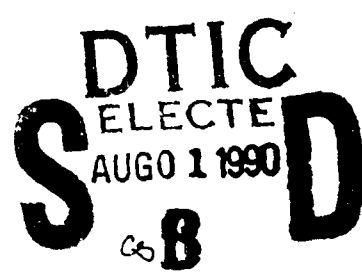


AD-A224 683

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204 Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 1990	3. REPORT TYPE AND DATES COVERED Thesis/Dissertation		
4. TITLE AND SUBTITLE SURVIVABILITY ENHANCEMENTS FOR MILITARY COMMUNICATIONS SATELLITES		5. FUNDING NUMBERS		
6. AUTHOR(S)  FREDERIC MARC ARRENDALE		7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AFIT Student at: Univ of Colorado		
8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/CI/CIA - 90-042		9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFIT/CI Wright-Patterson AFB OH 45433		
10. SPONSORING / MONITORING AGENCY REPORT NUMBER		11. SUPPLEMENTARY NOTES		
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release IAW AFR 190-1 Distribution Unlimited ERNEST A. HAYGOOD, 1st Lt, USAF Executive Officer, Civilian Institution Programs		12b. DISTRIBUTION CODE		
13. ABSTRACT (Maximum 200 words)				
				
14. SUBJECT TERMS			15. NUMBER OF PAGES 111	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT	

## THESIS ABSTRACT

Author: Frederic Marc Arrendale

Title: Survivability Enhancements for  
Military Communications Satellites

Military Rank and Service Branch: Capt, USAF

Date: 1990

Number of Pages: 111

Degree Awarded: M.S. in Telecommunications

Institution: University of Colorado

<b>Accession For</b>	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

## THESIS ABSTRACT

Recognizing the various potential threats against the United States' military communications satellites and the criticality of their operation during times of national emergency, it is especially crucial that we accurately assess those threats and then design systems that are survivable against those threats. Their importance for instantaneous delivery of command and control information to the various strategic and tactical forces is invaluable and must be protected. This thesis will introduce the subject of military communications satellites and compare them with their civilian counterparts from a survivability perspective, it will assess the threats against these command and control assets, and it will describe technological methods for enhancing their survival. The examination of these methods will include such topics as physical and EMP hardening, robustness or resistance to jamming, reconstitution of the network, and constellation designs which enhance survivability. Finally, conclusions are drawn and recommendations proposed based upon the discussion.

**THESIS ABSTRACT**

Author: *Frederic Marc Arrendale*

Title: Survivability Enhancements for  
Military Communications Satellites

Military Rank and Service Branch: Capt, USAF

Date: 1990

Number of Pages: 111

Degree Awarded: M.S. in Telecommunications

Institution: University of Colorado

## **THESIS ABSTRACT**

Recognizing the various potential threats against the United States' military communications satellites and the criticality of their operation during times of national emergency, it is especially crucial that we accurately assess those threats and then design systems that are survivable against those threats. Their importance for instantaneous delivery of command and control information to the various strategic and tactical forces is invaluable and must be protected. This thesis will introduce the subject of military communications satellites and compare them with their civilian counterparts from a survivability perspective, it will assess the threats against these command and control assets, and it will describe technological methods for enhancing their survival. The examination of these methods will include such topics as physical and EMP hardening, robustness or resistance to jamming, reconstitution of the network, and constellation designs which enhance survivability. Finally, conclusions are drawn and recommendations proposed based upon the discussion.

## BIBLIOGRAPHY

### Books

Bulkeley, Rip, and Graham Spinardi. Space Weapons: Deterrence or Delusion? Totowa, NJ: Barnes & Noble Books, 1986.

Carter, Ashton B. "The Current and Future Military Uses of Space." in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: The Aspen Strategy Group and University Press of America, 1987, pp. 29- 69.

Gagliardi, Robert M. Satellite Communications. Belmont, CA: Lifetime Learning Publications, 1984.

Gray, Colin S. American Space Policy: Information Systems, Weapon Systems and Arms Control. Cambridge, MA: Abt Books, 1982.

May, Michael M. "Safeguarding Our Space Assets." in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: Aspen Strategy Group and University Press of America, 1987, pp. 71 - 85.

Perry, William J., Brent Scowcroft, Joseph S. Nye, Jr., and James A. Shear. "Anti-Satellite Weapons and U.S. Military Space Policy: An Introduction" in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: Aspen Strategy Group and University Press of America, 1987, pp. 1 - 28.

Pratt, Timothy, and Charles W. Bostian. Satellite Communications. New York: John Wiley & Sons, 1986.

Roddy, D. Satellite Communications. Englewood Cliffs, NJ Prentice Hall, 1989.

Skaug, R., and J. F. Hjelmstad. Spread Spectrum in Communication. London: Peter Peregrinus Ltd, 1985.

Stares, Paul B. The Militarization of Space. Ithaca, NY: Cornell University Press, 1985.

Stares, Paul B. Space and National Security. Washington, D.C.: The Brookings Institution, 1987.

Van Trees, Harry L. ed. Satellite Communications. New York: IEEE

Press, 1979.

### Conference Proceedings

Binder, Richard, and Dennis Perry. "The Multiple Satellite System - Low-Altitude Survivable Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 30.3.1. - 30.3.6.

Bond, Fred E. "Long Range MILSATCOM Architecture." IEEE Military Communications Conference, Oct 17-20, 1982, Boston, Conference Record, pp. 11.1.1 - 11.1.5.

Boyd, R. W., S. L. Adams, M. I. Spellman, and L. V. Lucas. "Survivable Space Networks: The Physical Layer." IEEE Military Communications Conference, Oct 23-26, 1988, San Diego, Conference Record, pp. 26.6.1 - 26.6.6.

Cook, Charles W. "The U.S. Air Force Space Program." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, MITRE Document M85-3, pp. 39 - 42.

Cooper, Robert S. "Space Challenges." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, MITRE Document M85-3, pp. 65 - 72.

Day, M. H., and C. M. Lockhart. "Survivable Network Planning at AT&T Bell Laboratories." IEEE Military Communications Conference, Oct 5-9, 1986, Monterey, CA, Conference Record, pp. 24.1.1 - 24.1.4.

Frankel, Michael S. "Survivable Command, Control, and Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 30.1.1 - 30.1.4.

Hoernig, O. W., Jr., and D. R. Sood. "Command System Protection for Commercial Communication Satellites." IEEE Military Communications Conference, Oct 5-9, 1986, Monterey, CA, Conference Record, pp. 3.5.1 - 3.5.6.

