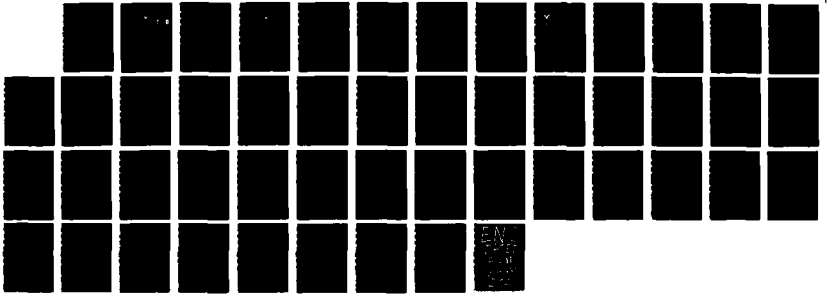
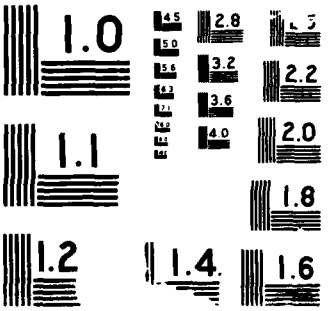
AD-A194 282 ELECTRONIC COMBAT ROADMAP FOR SPACE(U) AIR COMMAND AND STAFF COLL MAXWELL AFB AL K L HENRY APR 88 ACSC-88-1190 1/1

UNCLASSIFIED F/G 17/4 NL




1.0
1.1
1.2
1.4
1.6
1.8
2.0
2.2
2.8
3.2
3.6
4.0

AIR COMMAND AND STAFF COLLEGE

STUDENT REPORT

ELECTRONIC COMBAT ROADMAP FOR SPACE

MAJOR KENNETH L. HENRY 88-1190

"insights into tomorrow"

DISCLAIMER

The views and conclusions expressed in this document are those of the author. They are not intended and should not be thought to represent official ideas, attitudes, or policies of any agency of the United States Government. The author has not had special access to official information or ideas and has employed only open-source material available to any writer on this subject.

This document is the property of the United States Government. It is available for distribution to the general public. A loan copy of the document may be obtained from the Air University Interlibrary Loan Service (AUL/LDEX, Maxwell AFB, Alabama, 36112-5564) or the Defense Technical Information Center. Request must include the author's name and complete title of the study.

This document may be reproduced for use in other research reports or educational pursuits contingent upon the following stipulations:

- Reproduction rights do not extend to any copyrighted material that may be contained in the research report.

- All reproduced copies must contain the following credit line: "Reprinted by permission of the Air Command and Staff College."

- All reproduced copies must contain the name(s) of the report's author(s).

- If format modification is necessary to better serve the user's needs, adjustments may be made to this report--this authorization does not extend to copyrighted information or material. The following statement must accompany the modified document: "Adapted from Air Command and Staff College Research Report (number) entitled (title) by (author)."

- This notice must be included with any reproduced or adapted portions of this document.

REPORT NUMBER 88-1190
TITLE ELECTRONIC COMBAT ROADMAP FOR SPACE

AUTHOR(S) MAJOR KENNETH L. HENRY, USAF

FACULTY ADVISOR MAJOR BRUCE A. THIEMAN, ACSC/EDW

SPONSOR LT COL KENNETH D. RILEY
HQ AFSPACECOM/DOS

Submitted to the faculty in partial fulfillment of requirements for graduation.

AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY
MAXWELL AFB, AL 36112-5542

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-018

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT STATEMENT "A" Approved for public release; Distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) 88-1190	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION ACSC/EDC 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) Maxwell AFB AL 36112-5542	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO / WORK UNIT ACCESSION

11. TITLE (Include Security Classification)
EC ROADMAP FOR SPACE

12. PERSONAL AUTHOR(S)
Henry, Kenneth L., Major, USAF

13a. TYPE OF REPORT	13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
		1988 April	46

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

Space is considered to be the fourth combat arena for military forces. AFM 1-1 contains the doctrine from which "aerospace" forces develop their strategy and part of that doctrine is the use of electronic combat. This paper begins the effort to create a roadmap leading to the establishment of electronic combat doctrine in the fourth combat arena. It contains a rundown of space system vulnerabilities and the EC "tricks" which can be used to exploit them. The report concludes with areas requiring further study and recommends future work.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION
22a. NAME OF RESPONSIBLE INDIVIDUAL ACSC/EDC Maxwell AFB AL 36112-5542	22b. TELEPHONE (Include Area Code) (303) 293-2867 22c. OFFICE SYMBOL

PREFACE

Electronic combat is an important part of the struggle for control of the air in today's electronic battlefield. With the advent of a new, fourth combat arena in space, this tool, often referred to as "the battle of the beams," must be integrated into the mission of space control. Rooted firmly in the Air Force's basic doctrine stated in AFM 1-1, this report lays out a foundation for exploiting the vulnerabilities of space systems using the electronic combat "tricks of the trade." In actuality, it raises more questions than it answers and concludes with a partial listing of the many areas requiring further study.

ABOUT THE AUTHOR

Major Kenneth L. Henry graduated from the Air Force Academy in 1973 with a bachelor's degree in electrical engineering. His first assignment was with the B-1 Systems Program Office where he was responsible for the development of the original B-1's electronic defensive systems. In 1977 he entered the Air Force Institute of Technology (AFIT) and graduated 24 months later with a master's degree in electrical engineering, specializing in the design of a parallel microprocessor architecture for electronic countermeasures processing. Following AFIT, he went to SAC Headquarters for the next five and a half years.

At HQ SAC, Major Henry was first responsible for the analysis of scientific and technical intelligence on foreign radar systems and applying that information to the support of operational electronic countermeasures programs as part of the Electronic Warfare Integrated Reprogramming (EWIR) process. His second tour at HQ SAC was back on the B-1 program (now the B-1B) as the operational user's representative responsible for ensuring the operational requirements for the electronic defensive systems (now including a tail defense radar) were being met by the design.

Following his work at SAC, Major Henry was selected to fill a highly sensitive position on the Air Staff, responsible for providing intelligence support to many of the Air Force's special access required development programs. His work in this area was recognized in 1986 by the Association of Old Crows when he received their Special Medal.

Major Henry is currently a member of the Air Command and Staff College class of 1988. Upon graduation, he will be going to Headquarters Air Force Space Command at Peterson AFB in Colorado Springs, Colorado.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Part of our College mission is distribution of the students' problem solving products to DoD sponsors and other interested agencies to enhance insight into contemporary, defense related issues. While the College has accepted this product as meeting academic requirements for graduation, the views and opinions expressed or implied are solely those of the author and should not be construed as carrying official sanction.

"insights into tomorrow"

REPORT NUMBER 88-1190

AUTHOR(S) MAJOR KENNETH L. HENRY, USAF

TITLE ELECTRONIC COMBAT ROADMAP FOR SPACE

I. Purpose: To begin the process of building, i.e., define the contents of, an electronic combat roadmap for space and provide a foundation for the development of future doctrine and strategy.

II. Problem: Space represents a new combat arena for the future and no plan exists for the employment of electronic combat there. Electronic combat is an integral part of the "terrestrial" mission involving control of the air, the doctrine for which is presented in AFM 1-1. As the Air Force expands into the fourth military arena of space, so too must its doctrine and part of that doctrine will involve the use of electronic combat.

III. Data: The foundations for electronic combat use in space are already in AFM 1-1. Space control is a natural outgrowth of control of the air and just as electronic combat is an integral part of air control, it will be for space control. Also just like its terrestrial counterpart, electronic combat in space must seek to exploit vulnerabilities in the systems it's being targeted against. Space systems have a number of inherent vulnerabilities and there are many potential tools in the electronic combat "bag of tricks" which can be applied against them

IV. Conclusions: The creation of an electronic combat roadmap for space should be pursued. The task is a large one requiring the gathering of a vast amount of data and the conducting of many special studies. It is possible, however, to obtain the information required and create a roadmap which will result in the right kind of strategy for the future.

V. Recommendations: The military has been directed to conduct the mission of space control. Since electronic combat is a proven part of the air control mission, it should be a key portion of the space control mission. Its use in space must be based on a sound doctrine and we should have a well thought out roadmap to arrive at that doctrine. The Air Force should pursue the studies which are required to obtain the necessary data to create that roadmap.

Chapter One

INTRODUCTION

This paper begins the effort to create an electronic combat roadmap for space. That effort explores the existence of electronic combat vulnerabilities in United States and Soviet space systems which can be discovered and documented from open-source literature. It is intended to set the stage for a systematic exploitation of those vulnerabilities via development of a roadmap leading to an electronic combat strategy for space. The report begins with a discussion of electronic combat principles in general.

