unsophisticated passive and active decoys from valid contacts than it was during the Cold War.

---

171 Kimbrell, 85.
172 Cadirci, “Counter RF Stealth Technologies,” 94.
ISAR has likewise become sufficiently mature for use in missiles’ homing radars for the same purpose.\textsuperscript{173} It follows that future active offboard decoys, not to mention shipboard active EW systems, will need to make the false targets they project seemingly ‘look’ and ‘move’ like the real objects they simulate.

\textit{Advanced Active EW Countermeasures against COSS and ASBM Warhead Radars}

As a result, perhaps the most important emerging technology for future active EW systems is Digital Radiofrequency Memory (DRFM). Older active EW systems recorded and stored adversary radars’ pulses using analog devices. The longer a received pulse ‘circulated’ in one of these storage devices before being modified and rebroadcast, the more electronic noise it picked up from that storage device. Over time, specific details in the pulse’s waveform were lost to this accumulating noise. These missing details combined with the added noise made it much easier for the adversary radar’s signal processor to recognize the active EW system’s deceptive pulse rebroadcasts as being phony.\textsuperscript{174} DRFM overcomes this problem by converting received radar pulses into digital recordings. This vastly reduces the undesirable noise added into a recorded pulse. DRFM’s ability to make high fidelity copies of received pulses depends on the bit sampling rate and accuracy of the DRFM device’s analog-to-digital converter. The higher the sampling rate and accuracy, the better the copy. High instantaneous bandwidth receivers are also necessary so that the DRFM device can keep pace with an advanced radar’s rapidly-changing pulse-to-pulse frequency shifts.\textsuperscript{175}

\textsuperscript{173} Pace, “Digital Image Synthesizers: Are Enemy Sensors Really Seeing What’s There?,” 3-4.
\textsuperscript{174} Friedman, \textit{World Naval Weapon Systems}, xxii.
\textsuperscript{175} Helberg, “Electronic Warfare Technology Trends and Visions,” 5-6. Instantaneous bandwidth is the spectrum of frequencies a receiver can scan at a given moment in time. The wider the instantaneous bandwidth, the more sensitive the receiver is to a greater range of frequencies. This is especially important when dealing with modern interpulse frequency-hopping, intrapulse frequency-modulating radars. For more on instantaneous bandwidth, see Denk, 90.
Keeping an active EW system’s reaction time delay as short as possible is especially important. The active EW system needs to be fast enough to analyze, modulate, and transmit the deceptive pulse during the fraction of a second that the radar’s receiver is watching for reflections from the immediate area in which the false target is to be projected. The system needs to be fast enough to remain effective when the adversary radar’s close proximity to the defended warship further decreases the time available for processing—particularly when that adversary radar is mounted on an incoming missile’s warhead. DRFM technology provides active EW systems the required degree of computing agility.

Another key DRFM advantage resides in its signal processing and analysis capabilities. Until the 1970s, the primary factor constraining radar direction-finding/ELINT sensors’ capabilities were their receivers’ limited instantaneous bandwidths. Once detected, Cold War-era radars’ relatively simple pulse characteristics could be readily analyzed. Modern ‘Low Probability of Intercept’ radars, however, strive to camouflage their emissions within the operating area’s ambient RF environment in order to avoid identification by EW systems. These radars use far more complicated waveform designs in an attempt to make an EW system’s pulse analysis effort more difficult. In order to overcome these factors as well as the radar’s other pulse-to-pulse characteristic changes, DRFM-based signal processors use complex mathematics to first recognize an RF emission as being from an adversary radar, next compare the received waveform to a database of previously-detected and analyzed waveforms in order to identify the radar’s type and model, and then use the database as possible to analyze the received waveform’s...
components. When a high confidence match between the received waveform and the database is not possible, the DRFM-based signal processor will make ‘best guess’ analyses. The DRFM device will use these analytical conclusions to decide which deception jamming techniques should be used against the adversary’s radar at what times.  

DRFM, therefore, is critical to deceiving advanced radars whose complex pulse designs enable SAR or ISAR imagery capabilities. China’s SAR satellites, potential future ISAR-equipped HALE UAVs, and potentially SAR and/or ISAR-equipped ASBM warheads will use imaging to discriminate between valid contacts and unsophisticated decoys. It follows that future DRFM-based deceptive image generators mounted on unmanned vehicles and active offboard decoys will likely form a major part of the U.S. Navy’s active EW solutions to advanced countersurveillance, counteringassault, distraction, and seduction challenges. These deceptive image generators will analyze a received SAR or ISAR pulse, then perform intricate calculations to determine the subtle phenomena that would result from the pulse’s waveform reflecting off of a particularly-shaped real-world contact. The calculations required are so intensive that arrays of specialized high-performance microchips would be needed to provide the DRFM’s signal processor with the timely, detailed data needed to correctly alter the recorded radar pulses. As of 2004, U.S. Navy researchers had developed prototypes of these specialized microchips but had

---

178 Denk, 58, 64-65, 69.
179 To understand what this entails, imagine looking at a high-resolution photograph of a ship. The image generator would need to break that photo’s equivalent RF image up into individual finely-detailed shapes and edges, calculate the waveform-doctoring measures appropriate for simulating each shape and edge, calculate the waveform-doctoring measures needed to simulate reflections off the sea’s surface near the simulated contact (especially important for simulating the fake ship’s wake), calculate the RF wave phase shifts and timing delays needed to correctly reassemble the different shapes and edges into the original picture, and then accordingly modify and rebroadcast one or more pulses at the adversary’s SAR or ISAR system. Waveform-doctoring measures could include very fine amplitude variations, Doppler shifts, wave phase shifts, and timing delays. All of this would need to occur fast enough so that the deceptive pulses will arrive at the SAR or ISAR with the proper timing to project the simulated ship’s RF image in the desired real-world location.
not yet integrated them with DRFM.\textsuperscript{180} Given the apparent absence of subsequent progress disclosures within the open source literature, it is impossible to determine the U.S. Navy’s progress in maturing the above laboratory concept design or something similar into a viable system. All the same, the 2004 progress disclosure signifies that U.S. Navy applied research into DRFM-based SAR and ISAR countermeasures was well underway six years ago.

Of course, even after a U.S. Navy DRFM-based image generator is developed and fielded, it will be difficult for it to succeed operationally without continuous technical intelligence regarding Chinese SAR and ISAR systems. As noted previously, countermeasure designers need to understand many technical details about a targeted sensor in order to custom-tailor active EW techniques for use against it. This will require repeated U.S. Navy operational exposure to Chinese SAR satellites and ISAR-carrying aircraft. Clandestine technical intelligence collection will likely be necessary for information about COSS radars’ signal processing approaches, counter-EW measures, and other characteristics not readily discernable from laboratory analysis of recorded waveforms. Clandestine technical intelligence collection will almost certainly be necessary for information about any SAR and/or ISAR radars carried by the ASBM warhead.

Should the U.S. be able to consistently collect this information, it may potentially gain the ability to make DRFM image generator-equipped unmanned vehicles and offboard decoys look like warships to COSS’s and ASBM warheads’ radars. U.S. Navy assets could also conceivably use this technology to disguise warships’ RF appearances or to project false images of warships or other objects into empty waterspace. The Chinese would no doubt adapt their radars once initial U.S. anti-SAR/ISAR capabilities were operationally demonstrated or otherwise became evident. Nevertheless, U.S. Navy countermeasure developers would be better

\textsuperscript{180} Pace, 5-8.
placed to iteratively keep pace with Chinese radars’ counter-EW measures once viable DRFM image generator technology was in hand.

**EW Against COSS and ASBM Warhead Electro-Optical/Infrared Sensors**

Radar’s ability to rapidly search a wide area from a considerable distance away, precisely measure a contact’s range and kinematic behavior, and—assuming that the radar’s discrimination capabilities are effective—see through weather phenomena makes it the ideal primary sensor for surveillance and targeting, not to mention a very good sensor for weapons homing. Radars without imaging or other object discrimination capabilities, though, cannot easily determine the nature or identity of a contact. Radars’ susceptibility to active EW adds a complicating factor as well. Wide-area surveillance, targeting, and strike systems like COSS and the ASBM therefore often use electro-optics or infrared sensors back up radars.

Electro-optical and infrared sensors passively sense a contact’s visible-band and infrared emissions and reflections. While basic electro-optical and infrared sensors are capable of detecting only a single wavelength within their respective electromagnetic bands, multispectral sensors can detect several different infrared and/or visible-band wavelengths either individually or within non-contiguous blocks. Hyperspectral sensors break up the infrared and/or visible bands into contiguous blocks, then sample those blocks to form a complete spectral image of a scene.¹⁸¹

Multispectral and hyperspectral electro-optical and infrared sensors therefore provide secondary detection and tracking as well as contact identity-confirmation capabilities to a surveillance, targeting, and strike network. Visible-band and infrared radiation, however, suffer significant attenuation when traveling through the atmosphere. The atmosphere’s chemical

---

¹⁸¹ “Hyperspectral Imaging,” Wikipedia.
composition both absorbs and scatters this radiation, and different visible-band and infrared wavelengths experience different amounts of attenuation. Some blocks of the infrared and visible spectra are completely unusable by sensors because of this attenuation. Usable spectral blocks are still attenuated so heavily that electro-optical and/or infrared sensors often must close to within a few tens of miles of an object in order to detect and/or identify it. Haze, clouds, and precipitation reduce this range even further, sometimes to the point that these sensors become temporarily useless.¹⁸² Space-based infrared sensors must additionally cope with the Earth’s natural reflectivity saturating several large blocks of the infrared spectrum.

Defenders have two options for neutralizing electro-optical and infrared sensors. One is the millennia-old approach of using obscurant aerosols such as smoke to conceal a defended warship or to ‘legitimize’ a decoy.¹⁸³ The other, more advanced technique is to use a laser to damage or temporarily blind an electro-optical or infrared sensor. This is relatively straightforward against a sensor that can only operate at a single visible-band or infrared wavelength. A laser designed to transmit at the sensor’s detectable wavelength either saturates or permanently damages the sensor’s receptor elements. The laser beam does not need to be extremely powerful or particularly focused to have this effect, even from a distance.¹⁸⁴ The lasing platform only needs to be stable enough so that the laser can maintain its aim using targeting data provided by a telescopic sight.

Multispectral and hyperspectral sensors are more difficult to effectively lase. Contemporary lasers can only transmit within a relatively narrow block of preset wavelengths. These wavelengths are determined by the nature of the specific materials used within the laser to excite and amplify visible-band or infrared radiation. The defender must therefore use an array of

¹⁸² Payne, 117-123.
¹⁸³ Culora, 73-74.
multiple lasers to neutralize a multispectral or hyperspectral sensor. The more visible and infrared wavelengths that the adversary’s sensor can use, the more lasers the defender must employ against the sensor. This obviously presents the defender’s laser-carrying platform with power, space, and weight challenges. The defender must also know precisely what wavelengths are used by the adversary’s sensor in order to make sure lasers capable of covering the correct spectral blocks are included on the laser-carrying platform.185

Shipboard lasers are best reserved for terminal phase blinding of any electro-optical or infrared homing sensors carried by an ASBM warhead. In contrast, a large high altitude manned aircraft or HALE UAV equipped with a modular array of solid state lasers could be theoretically used against COSS high altitude reconnaissance aircraft, UAV, and/or space-based electro-optical and infrared surveillance sensors.186 By using airborne instead of shipboard lasers, the U.S. can avoid giving away the specific locations of ships in a battleforce. Employing the lasers from high altitude platforms also increases their utility due to decreased atmospheric attenuation of the laser beams. One of the specific benefits to using lasers as a blinding mechanism against an imagery satellite is that it forces the satellite to close the shutters protecting its sensors, change its orbit, or otherwise tolerate the blinding effect until it passes out of range. Closing the sensor’s shutters yields the same tactical effect as the direct blinding. Changing orbits burns some of the satellite’s precious maneuvering fuel, thereby eroding the satellite’s operational lifetime on the margins.