Kaldenbach, Brian, David R. Geissler, and Edward W. Ver Hoef. "A System Simulator for Low Orbit Satellite Communication Network." IEEE Military Communications Conference, Oct 19-22, 1987,

Washington, D.C., Conference Record, pp. 14.5.1- 14.5.5.

Leahy, Peter. "Small AJ Satcom Terminal Considerations." IEEE Military Communications Conference, Oct 31 - Nov 2, 1983,

Washington, D.C., Conference Record, pp. 229-233.

Paul, Heywood I., Charles B. Meader, Daniel A. Lyons, and David R. Ayers. "Forward Error Correction and Spatial Diversity Techniques for High-Data Rate MILSATCOM over a Slow-Fading Nuclear-Disturbed Channel." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 11.4.1 - 11.4.5.

Poliakon, Joseph A. "System Issues and Considerations Associated with Design of Ground Mobile Strategic Satellite Communication Terminals." IEEE Military Communications Conference, Oct 31 - Nov 2, 1983, Washington, D.C., Conference Record, pp. 253-258.

Quinn, Thomas P. "A Defense Department Perspective." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, MITRE Document M85-3, pp. 35 - 38.

Shacham, Nachum. "Protocols for Multi-Satellite Networks." IEEE Military Communications Conference, Oct 23-26, 1988, San Diego, Conference Record, pp. 26.3.1 - 26.3.5.

Sharifi, Hossein M., and Mahammed Arozullah. "A Centralized Multiple Satellite Network for Real Time Global Space, Land, and Mobile Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 40.3.1 - 40.3.5.

#### Government Documents

Donadio, Giuseppe. "Comparative Analysis of Passive Communications Satellites Employing the SHF and HF Spectrum for Use in a Strategic Role." Thesis submitted to the Naval Postgraduate School, Monterey, CA, Mar 1988.

Gill, Timothy Curtis, and Robert Leigh Trapp. "A Model for Evaluating Communications Satellite Interoperability." Thesis submitted to the University of Colorado for the Air Force Institute of Technology, Wright-Patterson AFB, OH, Oct 1985.

"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process." Report prepared by Computer Sciences Corporation for the Defense Nuclear Agency, Jun 4, 1976.

Murdock, William P., Jr. "Alternative Force Structuring Strategies for Military Satellite Communication Systems." Thesis submitted to the Air Force Institute of Technology, Wright-Patterson AFB, OH, Dec 1987.

Phillips, Barbara A. "A Prototype Knowledge-Based System to Aid Space System Restoration Management." Thesis submitted to the Air



Force Institute of Technology, Dec 1986.

Stover, Harris A. "Engineering Aids for the Design of Survivable Defense Communications Transmission Capability." Technical Note 11-82. Defense Communications Agency, Jan 1984.

Townley, Ralph K., David W. Brown, Martin O. Bernet, and Bernard L. Pankowski. "Selected Issues in DCS Integration." Technical paper prepared by Computer Sciences Corporation for the Defense Communications Agency, Aug 1987.

Tozer, T. C. "An Introduction to Military Satellite Communications." Memorandum No. 3976 of the Royal Signals & Radar Establishment. Malvern, England, Apr 1987.

#### Periodicals

Gits, Victoria. "Ball Project Part of 'Star Wars' Test." Daily Camera, Feb 15, 1990, Sec A, pp. 1 and 11.

Hughes, David. "Milstar Terminal Capability Demonstrated as Congress Debates Program Budget." Aviation Week & Space Technology, Oct 30, 1989, pp. 49-50.

Klass, Philip J. "Gains in Satellite Technology Shape Trends in C<sup>3</sup> Development." Aviation Week & Space Technology, Mar 20, 1989, pp. 251-253.

Perroots, Leonard H. "Soviet Beam Weapons are Near Tactical Maturity." Signal, Mar 1990, pp. 37-39.

SURVIVABILITY ENHANCEMENTS FOR MILITARY  
COMMUNICATIONS SATELLITES

by

FREDERIC MARC ARRENDALE

B.S., United States Air Force Academy, 1982

A thesis submitted to the  
Faculty of the Graduate School of the  
University of Colorado in partial fulfillment  
of the requirements for the degree of  
Master of Science  
Program in Telecommunications

1990

This Thesis for the Master of Science Degree by  
Frederic Marc Arrendale  
has been approved for the  
Program in Telecommunications  
by

*Hussain Haddad*

Hussain Haddad

*Robert A. Mercer*

Robert A. Mercer

*Russell E. Shain*

Russell E. Shain

Date 4/30/90

Arrendale, Frederic Marc (M.S., Telecommunications)

Survivability Enhancements for Military Communications

Satellites

Thesis directed by Professor Hussain Haddad

Recognizing the various potential threats against the United States' military communications satellites and the criticality of their operation during times of national emergency, it is especially crucial that we accurately assess those threats and then design systems that are survivable against those threats. Their importance for instantaneous delivery of command and control information to the various strategic and tactical forces is invaluable and must be protected. This thesis will introduce the subject of military communications satellites and compare them with their civilian counterparts from a survivability perspective, it will assess the threats against these command and control assets, and it will describe technological methods for enhancing their survival. The examination of these methods will include such topics as physical and EMP hardening, robustness or resistance to jamming, reconstitution of the network, and constellation designs which enhance survivability. Finally, conclusions are drawn and recommendations proposed based upon the discussion.

## ACKNOWLEDGMENTS

I would like to take this opportunity to thank the many people who have offered their support and encouragement throughout this endeavor. A special acknowledgement goes to Dr. Hussain Haddad, my committee chairman, for his inspiration, sincere guidance, and unfailing patience. Additionally, I would like to thank Dr. Robert Mercer and Dr. Russell Shain for graciously agreeing to serve on my thesis committee and for their valuable assistance and comments.

To my wife, Kimberly, thanks for patiently providing me the time and space to concentrate on this project. Your constant love and support made it that much easier. To my parents, who have stood by me through all of my academic pursuits, words cannot adequately express my sincere appreciation for your support and faith in my abilities. Thank you.