To serve as a starting point for the roadmap, Chapter Two contains a summary of electronic combat principles and relates those principles to potential missions in space. It begins with the most basic statement of Air Force doctrine in AFM 1-1 and uses ideas from the related publications: AFM 1-6, Military Space Doctrine, and AFM 1-9, Aerospace Doctrine for Electromagnetic Combat. Electronic combat's role in the space control mission completes the chapter and set the stage for the next step in the roadmap's development: investigation of potential electronic combat targets.

The potential for various types of space systems to be electronic combat targets is discussed on a satellite class-by-class basis in Chapter Three. The general characteristics of the various types of satellites is described along with any potential dependencies or weaknesses which could be considered vulnerabilities. Ways to exploit these vulnerabilities are discussed next.

Chapter Four contains a description of electronic combat means/methods, or, in other words, "tricks of the trade." It discusses the role of electronic support measures and outlines the more offensively-oriented branch of electronic combat, electronic countermeasures. Next, Chapter Five contains a discussion of how some of the generic techniques presented in Chapter Four could be applied to space.

Using the previous three chapters as a foundation, Chapter Six describes the contents of the required roadmap and discusses what has been, and what needs to be done to complete the roadmap.

It is actually a plan to create an electronic combat roadmap which would serve as a bridge between the present capabilities and those which would be required in the future.

There are many areas or subjects which must be covered by an electronic combat roadmap, many of which require much more information than currently exists. Chapter Seven addresses ways to obtain this information and recommends areas for further study. Some of the recommendations involve survey-level efforts while others would involve extensive, detailed analyses. This chapter concludes with some related questions intended to be thought provoking. The paper concludes in Chapter Eight with a wrap-up of the principles, vulnerabilities, and electronic combat tricks which are applicable in space, as well as a recap of the recommendations appropriate for building an electronic combat capability in space.

Chapter Two

ELECTRONIC COMBAT IN SPACE

PRINCIPLES OF ELECTRONIC COMBAT

Introduction

Before making a determination on the applicability of electronic combat (EC) for space, one should examine its basic principles. Since Air Force Manual 1-1 contains the "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives" (2:v), it should serve as a starting place. This manual defines EC as follows:

> [Electronic combat is] a specialized task performed by aerospace forces to control selected parts of the electromagnetic spectrum in support of strategic and tactical operations. [It] involves actions to protect friendly electromagnetic capabilities and actions to neutralize or destroy the enemy's electromagnetic capabilities. The purpose is to enhance the ability of our warfighting systems to achieve objectives, since the use of the electromagnetic spectrum can have a major impact on the success or failure of military operations (2:3-6).

The manual goes on to break EC down into its component parts.

Electronic Warfare

"[Electronic warfare is defined as] military action using electromagnetic energy to determine, exploit, or prevent hostile use of the electromagnetic spectrum and also includes actions designed to retain the friendly use of that spectrum" (2:3-7).

Command, Control, and Communications Countermeasures (C3CM)

"[C3CM is defined as] military action involving defensive and offensive operations in a strategy that is designed to deny information to an enemy, to protect friendly C3, to influence enemy actions, and to degrade or destroy enemy C3 capabilities" (2:3-7).

Supression of Enemy Air Defenses (SEAD)

"[SEAD] is aimed at gaining freedom of action to perform Air Force missions by neutralizing, destroying, or temporarily degrading enemy air defense systems" (2:3-7).

Doctrine

AFM 1-9, Aerospace Doctrine for Electromagnetic Combat provides more detail on the application of electronic combat principles to general warfare. "Spectrum superiority" is the goal. The overall capability is broken down into specific tasks involving destruction, disruption, and deception. Deception involves "creating false or misleading impressions" using electronic combat. Deception works best if it can be coordinated against multiple sensors used by the same system. Disruption is an action designed to "introduce delays into enemy operations which will prevent or degrade effective conduct of operations " Destruction is just what it implies, the physical destruction of enemy systems, but it can be done using a variety of methods from conventional munitions to nuclear radiation and high energy particle or laser beams (4:2-1 thru 2-2).

Other Services' Definitions

Other services definitions closely parallel the Air Force's but tend to concentrate on electronic warfare and breaking it down into its components of electronic support measures (ESM), electronic countermeasures (ECM), and electronic counter-countermeasures (ECCM) (10:1-5). Given these principles, are there applications for them in the space arena?

EC PRINCIPLES FOR SPACE

Is There a Role?

In addition to a proliferation of satellites and other systems actually located in space which perform their own specialized missions; landbased, seabased, and airborne weapon systems also use the services they provide. There is a "growing reliance of modern air, naval, and ground forces in space to warn, assess, command, detect, navigate, defend, and carry out a myriad of other military functions spanning the spectrum from strategic nuclear to low-intensity conflict" (30:78). Partially because of this dependency, "the US urgently needs a space control capability" (29:132). It is as a part of this space control mission area that EC can play an important role.

Space Control

The Department of Defense (DOD) recently published a policy for space which calls for "assured space mission capability and a comprehensive satellite control architecture" (1:5-1). The space control mission area is similar to other mission areas except, obviously, for the arena in which it's applied, the vastness of that arena, and the enormous complexity and expense incurred in operating in that arena. "Space control activities ensure freedom of action in space for friendly forces while, when directed, denying it to the enemy" (31:85). This policy is not much different than the conventional "control of the air (gaining air superiority)" mission referred to in AFM 1-9 in the section dealing with supression of enemy air defenses (4:2-2). According to the United States Military Posture Statement issued by the Joint Staff for FY 1988, the "DOD will develop and deploy a comprehensive space control capability with initial operations at the earliest possible date" (31:85). Although not specifically mentioned in AFM 1-1 as a separate mission (space is just another operating medium), the manual has the roots for this mission.

The Air Force mission, Strategic Aerospace Offense, has objectives which call for "neutralizing or destroying the enemy's war-sustaining capabilities or will to fight." An associated mission, Strategic Aerospace Defense, includes objectives "to integrate aerospace warning, control, and intercept forces to detect, intercept, and destroy enemy forces (in any medium) attacking our nation's war sustaining capabilities or will to fight" (2:3-2). These offensive and defensive missions, together, form the basis for space control. According to Air Force Manual 1-6, Military Space Doctrine, "space weapon systems can also be used when it becomes necessary to establish space control and superiority" (3:9) As in other types of battlefield and airspace control activities, one of the tools for doing the mission is EC.

EC's Role in Space Control

It has been demonstrated repeatedly throughout the history of modern combat, EC is vital to mission success. "Past conflicts have demonstrated that electronic combat must be included in all phases of military planning and is a vital factor in the overall success of any military operation" (5:204). At least one aspect of electronic combat, SEAD, is specifically mentioned in AFM 1-6, which calls for spacebased systems to "provide timely supression of enemy defenses to improve the penetration effectiveness of strategic and tactical [airbreathing] systems" (3:9). Equally important for all services, the assured use of the electromagnetic spectrum and denial of that medium to the enemy, means also considering how to apply EC to space. The joint EC Master Plan, which was delivered to Congress in April 1987, as well as, the individual services'

EC Master Plans, emphasize EC activities within DOD in all operational areas (6:55; 13:37,65). "Success in warfare - air, land, and sea - depends increasingly on the ability to deny the enemy the use of his electronic eyes and ears while assuring our own use both offensively and defensively." (12:--)

Chapter Three

POTENTIAL EC TARGETS AND THEIR VULNERABILITIES

POTENTIAL TARGETS

Introduction

Satellites and their related support systems are the basic target set for space-related electronic combat. Satellites can be categorized many ways including one which distinguishes between their ownership, i.e., military vs non-military. In many cases, however, functions which are generally peaceful in nature, e.g., navigation or communications, also have direct military applications, so the distinction becomes blurred. Within the military categorization, satellites can be further divided into weapons and non-weapons. Thus far, the only operational satellite weapon system is the Soviets' co-orbital anti-satellite (ASAT) system (26:52) but it may soon be joined by a US ASAT and components of the *US Strategic Defense Initiative (SDI)* anti-ballistic missile (also potentially anti-satellite) system. One useful way to discuss these various satellites is by mission area as does Colin Gray in American Military Space Policy (15:23-24). These areas are: surveillance/reconnaissance, attack warning/assessment, communication, navigation, meteorology, and geodesy. Although attack warning/assessment, geodesy, and meteorology satellites are really types of surveillance systems, each of these mission areas has distinct characteristics and is described, together with the two military classes of targets, in the following paragraphs. Note: due to a need to limit the scope of this research project, only the spacebased portions of these satellite systems will be discussed.