186 A solid state laser uses a solid crystalline material as its excitation and amplification medium. In contrast, the U.S. Missile Defense Agency’s existing Airborne Laser uses chemical reactions for the same purpose. Solid state laser technology, while still developmental, requires far less space and weight than contemporary chemical lasers. Also, while chemical lasers only have a set number of ‘shots’ until the often-hazardous chemical reactants powering them are depleted, solid state lasers can ‘shoot’ until the generator providing the laser with electrical power runs out of fuel. For more information on U.S. Navy research into potential solid state laser usage against electro-optical sensors, see Kiel, “A Vision for Directed Energy and Electric Weapons In the Current and Future Navy,” 4-5.
At least for the near future, though, the laser-based approach seems less affordable and flexible than the obscurant-based approach. Peacetime use of lasers against surveillance sensors is also provocative and potentially escalatory. Use of inexpensive advanced obscurants, not to mention night and weather as cover, gives a naval battleforce tools for countering overhead electro-optical and infrared surveillance and targeting sensors. By neutralizing these sensors, COSS would not be able to remotely confirm the validity of radar contact detections or images. This would severely limit the PLA’s ability to effectively target and fire a weapon such as an ASBM using data obtained solely via remote sensors. COSS would therefore need to dispatch scouts such as maritime reconnaissance aircraft or UAVs for closer-range investigations of contacts. Should hostilities break out, a naval battleforce’s defensive screens can neutralize or destroy these scouts long before the scouts’ sensors can detect and identify the battleforce’s warships. This would not be fundamentally different than the U.S. Navy’s anti-pathfinder measures during the Cold War.

**EW Against COSS RF Direction-Finding/ELINT Sensors**

There are three main tactics that are applicable against RF direction-finding/ELINT sensors: counter-Specific Emitter Identification (SEI), RF EMCON, and battleforce-level maneuver. Each of them are meant to deny critical information to a maritime surveillance and targeting network like COSS by modifying and restricting RF emissions or by evading the network’s locatable sensors.

As noted in the Cold War case, RF emission ‘fingerprinting’ complicates deception. An adversary ELINT sensor with these SEI capabilities, particularly one with an ELINT database that identifies the one-of-a-kind emissions characteristics of each individual RF system on a
given warship, can theoretically tell the difference between a real warship’s emissions and a
decoy’s deceptive emissions. The keys to neutralizing SEI are to deliberately alter and/or
suppress RF systems’ fingerprints. Since this fingerprint is largely caused by the electronic
‘noise’ resulting from RF systems’ individual components’ unique inherent electrical properties,
periodically replacing certain components within an RF system or exchanging components
between two RF systems of the same model can result in slight but potentially meaningful
fingerprint changes. The fingerprint is also sometimes affected by simply jarring some of an RF
system’s components during routine maintenance. Furthermore, naval battleforces’ future
advanced radars will be able to support counter-SEI efforts by generating pulse waveforms with
less inherent noise.\(^{187}\) This will not only decrease the amount of undesired system-inserted noise
in a pulse’s waveform, but also offer the option of inserting false noise sources into the
waveform in order to spoof an SEI system.\(^{188}\) It follows that installing the same low-fingerprint
RF systems on multiple warships types and classes, much as the U.S. Navy did during the 1970s
and 1980s with the *AN/SPS-49* air search radar, increases an adversary’s difficulties in
maintaining a high-confidence SEI database. This can result in the defender regaining flexibility
for using deceptive radar and radio emissions for countersurveillance, countertargeting, and
perhaps even distraction purposes.

**EMCON** will also continue to be highly relevant against maritime surveillance and
targeting systems like COSS. In order to avoid passive detection in peacetime and war, U.S.
Navy battleforces will need to limit their use of RF systems that can be exploited by Chinese

---

\(^{187}\) Future advanced radars will use digital synthesizers instead of analog oscillators as their waveform generators. Radar and radio systems convert the waves these devices generate into RF, amplify them by several orders of magnitude, and then transmit them into free space as a pulse. Analog oscillators rely on complex circuits to tune and modulate a wave. These circuits’ components’ inherent electrical properties impose undesired electronic noise on the waves they generate. Conversely, digital synthesizers use computer processors to tune and modulate a wave. This can significantly reduce the sources of undesired electronic noise imposed on the wave.

direction-finding/ELINT satellites, maritime reconnaissance aircraft and UAVs, warships, AGIs, and submarines. This means battleforces seeking to avoid detection will need to restore the ability to use Cold War-era tactics such as minimizing the use of non-directional radios and having AEW aircraft serve as aircraft carriers’ air traffic control centers. U.S. Navy warship crews might find it necessary to restore their proficiency in using visible-band and infrared flashing signal lamps for short-range communications in restrictive RF EMCON environments. Intermediate-term advances in laser technology may provide additional options for short-range high data rate communications during EMCON. Land and/or carrier-based UAVs could take on the Cold War-era airborne ‘middleman’ mission by carrying directional radio relay systems capable of supporting long-range line of sight voice and data communications between battleforce units. Unmanned vehicles’ active and passive sensors will also become increasingly important tools for extending the battleforce’s ‘eyes’ and ‘ears,’ especially during periods when the tactical situation calls for warships to employ the most restrictive EMCON conditions. Installation of the same radar models on multiple warship types, use of counter-SEI techniques, and selective EMCON of shipboard RF systems will prevent COSS RF direction-finding/ELINT sensors from easily distinguishing between warships within the battleforce’s formation. The bottom line is that safe and effective EMCON operations will require a U.S. Navy cultural shift away from relatively unrestricted use of RF systems and towards significantly increased communications and sensor discipline, not to mention a greater reliance on decentralized command and control.

---

189 “Laser Communications,” Office of Naval Research.
190 This would also hold true if ASBM warheads are equipped with RF direction-finding/ELINT sensors. If the warhead cannot distinguish between different warships by virtue of their respective radar emissions, the warhead’s ability to correctly lock onto an intended target becomes more complicated.
Battleforce-level maneuver presents additional countersurveillance and countertargeting options. The atmosphere refracts RF waves in varying amounts depending upon relative air density at a given altitude above sea level and the RF system’s carrier frequency. These effects are particularly significant the longer an RF wave has to travel or the denser the air layer it must penetrate. By routinely monitoring atmospheric conditions, battleforce commanders can predict the ever-shifting ranges at which their warships will be detectable by COSS RF direction-finding/ELINT sensors as well as radars. Since many COSS sensors either have fixed locations, predictable orbits, or can be detected before they themselves detect a battleforce, U.S. Navy commanders can use atmospheric condition monitoring to retain some flexibility regarding battleforce maneuvering plans and EMCON usage. It follows that battleforces will use reconnaissance aircraft and unmanned vehicles to locate commercial vessels or Chinese warships and AGIs within a given area. Battleforce commanders will use this reconnaissance data as a basis for adjusting their schemes of maneuver in order to evade detection and support deception.

**Active EW against COSS Satellite Communications**

Perhaps the greatest difficulty in wide-area surveillance and targeting is quickly communicating sensor data to a fusion center. Communications satellites serve as the critical links that make COSS and the ASBM reconnaissance-strike system work.

---

191 This includes ionospheric conditions as well. An OTH-B’s effective range and sensitivity varies in accordance with ionospheric conditions. Increased solar activity or other phenomena that alter ionospheric conditions will affect OTH-B performance, much as air density in the lower atmosphere will affect an aircraft or shipboard search radar’s performance. Naval battleforces can use speed and maneuver to take advantage of periods when ionospheric behavior decreases OTH-B performance.

In theory, artificial stimuli could also be used to alter ambient ionospheric conditions in a way that degrades OTH-B performance. No military system capable of doing this on a sufficiently large scale is known to exist, and the technology necessary for such a system is almost certainly immature. It is not clear that any such system could even be placed in a location from where it could affect Chinese OTH-B performance. For a technical explanation of the principles behind this concept, see “HAARP Research and Applications,” 13.
Assuming physical destruction of adversary satellites is undesirable for both political and practical reasons, it is useful to consider EW-based alternatives. The Cold War-era development of highly directional communications antennas made it incredibly difficult to intercept let alone jam a transmitting unit’s uplink beam. Satellites, though, can be easily tracked. A defender can theoretically launch small, short-lifetime satellites carrying low power communications jammers into orbits near an adversary’s surveillance or communications satellites. By placing these jammer-satellites relatively close to the boresights of the targeted satellites’ downlink antennae, the defender can use RF noise or deception jamming techniques similar to some of those used against radars to degrade or neutralize the satellites’ abilities to pass sensor data to ground stations. The jammer-satellites can similarly hamper uplinked communications from ground stations as well.

Much like the case with lasers, this approach can force targeted satellites to burn some of their limited maneuvering fuel as they move into new orbits away from the jammer-satellites. A sufficient stockpile of inexpensive, operationally-responsive jammer-satellites could therefore be tapped situationally in support of naval battleforce operations. Reducing a remote sensor’s window of opportunity to downlink contact data and/or increasing the amount of time it takes the remote sensor to finish a data download buys time for a naval battleforce’s movement to result in a non-actionable AOU. Co-orbital jammer-satellites also offer a potential vehicle for cyber

---

192 Notwithstanding numerous domestic and international political considerations, kinetic impact-based destruction of satellites is undesirable as the resultant debris would pose a severe and long-lasting hazard to one’s own safety of spaceflight. Emerging technologies such as space-based robotics suggest that ‘robotic saboteur’ systems could be used to neutralize a satellite without significantly endangering safety of spaceflight. The same might be true with small ‘assassin’ satellites equipped with HPM devices. However, use of such systems would be extremely escalatory outside of a general war. For a comprehensive analysis of the tradeoffs between different alternatives for anti-satellite warfare, see Latchford, 32-42.

193 Ibid, 23.
attacks against either targeted satellites or ground stations. The downside is that use of jammer-satellites would be incredibly provocative and escalatory outside of war. Jammer-satellites therefore would likely only become politically viable for use against COSS in the aftermath of a Chinese first strike.

**EW against COSS’s Maritime Situational Picture Database**

Another emerging countersurveillance and counternetting technique, while not very technical, requires significant operational discipline to be effective. Over the past decade, many countries began requiring that vessels use computerized Automatic Identification Systems (AIS) to broadcast their names, cargoes, itineraries, and other voyage details to coast guards and port authorities. This was viewed as a maritime security measure as well as a means for countries to keep track of the vessels approaching or traversing their territorial waters and offshore exclusive economic zones. In theory, a maritime surveillance system can fuse AIS data with the situational picture derived from radar and RF direction-finding/ELINT data to discriminate commercial vessels from warships. It follows that a ship detected by a wide-area sensor that is not broadcasting AIS will generally attract a maritime surveillance system’s attention, much as an aircraft that is not operating its transponder triggers the attention of air defense authorities. Defeating AIS-based data fusion therefore requires that warships broadcast false AIS identities. This may be insufficient on its own, though. The warships in a battleforce must also travel on headings, at speeds, and near shipping lanes or deep sea fishing areas consistent with their false AIS identities. Much as was the case against RORSAT, battleforces will likely need to use defensive formations that do not ruin their warships’ AIS covers by looking like traditional naval

---

194 An example of a similar tactical cyber attack capability is the rumored U.S. Air Force “Senior Suter” system. See Gasparre, “The Israeli ‘E-tack’ on Syria’ Part II.”
formations. Warships may also need to operate commercial navigation radars configured using counter-SEI techniques to attain additional credibility.