## CONTENTS

### CHAPTER

I. INTRODUCTION . . . . .	1
Notes . . . . .	9
II. UNIQUENESS OF MILITARY SATELLITE SYSTEMS AS OPPOSED TO THEIR CIVILIAN COUNTERPARTS . . . . .	10
Difference in Implementation . . . . .	11
Cost Factors . . . . .	16
Requirement for Survivability . . . . .	19
Notes . . . . .	22
III. ASSESSMENT OF THREATS TO MILITARY COMMUNICATIONS SATELLITES . . . . .	24
Nuclear Effects . . . . .	27
Blast . . . . .	28
Absorption and Scintillation . . . . .	29
Atmospheric Ionization . . . . .	31
Electromagnetic Pulse . . . . .	33
Radiation . . . . .	35
Anti-Satellite Weapons . . . . .	38
Nuclear . . . . .	39
Kinetic . . . . .	40
Directed Energy . . . . .	43
Direct Electronic Measures . . . . .	46
Jamming . . . . .	47
Spoofing . . . . .	48
Notes . . . . .	50

IV. TECHNOLOGICAL MEANS AND METHODS FOR MITIGATING, ELIMINATING, AND DEFEATING THE THREATS . . . . .	55
Individual Survivability Enhancements . . . . .	58
Nuclear Hardening . . . . .	58
Protection Against ASATs . . . . .	62
Electronic Counter Counter-Measures . . . . .	66
Proliferation and Multiple Satellite Systems . . . . .	79
Notes . . . . .	85
V. CONCLUSIONS . . . . .	89
BIBLIOGRAPHY . . . . .	93
APPENDIX . . . . .	97
Notes - Appendix . . . . .	101

## TABLES

## Table

1	Uplink Budgets for Three MILSATCOM Systems . . . . .	69
2	Downlink Budgets for Three MILSATCOM Systems . . . . .	70
3	Summary Table of Survivability Measures . . . . .	90-91
4	NAVSTAR Survivability Features . . . . .	99



## FIGURES

## Figure

- 1 Illustration of Antenna Null Realization . . . . .73
- 2 Jamming Protection Through Spread Spectrum . . . . .75
- 3 Multiple Satellite Network with Two Central Stations  
with On-Board Processing M User Satellites and L  
Small Ground Terminals . . . . .83

## ABBREVIATIONS & ACRONYMS

ABM	Anti-Ballistic Missile System
AFB	Air Force Base
AFIT	Air Force Institute of Technology
AFSATCOM	Air Force Satellite Communications Program
AJ	Anti-jamming Technique
ASAT	Anti-satellite weapon
BMD	Ballistic Missile Defense
C <sup>2</sup>	Command and Control
C <sup>3</sup>	Command, Control, and Communications
C <sup>3</sup> I	Command, Control, Communications, and Intelligence
CDMA	Code Division Multiple Access
CSS	Commercial Satellite Survivability (Task Force)
DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DCEC	Defense Communications Engineering Center
DCS	Defense Communications System
DEW	Directed Energy Weapon
DSCS	Defense Satellite Communications System Program
DNA	Defense Nuclear Agency
DoD	Department of Defense
EAM	Emergency Action Message
ECM	Electronic Counter Measure
EHF	Extremely High Frequency (30 GHz to 300 GHz)
EIRP	Effective isotropically radiated power
EMP	Electromagnetic Pulse
FDMA	Frequency Division Multiple Access
FLTSATCOM	Fleet Satellite Communications Program
FSK	Frequency Shift Keying
GEO	Geosynchronous Earth Orbit Satellite
GMF	Ground Mobile Forces
GPS	Global Positioning System; NAVSTAR
HEL	High Energy Laser
HEMP	High Altitude Electromagnetic Pulse
HOE	Homing Overlay Experiment
ICBM	Intercontinental Ballistic Missile
ICSS	Interoperable Commercial Satellite System
IEEE	Institute of Electrical and Electronics Engineers
IRBM	Intermediate Range Ballistic Missile
Kv/m	Kilovolts per meter
LEO	Low Earth Orbit Satellite
LPE	Low Probability of Exploitation
LPI	Low Probability of Intercept
MILSATCOM	Military Satellite Communications
MILSTAR	Military Strategic and Tactical Relay System; Also Milstar
MSS	Multiple Satellite System

nS	Nanosecond
NSTAC	National Security Telecommunications Advisory Committee
NTISSC	National Telecommunications and Information Systems Security Committee
NAVSTAR	Also known as the Global Positioning System (GPS)
PSK	Phase Shift Keying
R & D	Research and Development
Satcom	Satellite Communications; Also satcom
SDS	Satellite Data System
SGEMP	System-generated electromagnetic pulse
SHF	Super High Frequency (3 GHz to 30 GHz)
SLBM	Submarine Launched Ballistic Missile
SNR	Signal to Noise Ratio
TDMA	Time Division Multiple Access
TREE	Transit Radiation Effects on Electronics
TT&C	Telemetry, Tracking, and Command
UHF	Ultra High Frequency (300 MHz to 3 GHz)
USA	United States Army
USAF	United States Air Force
USN	United States Navy

## CHAPTER I

### INTRODUCTION

Nonetheless, despite the many vulnerabilities of military space systems, the substantially, though not exclusively, technical issue of space system survivability has yet to be debated in an adequately comprehensive manner.<sup>1</sup>

Colin S. Gray  
President  
National Institute  
for Public Policy

Our society has become more and more reliant upon technology and, in particular, information systems. This reliance upon information systems carries over into the realm of defense. Today's military cannot function without the transmission and computer systems needed to carry command, control, and communications (C<sup>3</sup>) information to its forces.

The importance of C<sup>3</sup> is one of the key distinguishing features of military communications as compared with those in the civilian sector. A baseline description of the function of C<sup>3</sup> is provided by Dr. Frankel:

A C<sup>3</sup> system is a collection of items that together constitute an entity whose function it is to: (1) provide to a decision maker, in a timely, all necessary information bearing on an issue requiring a decision; and (2) provide the support to disseminate the decision maker's decisions to the forces he or she controls. The various items that the entity comprises include, but are not limited to, people, processing resources, communication resources, and sensor resources. This entity is viewed as a system if, and only if, all items perform their respective functions synergistically to achieve the common goal of permitting effective decision-making.<sup>2</sup>

The information carried over the military's telecommunications systems could, foreseeably, change the events of future conflicts or national

emergencies. Their value could be said to be higher than any weapon in our arsenal for, without these systems, no weapon can be executed. Perhaps more importantly, these same communications systems play a major role in dissolving conflict, in quieting the distrust of a potential adversary, and in clearing the cloud of war.

Part of ensuring this nation's defense includes protecting these vital lines of communications. Unfortunately, an enemy fully recognizes their value and, in almost all scenarios, chooses to assign high target values to these precious assets. Especially lucrative are the critical nodes of our C<sup>3</sup> systems which, if destroyed or otherwise rendered ineffective, can essentially shut down a system or at least damage crucial circuits. A critical C<sup>3</sup> node might be a common point or confluence for circuits which would carry strategic or crucial defense-related information. These vital nodes could easily be our Achilles' heel in times of national emergency or war.