Surveillance/Reconnaissance Satellites

These are space systems whose missions involve watching or observing something; in this discussion, primarily intelligence-related activities, as opposed to similar missions like weather, etc. Surveillance systems are those which periodically (or regularly) visit or monitor a particular area, activity, frequency band, etc. Reconnaissance systems are those which are generally targeted against a specific activity looking for more detailed information (15:24). Surveillance and reconnaissance satellites have distinct orbital characteristics related to their

missions and, in general, "virtually all [these missions are] conducted from low-earth orbit because of technical necessity [generally the need for high resolution]" (15:26). Examples of this type of space system include the USSR's ELINT Ocean Reconnaissance Satellites (EORSATs) and Radar Ocean Reconnaissance Satellites (RORSATs) which "are designed to detect, locate, and target US and Allied naval forces for destruction by anti-ship weapons launched from Soviet [airborne and seabased] platforms" (21:41). Maneuverability, i.e., the ability to change orbits, is crucial for this class of space systems, although they probably can't maneuver fast enough to avoid an ASAT.

Attack Warning/Assessment Satellites

These are satellites, deployed by the US and the Soviet Union, to provide early warning of missile launches.

> The US early-warning system reportedly comprises three satellites in geosynchronous equatorial orbit at 22,300 miles altitude. These satellites, two over the Western Hemisphere and one over the Eastern, allegedly carry scanning infrared, light, and radiation detectors. The Soviet satellite-based early warning system comprises sensing vehicles (presumably infrared) launched into very eccentric elliptical orbits (15:27-28).

Maneuverability would not be required (unless desired for a defensive mechanism) for this class of satellites.

Communications Satellites

Introduction. Both superpowers have become dependent on this class of satellites for command, control, and communications (C³). The US is probably more dependent, however, with approximately 80% of all long distance communications being done via satellite (15:28). Of the variety of US communications satellites, the more important current ones are: the Defense Satellite Communications System (DSCS) II and III, the Air Force Satellite Communications System (AFSATCOM)(really not a separate satellite), the Fleet Satellite Communications System (FLTSATCOM), and the Satellite Data System (SDS). In the future the US will have the Military, Strategic, Tactical and Relay (MILSTAR) satellite communications program (15:30). These related systems have different characteristics depending on their mission and the technology available when they were built.

DSCS. DSCS satellites are in geosynchronous orbit and are associated with the Worldwide Military Command and Control System as well as intelligence, diplomatic, and other communications functions. The latest generation of these satellites , DSCS III,

can use super high frequencies (SHF), is hardened against nuclear effects, and has limited maneuver capability (15:30).

AFSATCOM. AFSATCOM is not a separate satellite, rather, it is a "package" which is piggybacked on other satellites. This system, carried in the host satellites' orbits, operates in the ultrahigh frequency band (UHF) and is used to communicate with intercontinental ballistic missile (ICBM) launch centers, airborne command posts, Strategic Air Command (SAC) bombers, and "Take Charge and Move Out" (TACAMO) aircraft (15:30).

FLTSATCOM. "The FLTSATCOM system [has] five satellites [which are in] synchronous orbit [and] operate [in the] UHF and SHF [frequency bands]." This system is shared by the Air Force, the Navy, and the National Command Authorities. (15:30) Twelve of a FLTSATCOM's twenty-three UHF and SHF channels are used by SAC Headquarters for communications to its bomber force and ICBM installations (7:180).

SDS. The SDS satellites, the last of which is inactive, had a mission unique from the other communications satellites in that their orbit (highly eccentric polar) was chosen so they could provide continuous coverage of Air Force facilities in the North Polar region (15:31).

MILSTAR. One of the future systems, MILSTAR, will have satellites in geosynchronous and elliptical polar orits. The system operates in the extremely high-frequency (EHF) band and will be used by virtually all types of military forces. In addition, the primary MILSTAR satellites may be backed up by spares orbiting at supersynchronous altitude (up to 95,600 nm) and capable of being maneuvered down to synchronous altitude. The MILSTAR satellites are designed to be hardened against nuclear and directed energy radiation, and they reportedly use laser crosslinks in addition to their other data links, uplink, and downlink (15:31; 28:289).

Soviet Systems. Soviet communications satellites use polar, elliptical, circular, and geosynchronous orbits and are launched frequently (2-3 launches of clusters of 8 satellites per year). These systems probably operate in the very high frequency (VHF) and UHF bands. The Soviets probably also use their civilian Molniya satellites for military communications (15:31-32; 28:304).

Navigation Satellites

The US and USSR both use navigation systems in space. The US Navy uses its TRANSIT system for surface ship and submarine navigation. These satellites are generally launched into nearly circular orbits at 90 degrees inclination (polar orbits). The United States' new navigation system, Navigation Satellite Timing

and Ranging, (NAVSTAR), is due to consist of 18-24 satellites and was expected to be operational by 1989 (this date is very much in doubt due to a lack of US launch capability). The 24 satellite system is supposed to be configured in three eight satellite rings in semi-synchronous orbits and would allow users to measure horizontal and vertical position to within 10 meters and velocity to within 0.03 meters per second (15:32-33; 28:293-294).

The Soviets have announced the development of a navigation satellite system, designated GLONASS, which is expected to be similar to NAVSTAR. It uses signals at 1.2 and 1.6 GHz and may also be compatible with NAVSTAR. The Soviets say their system is "intended for worldwide aircraft radio navigation" and is also probably useable by its navy (15:32-33; 28:306).

Meteorology Satellites

The US has a Defense Meteorological Satellite Program (DMSP) with satellites in circular, sun-synchronous, polar orbits capable of taking visible and infrared photographs of virtually the entire surface of the earth. The information DMSP satellites provide prevents other surveillance and reconnaissance satellites from wasting film, helps plan military missions, and checks for weather conditions which may affect missile launch or warhead re-entry. As in other types of space systems, the Soviet's spacebased meteorology program is similar to the US. Their latest version, called Meteor-2, can transmit data from its scanning infrared radiometer and passive microwave (millimeter wavelength) temperature sounder (among other instruments) directly to users on the ground. Their satellites have similar orbital characteristics as the US's (15:34-35; 28:291-292).

Geodesy Satellites

This is another mission performed by the US and the USSR. The US Defense Mapping Agency uses photographic mapping information, supplied by the Geodetic Satellite Program, to provide essential data for ballistic missile launch and impact-point location. In addition, these satellites provide the data from which the US cruise missile's terrain contour matching (TERCOM) maps are made. The USSR's program is similar to the US and for the accuracy necessary, both countries' satellites are in low-earth orbit (15:34-35; 28:291-292).

ASAT

The Soviet Union currently has the only opertional ASAT system in the world. Their system, consisting of an interceptor satellite launched by a SL-11 (SS-9) booster (21:50), has the capability of reaching targets at orbital altitudes of at least 2700 nautical miles. This weapon "attacks other satellites in orbit by maneuvering [using either an infrared or radar sensor

(11:82)] a conventional warhead within range and destroying its target with a multi-pellet blast" (26:52). Other potential Soviet ASATs include their nuclear-armed GALOSH ABM and possibly lasers they have deployed at Sary Shagan (26:52).

The United States, on the other hand, does not have an operational ASAT. The proposed US system, consisting of a miniature homing vehicle mounted on a combination short-range attack missile (SRAM)/ALTAIR booster and launched by an F-15, has only been tested against a satellite once. This test of a direct-ascent weapon, using an infrared sensor system for terminal homing and kenetic energy (impact) as its kill mechanism, was a success, i.e., the satellite it attacked was destroyed (18:86).

SDI

So far, a Strategic Defense Initiative (SDI) ballistic shield over the US is just a dream. Some concepts have evolved, however, and a multi-phase deployment plan is envisioned (16:7). The first phase of the plan for SDI doesn't call for exotic technology, rather, it may consist of a constellation of 300 to 400 satellites, armed with six to ten killer rockets each, in low-earth orbit to cover Soviet missile fields (16:8). Included in this Phase I deployment would be the surveillance satellites, in higher orbits over the Soviet Union, to detect missile launches, and the battle management system (16:8). Phase I would be the first layer in a multi-tiered system with the next layer, Phase II, merely consisting of more of the same type of kinetic kill rockets as in Phase I (16:11). At some later date, depending on the outcome of various research programs, some of the more exotic technologies may come into play. Included as future kill mechanisms for SDI are various types of groundbased (requiring spacebased adaptive mirrors) and spacebased lasers and the even more challenging particle beams (20:37-38). Due to the uncertainty of the longevity and configuration of the SDI program, its characteristics cannot be discussed in detail but some general characteristics of its components can be assumed and some general conclusions on their vulnerabilities can be assumed by similarity to other space systems.

VULNERABILITY ANALYSIS

Introduction

Analyzing the vulnerability of space systems or satellites can be approached from a variety of aspects. This research paper examines the subject of vulnerability two ways. The first is from the stand point of the satellites themselves, or, said another way, system vulnerability. The other way of looking at the subject is from the standpoint of the missions of the individual or groups of satellites, i.e., the susceptability of

those missions to temporary or permanent negation. There is, of course, some overlap between these two ways of looking at vulnerability, i.e., an exploited system vulnerability will probably disrupt a satellite's ability to support or perform a mission. There is, however, enough "separateness" for the two types of vulnerabilities to be examined individually, starting with system vulnerabilities. Mission vulnerability is very dependent on the "uniqueness" of the capability being provided, i.e., the ability to use other, possibly non-space related systems instead, and will be left to future studies.