### Table 3: Summary of EW Technologies and Tactics

<table>
<thead>
<tr>
<th>Technology/Tactic Name</th>
<th>Applicability against COSS and ASBM Reconnaissance-Strike System Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-radar Passive Offboard Decoys (Balloons, chaff, RF obscurant aerosols)</td>
<td>SAR satellites, reconnaissance aircraft/UAV radars, ASBM warhead radars</td>
</tr>
<tr>
<td>Active Offboard Decoys</td>
<td>ASBM warhead radars</td>
</tr>
<tr>
<td>DRFM-Based Advanced Active Techniques</td>
<td>SAR satellites, reconnaissance aircraft/UAV radars, ASBM warhead radars</td>
</tr>
<tr>
<td>Solid State Lasers</td>
<td>Electro-optical/Infrared sensors on satellites, reconnaissance aircraft/UAVs, ASBM warheads (if applicable)</td>
</tr>
<tr>
<td>Infrared and visible-band obscurant aerosols</td>
<td>Electro-optical/Infrared sensors on satellites, reconnaissance aircraft/UAVs, ASBM warheads (if applicable)</td>
</tr>
<tr>
<td>Counter-SEI</td>
<td>RF direction-finding/ELINT sensors on satellites, reconnaissance aircraft/UAVs, warships, AGIs, shore stations</td>
</tr>
<tr>
<td>Selective RF EMCON</td>
<td>RF direction-finding/ELINT sensors on satellites, reconnaissance aircraft/UAVs, warships, submarines, AGIs, shore stations</td>
</tr>
<tr>
<td>Battleforce-level maneuver</td>
<td>Space-based sensors, OTH-B, reconnaissance aircraft/UAVs, warships, submarines, AGIs, shore stations</td>
</tr>
<tr>
<td>Co-orbital satellite jamming</td>
<td>Space-based sensors, data relay satellites</td>
</tr>
<tr>
<td>AIS spoofing</td>
<td>COSS operators’ data fusion systems and tactical decision-making aids</td>
</tr>
</tbody>
</table>

**EW Integration with U.S. Navy Active Anti-ASBM Defenses**

As should be clear from the preceding discussion of EW technologies and tactics, no single approach offers a guaranteed ‘silver bullet’ against COSS or ASBM warhead sensors. EW therefore cannot serve as a stand-alone surrogate for active defenses. What U.S. Navy EW can do is combine with active defenses to increase the number of variables that Chinese maritime surveillance, targeting, and strike systems must overcome in order effectively employ ASBMs.

ICADS-like deception systems, selective RF EMCON, counter-SEI, and AIS-spoofing could be used to cause COSS operator confusion regarding their maritime situational picture’s validity. This might induce them to hesitate in committing scout resources or weapons against particular contacts or contact groupings. Conversely, these systems and techniques might be used

---

196 Credit for the idea of developing new ICADS-like systems belongs to CAPT Sam Tangredi, USN (Ret). CAPT Tangredi appears to have been the first to publicly suggest this concept. See Tangredi, 27.
to coax PLA decision-makers into wasting ASBMs against decoy groups. Jammer-satellites and high altitude solid state laser-carrying aircraft could also contribute to these ends following the outbreak of hostilities, though infrared and visible-band obscurants might end up being more cost-effective than the laser aircraft concept.

Once it becomes clear that an ASBM raid has been launched against an actual battleforce, it stands to reason that the battleforce gains little by maintaining the most restrictive EMCON measures. Future advanced shipboard radars will improve U.S. Navy battleforces’ abilities to track ASBMs as well as support BMD interceptor engagements against them. Assuming that ASBM warheads conduct quick SAR scans of the target area during their midcourse phases in order to guide trajectory adjustments for atmospheric reentry, ICADS-like systems and/or active offboard decoys could use DRFM-based image generators to distract the warheads into committing themselves against false targets. Battleforce missile defense-capable radars will be critical in evaluating the effectiveness of this active EW by tracking ASBM warheads’ maneuvers. In turn, battleforce RF direction-finding/ELINT systems allow correlation of warheads’ radar emissions to specific exoatmospheric objects being tracked by battleforce radars. This would contribute greatly to battleforce radars’ efforts to discriminate the warheads from any decoys or debris released by the ASBMs.

If the battleforce’s radars determine that specific ASBM warheads have irrevocably aimed themselves at false targets prior to reentry, the battleforce’s active missile defense systems can spare use of terminal phase BMD interceptors against them. The radars will also be critical

197 In order to do this, battleforce RF direction-finding/ELINT systems would need to be capable of extremely precise measurement of a warhead’s radar’s emissions’ angle of arrival at the direction-finder’s antenna. This could be accomplished by correlating and crossfixing RF direction-finding/ELINT data from multiple dispersed battleforce sensors.
198 This could be done if the ASBM MaRV warheads’ kinematic limitations are well understood by the U.S. These kinematic limitations will be dictated by how much fuel the MaRV or its post-boost vehicle can carry for exoatmospheric maneuvers, how much kinetic energy the MaRV has by virtue of its velocity, and how aerodynamic
for sequencing terminal phase EW countermeasures prior to and during the warheads’ use of homing sensors. Effective decoy, chaff, and/or obscurant placement patterns and reseeding, not to mention EW technique selection and timing, depends largely on knowing the reentering warheads’ velocities, altitudes, azimuths relative to defended warships, and times remaining to impact as only a radar can provide.\textsuperscript{199}

The split-second timing needed for many of these actions requires integration of active missile defense control systems and EW control systems. This enables deconfliction between BMD interceptor engagement scheduling and EW countermeasure scheduling to ensure that neither unacceptably reduces the other’s effectiveness.\textsuperscript{200} This coordination could also help prevent an active missile defense system from becoming saturated at a critical time while an EW system has resources available for tasking or vice-versa. It follows that this integration helps the active missile defense control system decide whether terminal phase interceptors no longer need to be launched against a specific inbound warhead thanks to successful EW.

While EW will not necessarily increase BMD interceptors’ inherent lethality, and BMD interceptors will definitely not increase EW effectiveness, their coordinated use can increase the battleforce’s ASBM defense’s overall effectiveness. Past analysis of a Cold War-scale anti-ship missile raid suggests that defensive EW might have been able to defeat approximately half of the inbound missiles not destroyed by BMD interceptors.\textsuperscript{201} Let us assume that this theoretical success rate holds true for ASBM defense once the relevant defensive EW systems and tactics are developed. Returning to the ASBM salvo-sizing thought experiment from Section III, if we

\textsuperscript{199} Kimbrell, 85
\textsuperscript{200} For instance, chaff and some kinds of active EW transmissions might degrade the battleforce’s missile defense radars’ performance. Some degradation is probably unavoidable, but it might nevertheless be held to tolerable amounts if active defenses and EW countermeasures are effectively coordinated in time and space.\textsuperscript{201} Harney, “Broadening the Trade-Space in Designing for Warship Survivability,” 56.
arbitrarily assume that 10% of the ASBMs fired in a raid suffer system failures and 40% are destroyed by BMD interceptors, then the above defensive EW success rate would claim another 20% of the original raid’s size.\textsuperscript{202} Since a ‘fractional’ ASBM is impossible, the PLA would therefore theoretically need to launch nine ASBMs in order to score the needed three hits to incapacitate an aircraft carrier. The PLA would also need to launch three ASBMs to secure a reasonable chance of scoring the one hit needed to incapacitate a single large surface combatant. An ASBM raid against a battleforce consisting of one carrier and six large surface combatants would consequently require 27 missiles.\textsuperscript{203} Given all these arbitrary assumptions, defensive EW’s probabilistic effects would increase the PLA’s required number of ASBMs per salvo by 50% over the example in Section III. This would also theoretically limit the PLA to five ‘full-sized’ ASBM salvos with one additional raid of five ASBMs before its inventory is spent. Effects such as these strongly suggest that EW and active defenses should not be competed against each other when deciding upon defensive capability investment priorities.

If marginal tradeoffs must be made, though, the investment prioritization decision would appear to hinge upon the quality and quantity of U.S. intelligence on COSS and the ASBM reconnaissance-strike system, U.S. leaders’ confidence in that intelligence, and whether or not this intelligence exposes EW and deception-exploitable Chinese vulnerabilities. As stated in

\textsuperscript{202} This does not attempt to judge the effects of a truly layered defense against an ASBM raid. Even if BMD interceptors and individual EW techniques each have low probabilities of effectiveness against ASBM warheads if used once on their own, the laws of probability state that the number of warheads that survive to endgame decreases as the number of defensive layers increases. An example of this is a layered defense in which a single ASBM must survive two separate BMD interceptor engagement opportunities and one deceptive EW opportunity during the midcourse phase followed by at least one BMD interceptor engagement opportunity and multiple distraction and seduction technique opportunities during the terminal phase. The thought experiments in this paper do not assume how many engagement opportunities exist against an inbound ASBM. Therefore, with appropriate layering, a notional defense’s probability of success could be even higher than what is assumed here for illustrative purposes.

\textsuperscript{203} Since the arbitrarily-selected probabilities of a single ASBM not suffering a system failure during launch or flight (90%), not being destroyed by defensive interceptors (60%), and not succumbing to defensive EW (80%) are independent of each other, this thought experiment’s joint probability of an ASBM successfully hitting a target is 0.9 x 0.6 x 0.8 = 0.432. The rough number of ASBMs therefore needed for a single hit is $1/0.432 = 2.314$, which must be rounded up to 3 since there cannot be a ‘fractional’ ASBM.
Section V, this intelligence must cover the systems’ technical details, employment tactics, and doctrine as well as PLA leaders’ and COSS operators’ decision-making procedures and tendencies. If U.S. leaders collect comprehensive intelligence on these subjects, if they are highly confident that this intelligence is accurate, and if the intelligence reveals exploitable Chinese vulnerabilities, then it might be possible to improve battleforce defenses more by prioritizing marginal investment in EW and tactical deception capabilities. However, if intelligence on Chinese vulnerabilities is limited, if U.S. leaders are not highly confident in its accuracy, and/or if successful exploitation appears relatively uncertain, then prioritizing marginal investment in active defenses would seem advisable.

In practice, U.S. leaders weighing anti-ASBM capability investment decisions would almost certainly want to take advantage of whatever intelligence they possessed and had reasonable confidence in while simultaneously hedging against the risk of misplaced faith in that intelligence. Arming a battleforce primarily with non-kinetic countermeasures and only piecemeal active defenses exacerbates the consequences of an intelligence failure. Arming a battleforce primarily with active defenses and only piecemeal EW and tactical deception capabilities cedes the operational and tactical opportunities as well as the battleforce survivability enhancements that accurate intelligence would enable. As technical, tactical, and operational uncertainty can never be fully eliminated, investing in both kinetic and non-kinetic ASBM defenses would likely yield the best overall capability.

New-construction warships’ requirements for low observable ‘stealth’ design features, namely drastically reduced hull and superstructure radar cross sections, present a more promising area for potential investment prioritization tradeoffs. As noted in this Section as well as the Section IV Cold War case study, EW has continuously evolved in response to the past half
century’s rapid evolution in maritime sensor capabilities. A warship’s inherent stealth design features, on the other hand, cannot keep pace with sensor evolution. Each sensor generation’s increased sensitivity correspondingly devalues the warship design’s fixed amount of signature suppression.\textsuperscript{204} Extreme low observability also drives a warship’s design such that displacement and internal volume must be increased significantly.\textsuperscript{205} Given that U.S. Navy large surface combatants’ and aircraft carriers’ budgeted lifetimes are 35 and nearly 50 years respectively, incremental EW system improvements appear to provide more defensive potential over the long haul than inherent stealthy design features. This is not to say that some degree of low observability is not desirable in warship design.\textsuperscript{206} It does mean that disciplined engineering tradeoff analysis is necessary to determine whether a future warship is better served over its lifetime by prioritizing up-front investment in an inherently stealthy design or by prioritizing continuous investment in battleforce EW systems’ iterative evolution.