Arguably the most critical nodes of our defense C<sup>3</sup> systems are our military's communications satellites. As satellite systems have been brought on-line, the uniformed services have integrated their usage into every phase of operation. Today, they are used to transmit every type of traffic from routine logistical reports to emergency action messages which could be used as the "go to war" messages in the event of nuclear conflict.<sup>3</sup> From their book, Space Weapons, Bulkeley and Spinardi state that "more than half of all long-range US military communications are now routed via satellites," and they also go on to explain that estimates vary upwards to 80 percent.<sup>4</sup> Another source strengthens those upper estimates by stating "that between 70 and 80 percent of all U.S. long-haul military C<sup>3</sup> is transmitted via satellite relays."<sup>5</sup> Choosing

either figure, the military's imbedded dependence upon these assets is undeniable.

This increasing dependence upon satellite communications by the military can be explained many ways. First, they afford the means to communicate with deploying/deployed forces where no communications infrastructure previously existed. Such a capability is afforded by the wide coverage area offered by high altitude communications satellites, most of which reside in geosynchronous orbit. This sweeping connectivity extends to our naval task forces, strategic aircraft, and ground forces. As Colin S. Gray explains:

In part, this growing dependence reflects increasing technical virtuosity and convenience, but it also reflects American strategic geography. Unlike the Soviet Union, the U.S., because of its geopolitical condition as an insular power, deploys its forces worldwide. It is both technically efficient and politically non-troublesome to use satellite relays to the degree feasible.<sup>6</sup>

Thus, we rely heavily on satellite links to extend command and control to our dispersed forces throughout the globe.

Second, while they provide reliable, cost-effective telecommunications to military installations and assets around the globe, they are also inherently less affected by propagation and range problems experienced by other types of long-haul communications such as HF or VHF/UHF, respectively.

Third, the changing nature of the military will continue to promote increased use of military communications satellites. Specifically, the military's need to move more and more data, be it in the form of reconnaissance, intelligence, logistical information, or command and control data, will continue to drive this insatiable demand. Satellite

communications offers a much improved throughput over other aging terrestrial systems. Tozer describes this trend:

The demands for military usage of Satcoms are continually increasing. This is due partly to increased requirements for communication (especially from small terminals) in the face of enemy threats, and partly to enhanced end-user complexity (e.g. computers and sensors exchanging quantities of digital information).<sup>7</sup>

As society suffers through the growing pains brought on by the increased demands of the information explosion, so does the military. Satellite communications offer some relief in the form of a reliable, wide pipe (meaning wide bandwidth which equates to greater information carrying capacity) for telecommunications transfer.

Recognizing the importance of these satellites, and our increasing dependence upon them, for both national defense and our military capability, it is imperative that we build future systems so that they are survivable through all levels of conflict. That is, we must make a commitment to design these system from conception with survivability as one of the key features. Recognizing their extreme importance and the emerging threats against them, the 1982 National Space Policy dictates that we now incorporate survivability and endurance into our space systems. A portion of the policy demands:

Survivability and endurance of space systems, including all system elements, will be pursued commensurate with the planned use in crisis and conflict, with the threat, and with the availability of other assets to perform the mission. Deficiencies will be identified and eliminated, and an aggressive, long-term program will be undertaken to provide more-assured survivability and endurance.<sup>8</sup>

This policy was preceded by a 1979 presidential directive which also spelled out the need for survivable defense communications. Extracts from this directive, as recorded in a Defense Communications

Engineering Center (DCEC) paper, describe the pervasive and multifaceted nature of defense communications:

'It is essential to the security of the United States to have telecommunications facilities adequate to satisfy the needs of the nation during and after any national emergency. This is required in order to gather intelligence, conduct diplomacy, command and control military forces, provide continuity of essential functions of government, and to reconstitute the political, economic, and social structure of the nation. Moreover, a survivable communications system is a necessary component of our deterrent posture for defense.' Among many other things, the directive requires, 'Connectivity between the National Command Authority and strategic and other appropriate forces to support flexible execution of retaliatory strikes during and after an enemy nuclear attack.'<sup>9</sup>

These directives and policy statements illustrate that the idea of enhancing the survivability of our military space systems, and particularly our communications satellites, is not new or novel. Among other documents, they serve as a mandate to incorporate adequate survivability features into our military communications satellites.

A respected panel of authors from the Aspen Strategy Group, including William J. Perry, Brent Scowcroft, Joseph S. Nye, Jr., and James A. Shear, state that the number one priority for a comprehensive U.S. military space policy should be to expand satellite survivability measures. They warn that while many verbally support the push for survivability measures, adequate funding remains a serious problem. Their pessimism with the country's resolve is evident:

Complacency is easy in the face of threats that have yet to fully materialize, much less tested in conflict situations. There is also the temptation to view negotiated restraints as a substitute for our own protective measures. This misses the point that once arms control restraints are adopted, protective measures become more important (though possibly less costly) as an inducement to Soviet compliance and a hedge against breakout. Our survivability programs must aim not only to defeat the option of easy (inexpensive) attacks, but to ensure that our satellites are capable of surviving all but the most massive, visible threats in performing their missions.<sup>10</sup>



Still, while it may seem "common sense" that given our dependence upon these critical assets, we naturally would have always planned for these systems' survivability. This has not always been the case. For various reasons, including cost, ignorance (real or otherwise) of ever-emerging technical threats, and the re-directing of funds designated for the enhancement of survivability, we have not adequately incorporated survivability features into our military satellite communications systems. In a speech to the National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, Dr. Robert S. Cooper, then Asst. Secretary of Defense (Research and Technology) and Director, Defense Advanced Research Projects Agency (DARPA) admitted, "Another interesting fact: until the decision to build the MILSTAR satellite system, little or no attention has been paid to the idea of trying to make survivable space communication systems."<sup>11</sup> While advances have been made, there are still many technological ways that we can improve the survivability of our military communications satellites.

Before survivable satellites can be developed, an accurate assessment of real and probable threats must be conducted. Reconnaissance, espionage, and other intelligence gathering techniques provide us with information for assessing how an enemy might choose to attack our space assets. This process requires some further accurate forecasting and projections as to what capabilities an enemy might actually possess or develop during the lifetime of a particular space system. By looking at what type of offensive weapons our own country is trying to develop, we can hypothesize where our enemies might be directing their efforts and how we might protect

against similar weapon systems. Also, if we are researching a particular type of technology, can we be sure that our R & D is not being "stolen" or "sold" to the other side?