System EC Vulnerabilities

General. Before discussing specific vulnerabilities of individual space systems its important to note that many, if not all of them, are related to weight. What is eventually put into orbit to perform a specific mission is related to the ability to first get it off the ground. This fact determines (limits) not only the weight of the actual satellite but also the amount of additional fuel it can carry for housekeeping (maintaining a stable orbit) and maneuvering. Also limited is the amount and types of additional subsystems (perhaps some for defense) a satellite can carry. Whether or not they're actually related to weight, other systems vulnerabilities include: the use of and dependence on various types of sensors, lack of redundance (intra- and inter-satellite), and dependence on groundbased control (uplinks, downlinks, and beacon signals).

Use of/Dependence on Sensors. Almost all satellites have a sensor of some type while some satellites actually depend on a sensor to support their primary mission. Many space systems can use sensors like star trackers to maintain their on-orbit stability, but the ones which could be the most vulnerable are exemplified by photo reconnaissance, radar surveillance, electronic surveillance, attack warning/assessment, meteorology, and geodesy satellites and ASAT interceptors. Photo reconnaissance satellites depend on a high resolution camera which records images either on film or digitizes them for transmission to the ground. Radar surveillance satellites depend on a radar signal reflected from potential targets and on-board processing. Electronic surveillance satellites depend on a variety of receivers to collect signals intelligence (SIGINT). The most important attack warning/assessment satellites, those which watch for incoming ICBMs, use infrared sensors to detect the exhaust plume from boosters. Meteorology satellites take pictures of weather formations (depending on cameras again) and make measurements of other critical weather parameters using a variety of sensors. Geodesy satellites also depend on photographic information. Finally, the ASAT interceptors which exist use either radar or an infrared sensor to detect and track their potential targets. In addition, almost all of these sensor

dependent satellites also depend on a connection with groundbased sites to relay their vital information to decision makers.

Lack of Redundance. The effects of many attacks, physical or electronic, can be mitigated by using spare or redundant subsystems or circuits. This practice can be applied within a particular satellite or by restructuring the workload of a family of satellites within a constellation. Also, this technique can be carried to the extreme where complete backup satellites are kept dormant in orbit as spares. Unfortunately, all of these mitigating practices are costly in terms of weight and system complexity and are expensive to implement, leaving potential vulnerabilities. In addition, some aspects of satellites can't be "backed up" by other systems. Communications satellites, for example, couldn't be replaced by land circuits (there aren't enough of them) and reconnaissance satellites fly over denied areas.

Dependence on Signals To/From the Ground. Thus far, in the use of space, satellites have been put in orbit for one primary mission, i.e., to support groundbased entities. To do this job, they must communicate information to groundbased sites, as previously discussed, but, in addition, they must be commanded from and respond to commands from the groundbased authorities. Functions of these command links include targeting reconnaissance satellites and passing housekeeping maneuver commands to satellites to maintain their positions. These uplink and downlink signals are susceptable to intentional and unintentional (especially during high levels of sunspot activity or during nuclear events) perturbations. In addition, a whole class of satellites, i.e., those for navigation, must radiate signals to perform their primary missions. Like navigation satellites, communications satellites cannot perform their missions unless they radiate and receive signals at various radio frequencies. Along with their primary communications channels, these satellites must also receive and use prioritization information to sort out their many users. Finally, many satellites use a beacon signal to enable groundbased entities to track their positions using time-difference-of-arrival interferometry.

Conclusion. The variety of vulnerabilities discussed in the preceeding paragraphs are generally related to either weight restrictions or mission requirements. The vulnerabilities vary in criticality, sensitivity, and degree/ease of disruptability. Many of them are potential targets of various forms of electronic combat techniques.

Chapter Four

ELECTRONIC COMBAT MEANS

THE "BAG OF TRICKS"

Introduction

Before one can examine the application of electronic combat to space, one should examine, the basic electronic combat tools, functions, and techniques. The launching of the first intelligence payload into orbit in 1962 (23:64) expanded the electronic battlefield, a creation of World War II, into space. The system which was launched can easily be categorized as related to electronic combat, falling into the electronic warfare component and further delineated as being a member of the electronic support measures sub-component. The techniques used in World War II included direction finding (DFing) to locate enemy emitters (including radios associated with troop concentrations); attack warning by listening for enemy radio-navigation signals; electronic jamming of navigation, radio, and radar signals; and the use of chaff (called "window"). Technology advances throughout the systems used in modern warfare since the days of the so called "Wizard War" (23:10), have created a dependence on electronic aids. Many experts agree "[without these aids] highly mechanized and automated warfare would be near impossible" (23:10). It should be no surprise, therefore, that there are a myriad of opportunities to apply "wizard warfare" to space.

Electronic Intelligence Gathering

Electronic combat is already taking place in space in the form of electronic support measures (the ability to monitor enemy radio frequency emissions). Space systems currently used to perform this function were discussed in general in Chapter Three. Some specific examples, for which unclassified, open-source information exists, include various US reconnaissance/-surveillance systems, and the USSR's COSMOS SIGINT collectors. In addition to the high technology receivers and signal processing equipment these systems must have, they depend on large antennas to gather the extremely weak signals from threat systems' antenna sidelobes. These systems already exist and must continue to be an active part of our spaceborne electronic combat

strategy but they will not be discussed further except for the fact that our intelligence systems susceptability to intelligence gathering from enemy systems must be considered (23:64-67).

Electronic Support Measures

This type of electronic combat is generally composed of two broad classes of equipment; the intelligence gathering systems (the spaceborne portion of which has already been discussed) and warning receivers of various types. The most common type of warning receiver in use today (and this doesn't even count the thousands in cars on the highway) is the radar warning receiver (RWR).

> Designed to search for signals from hostile radars, RWRs can detect emissions from surveillance and tracking radars, air [or space] interception radars, and the command links used to guide many [types] of missiles [perhaps including ASAT interceptors]. Once the signal has been identified, aircrew [or space asset control authorities or on-board artificial intelligence subsystems] are given a warning signal, plus an approximate indication of the bearing, frequency, and threat category (23:70).

RWRs are used to provide warning and to identify an approaching threat to a friendly system while there is still time for some type of countermeasure to be implemented. Its task involves receiving and processing energy from threat radars. An associated antenna provides significant amplification of an incoming signal to compensate for its low amplitude. The RWR categorizes the threat usually by including a library of common threat parameters in the RWR signal processing subsystem with which to compare the measured parameters of the potential threat. Finally, an RWR may perform another vital function as a "block in a feedback loop" involving the application of some type of countermeasure. The RWR's function in this loop is to check and determine if the countermeasure has been successful in breaking the enemy's ability to track the friendly system being protected (23:70-77).

A new class of warning receivers beginning to be deployed involves the ability to detect emissions in frequency bands not associated with radar. These include infrared, ultraviolet, and laser frequencies and in the future will have to be expanded to include the more exotic beam weapons. An infrared or ultraviolet warning receiver can be used to detect an incoming missile by the heat of its rocket motor, or the temperature of its skin due to internal or atmospheric heating. Laser warning receivers may be important in detecting the use of laser rangefinders, laser weapons, or in the future, an adaptation of the radar using a laser beam (a LADAR) instead of a radio frequency beam to do

detection and ranging. Warning receivers to detect the presence of nuclear radiation already exist and will probably be the forerunners of receivers to detect the employment of particle or beam weapons when and if they're deployed (23:70-77).

Electronic Countermeasures (ECM)

This is one form or branch of electronic warfare where a friendly system jams or deceives an enemy system.

> Obvious targets in electronic warfare [actually electronic countermeasures] include enemy surveillance, target acquisition, and tracking systems, plus the guidance systems of missiles [including ASAT interceptors] and smart weapons. EW [ECM] may also be used to good effect against speech, data, and missile guidance communications links (23:96).

Different techniques are applicable against different types of targets. Note: Although not addressed in this paper, electronic counter-countermeasures (ECCM) is an equally important aspect of electronic combat. An effort must also be made to determine the impact of defending US space systems against the enemy's use of electronic countermeasures. First, a look at some "brute force" jamming techniques.