Lastly, it is important to note that the thought experiment’s theoretical defensive EW success rate does not account for offensive EW’s and tactical deception’s less quantifiable potential roles in battleforce defense. Although the thought experiment’s 34-missile ASBM salvo would heavily stress a U.S. Navy battleforce’s overall defenses if it were aimed correctly, it also would impose a severe cost on the PLA’s ASBM inventory in the event it was aimed poorly or decoyed entirely. As Section VII will show, the challenge will be in implementing emerging EW

\textsuperscript{204} Harney, 53-55.
\textsuperscript{205} Friedman, \textit{U.S. Destroyers}, 434. For more information on how displacement and design complexity relate to warship procurement costs, see Mark V. Arena et al., “Why Has the Cost of Navy Ships Risen? A Macroscopic Examination of the Trends in U.S. Naval Ship Costs Over the Past Several Decades,” xv.
\textsuperscript{206} Some EW techniques require the defended warship’s electromagnetic signatures to be beneath certain thresholds in order for offboard decoys to distract or seduce inbound missiles. Engineering analysis is necessary, though, to determine if these EW techniques are the best ones for protecting that particular warship class. If these techniques are in fact the best, then the next stage of engineering analysis must examine how much additional investment in signatures reduction below the minimum threshold is desirable compared to investment in other defensive capabilities.
technologies within real-world systems and tactical concepts so that they not only enhance battleforce ASBM defense but also make deception against COSS viable.
VII. Anti-ASBM EW Implementation Concepts for the U.S. Navy

Current U.S. Navy EW Development Programs of Record

In discussing its measures to “deter and defeat aggression in anti-access environments,” the U.S. DOD’s 2010 Quadrennial Defense Review (QDR) notes a decision to increase investment in selected EW capabilities that can help counter potential adversaries’ advanced surveillance and strike systems.\(^{207}\) This language, combined with the QDR’s discussions of other capabilities necessary for U.S. military operations against a near-peer military’s anti-access/area-denial capabilities, is unmistakably directed against the PLA threat. The U.S. Navy’s Chief of Naval Operations, Admiral Gray Roughead, elaborated on this direction by noting in his 2011 guidance message that the Navy would “direct resources to game-changing technologies and concepts, especially those at the left end of the effects chain and in information dominance.”\(^{208}\)

The 2010 Naval Operations Concept, an explanatory document supporting the U.S. Navy, Marine Corps, and Coast Guard’s 2007 strategic vision document, further notes that battleforce information operations are one of the enabling components of U.S. Navy sea control capabilities within an anti-access environment.\(^{209}\)

The U.S. Navy’s two main developmental EW systems at present are the Surface Electronic Warfare Improvement Program (SEWIP) for warships and the Next Generation

\(^{207}\) “Quadrennial Defense Review Report,” 34.
\(^{208}\) “CNO Guidance for 2011,” 5. For clarification, the phrase “left end of the effects chain” represents another way of describing surveillance and targeting capabilities, i.e. the prerequisite steps to executing a strike or similar action that generates ‘effects’ upon the adversary.
\(^{209}\) “Naval Operations Concept 2010: Implementing the Maritime Strategy,” 56. Of note, sea control is a classical maritime strategic term that defines a navy’s ability to use a specific ocean area at a specific time for one or more specific purposes. If one has attained local area sea control relative to an adversary, one can use that control to attrite the adversary’s naval forces, protect one’s own sea lines of communication, or provide a maritime sanctuary for one’s projection of national power ashore against the adversary. Conversely, sea denial is the classical maritime strategic term that defines use of naval and/or land-based maritime forces to prevent an adversary’s navy from securing sea control of a specific ocean area at a specific time.
Jammer (NGJ) for tactical aircraft. SEWIP represents a series of incremental improvements to the legacy AN/SLQ-32 shipboard EW system. The first two SEWIP ‘block’ increments programmed within the Navy’s budget focus on improving upon or otherwise replacing AN/SLQ-32 radar detection and signal processing components. They do not add active EW capabilities. NGJ on the other hand will provide robust active EW capabilities against advanced radars. Media articles imply NGJ will be agile enough to react to pulse-to-pulse changes in an adversary’s radar transmissions, use “tailored waveforms to unlock enemy electronics,” and transmit “in-band in a more deceptive construct than just simply putting out jamming noise.”

All three of these capabilities strongly suggest use of DRFM. NGJ, though, is being designed for tactical aircraft self-protection and standoff active EW against an adversary’s air defenses. While its technologies are likely extensible for use in other future active EW systems, it is not clear that anti-COSS or anti-ASBM warhead capabilities are included in its current requirements.

Current U.S. Navy EW Applied Research Efforts

Active EW capability development against COSS and ASBM warhead sensors, however, is evident in the unclassified portion of the U.S. Navy’s budget. In its fiscal year 2011 budgetary request, the Navy described an ongoing project that is developing next generation countermeasures against ASBM warheads and other anti-ship missiles by adding active EW capabilities to SEWIP as well as improving the Nulka active offboard decoys. Another project

---

212 In the U.S. Navy’s fiscal year 2012 budget request submission, SEWIP active EW capability development (also known as SEWIP Block 3) reportedly transitions from the applied research stage into a formal acquisition program of record. The Navy has supposedly requested about $413 million through fiscal year 2016 for SEWIP Block 3. Media reports indicate that the SEWIP Prime Contractor, Lockheed-Martin, has already built a SEWIP active EW technology demonstrator. Developmental testing and evaluation using this demonstrator is to be conducted during fiscal year 2012, and operational testing and evaluation of SEWIP Block 3 is scheduled for fiscal year 2015. A
aimed to develop a network that would allow an entire battleforce to coordinate use of EW against advanced missile threats. These projects are reportedly structured to become acquisition programs of record upon reaching a certain degree of technical maturity.\textsuperscript{213} Several component-level applied research efforts supporting these projects were initiated in fiscal year 2010, and at least one effort was planned for expansion during fiscal year 2011.\textsuperscript{214} It goes without saying that additional ongoing research and development efforts mirroring these might be funded within the classified portion of the Navy’s budget.

Some of the U.S. Navy’s requirements for next generation EW systems can be derived from statements by the Office of Naval Research (ONR). In their January 2010 “industry day” presentation to potential contract bidders, ONR’s EW Program Manager expressed the Navy’s desire for small, lightweight, low-power EW payloads for use in manned and unmanned vehicles. He noted the Navy’s interest in coordinating active EW techniques and algorithms between multiple EW-capable platforms as well as conducting research into EW integration with active missile defenses. He also highlighted the Navy’s need for electro-optical, infrared, and RF EW systems capable of receiving and transmitting across much wider spectral blocks such that fewer frequencies are left open for an adversary’s unfettered use. He lastly observed the Navy’s desire for EW systems with faster signal processing and active techniques generation capabilities.\textsuperscript{215}

These technologies’ current maturities are indicated by the fact that the presentation was geared towards soliciting contractor bids for ONR “Discovery and Invention” projects. According to the presentation, Discovery and Invention projects transition basic scientific research into a concept technology. Successful projects increase a new technology’s maturity to the point that prototype components can be tested individually within a laboratory environment. Most of these projects are intended to last one to three years, at which point an investment decision regarding whether to continue into several more years of formal development of a system based upon the concept technology would need to be made. Projects funded during fiscal year 2009 included multi-wavelength laser technology for use against infrared sensors, obscurant technology capable of rendering an area opaque to multiple bands of the electromagnetic spectrum, and a directed energy technology capable of neutralizing electromagnetic sensors.216

ONR’s areas of interest for fiscal year 2010-initiated EW Discovery and Invention projects include techniques for realistic false target generation and control as well as remotely detecting, identifying, and preventing battleforce detection by an adversary’s passive sensors. These techniques are to be designed for use in offboard systems that are not supposed to rely on communications or sensor emissions from defended warships in order to function. ONR also appears involved in the ongoing technology development projects mentioned in the Navy’s fiscal year 2011 budget request.217

Near-Term Tactical and Operational Concepts for Defeating the ASBM

U.S. Navy development of advanced EW capabilities applicable against COSS and ASBM warhead sensors is clearly underway. However, it appears that most of these technologies

may take the better part of a decade to mature to the point that they can be successfully
implemented within battleforce systems. For the next few years, therefore, the minimum set of
U.S. Navy EW countersurveillance and countertargeting tactics available for use prior to a PLA
ASBM first salvo will consist of the following:

<table>
<thead>
<tr>
<th>Tactic Name</th>
<th>Probable Effectiveness Against COSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF EMCON</td>
<td>High against RF direction-finding/ELINT sensors due to denial of telltale RF emissions; denies information that is highly useful for cueing other COSS sensors. Also likely effective if ASBM warhead is equipped with an RF direction-finding sensor and selective RF EMCON is employed by HVUs to prevent themselves from being identified.</td>
</tr>
<tr>
<td>Battleforce evasion of locatable Chinese sensors or sensor-carrying platforms</td>
<td>High against space-based sensors with known orbital characteristics, OTH-B, and scouts that are detected beyond the range that they themselves can detect the battleforce’s ships; low against scouts practicing evasion or RF EMCON of their own.</td>
</tr>
<tr>
<td>Weather masking</td>
<td>High against airborne/space-based infrared and electro-optical surveillance sensors; medium against OTH-B; low against airborne/space-based/ship-based surveillance radars.</td>
</tr>
<tr>
<td>Infrared/Visible-Band Obscurants</td>
<td>High against airborne/space-based infrared and electro-optical surveillance sensors.</td>
</tr>
<tr>
<td>Dispersed battleforce formations</td>
<td>High against OTH-B and airborne/space-based wide-area search radars if properly coordinated with other countersurveillance and countertargeting tactics; low if not coordinated.</td>
</tr>
<tr>
<td>SEI spoofing</td>
<td>High against ELINT sensors due to denial of fingerprinting phenomena; best used in concert with other deceptive measures.</td>
</tr>
<tr>
<td>AIS Spoofing</td>
<td>High if properly coordinated within an overall tactical deception plan (includes counterintelligence measures); low if not incorporated within plan or plan is otherwise ineffective.</td>
</tr>
<tr>
<td>Deceptive communications</td>
<td></td>
</tr>
<tr>
<td>Deceptive use of actively-transmitting sensors</td>
<td></td>
</tr>
<tr>
<td>Deceptive battleforce-level maneuver</td>
<td></td>
</tr>
<tr>
<td>Decoy Groups</td>
<td></td>
</tr>
</tbody>
</table>

Large surface combatants conducting BMD patrols near Okinawa or in the Sea of Japan
prior to a notional Chinese first strike would likely be unable to take advantage of the tactics in
Table 4. These BMD patrol stations would be completely dependent on their interceptor missiles
as well as any fielded anti-ASBM EW capabilities. Other U.S. Navy battleforces whose missions
grant them more flexibility to use Table 4’s concealment and deception tactics would nonetheless also need to augment their interceptor missile inventories with anti-ASBM EW. Interim EW self-defense capabilities against ASBM warheads may include modified Nulka rounds or other existing offboard decoys. Expanded EW self-defense will likely become possible later in the decade once SEWIP gains active EW capabilities and enhanced-capability Nulka rounds or other future active offboard decoys enter service. Advanced millimeter-wave RF, infrared, and visible-band obscurants already used by the other U.S. armed services might also be adaptable in the near-term for self-concealment of warships from ASBM warhead sensors.218