Regardless, it is incumbent upon the military and defense contractors to develop and design survivable military satellite communications systems (MILSATCOMs). While survivability is the goal, degrees of survivability are difficult to measure or guarantee. The targetability of a system, in this case a communications satellite, has direct bearing upon that systems' survivability. Day and Lockhart describe the relationship between survivability and targetability:

Survivability is the ability of a system or system component to survive a particular threat or damage scenario. To assess survivability, the threat needs to be carefully defined, and modeling or testing (with appropriate extrapolation to the real threat) needs to be done. Targetability relates to the ease of destroying a system when directly attacked. Under a particular damage scenario, certain elements of a system may survive because they are not directly targeted, although they would be destroyed.<sup>12</sup>

From accurate threat assessments we can incorporate technological advancements into these satellites' design and development to afford them the most survivability for the money, or that is theoretically possible. This process is tempered with the realization that should an enemy want to eliminate a system, and is willing to expend the appropriate resources, he can most certainly neutralize it. Ultimate invulnerability is impossible. Nonetheless, our goal should be to incorporate the most survivability for a set cost.

Following this methodology, this thesis will demonstrate the uniqueness of military communications satellites as compared with their civilian counterparts. Such a comparison serves to justify the incorporation of the recommended survivability enhancements for

military communications satellites. This comparison will focus on three major design differences between the two types of systems: differences in implementation and use, cost factors, and the requirement for survivability. The end results of these three design factors are often indistinguishable; they are treated as affecting the whole system. Each directly impacts the other and they can be considered part and parcel of the other.

Next, threats to military communications satellites are examined. These range from consequences of a nuclear threat environment to anti-satellite weapons (ASATs) to intentional jamming. Both existing and emerging threats are addressed.

The major thrust of the thesis rests with proposed methods for countering these threats. These methods include nuclear hardening techniques, spread spectrum and multiple access techniques, protection measures against ASATs, resistance to intentional jamming, and possible proliferated deployment strategies.

Following the analysis of possible survivability enhancements, conclusions are drawn based upon the entire discussion.

## NOTES - CHAPTER 1

<sup>1</sup>Colin S. Gray, American Military Space Policy: Information Systems, Weapon Systems and Arms Control (Cambridge, MA: Abt Books, 1982), p. 51.

<sup>2</sup>Dr. Michael S. Frankel, "Survivable Command, Control, and Communication," in Conference Record from IEEE Military Communications Conference (Washington, D.C.: Oct 19-22, 1987), pp. 30.1.1.

<sup>3</sup>Gray, p. 30.

<sup>4</sup>Rip Bulkeley and Graham Spinardi, Space Weapons: Deterrence or Delusion? (Totowa, NJ: Barnes & Noble Books, 1986), pp. 45 and 329.

<sup>5</sup>Gray, pp. 28-29.

<sup>6</sup>Gray, pp. 29.

<sup>7</sup>T. C. Tozer, "An Introduction to Military Satellite Communications," Memorandum No. 3976 of the Royal Signal & Radar Establishment (Malvern, England: Apr 1987), pp. 2.

<sup>8</sup>Gray, pp. 111-112.

<sup>9</sup>Harris A. Stover, "Engineering Aids for the Design of Survivable Defense Communications Transmission Capability," Technical Note No. 11-82 (Defense Communications Agency, Jan 1984), pp. 6.

<sup>10</sup>William J. Perry, Brent Scowcroft, Joseph S. Nye, Jr., and James A. Shear, "Anti-Satellite Weapons and U.S. Military Space Policy: An Introduction" in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime (Lanham, MD: The Aspen Institute for Humanistic Studies and the University Press of America, 1987), p. 24.

<sup>11</sup>Dr. Robert S. Cooper, "Space Challenges," from National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the MITRE Corporation, Oct 25-26, 1984 (Boston: MITRE Document M85-3, 1984), pp. 65.

<sup>12</sup>M. H. Day and C. M. Lockhart, "Survivable Network Planning at AT&T Bell Laboratories," in Conference Record from IEEE Military Communications Conference (Monterey, CA: Oct 5-9, 1986), pp. 24.1.4.

## CHAPTER II

### UNIQUENESS OF DEFENSE SATELLITE SYSTEMS AS OPPOSED TO THEIR CIVILIAN COUNTERPARTS

To support the justification for enhanced survivability measures for future MILSATCOMs, a comparison should first be conducted between military systems with their civilian counterparts. Certain fundamental differences in the design concepts exist between the two systems. Three major themes polarize their development efforts and it is through their analysis that we see differentiation between the systems. First, their *raison d'être* are different. One exists for revenue production; the other for defense. Second, the basic economics of these systems place different values upon certain key factors such as efficiency and amortization of costs. These economic factors directly impact cost outlays for satellite features. Third, the overriding need for incorporation of survivability enhancements changes the complexion of military systems as compared with civilian ones.

These factors do not fall neatly into three separate categories. While an effort is made to keep each separated from its associated effect upon satellite design, this task is nearly impossible since they are not entirely distinct, and each affects the others. They are so similarly related that their effects intertwine with each other. Oftentimes, the quest to incorporate a certain set of design features (A) to achieve one

result (X) will dovetail with an entirely different set of features (B) to achieve similar design results (X').

### Difference in Implementation

From conception, civilian and military communications satellite systems are designed to meet varied specification requirements. These requirements are drafted by the sponsoring agencies who wish to implement a satellite communications system, e.g. the US Navy or Intelsat. Each agency incorporates features available through the existing technology which they feel will best fit their peculiar needs. As a result, we see that while each system performs the basic function of providing telecommunications services, they are each tailored to best fit their individual design requirements.

A civilian concern, in the telecommunications business, would typically seek to build a relatively inexpensive, large channel capacity, efficient, and long duration-in-orbit satellite. Generally, their primary motive for developing such a system is to lease the circuits or channels at a net profit. To minimize their costs, the satellite should be as lightweight as possible since a civilian concern would have to pay fees to have their satellite launched. The heavier the satellite the greater the cost to boost it into orbit. This is a prime concern since almost all commercial communications satellites need to be boosted to geosynchronous orbit (approx. 35,786 km).<sup>1</sup> Such an orbit offers the benefits of reduced costs for telemetry, tracking, and command (TT&C), wide earth area coverage, constant coverage of the same area, and satisfactory look angles from the United States. Launch costs and spacecraft costs are two of the major investments that must be

amortized over the life of the satellite system. Since civilian systems are generally launched to produce revenue through provision of services, the less money spent on the launch and spacecraft the quicker the concern generates profits. Also, such a satellite should carry enough flexible transponders to meet market demand. Too many idle channels mean a less than efficient satellite (although future expansion is of prime consideration).