Noise Jamming. Noise jamming is an electronic countermeasure designed to jam or overpower enemy radars. This is probably the oldest (and most primitive) form of jamming. It seeks to overload or saturate the receiver of a threat radar with unwanted radio frequency noise, making it impossible for it to distinguish its own transmitter's signal reflected from the the target. There are two sub-types of noise jamming; barrage and spot jamming. Barrage jamming is an easier technique to apply since it doesn't require precise measurement of the target radar's parameters. This technique involves spreading the output of a jammer's transmitters over a wide range of frequencies (to compensate for the uncertainty in the enemy's frequency) in an attempt to get enough noise into the enemy's receiver to obscure the return reflected off of the friendly target. This technique not only wastes energy but it can cause detection of the friendly system by hostile ESM or ELINT receivers or it can serve as a noise source for an anti-radiation homing missile. The other technique, spot jamming, is more precise (less wasteful) but it requires knowledge (either a-priori or real-time) of the enemy radar's frequency. With this technique, the jammer's output power can be concentrated in a narrow frequency band causing more of it to be received by the enemy's radar receiver thus making it harder for it to distinguish its own reflected signal (23:96-97). The two of the most important variations of these basic noise jamming techniques are inverse gain and pseudo-random noise. Inverse gain jamming is used against scanning radars and it

involves adjusting jamming power in an inverse relationship with the enemy radar's received effective radiated power as its beam sweeps across the target. Properly applied, this technique makes it difficult or impossible for the radar to detect from where in its scan the target signal is being reflected. Pseudo-random noise jamming involves turning the jammer on and off at near random times making sure it's on only when the enemy radar is transmitting a pulse. This technique also conserves jammer energy and allows more than one threat to be jammed simultaneously with one jamming transmitter (25:--).

Deception Jamming. The other major category of electronic countermeasures involves deception. "The goal of deception jamming is to provide the hostile radar with false data" (23:100). Techniques include repeater jamming, gate stealing, cross-eye, and two camoflage techniques known as velocity and range bin masking.

Repeater Jamming. This type of jamming involves receiving the enemy radar's pulse, delaying it or perhaps modulating it in some way, and retransmitting it to be received as would a normal echo. The spurious signal, however, could cause the radar to derive false range or bearing information about its target (23:100; 25:--).

Gate Stealing. These techniques operate on the premise that a radar receiver is not always in a "listen" mode. To prevent itself from being overloaded with internal and external noise, a receiver will normally be turned off until it expects a reflected pulse from a target. There are numerous ways for a receiver to predict when this will happen and the process is generally called "gating" (23:102). Some receivers are gated in the time domain and since time (for a pulse to be reflected from a target) is used to determine target range, this process is called range gating. Other receivers (associated with pulse Doppler radars) measure frequency shifts to determine target velocity and they use a similar technique known as velocity gating. In either case, the job of the jammer is to "steal" these gates and cause the receiver to listen at the wrong time. This involves transmitting a replica of a target's reflected pulse at the same time as the real reflected pulse. Then, by gradually increasing the strength of the fake pulse and adding a time (or frequency) shift, the enemy radar will begin tracking the fake pulse instead of the real reflection (23:102). Once the gate has been stolen, most jammers will turn off, leaving the enemy radar with nothing to track until it can relocate its original target. Of course, not all radars are so easily fooled (25:--).

Cross-Eye. Certain types of radars, known as monopulse, measure target position nearly instantaneously from a single reflected pulse. One technique which is being developed

to counter this type of radar is known as cross-eye. This technique "involves transmitting a fake echo from two antennas spaced as widely apart as possible after introducing a deliberate phase difference" (23:108). The phase difference will cause the victim radar antenna to point in the wrong direction and measure an incorrect target azimuth. Errors will be proportionate to the distance between the jammer's antennas (23:108; 25:--).

Bin Masking. Although certainly not the only other kind of jamming techniques, the bin masking types will be the last one discussed here. These techniques take advantage of the modern, state-of-the-art radars which use digital computers to do signal processing and present an artificial display to a human operator. To do its job, the computer will divide its range and/or velocity coverage (spectrum) into smaller subsections, normally referred to as "bins," and look in them for targets. This artificial processing creates an opportunity for a jammer to introduce false information in the "bins" around the one in which the target is contained, obscuring it. If done properly, since these radars use artificial, computer-generated displays, there will not even be any indication the radar is being jammed (25:--).

Chaff, Flares, Decoys, and Penaids. Other actions taken which may or may not involve electromagnetic radiation against an enemy radar can be as important or more important in the electronic warfare struggle. Among the items in this particular "bag of tricks" are chaff, flares, decoys, and penetration aids (called penaids). In many cases these may be the most cost-effective form of countermeasures for a given situation.

> Chaff will deal with radars and radar-guided weapons, flares can be used against IR-guided [infrared-guided] missiles and tracking systems, and decoys can confuse long-range sensors and will help ballistic missiles break through ABM [anti-ballistic missile] defences by multiplying the number of targets (23:84).

Chaff. Chaff is another simple form of countermeasures like noise jamming. In fact, the effects are, in a way, very similar. Chaff is basically a large number of small pieces of a conducting material cut to an optimium length (normally in the centimeter range) selected to reflect the maximum amount of a victim radar's energy. These tiny strips of material cause the radar to see only a cloud of noise from its reflected signal, thus obscuring the target. There are a variety of ways of employing this technique ranging from many small packages to create many false targets to huge clouds to mask the flight of multiple penetrators. Dispensing methods include tightly compacted bundles released into the airstream around an aircraft, cannon shells, and rockets. One limiting factor in chaff use in the atmosphere is that a chaff cloud will begin to slow down

immediately causing the aircraft to rapidly fly away from its masking effects. In space, since there are no atmospheric effects to slow down the chaff, this may not be a problem (23:84-89).

Flares. Flares are a lot like chaff, operating at a much higher frequency, i.e., the infrared region of the electromagnetic spectrum. Basically, a flare is designed to burn at a very high temperature, at the same wavelength (or wavelengths) as the target they're trying to protect, thus offering a better target for an infrared tracker or heat-seeking missile to go after. Unlike chaff, flares are an active type of countermeasure, i.e., they require combustion. Problems which influence their use include their endurance (burn time), selecting the proper infrared (or perhaps ultraviolet) wavelength (or wavelengths depending on the sophistication of the seeker being decoyed), and deployment triggering (i.e., knowing exactly when to use them against what are normally passive seekers which don't give the target any idea it's being tracked). In space, combustion, of course, would also be a concern due to the lack of oxidizer in that environment (23:89).

Decoys. Decoys (in the context of protecting aircraft or spacecraft) are basically small aircraft (or spacecraft) designed to mimic the electromagnetic (perhaps including infrared and ultraviolet wavelengths) signature of the target they're trying to protect. This can be done by a variety of passive and active measures. In one example, the ADM-20A QUAIL, a small pilotless aircraft, "used built-in ECM equipment to simulate the radar signature of another B-52, creating a false target" (23:92). (25:--)

Penaids. The term "penaids" is usually used to describe a collection of techniques to help ballistic missile warheads penetrate ABM defenses. These tricks are, of course, highly classified, but one system which has been made public is a canister carried by the Minuteman II. "No details of the techniques used are available, but a combination of chaff packages, active jamming, decoys, and infrared-emitting aerosols seem probable" (23:92). With the advent of SDI, and in the presence of the Soviets' already deployed ABM system, penaids are likely to be carried on most or all ballistic missiles (23:92-93).

EO and IR Jammers. Some of the techniques like flares and other penaids previously described are designed to operate in the infrared (IR) or optical (also referred to as electro-optical or EO) regions of the electromagnetic spectrum. Recently, some more aggressive techniques have begun to be developed. These include EO and IR jammers.

IR Jammers. Since a lot of IR-guided weapons use a rotating scan for their seeker to track a target, a weakness is present which may be exploited. "The basic method involves generation of a false source of flickering IR energy which the missile will interpret as evidence that the seeker is not pointed directly at the target" (23:112). The missile's guidance program will then create correction commands and will actually guide the missile away from the target. The IR flickering required can be done by mechanically or electronically shuttering a high intensity IR source (23:112-113).

EO Jammers. Visually or electro-optically guided weapons have been a concern for some time since they are both hard to detect and hard to counter. Although highly classified, there is some recent work in this area on "detection systems [that] can warn the aircrew [or spacecrew?] that they are under attack, while decoys and jammers may be used to confuse tracking and homing devices" (23:113). There is even one program, the Expendable Laser Jammer, which reportedly is intended to deal with laser-guided weapons (23:113-114).

Communications Jamming. While most, if not all, of the previously described techniques are related to targets and ways of protecting them from radar detection/tracking and missile seekers, there is another branch of electronic countermeasures which cannot be ignored: communications jamming. Since communications satellites may be among the most numerous in space, this area may be very important for space-related electronic combat.

> Radio links are another prime target for EW, and one which has been exploited in several recent conflicts. Voice, data, and even missile-command links are all vulnerable to jamming. If their operation is disrupted, the result can be chaos which an enemy will be quick to exploit" (23:116).