<table>
<thead>
<tr>
<th>System Name/Type</th>
<th>Probable Effectiveness Against ASBM Warhead Sensors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modified existing Nulka rounds</td>
<td>Unknown due to classified nature of current Nulka capabilities as well as potential for notional interim modifications to existing rounds. If modified rounds cannot transmit millimeter-wave RF, then low. If ASBM warhead’s terminal radar has ISAR capability and modified rounds cannot perform false ISAR image generation, then low. If ASBM warhead’s terminal radar does not have ISAR capability and modified rounds can transmit millimeter-wave RF, then varies depending on quality of intelligence regarding ASBM terminal radar characteristics and counter-EW measures.</td>
</tr>
<tr>
<td>New enhanced-capability Nulka rounds or other future active offboard decoy with false ISAR image generation capabilities</td>
<td>Varies depending on quality of intelligence regarding ASBM terminal radar characteristics and counter-EW measures.</td>
</tr>
<tr>
<td>SEWIP Block 3 (Active EW capability)</td>
<td>Will likely vary depending on coordinated use with Nulka or other active offboard decoys as well as quality of intelligence regarding ASBM terminal radar characteristics and counter-EW measures. May be particularly useful if ASBM warhead uses exoatmospheric SAR for target search depending on quality of intelligence regarding the SAR’s characteristics and counter-EW measures.</td>
</tr>
<tr>
<td>Passive offboard balloon decoys</td>
<td>Will likely vary depending on coordinated use with active EW systems as well as quality of intelligence regarding ASBM terminal radar characteristics and counter-EW measures.</td>
</tr>
<tr>
<td>Millimeter-wave RF/Infrared/Visible-band obscurants</td>
<td>Medium to high if deployed over defended warships as well as nearby empty waterspace to create a shell-game effect. Low to medium if this is not done.</td>
</tr>
<tr>
<td>Existing chaff rounds</td>
<td>May be useful as an obscurant if ASBM warhead uses exoatmospheric centimeter-wave SAR for target search. Unlikely to be effective against ASBM warhead’s millimeter-wave terminal radar.</td>
</tr>
</tbody>
</table>

218 Culora, 73-74.
It is important to remember that COSS appears to have only very recently attained an initial operational capability and that deployment and integration of its full ‘first generation’ architecture likely will not be complete until the mid to late 2010s. Depending on COSS’s near-term capabilities, the above countersurveillance and countertoargenting measures might be enough to delay, passively disrupt, or prevent ASBM targeting during the coming half decade or longer. The above EW self-defenses might also be able to distract or seduce some of the ASBMs fired against a battleforce. Ultimately, though, the absence of robust and diverse active EW countermeasures against the ASBM warhead means that battleforce defenses’ near-term probability of success against an effectively-targeted war-opening ASBM salvo will largely hinge upon U.S. Navy BMD interceptor capabilities and inventory numbers.

Following the first ASBM salvo, however, the U.S. will be able to initiate sequential Joint operations that aggressively neutralize COSS’s land and space-based sensors, scout assets, and data fusion capabilities. As previously noted, COSS’s many vulnerabilities open it to systematic, incremental neutralization and/or destruction in the aftermath of a Chinese first strike. Depending on the scope of that first strike and/or the PLA’s follow-on offensive actions, the U.S. might be handed ready-made justifications for retaliatory physical attacks against COSS assets. The OTH-B radar arrays’ huge sizes and fixed locations make them particularly attractive targets early in the anti-COSS campaign. Without OTH-B, COSS must rely on space-based sensors as its primary ocean surveillance assets. U.S. Navy submarines’ relative invulnerability to COSS sensors makes them likely candidates for executing land-attack cruise missile strikes against the OTH-B arrays as well as other high priority land-based COSS assets during the first hours and days of a notional war.219 U.S. Navy battleforces would also be free to seek out and

219 It is possible that the PLA might develop and field relocatable OTH-B systems that could monitor maritime areas the fixed-location OTH-B cannot. Relocatable OTH-Bs could also serve as backups if the fixed-location OTH-B
destroy COSS’s secondary scout assets such as maritime reconnaissance aircraft, UAVs, surface combatants, submarines, and AGIs. All of these measures would be additive to battleforces’ continued use of the technologies and tactics described in Tables 4 and 5. Much as how Cold War analysts believed the Soviet maritime surveillance and reconnaissance-strike system’s combat endurance was overrated, an anti-COSS campaign lasting several weeks would at minimum heavily limit the circumstances under which the PLA could effectively employ ASBMs and at maximum might render the ASBM arsenal nearly impotent regardless of how many missiles remained available for use.

Another critical consideration involves the Cold War case’s principle that a deception effort loses effectiveness once a battleforce reveals itself by conducting a strike or other major unconcealed tactical action. Combined with inherent logistical constraints, this suggests battleforce and/or decoy operations within ocean areas still effectively monitored by COSS would likely be limited to missions of no more than a few days’ duration during the initial phases of a notional war. The actual battleforces would execute brief, tailored-mission operations, after which they and any supporting decoy groups would temporarily withdraw. These missions might include aircraft carrier-led sea control operations geared towards attrition of PLA maritime strike-capable aircraft, surface combatants, and submarines. They might also include carrier-based strikes against any land-based PLA targets along the First Island Chain.

The above tactical concept would be repeated multiple times by multiple different battleforces over the course of the first days and weeks of a conflict. Each successive operation was disabled or destroyed. On one hand, the U.S. would need to conduct extensive ELINT and overhead imagery analysis to locate and target potentially-camouflaged relocatable OTH-B arrays. On the other, relocatable OTH-Bs might not be as sensitive as the fixed-location system if the need for mobility limited them to shorter array lengths and less available transmit power. Relocatable OTH-Bs are also only mobile in the sense that they can be disassembled, transported to a new location, and reassembled over the course of several days or weeks. This means that once found they can be struck just as easily as a fixed-location OTH-B. U.S. intelligence will need to watch for indications that the PLA is developing a relocatable OTH-B capability. For an example of a U.S. relocatable OTH-B system, see “AN/TPS-71 ROTH (Relocatable Over-the-Horizon Radar),” Federation of American Scientists.
would contribute to the overall maritime access-restoration campaign. As COSS’s coverage was accordingly eroded, the duration of individual operations would likely lengthen. Significant, sustained attrition of COSS’s infrastructure and PLA maritime strike-capable platforms would also likely be a prerequisite for carrier operations within a few hundred miles of the Chinese coast or major amphibious operations south of the main Japanese islands. All this dovetails cleanly with unclassified campaign-level concepts describing the conduct of a notional Sino-American war in East Asia. 220

Any hypothetical U.S. Navy combat operations in the Western Pacific against China during the 2010s would without doubt be incredibly challenging and risky. The Cold War case study’s principles and the preceding analysis of COSS strongly suggest, though, that U.S. Navy operational success would hardly be impossible even in the face of the PLA’s growing ASBM arsenal. It certainly seems that the faster that COSS can be blinded and/or picked apart, the faster that the U.S. Navy will gain tactical flexibility for Western Pacific combat operations.

Intermediate-Term Tactical and Operational Concepts for Defeating the ASBM

Assuming the EW technologies currently in the U.S. Navy’s applied research pipeline enter service between the late 2010s and the mid 2020s, new tactical concepts become available to U.S. Navy operations planners. Despite its troubled developmental history, the U.S. Navy’s Littoral Combat Ship’s (LCS) exceptional payload capabilities make it an ideal platform for hosting a notional new ICADS-like modular deception system and/or notional ‘mini-ICADS’ systems installed on existing unmanned vehicles. 221 ICADS-like systems’ initial capabilities

221 Murphy, “Littoral Combat Ship: An Examination of its Possible Concepts of Operation,” 43, 47. LCS is the U.S. Navy’s new small surface combatant. LCS’s primary missions will be ASW, anti-surface warfare, and mine countermeasures.
might include communications deception and simulation of battleforce RF systems. Later capabilities might include DRFM-based image generators for deceiving Chinese SAR and ISAR. LCSs equipped with ICADS-like systems could notionally be used within a battleforce not only for countersurveillance and countertargeting but also to distract ASBMs launched against that battleforce.

Furthermore, LCS’s 45+ knot sprint speed allows it to rapidly reposition itself at a distance from a battleforce.\(^{222}\) With ICADS-like capabilities, several dispersed LCS groups could each notionally simulate a battleforce’s emissions. As noted previously, this could be used to confuse COSS operators as to which contact grouping is real, or alternatively to draw scouts and/or ASBMs away from the actual battleforce. A LCS decoy group could use its sprint speed to reposition itself several times over the course of a few days and simulate a single false battleforce in different locations or several different false battleforces in different locations. This could be done to distract Chinese attention from actual U.S. Navy battleforce operations elsewhere in the combat zone, or to erode the Chinese ASBM inventory at a time when actual battleforces are temporarily positioned outside ASBM range. It goes without saying that if the U.S. was able to induce PLA decision-makers to waste one or more ASBM raids against decoy groups early in a notional war, the corresponding attrition of the ASBM inventory and possible erosion of PLA confidence in COSS could prove invaluable to subsequent U.S. Navy operations.

LCS decoy groups could also be used in support of trans-Pacific supply convoys or transiting battleforces approaching the main Japanese islands. In addition to serving as EW-specialized escorts within these types of formations, distant LCS decoy groups could be used to simulate convoys or battleforces. As before, this could be used to confuse the COSS picture and/or attract ASBM raids away from defended formations. These missions would not require

\(^{222}\) Ibid, 47.
sustained operations at high speed, and few COSS assets other than space-based sensors and submarines would be able to sustain wartime surveillance or reconnaissance beyond the First Island Chain. U.S. Navy oceanic ASW operations would reinforce the LCS decoy groups’ potential utility in simulating transiting convoys and battleforces.

Obscurants, weather, and night could be used to prevent overhead COSS electro-optical and infrared sensors from identifying the LCS groups as decoys. Land and carrier-based aircraft could also be used against COSS scouts for the same purpose. This could be done either through use of deception equipment simulating U.S. Navy E-2 Hawkeyes’ and CAP fighters’ RF emissions and communications, or through use of force following the outbreak of hostilities. A small number of large surface combatants such as Aegis destroyers might be assigned to the decoy groups to aid in the deception and/or provide the groups with expanded self-defense capabilities depending on the tactical circumstances. Assuming the new ICADS-like system could effectively simulate modern battleforces and that other EW countermeasures such as selective EMCON and SEI-spoofing were effective, COSS operators would find it extremely difficult to tell whether their tactical picture indicated the presence of multiple battleforces, one battleforce and several decoy groups, no battleforces and many decoy groups, or something else entirely.

A notional first ASBM salvo’s effectiveness could be further eroded through other potential uses of emerging EW technologies. Battleforces could make use of notional Unmanned Surface Vehicles (USV) and low altitude UAVs equipped with DRFM-based image generators and obscurant-sprayers. Self-deploying USVs such as a derivative of the Defense Advanced Research Projects Agency’s (DARPA) Anti-Submarine Warfare Continuous Trail Unmanned Vessel (ACTUV) might also be able to serve as DRFM-based image generation decoys within a
battleforce or otherwise be used to augment LCS decoy groups.\textsuperscript{223} Notional Nulka variants or follow-on active offboard decoys could also employ DRFM-based image generation capabilities against incoming ASBM warheads. Shipboard solid state lasers could disable any electro-optical or infrared homing sensors carried by an ASBM warhead. Battleforce EW data networks and distributed EW control systems could enable real-time coordination of EW techniques and tactics between dispersed warships, aircraft, unmanned vehicles, and decoys. Integration of EW control systems with battleforce missile defense control systems could allow for improved coordination of kinetic and non-kinetic engagements against inbound ASBM warheads.