Designs for military communications satellites are, or should be, less governed by economics and efficiency. While the entire system must be completed within a set of budgetary constraints, just like its civilian counterpart, its reason for being is not to turn a profit. Rather, its success is measured in its contribution to the overall defense. This term does not lend itself to easy measurement as does the profit margin for the civilian system. Questions come to mind as to how much "defense" is afforded by the introduction of another satellite communications system? Is it really needed, what are its contributions, and can it be budgeted for? Also, by virtue of the nature of its clientele, does it need to be as efficient as a civilian system? As a matter of fact, it might actually slow down its data rates (stressed mode) so that transmission will be less likely to be disturbed by a nuclear event (making the medium less efficient). The entire nation bears the costs for a defense system, at Congress' discretion, whereas a civilian system may be financially supported by only a few concerns. Lastly, since a military system is not trying to recoup its launch costs it may not have a requirement for a long-duration orbit.

Satellite communications offers many unique benefits to the military. It serves as a powerful medium to stretch their lines of

command to remote areas of the world. This is necessary since the United States normally projects military power to other areas of the globe, as opposed to fighting on its own soil. Fred Bond suggests that international crises and dangerous confrontations are on the rise and that rapid response by the U.S. and other involved nations is required to contain escalation. "Often heavy communication capacity is suddenly required where little exists. The consequence is communication traffic overload, which can lead to dangerous confusion." He further adds that a deploying force must be prepared to maintain a total self-contained communication capability.<sup>2</sup> Satellite communications proves nearly ideal for such a scenario.

Tozer describes MILSATCOMs' attractiveness to the military using similar arguments. He claims they are popular because of "their wide coverage area, which permits operations at short notice in virtually any part of the world, without reliance on a national communications infrastructure."<sup>3</sup> In comparison with HF and VHF/UHF, which suffer from unpredictable propagation and limited range respectively, satellite communications provide a 'high availability' medium. Also, the bandwidth and capacity offered are considerable (typically 100's of MHz @ SHF). When compared with other military communications systems he concludes, "[f]or many tactical scenarios however, Satcoms may represent the only viable means of communication."<sup>4</sup>

While not all MILSATCOMs specifically serve rapid deployment, the essence of their being contrasts greatly with fixed, in-place commercial services where links are established and maintained for long durations, i.e. years. Civilian companies can employ huge and sophisticated ground stations with large aperture antennas. The latter affords high



gain for reception and reduces costs of signal conditioning equipment. CONUS military ground stations may be able to take advantage of these same economies of scale. It is in considering the intended recipient of command and control information that we see the true military terminals. They may be on surface fleet vessels, aircraft, or in shelterized containers. In almost all of these cases, the terminals are constrained by size limitations. Also, ease of use and the ability to rapidly erect antennas are prime considerations for these systems.

At present, no other media matches the capability of satellite communications to provide quick, highly reliable, high capacity communications from a deployed location. Their popularity is obvious from the proliferation of ground mobile forces (GMF), airborne, and shipboard terminals. Such "[e]ffective communications that can survive in a wartime environment are necessary to keep military commanders informed, to direct the use of our complex weapons against the enemy, and to control the trend toward chaos that so often accompanies warfare."<sup>5</sup> Protection of these security enhancing assets should be a high priority in peacetime and, especially, in wartime. Likewise, our military communications satellites should be made survivable against an enemy's efforts to neutralize them during conflict.

Arising from this difference in perception for the need for survivability enhancements, we see many contrasting design requirements. One example, and a key difference, is the fact that civilian systems do not, as a rule, plan for and employ encrypted or protected links. Within their own realm they perceive few or no enemies who would go to the drastic extremes of seeking to disrupt or intercept their communications. For many, this type of tactic seems outside the

realm of "fair" competition. Their decision to leave their links unencrypted applies equally to their information bearing as well as their TT&C links.

On the contrary, military systems bulk encrypt their information and TT&C links. The perceived threat to these links is much greater and the threatening parties can bring more resources to bear towards these efforts. Recent times, though, have brought a change of perspective to the civilian telecommunications community. The National Security Telecommunications Advisory Committee, instituted by government to draw upon industry advice and expertise to enhance the survivability of commercial communications systems, has demanded that satellite systems protect their command/control uplink.<sup>6</sup> This initiative was espoused by the Commercial Satellite Survivability (CSS) Task Force in their 1983 report:

'Commercial satellite communications systems are vulnerable to hostile actions which could deny service in emergency situations, particularly actions by a relatively unsophisticated antagonist... For example, today's satellite command links provide only modest protection against electronic intrusion.'<sup>7</sup>

To further enforce this proposal, the National Telecommunications and Information Systems Security Committee (NTISSC) has recently promulgated a policy that "declares that future government use of commercial satellites shall be limited to those using 'accepted techniques necessary to protect the command/control uplink.'"<sup>8</sup>

Indeed, the government, including the military, has a vested interest in the protection of civilian satellite communications systems. Many of the military's circuits run over channels leased from civilian concerns. There are also plans for the government to seize and use civilian circuits in time of national emergency.

### Cost Factors

Cost considerations and economic prioritization in developing these two types of systems are quite different. Reduction of costs and keeping costs to a minimum ranks among the top priorities for civilian systems. Military systems, on the other hand, rank other features such as mobility and survivability much higher. Therefore, military planners justify the increased expenditure of funds as necessary to meet these added requirements. Unfortunately, incorporating survivability features into a system can be a very expensive proposition. One report describes these diverging priorities:

In general these attributes require designs that are diametrically opposed. Low cost implies highly efficient use of the resources that comprise the system. Survivability, on the other hand, implies capacity and resources that may never be utilized (unless the system must actually operate against the threat).<sup>9</sup>

Civilian systems, whose major function is to produce revenue, seldom choose to incorporate these costly features, except as noted above with the requirement to protect their command/control uplink.

Foreseeable problems develop when military systems are designed with the same methodology and priority structure that civilian systems employ. An efficient, cost-saving system might work well during unstressed, peacetime operations. And, since we spend the vast majority of our time in peacetime, it is tempting to follow such a strategy for budgetary reasons. But, it would be during war-type conditions that vulnerabilities may surface. Stover describes the dangers of following the easy path:

However, because we spend most of our lives in peacetime, performing peacetime activities, many of us have a natural tendency to think too little about wartime situations. We have a

very strong tendency to follow the example of civilian communications companies and emphasize those peacetime operations of the DCS [Defense Communications System] that will permit amortization of equipment costs. Although this might be very costly when war occurs, restrictive budgets encourage us to follow that natural tendency. We compensate for this tendency primarily by adding supplemental wartime equipment, much of which is not regularly exercised during peacetime, by making minor modifications to the peacetime equipment and facilities, or by making changes in operating procedures. These are rather weak approaches for providing wartime communications capability. In the design of the DCS we must be primarily and fundamentally concerned with its wartime capability. We must be more interested in the connectivity of a damaged network than in the efficiency of an undamaged one. Here "efficiency" refers to things that enhance profits in a commercial network; they often detract from communications survivability.<sup>10</sup>

Along with condemning this type of planning for a military system, Stover also suggests that survivability enhancements should be part of the design of a system from the very beginning. Band-aid measures, often accomplished to appease the requirements of a new policy, seldom work as effectively as ingrained technologies. Many times it is more expensive to alter an existing system than to have built it from the beginning with the features desired.