In communications jamming (as there was in radar jamming) there is a choice between unsophisticated noise or barrage type techniques and other more sophisticated techniques designed to counter the more modern digital data links. In general, however, "spot jamming [or specialized digital techniques designed against specific data links] is the most effective since it concentrates the effect of the jamming, while leaving most of the frequency band unjammed, and thus free for friendly communications" (23:116). Also as in radar jamming, the more sophisticated and concentrated jamming requires more detailed information on the enemy systems' parameters and will be more susceptable to changes in those parameters (23:116-118; 25:--).

Stealth

"One new factor [which isn't really new but which has recently gotten a lot of publicity] in the electronic battle between aircraft [and spacecraft?] and anti-aircraft [and anti-spacecraft?] weapons and sensors is the use of stealth technology" (23:40). This technology isn't really a specialized science, rather, it involves a combination of several different techniques including: "careful shaping of the airframe [or spaceframe?], the use of radar absorbing materials" (23:40), general radar cross section reduction, supression of electronic and infrared emissions, and the use of specialized ECM tailored specifically for the stealth-type vehicle (23:40-47). In any case, "none of these techniques is new, but used in combination, their effectiveness is greatly multiplied" (23:40).

Conclusion

The preceding paragraphs have been a brief description of what is in the electronic combat "bag of tricks" to contribute to any battlefield from the earth's surface to space. What follows is an attempt to select/describe some of these techniques for that unique battlefield associated with space.

Chapter Five

EC APPLIED TO SPACE

Introduction

The battle (application of electronic combat in space) has actually already begun. In reality, space is just another operating medium for aerospace forces and it should be no surprise if the enemy brings all of his forces to bear to deny the US the advantages of its use. On the other hand, it should be just as obvious to the United States that electronic combat is an important tool to use in performing the vital mission of space control, i.e., denying the use of space to the enemy and ensuring its availability for our own use. Finally, the United States military's almost total dependence on spacebased communications assets for long-distance communications makes it vital to consider counter-countermeasures an integral part of our efforts. A lot has (or reportedly has) already been done.

Efforts So Far

Since they're normally highly classified, these attempts don't get much visability but there has been activity in developing ASATs, jammers, warning receivers, lasers, and other beam weapons for use in space and against space assets. Even though they don't seem to fit into the stereotype picture of the "battle of the beams," ASATs are a vital part of electronic combat. Physical destruction is a viable technique and supression of enemy air defenses also falls under the electronic combat umbrella. As previously discussed, the USSR already has an operational ASAT and the US is developing one. Reportedly the Soviets have also experimented with electronic countermeasures against "ground command transmissions to satellites [which are] essential for keeping them in the desired orbit, [and they have also tried] to deceive the satellites by giving them false commands to descend into the low atmosphere where they would burn up" (9:294). Whether or not these reports are true, they represent applications of electronic combat to the space environment worthy of further consideration.

The United States has also supposedly

> developed a series of jammers [including a "series of ECMs to degrade Soviet reconnaissance satellite performance - particularly those used for tracking US Naval surface ships and submarines" (9:296)] to counter an electronic attack ... [but] finally opted for passive ECMs such as chaff and false IR targets capable of deceiving a killer-satellite (9:295).

"IR decoys have [also] proved to be particularly effective for protection against ICBMs ... to divert the deadly weapon from its true target" (9:295-6). Recognizing the importance of attack warning/assessment satellites, the US has "developed radar and IR warning receivers for installation on [these] satellites to provide them with early warning of the approach of a hostile satellite, allowing them time to manoeuvre away from it" (9:296).

Lasers have also reportedly been used against space assets.

> On two occasions, 18 October and 17 November 1977, two USAF satellites used for transmission of data required for wartime operations by Strategic Air Command's bomber force, as well as other US Early Warning satellites, were put out of action for almost four hours. CIA experts suspected that the black-out was due to deliberate jamming by the Soviets using a laser, either based on the ground, or in a killer-satellite which they were testing (9:293-4).

Where do we go from here? A plan to answer this question is presented in the next chapter, but first some general information must be considered.

<u>What's Next?</u>

In the opinion of one expert,

> There are two kinds of countermeasures applicable in space warfare: countermeasures against the platforms or space-stations (shuttle, Soyuz, satellites, etc.) and countermeasures against 'directed-energy' weapons. Both require threat warning receivers for immediate detection of enemy radar, laser or IR source (booster, exhaust, etc.). Against the platforms, similar ECM equipment to that used on Earth could be employed: on-board jammers and expendable jammers, chaff, IR flares, radar absorbing shields, and so on. Against the laser beam, laser decoys, mirrors, and space mines could be used - or any other electro-optical countermeasures

(ECCM) which emerge from technological progress (9:305).

Actually, what's being said here is that virtually any of the electronic combat techniques which are applicable on earth, and in the earth's atmosphere, are applicable to space warfare. There are, however, some important considerations which must be factored into the equation.

Considerations

Weight, Cost, and Complexity. Before rushing headlong into designing, developing, and deploying spacebased electronic combat capabilities, weight, cost, and complexity must be dealt with. The same weight restrictions that apply to the satellites themselves must also be taken into account when dealing with any type of electronic combat subsystem "add-on " As an example, nuclear/laser hardening "costs" between 20 and 30 percent of a satellite's launch weight depending on its required endurability. Increased launch weight isn't the only factor involved. Counter-countermeasures for communications links cost money and complexity. A satellite's research and development cost can be increased by 30 percent to achieve a high degree of anti-jam capability for its links and it can experience more than a 1000 to 1 degrade in its capacity to transmit information compared to an unprotected link. Finally, increased maneuver capability to avoid a direct attack can not only increase launch weight significantly, due to increased fuel loading, but can also increase satellite acquisition cost by up to 30 percent (27:42-3).

Environmental. Electromagnetic radiation (radio, radar, infrared, visual light, etc.) is unaffected by the environment of space (it's actually enhanced compared to radiation in the atmosphere due to the lack of absorption and other effects) but its about the only thing that is. The vastness of space and the geometry of potential encounters must be taken into account. Jammers, for instance, must be properly positioned to get sufficient energy into an enemy's receiver to overpower or deceive its intended operation. Laser links between satellites or to/from earth and space will be particularly difficult to intercept and jam due to the tightness of their beams and the necessity to be properly placed to "see" them.

The lack of atmosphere can also hamper application of electronic combat techniques like flares and chaff. Flares, of course, must have an oxidizer to burn and although this can be provided or another type of infrared producing reaction can be developed, these things must be considered. Use of chaff will be enhanced and degraded. Since there's no wind resistance, it wouldn't slow down, and leave the target its trying to screen, like it does in the atmosphere, but dispersal may be a problem.

i.e., once put into motion to spread it into a cloud, a chaff package will continue to disperse unchecked by wind resistance and gravity.

Conclusion. Most of what's in the electronic combat "bag of tricks" should be applicable to space. The important aspects of application of the various techniques are the cost of using them in space (in terms of weight, cost, and complexity) and the "differentness" of the physical environment. Careful planning is required to determine the most cost-effective way to achieve the best results in either enhancing US capabilities or degrading enemy capabilities (or both) and this will be the subject of the next chapter.

Chapter Six

A PLAN TO CREATE A SPACE EC ROADMAP

INTRODUCTION

The basis for building a roadmap to achieve a level of electronic combat capability in space has been discussed in Chapters Two, Three, and Four. This chapter will describe the contents of the required roadmap, and discuss what has been done and what needs to be done to complete the roadmap.

Why a Roadmap?

The lack of a coherently stated space control doctrine in AFMs 1-1 and 1-6; the potential for our space systems to be electronic combat targets; the potential for offensive use of electronic combat against our enemies' space systems; and the variety of electronic combat means/methods at our disposal, all point to the need for some kind of a master plan. This plan is, however, an "end product" and the method to build that product is a roadmap. As stated in Chapter One, an electronic combat roadmap for space would serve as a bridge between where we are now and where we need to be. It documents what is being done and presents a coherent plan for achieving future capabilities.

ROADMAP DESCRIPTION

Introduction

There are no firm guidelines for construction of a roadmap of the type proposed by this report but there are some "common sense" items or sections which should be included. This includes a threat description, a "friendly systems" description, a statement or exploration of possibilities, and a set of requirements. The first two sections are the "where we are," and the other two are the "where we need to go." What's missing is a discussion on "how we get there?" This report will deal with laying the foundation getting there but since the decisions required to "flesh it out" must be made at very high levels and would of necessity be highly classified, the "how we get there" part of the roadmap will not be discussed. Although a timeline section will be addressed, also missing will be a discussion of

"when do we get there?" The answer to a "when do we need it?" type question is: now, or yesterday, but a practical answer depends on the level of committment and the priority given to some very detailed and complicated analyses.