Additional emerging EW technologies could be employed following the first ASBM salvo. Small jammer-satellites could be situationally-launched to disrupt COSS sensor and data relay satellites’ communications, thereby blinding COSS at tactically opportune times and/or forcing COSS operators to burn precious maneuvering fuel to move these satellites into potentially less-optimal orbits. Land and and/or sea-based manned aircraft could be designed to carry notional customizable solid state laser arrays for blinding electro-optical and infrared sensors employed by Chinese satellites, long-range maritime reconnaissance aircraft, and/or UAVs. Future U.S. HALE UAVs could also conceivably fill this role. These intermediate-term EW and tactical deception capabilities, which are additive to many of the near-term ones described in Table 5 as well as all of the ones in Table 4, are summarized in Table 6 below.

\textsuperscript{223} Sweetman, “DARPA Pushes Out the Robo-Boat.”
### Table 6: Potential Intermediate-Term U.S. Navy Countersurveillance/Countertargeting Tactics and ASBM Self-Defense EW Systems

<table>
<thead>
<tr>
<th>System Name/Type</th>
<th>Probable Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>New ICADS ‘Increment 1’ with communications deception and simulation of battleforce RF systems</td>
<td>High if properly coordinated within an overall tactical deception plan (includes counterintelligence measures); low if not incorporated within plan or plan is otherwise ineffective.</td>
</tr>
<tr>
<td>New ICADS ‘Increment 2’ that adds DRFM-based image generator</td>
<td>Varies depending on quality of intelligence regarding SAR satellite, airborne reconnaissance aircraft/UAV, and ASBM SAR/ISAR radars’ characteristics and counter-EW measures.</td>
</tr>
<tr>
<td>ACTUV variant with DRFM-based image generator</td>
<td>Radar deception effectiveness varies depending on quality of intelligence regarding SAR satellite, reconnaissance aircraft/UAV, and ASBM SAR/ISAR radars’ characteristics and counter-EW measures. Obscurant spraying effectiveness would be medium to high if deployed over defended warships as well as nearby empty waterspace to create a shell-game effect. Low to medium if this is not done.</td>
</tr>
<tr>
<td>New USVs and low-altitude UAVs with DRFM-based image generators and obscurant-sprayers</td>
<td>Radar deception effectiveness varies depending on quality of intelligence regarding SAR satellite, reconnaissance aircraft/UAV, and ASBM SAR/ISAR radars’ characteristics and counter-EW measures. Obscurant spraying effectiveness would be medium to high if deployed over defended warships as well as nearby empty waterspace to create a shell-game effect. Low to medium if this is not done.</td>
</tr>
<tr>
<td>New enhanced-capability <em>Nulka</em> rounds/follow-on advanced offboard decoys</td>
<td>Varies depending on quality of intelligence regarding ASBM terminal radar characteristics and counter-EW measures.</td>
</tr>
<tr>
<td>Shipboard solid state lasers</td>
<td>Medium to high if ASBM warhead uses infrared/electro-optical terminal homing sensors depending on quality of intelligence regarding which infrared/visible-band frequencies these sensors are designed to detect.</td>
</tr>
<tr>
<td>Airborne solid state lasers</td>
<td>Medium to high against airborne/space-based infrared and electro-optical sensors depending on laser propagation conditions in atmosphere and quality of intelligence regarding which infrared/visible-band frequencies these sensors are designed to detect. Highly provocative if used prior to Chinese initiation of hostile actions.</td>
</tr>
<tr>
<td>Jammer-satellites</td>
<td>Varies depending on quality of intelligence regarding COSS satellites communication systems’ characteristics and counter-EW measures. Any cyber attack-insertion capabilities would be dependent on quality of intelligence regarding COSS network architecture and security measures. Would need to be inexpensive and capable of being launched on short notice in order to provide responsiveness to COSS satellite orbit changes. Highly provocative if used prior to Chinese initiation of hostile actions.</td>
</tr>
<tr>
<td>Battleforce distributed EW coordination networks</td>
<td>Enables use of more complex EW techniques, makes battleforce EW systems and active missile defenses more efficient, and boosts combined defensive effectiveness. Utility hinges on effectiveness of battleforce’s individual EW and active missile defense systems as well as resistance to jamming or cyber intrusion.</td>
</tr>
</tbody>
</table>

It is important to note that Table 6’s capabilities would enable significant COSS degradation without the need to strike targets on land. In the improbable event that China restrained itself from striking targets on allied or U.S. sovereign soil at the start of a notional war and U.S. political leaders chose not to vertically escalate by authorizing counterstrikes against
PLA targets on Chinese soil, COSS’s OTH-B arrays, satellite ground stations, and data fusion center(s) would be physically spared. Recall, though, that OTH-B is insufficiently accurate for directly cueing ASBM strikes. Terrestrial scouts and/or space-based sensors are necessary to narrow a contact’s AOU to the point that it can be targeted by an ASBM raid. Table 6’s intermediate-term EW capabilities would therefore be of great help under such circumstances. These capabilities would become even more critical should a hypothetical 2020s-timeframe second generation ASBM allow the PLA to strike battleforces steaming well beyond the DF-21D’s assumed range.

If the U.S. Navy gains these advanced EW countermeasures and selectively demonstrates their capabilities during peacetime as per the Cold War case study principles, CCP and PLA leaders weighing ASBM use in a future war would be confronted by scores of additional operational and tactical variables. Whereas the variables related to U.S. Navy BMD interceptors’ capabilities and inventory sizes are quantifiable, EW and deception-related variables cannot be easily quantified. The greater the uncertainties generated by these new variables, the greater the strategic uncertainties posed to CCP leaders regarding whether or not the PLA could swiftly cripple U.S. Navy forward deployed forces in East Asia at the start of a notional war.

Operational and Policy Prerequisites for Effective EW and Deception

As promising as these technologies and tactical concepts appear, it is crucial to avoid overconfidence in them. Per the principles derived from the Cold War case study and the discussion in Section VI, even if the underlying hardware and software technologies are proven to work, proper tailoring of EW techniques and deception tactics depends upon collection of accurate intelligence about the adversary’s sensors, counter-EW measures, data transmission and
fusion systems, and decision-making processes and tendencies. Blindly assuming that this intelligence is correct is a recipe for disaster in combat. Not having intelligence resources allocated towards monitoring and assessing the adversary’s reactions to EW and deception as an operation unfolds would be equally disastrous. Operations must be designed to take full advantage of successful EW and deception while simultaneously hedging against the risk that EW capabilities and deception tactics will not be as combat-effective as anticipated.224 The apparent U.S. success in collecting technical and operational intelligence against Soviet maritime surveillance, reconnaissance, and strike capabilities during the Cold War suggests that this challenge can be met with a reasonable degree of confidence over time given proper resources and prioritization. All the same, the risk of intelligence failure can never be fully eliminated. It consequently bears repeating that EW and tactical deception cannot serve as a complete substitute for active defenses.

Beyond clandestine intelligence collection and counterintelligence activities, the U.S. Navy will need to periodically demonstrate carefully-selected deception capabilities as part of real-world peacetime operations within COSS’s coverage zone. In keeping with the Cold War case study’s principles, just as the U.S. Navy once regularly conducted these types of demonstrations as part of exercises and operations within view of SOSS, U.S. Navy will need to do the same within view of COSS. Demonstrations allow the U.S. Navy to gauge COSS capabilities, learn indirectly about PLA leaders’ COSS-based decision-making tendencies, and condition PLA leaders and COSS operations with respect to what U.S. Navy operations, tactics, deception would ‘look like’ in actual combat.225

---

224 Vego, “Operational Deception in the Information Age,” 62, 64.
225 Ibid, 62.
This effort to condition Chinese perceptions of ‘likely’ U.S. Navy behavior in a notional war might very well be more vital to the ultimate success of U.S. Navy wartime deception than the actual deception tactics employed in combat. It is often easier to entice an adversary into interpreting a situation and making decisions in accordance with his long-held beliefs than it is to get him to change those beliefs. The most effective deception efforts often avoid trying to alter the adversary’s preconceptions. Instead, it strives to show him something very similar to what he expects to see. This is intended to entice him to take actions in accordance with his doctrine and training that can be exploited. It follows that there might be practical limits to the ways in which decoy groups or similar measures can be employed without tipping the adversary off that an attempt is underway to mislead him. Peacetime demonstrations can help discover whether and in what ways such limits exist.\(^{226}\)

Moderation in using tactical deception during peacetime as well as wartime operations is particularly important. A given EW technique customized for use against a specific sensor or a given tactical deception ‘trick’ against adversary decision-makers experiences diminishing returns over time. Once a technique or tactic is revealed during real-world operations, an adversary will use data collected about it to inform modifications of their systems, tactics, procedures, and decision-making tendencies. It can take the adversary considerable time to develop appropriate counter-EW measures once he understands the techniques being used against him, and it may take still longer for those counter-EW measures to be widely introduced within his forces. It is safe to assume, though, that the urgency of wartime operations means that once a particular technique or tactic is used for the first time in combat it risks becoming a ‘spent round’ more rapidly. As a result, continuous EW technical and tactical innovation in peacetime is

necessary to sustain defenses in wartime.\textsuperscript{227} A constantly-improved peacetime arsenal of EW-based countermeasures is therefore vital if techniques and tactics deemed obsolescent or ineffective are to be seamlessly replaced during war. This suggests it may be wise to primarily test techniques and tactics deemed close to their forecasted natural ‘expiration dates’ during peacetime demonstrations.

A major component of continuous peacetime technical and tactical innovation is battleforce training at sea. While occasional demonstrations in the Western Pacific will provide training opportunities, they will not occur frequently enough for developing and sustaining necessary operational proficiency with EW and tactical deception. As noted earlier, personnel can only reliably execute in combat what they’ve routinely and thoroughly practiced in peacetime under stress. This sounds straightforward but it is not. Operating amidst heavy use of EW is far more complex than operating in relatively permissive environments. EMCON somewhat reduces a battleforce’s sensing capabilities as well as places an increased premium on individual units understanding and autonomously executing their battleforce commander’s tactical plans and intentions. Battleforce sensors and communication systems might not perform as they normally do when used in combination with some forms of own-force EW. Warship and aircrew safety might be endangered if crews are unfamiliar with operations during heavily restrictive EMCON or intense active EW. Lastly, as tactical deception measures may require expending more fuel and stores than traditional operations, peacetime training is necessary for commanders and crews to become familiar with the additional logistical demands these measures will impose on battleforce planning. The only way to mitigate these fog and friction-inducing risks is to aggressively train against them. Shore-based training via simulation can provide basic-level exposure to some of the necessary skills, but real proficiency can only come with repeated

\textsuperscript{227} Payne, 98.
practice using real systems, warships, and aircraft within the natural and less-predictable ocean environment. This will demand a cultural willingness to tolerate additional peacetime operational expenses and safety risks. Without this willingness to train realistically and routinely, all the advanced EW technologies and clever deceptive tactics in the world may be rendered useless in battle.