This leads to another major cost factor suffered by military systems that civilian ones seldom battle. The modification of existing systems can be prohibitively expensive for civilian concerns whereas military systems have little choice but to adapt to new, emerging threats. This presumes that the military always wants to preserve its telecommunications capabilities for the eventuality of conflict. To preclude the high costs of modification, a prudent investment would be the incorporation of many diverse survivability enhancements in the original plans for a satellite communications system. As Stover notes:

Needed survivability cannot be achieved both economically and effectively by frequently mending vulnerabilities of an existing system as they occur. (This is partly because retrofit of an existing system is very expensive and because it is not always

effective. Although there are situations where retrofit is an optimum cost solution, those usually occur when we do not apply enough foresight to avoid them.). . . . An enemy can devise new methods of attack much more rapidly. We can never catch up using this approach. We need to use foresight and design rather than afterthought and modification. To achieve maximum survivability per unit of cost, survivability must be constantly planned into the system from the beginning to end.<sup>11</sup>

This is one way to make our military systems more economically efficient and cost effective. In this respect, both communities strive for the same objectives.

Budgeting for survivability enhancements and actually incorporating them are often two different things. In the past, Dr. Charles Cook, then Deputy Assistant Secretary of the Air Force for Space Plans and Policy, claims that our military planners have robbed from the survivability coffers:

We are now making a concerted effort to make our space systems more robust and survivable. While space system survivability has been talked about for many years, its planned funding often served as a first source of money to cover other needs, such as the costs of correcting performance shortfalls or offsetting program overruns. Today that is changing. Our commanders-in-chiefs are beginning to realize their dependence on space systems. Consequently, aggressive action is now under way to enhance the survivability of critical satellites.<sup>12</sup>

The MILSTAR system is a case in point. An Oct 1989 article in Aviation Week and Space Technology states that the House Appropriations Committee has called for the cancellation of this program after the launch of the first three satellites in Fiscal Year 1990. It goes on to state that the House of Representatives doubts the commitment of the armed services to the program and accuses the Air Force of "shifting Milstar satellite funds to other purposes."<sup>13</sup>

If the armed services do not carry the torch of commitment to increased survivability of our military communications satellites, then who will? Is survivability of these assets crucial to our defense?

### Requirement for Survivability

Most indicators point to the fact that these systems are indeed crucial to the military and that they should be protected. When compared with the civilian environment, it is the unique mission of the military and the existence of potential foes which makes survivability so essential. As these systems become more capable and vital to the conduct of military operations, their unimpeded use in future conflicts could prove decisive. "To ensure that these systems will be available when the DoD requires, the United States Space Policy calls for the increased survivability of all elements of space systems."<sup>14</sup> Again, another mandate exists requiring us to strengthen our military satellites' survivability capabilities.

At this point a definition of survivability is offered in the context of this discussion of satellite communications systems:

"Survivability" measures the resistance of a system to sustaining damage from enemy attack, along with its ability to perform in a partially damaged state and its ability to restore some of its destroyed capabilities. . . . Survivability goes hand in hand with "Responsiveness" which measures the ease with which a system can adapt to changing conditions, for example, its ability to extend its boundaries, reconfigure its connectivity, accommodate traffic peaks, and interoperate with other systems. . . .<sup>15</sup>

This list only partially describes the numerous technological means by which a satellite system might enhance its survivability and responsiveness. Still, a jagged line is drawn between the civilian and military communities over the requirement for survivability.

This key differentiating factor permeates through MILSATCOM design. Tozer states that "Milsatcoms are distinguished from civil systems by the requirement to provide survivability under threat...."<sup>16</sup>

They incorporate features "to provide protected communications under jamming threat, such as special antennas and spread spectrum processors. Additionally, they may be hardened against nuclear effects, and employ secure encrypt/decrypt coding for TT&C."<sup>17</sup> As mentioned above, for the most part, civilian concerns choose not to employ these strategies because the perceived threat is acceptably low and the cost of incorporation prohibitively high.

MILSATCOM systems, as alluded to above, were deployed in the past with economics as the major consideration. This caused certain features to be slighted. For example, "survivability and freedom of action throughout the conflict spectrum were given much less attention."<sup>18</sup> This also resulted in the deployment strategy that we see today where the U.S. relies on a few, large, sophisticated, geostationary communication satellites. Many suggest that a weakness exists. "If, during a conflict, an enemy denied the U.S. use of these critical communication links (by electronic warfare or anti-satellite weapons), U.S. military command and control would be severely degraded."<sup>19</sup>

This requirement for survivability in MILSATCOM systems must be planned from the ground up with primary consideration toward their operation during conflict. Stover characterizes this process:

A major difference between wartime and peacetime communications systems is the wartime need for survival of enough communications to make the most effective use of our defense forces and weaponry, even in the face of a concerted enemy effort to destroy both the weapons and the communications. Needed survivability cannot be achieved both economically and effectively by frequently mending vulnerabilities of an existing system in response to new enemy threats as they occur. Neither can we afford to replace an existing system with a new survivable system. Instead, to be both successful and affordable, survivability must be achieved through an evolutionary process.<sup>20</sup>

One of the first steps in this process is to accurately assess the existing and potential threats against military communications satellites. An analysis must be made as to what techniques and technologies a prospective enemy might be able to employ against our communications satellite assets.



## NOTES - CHAPTER II

<sup>1</sup>Dennis Roddy, Satellite Communications, (Englewood Cliffs, NJ: Prentice Hall, 1989), p. 47.

<sup>2</sup>Fred E. Bond, "Long Range MILSATCOM Architecture", in Conference Record from IEEE Military Communications Conference, Oct 17-20, 1982, Boston, p. 11.1.2.

<sup>3</sup>T. C. Tozer, "An Introduction to Military Satellite Communications," Memorandum No. 3976 of the Royal Signal & Radar Establishment, Malvern, England, Apr 1987, p. 2.

<sup>4</sup>Tozer, p. 2.

<sup>5</sup>Harris A. Stover, "Engineering Aids for the Design of Survivable Defense Communications Transmission Capability," Technical Note 11-82, Defense Communications Agency, Jan 1984, p. iii.

<sup>6</sup>Otto W. Hoernig, Jr. and Dr. Des R. Sood, "Command System Protection for Commercial Communication Satellites," in Conference Record from IEEE Military Communications Conference, Oct 5-9, 1986, Monterey, CA, p. 3.5.1.