Threat Description

Encompassing the entire spectrum of potential threats to US space systems is not the purpose of this section of the roadmap. What is intended is a more detailed description of potential targets for offensive electronic combat than was provided in Chapter Three. Additionally, a description of any enemy electronic combat capabilities in space or directed toward US space systems should be included. To keep the scope of the roadmap manageable, these descriptions need not be complete, fine-grained technical specifications but should provide a summary of the known threats, a summary of what's known about them, and a reference to a more complete technical description. Where information is not known, but is vital to the completion of the roadmap, this section should also highlight that fact and lay out requirements for additional information/intelligence gathering and reporting.

Friendly Systems Description

Like the previous section, this one need not be a technical encyclopedia, but should summarize the critical technical characteristics of US space systems which will play a role as targets or weapons in the space control/electronic combat arena. Classification and access will be a problem even with the "summary-level" information required for this section, but an effort should be made to make this section as complete as possible because it will serve as part of the baseline for determining future capabilities. Generally this section should contain basic technical characteristics, a description of any electronic counter-countermeasures features, and a description of any built-in electronic countermeasures capabilities.

Possibilities

This section should examine the types of electronic combat means/methods which should be used in performing the space control mission, as well as information on how and when they should be applied. It should detail, on a mission-by-mission basis, what can be done by electronic combat and where in the spectrum of conflict (from low-intensity through nuclear and beyond) it can/should be done. In addition, endurability (how long a countermeasure's effects can be maintained) and perishability (the potential for technique negation) must be explored. These are, of course, extremely complex and interwoven concepts which must be the subject of a great deal of rigorous analyses which will be discussed in the next chapter.

Requirements

Next to actually obtaining the funding to do the job, just filling in this section may be the most difficult task to complete. The task will include describing the types of electronic countermeasures and counter-countermeasures which are required for each particular space system/mission. This section builds on the previous section which describes what can be done by making a statement of what should/must be done. Guidelines or generic requirements for electronic counter countermeasures capabilities must be a part of this section as well as, a definition of what electronic countermeasures and other electronic combat techniques should be in the US space control arsenal.

Timeline

Although not intended as a detailed, rigid schedule, this section should provide a description of the various tasks and studies which must be done, assign responsibility for the jobs, and provide general guidance on the importance and time sensitivity for each job. Enough detail must be included in this section, or in attachments to the roadmap, to enable the tasked agency to carry out its assigned task. In addition, the roadmap must be approved at a high enough level to ensure the tasked agency takes the job seriously and also has the authority to get the job done.

CREATING THE ROADMAP

Introduction

What has been described so far, in this chapter, is a skeletal framework for what will precede the roadmap and what it should contain when it is complete. The next task is determining what must be done and who should do it to actually create the roadmap. Much of this will be further developed in the next chapter as recommendations for further study. Generally, the first two tasks must be completed before the next two can be finished, but there may be ways of segmenting or subdividing each task to allow the appropriate parts of all four tasks to be done for one specific mission or system at a time.

Tasks/Responsibilities

Actually the tasks which must be done are fairly well laid out in general by the description of the roadmap. The first two sections are survey-type tasks involving a search of information which is held by various agencies. The other two sections will require analyses.

Threat. The threat information, much of which is published regularly by intelligence agencies (like the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, and the intelligence staffs of the Army, Navy, and Air Force) should be readily available at the appropriate security classification level. Because of their familiarity with the data and their acceptability by the rest of the intelligence community, this task should be done by one of the intelligence agencies; such as DIA or perhaps the J-2 of the US Space Command. Almost as important as the task of collecting the information already on hand, will be the identification of what isn't known and obtaining that information.

Friendly Systems Description. The information required to complete this section will be held by various agencies including the organization of the Secretary of the Air Force (Space Systems Division), the Office of the Secretary of Defense (C3I), and the Organization of the Joint Chiefs of Staff (J-2 and J-6). Data on fielded systems will most likely be the property of their users. Developmental systems are the responsibility of Systems Command in the Air Force and similar agencies in the other services and they will control the information on these systems. Gathering the information required in this roadmap section will require "clout" and access. The holders of the information will be reluctant to release it and it will almost certainly be protected by special access caveats. US Space Command also seems to be the appropriate agency to do this job since they're the designated operator of all DOD space systems.

Possibilities. Creating this section will be an enormous task requiring technical capability and imagination. It will involve examination and analysis of the missions and capabilities of the various space systems, the usefulness of those missions and capabilities to the space systems' users, and the degree to which the users depend on the capabilities provided (including a look at other surface based or airborne systems which could take their place). Coupled with the examination of capabilities, will be an analysis of when in the spectrum of conflict the capabilities are important. Due to the scope/complexity of this task, it may have to be done by contractors with the study efforts managed by a DOD focal point or by USSPACECOM/J-5.

Requirements. These must flow from the doctrine and strategy which are developed for space control and the part which electronic combat plays in that mission. It may be impossible to break requirements down to an individual systems basis for all systems but an attempt should be made to establish basic requirements for general mission categories. Since doctrine and strategy are developed at the uppermost levels of the services, a tri service working group should be established (with OTCS oversight) to create the foundation for requirements as well as a minimum level of mandatory capability. Inputs should flow from

the Strategic Air Command and the Air Force Space Command's X and XP offices as well as USSPACECOM's J-3 and J-5.

CONCLUSION

This chapter doesn't provide the answer to the basic question of how the United States should build the appropriate level of electronic combat capability for space. It doesn't even provide a detailed roadmap to achieve that capability. What it does provide is an examination of what needs to be in that roadmap, why these bodies of information are important, and how they should be obtained. As alluded to in this chapter, some of the information to build the roadmap is readily available (although it may be difficult to obtain) and some will require detailed studies and analyses. The latter group will be the subject of Chapter Seven of this paper which will be on recommendations for further study.

Chapter Seven

RECOMMENDATIONS FOR FURTHER STUDY

INTRODUCTION

The most obvious areas requiring further study are those which will help in actually building the space electronic combat roadmap. Of these areas, there are some which are absolutely vital and which will require tough research and analysis efforts. There are other areas whose study will help build the roadmap but which are less difficult to do. Finally, there is a third set of studies which are more like "related questions" which could potentially impact the application of the roadmap's findings to operational systems.

RESEARCH AND ANALYSES

Introduction

There are two vital efforts in this area which must be done to achieve any coordinated, coherent capability for electronic combat in space. The first is an exploration of space control doctrine and the subsequent creation of space control strategy. Any force development must be done in conjunction with the principles of a well-developed doctrine and strategy. The other effort is just as important. This one involves exploration of the utility of the various systems used by the US and our potential adversaries and an examination of both sides' dependence on these capabilities.

Doctrine/Strategy Development

Electronic combat in space is not a "stand-alone" mission. It must fit in with established doctrine and strategy for operating military forces in space. The foundation for the space electronic combat roadmap, begun in Chapter Two of this paper, is based on existing Air Force doctrine, the principles of electronic combat, and a growing awareness of the importance of the space medium and US military capabilities in that medium. The need is obvious but is not being completely fulfilled. The similarity between the status of space doctrine today and air doctrine just after World War I is amazing. Even Hap Arnold

said, "Actual wartime use has confirmed the utility of aircraft for reconnaissance. Beyond that, however, their use [is] more or less a matter of conjecture" (60:42). What is required is a careful examination of the two sources of doctrine for space, AFM 1-1 and 1-6, and an effort to include in them statements which say what we believe we can do in space. From that statement of doctrine; considering the constraints of technology, legality, cost, complexity, and others; space control strategy must be formulated. The use of electronic combat must be clearly articulated for the space control mission like it is for similar "terrestrial" missions. Finally, this doctrine and strategy must find its way into AFM 1-9, the Doctrine for Electromagnetic Combat.

Although the coordination and approval for doctrine and strategy must take place on the Air Staff, the formulation process can at least be begun at Air Command and Staff College, perhaps as a student research project.

Utility/Dependency Analyses

Before any effort is expended in developing or actually using a particular capability, one should have at least an idea of what its effects will be and what results or impacts on the enemy are expected. These ideas are the crucial questions which are asked as part of utility/dependency analyses. In the context of exploring the use of electronic combat in space, these analyses should center on space systems but should be broad enough to encompass other systems capable of performing the same or similar missions. They must explore the essential questions of when to use a particular technique or capability: what enemy signal, subsystem, or system to use it against; and what other signals/systems must also be countered. In addition, the questions of technique/capability endurability and perishability, mentioned in Chapter Six, must be answered. The best way to explain a utility/dependency analysis is through an example.

The scenario for this example is ocean surveillance. Space systems which are available to the enemy are his ocean surveillance satellites (described in Chapter Three) and their associated groundbased command and control systems. The analysis will center on what electronic combat techniques/capabilities can be used by friendly forces to hide naval fleet movements. Questions which must be answered include:

- What techniques are there to use (ASAT, jammers, smoke, weather, chaff, spoofing, deception, etc)?

- When should they be used and for how long?

  -- Before sailing?

-- During maneuvers at sea?

-- Nighttime or daytime?