The need for comprehensive training at sea leads to one final consideration. Even if it turns out the PLA has no answer for specific U.S. Navy EW techniques and technologies, a deception effort can fail if it is not properly organized and executed. Consequently, tactical deception must be planned and coordinated by the battleforce commander. Deception plans must be integrated within the battleforce commander’s overall plans for an operation so that all units or groups under his tactical control understand their respective roles in sustaining the deception’s effectiveness. If this does not happen, individual units’ uncoordinated actions may cumulatively undermine the deception. Strict operational security and appropriate EMCON measures must be enforced to prevent inadvertent disclosures. Any such disclosures must be ‘spun’ as best as possible to make them appear consistent with the deceptive ‘story’ of U.S. Navy operations in a given area at a given moment that the commander wants implanted within PLA leaders’ minds. Battleforce actions that cannot be concealed from COSS should also be executed in such a way that they reinforce the ‘story.’ The ‘story,’ itself, must be plausible as well as consistent with the previous peacetime conditioning efforts. The battleforce commander’s overall plan must allow sufficient time for COSS to receive and analyze the cumulative deceptive stimuli, and for PLA leaders to make decisions based on the resultant operational-tactical picture. Most importantly,

---

228 Hoyler, 99-100.
229 Blanks, 35.
deception must always be planned and executed as a supporting activity to the main operation. It is never an end in its own right.\textsuperscript{230}

Conclusion: Implications for U.S. Conventional Deterrence in East Asia

China’s maritime surveillance, reconnaissance, and ASBM strike systems certainly appear far more capable than their Soviet Cold War-era equivalents. Chinese sensor networks’ sensitivity, discrimination, accuracy, and low-latency reporting capabilities no doubt benefit from the past quarter century’s global advances in technology. The ASBM itself offers far greater tactical speed, reach, accuracy, and responsiveness than the Soviets could ever have dreamed possible. Nevertheless, the Chinese ASBM concept seems vulnerable to many of the same strategic, operational, tactical, and technical shortcomings that plagued the Soviets’ land-based maritime bomber concept. The U.S. Navy achieved three decades of apparent successes exploiting the Soviet maritime bomber concept’s shortcomings by combining a wide variety of EW technologies and deceptive tactics. EW’s post-Cold War evolutionary progress suggests that the technical, tactical, and doctrinal tools needed for similar blinding and deception capabilities against China’s Ocean Surveillance System and ASBM strike system are within reach. Just as was the case during the Cold War, the difficulty of conducting an effective anti-ship missile strike increases as the number of defensive variables the strike must overcome increases. In this light, the anti-ASBM capabilities of individual active defense and EW systems matter less than how they are holistically used within a battleforce’s defense. It follows that U.S. Navy active missile defenses’ utility against China’s ASBM reconnaissance-strike system can be significantly increased when paired with emerging EW technologies and novel tactical deception concepts.

Several prerequisites must be met, however, for our central hypothesis to be true. Effective intelligence and counterintelligence operations are critical to supporting EW and tactical deception development, not to mention operational employment. Periodic real-world
demonstrations of selected EW and tactical deception capabilities are necessary in order to test them against an adversary’s sensors as well as mentally condition the adversary’s decision-makers. Continuous EW and tactical deception innovation is essential during peacetime in order to maintain a deep and ready wartime stockpile of highly-perishable exploitation techniques. The inherent complexities and risks associated with EW and tactical deception makes routine, realistic, and comprehensive battleforce-level training at sea in their use obligatory. Lastly, tactical deception success hinges upon disciplined planning, organization, and execution by a battleforce commander and his or her subordinate units. None of these prerequisites are simple to achieve, but neither are they impossible, impractical, or historically unprecedented.

Our attention finally turns to how improved anti-ASBM capabilities can influence U.S. conventional deterrence against Chinese aggression in East Asia. Conventional deterrence is quite different from its more thoroughly studied nuclear sibling. Leaders of a country or alliance considering conventional aggression against a nuclear-armed country or alliance must weigh the risk that an initially successful conventional campaign will ultimately prove pyrrhic regardless of whether or not the aggressor also possesses nuclear weapons. A defender’s credible nuclear deterrence by punishment policy against conventional and nuclear aggression heightens the danger that even if only a small portion of the defender’s nuclear arsenal survives the aggressor’s first strike or offensive campaign, the defender will still be able to inflict intolerable retaliatory damage on the aggressor. The nuclear-armed defender can also create conditions and processes that all but force his retaliation if the aggressor violates the deterrent threat, thereby presenting the aggressor with the overt last clear chance to prevent mutual immolation.231

In contrast, the threat of punishment alone is less effective within a conventional deterrence context. Aggressors have historically been willing to tolerate harsh conventional

---

‘punishment’ over a short period if they are convinced little can be done to prevent them from rapidly and irreversibly achieving their offensives’ political objectives. The defender’s ability to rapidly block the aggressor’s attainment of his war aims therefore presents the key to conventional deterrence credibility. If an adversary tends to be opportunistic, then a defender’s theater-deployed conventional deterrent must be sized and postured such that the adversary concludes conditions offer little hope for a quick, low-cost conventional *fait accompli*. Conversely, an adversary may conclude that he has little to lose by igniting a potentially prolonged general conventional war. This might be caused by domestic economic, demographic, ideological, and/or power bloc pressures acting upon the adversary country’s political leaders. It might also be caused by these leaders fearing the domestic and international implications of their country’s perceived relative decline within the international order. Under these ‘desperation’ circumstances, a defender’s theater-deployed conventional deterrent must be sized and postured such that the adversary concludes he faces a high probability of being rapidly defeated in total and/or overthrown. Regardless of which conventional deterrence approach is

---

232 Denial does not necessarily mean that the attacker can be prevented from penetrating defenses, inflicting heavy damage on the defender, and/or perhaps even overrunning sizable portions of defended territory. It does mean that the defender has sufficient surviving combat potential to prevent the attacker from consolidating his gains. The more it appears that the defender’s theater-deployed forces and materiel will allow him to indefinitely draw out a conventional campaign, the less confidence and/or greater uncertainty a would-be aggressor might have that his opportunistically-desired war could be short and low-cost. It is also important to point out that blockading, bombarding, or seizing a piece of territory by force only represents an aggressor’s achievement of a military objective. In contrast, this aggressor’s political objective can only be achieved if the combatants and their allies reach formal or otherwise de facto agreement that the aggressor’s military gains are not reversible in the foreseeable future, or at least not without the defeated party trading away something of value to the aggressor. These political and military factors are what can make conventional deterrence by denial so potent against an opportunistic opponent.

233 In China’s case, a perception that a Taiwanese government was about to declare formal political independence from the mainland might fall under this scenario. The CCP has spent so much overt political and ideological capital on the Taiwan issue over the last half century that this possibility cannot be discounted.

234 Conventional deterrence against a desperate adversary is much harder to effectively communicate as well as make credible than a deterrence by denial strategy against an opportunist. If the defender chooses to mass overwhelming forces against a seemingly desperate adversary, the adversary may interpret the defender’s actions as a signal of imminent hostile offensive intent and may take preemptive offensive action accordingly. The adversary might also take preemptive offensive action if he sensed that his window of opportunity was closing fast due to the defender’s force-massing. If an adversary fears the uncertainties of national decline more than the uncertainties of
chosen, the defender’s peacetime ‘signaling’ by moving forces to or within a given theater as a crisis escalates is largely irrelevant and may even be counterproductive. The primary factors that matter in the adversary’s calculations are the defender’s combat-ready conventional units and logistics already in the theater that can deny or defeat any offensive under consideration, the defender’s apparent political will to resist and/or escalate, and the adversary’s own tolerance for political and material costs and risks.235

U.S. conventional deterrence against Chinese aggression appears geared towards a strategy of denial. As observed throughout this paper, the U.S. relies heavily upon naval use of the Western Pacific to blunt notional PLA offensives in East Asia. Strategic airlift can move U.S. forces and supplies into the region swiftly, but not necessarily in the amounts required to arrest a notional fast-moving PLA campaign for a limited political objective.236 Long-range conventional strikes as well as submarine warfare can severely damage PLA forces and/or China’s military-economic potential, but they may not be able to compel the PLA’s retreat from any First Island Chain territories captured in a Chinese offensive on their own. Nor would they be able to reassert

losing a conventional war, no amount of conventional power may deter him from attacking. Massing overwhelming forces as a deterrent might work when the adversary is several orders of magnitude weaker than the defender or the defending alliance. It is unlikely to be stable let alone effective against a near-peer or peer-level adversary. This is why nuclear deterrence played such a critical role in deterring Soviet conventional aggression in Europe—no matter how much NATO’s qualitative conventional capabilities improved over time, they were never considered sufficient on their own for deterring a potential Soviet Central European war of ‘desperation.’ Only the threat of initiating an escalation process that could ultimately lead to mutual nuclear immolation was considered credible in the ‘Soviet desperation’ scenario. See Betts, “Conventional Deterrence: Predictive Uncertainty and Policy Confidence.”


236 It is unlikely that U.S. strategic airlift would be able to deliver sufficient forces and materiel in enough time to prevent surprise PLA invasions of lesser islands in the Taiwan Strait or along the First Island Chain. Even then, PLA Air Force CAP and surface to air missile batteries would likely block U.S. airlift of reinforcements. This would be particularly true for any PLA operation conducted against Taiwan’s lesser islands. Since it would likely take some time for the U.S. and its victimized ally/allies to reduce PLA air defenses over any captured territories as well as theater strike capabilities, allied forcible entry operations against the captured territories would almost certainly become necessary if restoration of the status quo ante is desired. This suggests one way in which Chinese aggression for limited political objectives could easily cascade into a far larger-scale conflict.

It goes without saying that strategic airlift would not be able to decisively aid in the Taiwanese main island’s territorial defense for these same reasons.
control over regional sea lanes on their own.\textsuperscript{237} Naval surface forces play a major role in the U.S. East Asian conventional deterrent by virtue of their unique and historically-demonstrated abilities to assert a visible peacetime presence, exercise sea control, and insert and sustain large-scale ground forces.\textsuperscript{238} It follows that COSS and the ASBM are intended to upend the combat effectiveness of these maritime components of America’s East Asian conventional deterrent, and in turn weaken the political credibility of America’s overall East Asian deterrence by denial strategy.

U.S. leaders might respond to China’s theater military strategy by reassigning some share of aircraft carriers’ East Asian contingency sea denial and long-range land-attack missions to submarines and long-range aerospace forces. They might opt to go further by prioritizing procurement of new submarines and long-range manned and/or unmanned strike aircraft over procurement of new carriers and shorter-ranged manned aircraft such as the Joint Strike Fighter. Although these measures might make U.S. Navy forward deployed firepower more survivable during the first days or weeks of a notional East Asian war, they would not be able to completely cover all of the war’s probable maritime combat tasks. Just about any conceivable East Asian contingency might require carrier strike group, amphibious ready group, surface combatant action group, maritime BMD group, and/or convoy escort group operations within ASBM range.

\textsuperscript{237} This should not be interpreted to mean that land-based airpower, whether based in-theater or in the United States, would not be able to challenge and/or deny PLA control over various waters or territories. The same applies for submarines and sea-based airpower. These area denial effects would be major U.S. campaign if not strategic objectives. However, since area control can only be asserted by physically occupying a specific piece of territory or the ocean’s surface at a specific time, ground and naval surface forces would respectively be needed—albeit supported heavily by air and submarine forces to help sustain and exploit that control.

\textsuperscript{238} In an East Asian conventional deterrence context, the U.S. large-scale ground force insertion capability applies primarily to reinforcing the Japanese islands or South Korea in a notional crisis or conflict. U.S. ground forces would serve three purposes: demonstrating commitment and resolve to these treaty allies, supporting deterrence by inserting forces in theater that can be redeployed further forward to enhance allied territorial defense, and massing forces for potential rollback operations against any PLA or North Korean-occupied allied territories. This ‘theater entry’ force insertion should be distinguished from forcible entry amphibious operations against occupied territories. However, U.S. forcible entry capabilities do fall under the broader category of large-scale ground force insertion capabilities.
as a notional crisis peaked. Each of these surface group types would also inevitably have to operate within ASBM range as a notional war unfolded.²³⁹

Some but not all U.S. Navy Western Pacific surface operations could theoretically be delayed until the U.S. theater-level commander judged that COSS capabilities had been adequately eroded. The amount of time that any particular surface operation could be delayed would be affected by highly dynamic, interlinked, and unpredictable operational, strategic, and political pressures. Chief among these pressures is the likelihood that a U.S. decision to temporarily hold back or withdraw major surface forces from the ASBM coverage zone as regional tensions rose without prior political and military coordination with allied leaders would be interpreted as a signal of weakened U.S. commitment to defensive treaty obligations. This perception would stick no matter how much U.S. diplomats and political leaders strived to reassure otherwise. It might also misinform Chinese leaders’ political and military-operational estimates regarding a desired PLA offensive’s probability of success.²⁴⁰

The bottom line is that neither submarines nor long-range land and sea-based strike capabilities would allow the U.S. to indefinitely delay let alone completely avoid surface forces’

²³⁹ The earliest surface force missions in a notional war might include offshore BMD support of U.S. and allied airbases, maintaining sea control of ‘rear-area’ sea lines of communications, trans-oceanic reinforcement and resupply convoy escort, and carrier-based aircraft protecting U.S. Air Force long-range strike, refueling, and/or reconnaissance and surveillance aircraft. While these missions would likely be conducted along or outside the First Island Chain, many would be within ASBM range. Just because U.S. Navy surface forces might not frequently operate within the East or South China Seas until significant COSS and ASBM capability attrition had been achieved does not mean that they would be able to completely defer doing so during that phase. The possibility of U.S. amphibious operations in the Ryukyus or other lesser islands along the First Island Chain during the first months of a notional war similarly cannot be excluded. See Van Tol, 56, 60, 74, 76, 117.

²⁴⁰ This would be especially true as a notional crisis escalated. If U.S. leaders want to retain the flexibility to withdraw major surface forces from the ASBM coverage zone during a period of heightened regional tensions or a full-blown crisis, they absolutely must work with their allied counterparts while tensions are relatively low to integrate this option within their combined standing contingency plans. Even so, operational, strategic, and/or political demands during a notional war might compel U.S. leaders to conduct major naval operations inside the ASBM coverage zone earlier than they might prefer otherwise. Examples might include the need to urgently restore sea lines of communication to South Korea or to isolated Japanese islands in the Ryukyus or Senkakus, or perhaps introduce ground forces in those areas to forestall or arrest PLA offensives (or in the South Korean case, notional Beijing-sponsored/shielded North Korean aggression).
exposure to the ASBM threat during notional Western Pacific combat operations. The alternative to risking surface forces would be to scale back what the U.S. aimed to achieve in a notional conflict, which in turn would risk eroding American grand strategic credibility along with allies’ and partners’ resolve. Needless to say, this would also increase the risk that the conflict’s political settlement might end up being unfavorable as well as embarrassing to American interests and prestige.

The necessity of investing in anti-ASBM active defense, EW, and tactical deception capabilities is therefore derived more from strategic choices than from the Fleet’s actual force structure. ASBM defense systems’ procurement quantities would likely be affected on the margins if Fleet force structure varied, but the need to procure these systems in sizable quantities would not. If anything, a force of fewer carriers would make those remaining even more valuable and would increase—not decrease—the need to robustly defend them. The number of large surface combatants assigned to protect carriers during major combat operations might actually be increased under these circumstances. The need to protect surface forces such as BMD-capable combatants, amphibious warships, and supply/maritime prepositioning ships would also remain unchanged, as these ships’ roles cannot be duplicated by submarines, long-range strike systems, or strategic airlift.

While there is no such thing as an impenetrable, ‘perfect’ defense, these battleforce defensive measures do have two simultaneous and complementary effects. First, they increase the amount of military power—and by extension diplomatic and economic power—a near-peer aggressor must expend to achieve his political objectives. Second and perhaps more importantly, they can increase the aggressor’s uncertainty regarding whether or not his desired adventure can be accomplished at an acceptable political and material cost.
The longer it takes to reduce the defender’s offensive and defensive combat potential, the more time the defender has to use all forms of strategic national or alliance power to keep the aggressor from attaining his political objectives and perhaps even rally to defeat him outright. As shown throughout this paper, EW systems and deceptive tactics complicate an attacker’s maritime strike planning by increasing the number of non-readily quantifiable variables that his strikes must overcome in order to succeed. EW combines with active defenses to increase the overall effectiveness of battleforce defense, thereby forcing an attacker to increase his salvos’ sizes in order to increase his probability of neutralizing targeted warships. Used effectively, tactical deception can also delay the attacker’s strikes long enough for naval battleforces to achieve their missions or otherwise disorient the attacker to the point that he completely hesitates to strike. Particularly skillful tactical deception might even be able to lure the attacker into wasting some of his missile inventory against ‘phantom’ warships or battleforces.

Furthermore, it seems highly likely that the attacker’s ocean surveillance and reconnaissance-strike systems’ combat potential will degrade rapidly following an outbreak of hostilities. This means that if the defender’s forward deployed warships obtain a higher chance of surviving the first few salvos, the defender will be better able to restore a high degree of naval combat potential in theater when the survivors merge with reinforcement battleforces and the time comes to reclaim the operational-strategic initiative. It follows that large inventories of shipboard BMD interceptors are necessary to hedge against the risk that the defender’s kinetic and non-kinetic erosion of the attacker’s ocean surveillance and reconnaissance-strike systems proves ineffective or insufficient.

All of these defensive elements and considerations provide for a far more robust denial capability. If this is effectively communicated to a would-be aggressor, it might affect his
confidence in his ability to win quickly, cheaply, and decisively. Deterrence is, after all, mostly a political question: military considerations and perceptions serve as inputs to the political calculus. As a former Chinese missile designer recently put it, ASBMs serve as “political chips” regardless of how they might perform in combat because of the sense of threat they impose.\footnote{Pomfret, “Military Strength is Eluding China.”} A near-term overt DF-21D demonstration against a moving target at sea would likely increase the political-level sense of threat and intimidation regardless of whether or not such a ‘test’ appeared rigged to experts.\footnote{See 1. Kato, “China's Anti-Ship Missile is Nearly Operational;” 2. Erickson and Yang, 76-77.} While Chinese sources might claim that the ASBM serves as the PLA’s own tool for conventional deterrence by denial, it can just as easily be used as a coercive tool similar to the role played by the PLA’s land-attack Short Range Ballistic Missile (SRBM) forces deployed opposite Taiwan.

PLA peacetime coercion using its ballistic missile arsenal is in fact consistent with Chinese deterrence theory. Whereas deterrence theory in the West centers on dissuading an adversary from taking a proscribed action, Chinese deterrence theory blends dissuasion as well as compellence of an adversary. This theory, also known as weishe zhanlue, embraces Sun Tsu’s classical maxim on the benefits of ‘winning without fighting’ by means of military posturing and provocative capability demonstrations. Modern Chinese strategy has often embraced maintenance of crisis conditions, manipulation of tensions, and general brinksmanship as a means of achieving political objectives short of war. It is thus intriguing that Chinese leaders’ declaratory deterrence statements and policies during several major regional crises over the past half century have not explicitly identified the actions or behaviors that they wish to deter their adversaries from taking. Chinese deterrence statements prior to the PLA’s offensives against U.N. Forces on the Korean Peninsula in fall 1950, India in fall 1962, and Vietnam in winter 1979
seemed geared more towards preserving options for offensive strategic military surprise rather than articulating proscribed actions. There is some evidence in each of these three crises that CCP leaders were leaning towards or had already decided on taking offensive compellent action as their adversaries’ conventional forces were either inadequately postured or numerically insufficient for credibly deterring Chinese offensive action. Outside of a ‘desperation’ scenario, there does not appear to be any historical evidence that CCP leaders would order a PLA offensive if they did not believe they had a high probability of achieving their political objectives.243

The best way to counteract ASBM-related political effects and reinforce America’s East Asian extended conventional deterrence credibility is therefore to induce Chinese leadership perceptions that U.S. surface forces have low susceptibility to COSS and the ASBM, that an operationally-relevant portion of forward deployed U.S. surface forces in the Western Pacific would likely survive any surprise first ASBM salvo, that this means U.S. surface forces cannot be quickly or cheaply prevented at standoff distances from fulfilling their roles in blocking and then reversing Chinese aggression in East Asia, and that U.S. political leaders are resolved not to settle for any outcome of a Chinese-initiated conflict other than restoration of the status quo ante. This would need to be done while simultaneously instilling a sense of confidence and reassurance in allied and partner countries’ leaders’ minds.

Periodic U.S. Navy demonstrations of selective tactical deception capabilities can help with communicating these deterrence and commitment messages. Some naval deception capabilities could be demonstrated during routine Western Pacific presence operations, and others during routine exercises with regional allies’ and partners’ navies. By periodically

revealing selected COSS weaknesses in peacetime to Chinese and East Asian leaders, these demonstrations can communicate the difficulties the PLA would face in targeting U.S. Navy battleforces under combat conditions. This American-induced deterrent perception is not fundamentally different than China’s desire to induce the deterrent perception that the ASBM would be effective against U.S. Navy battleforces. As naval analyst Norman Friedman notes, it is “easier to assert a...capability than to make the limits of that capability obvious.”

There is ample precedent for this approach. Ocean Venture/Magic Sword North ’81 is but one example of the numerous U.S. military exercises conducted during the early to mid 1980s along the Soviet periphery as part of a larger U.S. political-military psychological campaign aimed at deterring Soviet aggression. While a 1980s-scaled and scoped psychological campaign is neither necessary nor desirable against China today, it does outline a conceptual method for communicating U.S. political resolve and naval credibility in support of conventional deterrence by denial. A private diplomatic outreach campaign paired with a long-term U.S. Navy psychological campaign could plant the perception amongst Chinese as well as other East Asian leaders that COSS cannot provide the ASBM reconnaissance-strike system with infallible targeting support let alone maritime omniscience, and that the U.S. would not allow land-based COSS assets to enjoy sanctuary on Chinese soil in the event of a war. If successful, the U.S. could take a large step towards devaluing the ASBM as a coercive political tool. This would

---

244 CCP leaders would likely view these demonstrations through their melded deterrence-compellence lens. This presents another reason why the demonstrations cannot be conducted infrequently: debuting these tactical deception capabilities during a period of high tensions could be counterproductive to deterrence messaging. By conducting them periodically during normal peacetime conditions and coordinating them with a private diplomatic narrative, the U.S. can mitigate the risk that the deterrence messages they are meant to communicate are drowned out or misperceived in a crisis.
245 Friedman, “Blocking the Path.”
contribute in no small way to reinforcing the U.S. East Asian conventional deterrence strategy’s credibility.
Bibliography


“Commander Second Fleet Calendar Year 1981 Command History.” Box 234, Operational Archives Branch, Naval Historical Center, Washington D.C.


“Countering the Anti-Ship Missile: Phase 1 Summary.” Alexandria, VA: Center for Naval Analyses, Naval Warfare Analysis Group Study #62, December 1971, CNA Reports Collection, Operational Archives Branch, Naval Historical Center, Washington, D.C.


“ONR Electronic Warfare S&T Industry Day.” Presentation by Dr. Peter Craig, Electronic Warfare Program Manager, C4ISR Department, Office of Naval Research, January 7, 2010.