- What should they be used against?

-- Satellites?

-- Control links?

-- Sensors?

-- Control facilities?

- What information does the enemy obtain from the satellites, i.e., what is their **utility**?

- What other systems (reconnaissance aircraft, submarines, agents in ports, etc.) does the enemy have which can augment/replace any negated space capability, i.e., what is the degree of **dependency** on the space system?

- What is the enemy's capability to replace a negated or destroyed satellite?

- What are his reactions likely to be?

-- Military?

-- Political?

These are just some of the questions which must be asked and answered for only one scenario. The same kind of information would be required for other individual scenarios and also for the integrated, interwoven, large-scale scenario of a theater or nuclear war. Perhaps the best way to begin this task is by looking at the individual, more easily-defined scenarios and then expanding to the broader, more all-encompassing scenarios. Note: Just as this type of analysis is important for studying the application of countermeasures by US systems against enemy systems, the reverse is also true. A utility/dependency study of enemy countermeasures against US space and related systems would be very useful in developing electronic counter-countermeasures.

ROADMAP SUPPORT STUDIES

Introduction

These are the studies which will help build the roadmap. Two of them have already been explored in Chapter Five: the

threat and friendly systems sections of the roadmap. Another one involves this research paper itself. There are probably many more.

Threat Information Study

Chapter Six calls for an extensive compilation of information on enemy systems as an integral part of the roadmap. This would be a large task. However, as a first step, perhaps what can be done is a survey of information sources (sort of a literature search or a building of a bibliography) to provide a foundation for the more complete information compilation. This is another area which may be able to be done by an Air Command and Staff College student as a research project. NOTE: DIA is already involved in doing some of this.

Friendly Systems Information Study

Like the effort on threat systems, the scope of the task called for in Chapter Six in this area is also large. Again, as a first step, a survey-level project should be done. This one will probably be more difficult than the one on threat systems because in a lot of cases, information on our own systems is harder to get than on enemy systems. Again, at least an idea of "what's out there" should be compiled. Probably classified, this task may be too large and difficult for a student research project. NOTE: This study is being done, in part, by the Office of the Secretary of Defense (C3I) Organization of the Joint Chiefs of Staff.

Roadmap Plan Study

This project is essentially a re-do of this research paper but at a classified level. It would involve primarily the information presented in Chapters Three and Four, substituting the "real" data for that which was extracted from open-source publications. The goal of this effort would be to either validate or refute the ideas presented in this paper. This can be sponsored by Air Staff or the Office of the Secretary of the Air Force.

RELATED QUESTIONS

Introduction

Not intended to be anything like a complete list of related topics to be studied, these are just some ideas or questions which may have a bearing on the general subject of electronic combat employment in space.

Legality

Is the use of electronic combat in space legal? Does it impact any existing treaties or laws? These questions must involve participation by USSPACECOM and the Judge Advocate General.

Wargaming

Is it possible to model the use of electronic combat in space using existing wargames? Can the results of such use be predicted? Do the models need to be modified? Studies to answer these questions are underway at USSPACECOM, AFSPACECOM, the Air Force Center for Studies and Analysis, the Organization of the Joint Chiefs of Staff, and the Air Force Wargaming Center.

Non-Military Space Systems

If a national aerospace plane is to be developed, should it have electronic combat systems like a radar warning receiver, a jammer, or chaff/flares? Should the space shuttle? Should the space station? These questions should be the responsibility of the National Aerospace Plane Joint Program Office and NASA.

CONCLUSION

There are many other areas to be studied and questions to be asked than the ones briefly mentioned in this research paper. The gathering of information is important but the formulation of doctrine/strategy and the prediction of effects/results are vital.

Chapter Eight

CONCLUSION

This paper has explored the principles of electronic combat and the functions which comprise that mission. It has examined the types of space systems used by the United States and the Soviets which are potential targets for electronic combat techniques/methods. Also investigated were the contents of our electronic combat "bag of tricks." Finally, some ideas on how to actually build an electronic combat in space roadmap were presented along with a description of studies and analyses which must be done and some related questions which might be answered. What should be clear is that no matter how many objections have been, and will be raised, the military is in space probably to stay. We have some clearly defined objectives for operating in that medium. To support these objectives, a doctrine and strategy must be developed and an integral part of that doctrine and strategy will be the use of electronic combat. There's a lot of work to be done, but the recommendations for further study and construction of a roadmap, if implemented/continued, will go a long way in enhancing US capabilities in the fourth military arena -- space.

BIBLIOGRAPHY

1. 1987 Air Force Issues Book, Office of the Vice Chief of Staff, Department of the Air Force, Washington, DC, Spring 1987.

2. AFM 1-1, United States Air Force Basic Doctrine, Department of the Air Force, GPO, Washington, DC, 16 March 1984.

3. AFM 1-6, Military Space Doctrine, HQ USAF/XOXID, GPO, Washington, DC, 15 October 1982.

4. AFM 1-9, Doctrine for Electromagnetic Combat, HQ USAF/XOXLD, GPO, Washington DC, 18 September 1979.

5. Bassett, Lt Col Fred and Lt Col Barry Britton, Eds., "Electronic Combat," Warfare Studies and Space, Handbook for Air Command and Staff College, Maxwell AFB, AL, 1987.

6. Bolino, John, "Joint EC Test and Evaluation," Journal for Electronic Defense, Vol. 10, No. 8, August 1987.

7. Burrows, William E., Deep Black - Space Espionage and National Security, New York, Random House, 1986.

8. Church, George J., "Exploring the High-Tech Frontier," Future Defense and Space Technologies, AWC Associate Programs Vol. I, Ch. 20, 20th Ed., pp. 13-17, Maxwell AFB, AL, 1987.

9. De Archangelis, Mario, Electronic Warfare: From Tsushima to the Falklands and Lebanon Conflicts, New York, Sterling Publishing Company, 1985.

10. FM 34-20, Military Intelligence Group (CEWI)(Corps), Headquarters, Department of the Army, GPO, Washington DC, 6 May 1983.

11. Friedman, Col Richard S., et al., Advanced Technology Warfare, New York, Harmony Books, 1985.

12. Gallotta, A. A., Jr., an Association of Old Crows Letter to the Honorable Sam Nunn, 25 June 1987.

13. Giordana, Robert F., "Army Intelligence Electronic Warfare," Journal of Electronic Defense, Vol. 10, No. 10, October 1987.

CONTINUED

14. Graham, Gen Daniel, High Frontier, New York, Doherty Associates, Inc., April 1983.

15. Gray, Colin S., American Military Space Policy, Cambridge, MA, Abt Books, 1983.

16. Gross, Richard C., "Troubles for SDI," Defense Science and Electronics, Vol. 6, No. 5, May 1987.

17. Hartinger, Gen James V., "The New Space Command," a speech given to the Paul Revere Foundation, Wichita, Kansas, 1 December 1982, filed with AFM 1-6 in the Air University Library, Maxwell AFB, AL.

18. Hobbs, David, Space Warfare, New York, Salamander Books, Ltd., 1986.

19. Holly, I. B., Jr., "Looking Backward to See Ahead in Space," Thinking About War, Handbook for Air Command and Staff College, Maxwell AFB, AL, 1988.

20. Hooper, Larry, "Politics Pressures SDI," Defense Electronics, Vol. 19, No. 2, February 1987.

21. Johnson, Nicholas L., The Soviet Year in Space - 1986, Colorado Springs, Teledyne Brown Engineering, January 1987.

22. Menoher, Col Paul, USA, "Army IEW Master Plan," Journal of Electronic Defense, Vol. 10, No. 10, October 1987.

23. Richardson, Doug, Techniques and Equipment of Electronic Warfare, New York, Arco Publishing Company, Inc., 1985.

24. Rider, Rick, "Star Wars ... Threat or Opportunity?", Journal of Electronic Defense, Vol. 10, No. 5, May 1987.

25. Schleher, Curtis D., Introduction to Electronic Warfare, Dedham, MA, Artech House, 1986.

26. Soviet Military Power - 1987, United States Department of Defense, Office of the Secretary of Defense, GPO, Washington DC, 1987.

27. Thieman, Maj Bruce A., USAF, Space Resource Allocation Exercise, Air Command and Staff College Student Report No. 87-2480, Maxwell AFB, AL, 1987.

28. Turnill, Reginald, Ed., Jane's Spaceflight Directory - 1986, London, Jane's Publishing Company Limited, 1986.

29. Ulsamer, Edgar, "At Risk in Space," Air Force Magazine, Vol. 70, No. 9, September 1987.

30. _____, "Strategic Connections in Space," Air Force Magazine, Vol. 70, No. 8, August 1987.

31. United States Military Posture - FY 1988, prepared by the Joint Staff, Organization of the Joint Chiefs of Staff, GPO, Washington, DC, 1987.

END
DATED
FILM
8-88
DTIC