<sup>7</sup>Hoernig and Sood, p. 3.5.1.

<sup>8</sup>Hoernig and Sood, p. 3.5.1.

<sup>9</sup>R. W. Boyd, S. L. Adams, M. I. Spellman, and L. V. Lucas, "Survivable Space Networks: The Physical Layer," in Conference Record from IEEE Military Communications Conference, Oct 23-26, 1988, San Diego, p. 26.6.1.

<sup>10</sup>Stover, p.1.

<sup>11</sup>Stover, p. 2.

<sup>12</sup>Dr. Charles W. Cook, "The U.S. Air Force Space Program," a speech from the National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the MITRE Corporation, Oct 25-26, 1984, Boston, MITRE Document M85-3, 1984, p. 41.

<sup>13</sup>David Hughes, "Milstar Terminal Capability Demonstrated as Congress Debates Program Budget," Aviation Week & Space Technology, Oct 30, 1989, pp. 49-50.

<sup>14</sup>Barbara A. Phillips, "A Prototype Knowledge-Based System to Aid Space System Restoration Management," Thesis submitted to the Air Force Institute of Technology, Wright-Patterson AFB, OH, Dec 1986, p. 1.

<sup>15</sup>Ralph K. Townley, David W. Brown, Martin O. Bernet, and Bernard L. Pankowski, "Selected Issues in DCS Technical Integration," Technical paper prepared by Computer Sciences Corporation for the Defense Communications Agency, Aug 1987, pp. 8-1 through 8-3.

<sup>16</sup>Tozer, pp. 7.

<sup>17</sup>Tozer, pp. 4.

<sup>18</sup>William P. Murdock, Jr. "Alternative Force Structuring Strategies for Military Satellite Communication Systems," Thesis submitted to the Air Force Institute of Technology, Wright-Patterson AFB, OH, Dec 1987, p. 2.

<sup>19</sup>Murdock, p. 2.

<sup>20</sup>Stover, p. 12.

## CHAPTER III

### ASSESSMENT OF THREATS TO MILITARY COMMUNICATIONS SATELLITES

To design effective, protective measures for military communications satellites an assessment must first be made of existing and potential threats against those satellites. This process involves intelligence gathering and reconnaissance to determine what types of threats our potential adversaries might be developing. Also, it helps to look at our own technological endeavors and achievements to hypothesize what our enemies may be capable of in the future. In the same way that other technologies are advancing, so goes the effort to develop better, more threatening methods of eliminating or neutralizing an opponent's satellites. Considering the various types, communications satellites are especially lucrative targets since they serve as critical nodes in the military's command, control, and communications infrastructure. Their value continues to rise as the military grows increasingly dependent upon these satellites to carry the bulk of their long-haul traffic and to communicate with their deployed forces.

The spacecraft portion of a satellite communications system faces many different types and varying degrees of threats. Even though satellites are built to "withstand the rigors of launch and the barrenness of space", they are still relatively fragile objects constructed of lightweight materials and packed full of sensitive electronic

components.<sup>1</sup> As a class of targets, they may be considered relatively soft since disablement rather than total destruction may well be all that is required. By sufficiently damaging or disrupting the vital subsystems that keep them functioning, the spacecraft may be neutralized.<sup>2</sup> The various threats to these systems cover the continuum from partial link disruption to complete annihilation.

Not only are the threats varied, but they are also constantly evolving. This creates many problems and requires an element of forecasting or fortunetelling be included in the planning of survivability features. Once a space system is launched its basic survivability characteristics cannot be altered. An effort to include adaptive survivability measures would be the most attractive alternative, but equally difficult to develop. Dr. Charles W. Cook, then Deputy Assistant Secretary of the Air Force for Space Plans and Policy enunciates what may be the overriding criteria when he states, "This difficulty in implementing appropriate survivability is aggravated at times by the cost of survivability measures."<sup>3</sup>

Before launching into an examination of specific types of threats, a statement should be made as to what is meant by threat effectiveness. When discussing whether a weapon is effective, we must examine two separate facets of this idea. First, can the weapon eliminate, destroy, or neutralize its target. Second, has the mere existence of this weapon caused "virtual attrition". This means that the opposing side has been forced to forfeit part of the target vehicle's payload in order to incorporate protective measures against this weapon. For example, suppose the existence of a High Energy Laser (HEL) caused the target vehicle to incorporate ablative shielding. This ablative shielding takes

away from the true productive payload. As it turns out, the U.S. is far more affected by "virtual attrition" since we do not possess as many large throwweight boosters as the USSR.<sup>4</sup>

Following this line of discussion, another key point affecting threat analysis needs to be made. From the beginnings of the space age the U.S. and USSR have subscribed to two different philosophies of satellite deployment. The United States chose a strategy of using relatively few, very technically capable, long lifetime satellites. These satellites were often designed to accomplish multiple missions. The USSR, on the other hand, followed an employment strategy which called for numerous, less technically complex, shorter lifetime, single mission satellites.<sup>5</sup> "To support its space force structure, the Soviet Union launches about 100 satellites each year (1980 to 1985). During the same period the U.S. launched about 25 satellites per year."<sup>6</sup> Their greater launch capacity and larger satellite fleet afford the Soviets a very flexible response capability during higher levels of conflict. Effectively, they would be able to absorb losses against individual satellites better than the U.S. In comparison, the current U.S. strategy would seemingly become less responsive during increased tensions. We would place more value upon and be more dependent upon each and every satellite. "This strategy has caused the U.S. to depend on limited launch resources and a few, high value satellites."<sup>7</sup>

One might conclude from this analysis that the USSR could more readily risk a battle of attrition of space assets due to their increased number of spacecraft and greater launch capacity. This lends credence to the argument for better protection for our own satellites, as well as the development of our own quick launch capability. This paper chooses to

examine the former by first analyzing the threats against our military communications satellites.

Threats to military communications satellites generally fall into three main categories. The first area to be examined is that of nuclear effects upon communications satellites and the atmosphere. This area encompasses such effects as direct blast, absorption and scintillation, atmospheric ionization, electromagnetic pulse (EMP), and radiation. The second area discusses various types of anti-satellite (ASAT) weapons. These fall into three major categories: nuclear, kinetic, and directed energy. The last area explores direct electronic measures. Included are intentional disruptive techniques such as jamming and spoofing.

#### Nuclear Effects

This category of threats covers the wide range of effects caused by the detonation of nuclear weapons. The concentration here is on the non-deliberate effects caused by the weapons, not the weapons as ballistic missiles, themselves. As we have known for some time, the destructiveness of nuclear weapons to communications capability comes not just from the blast effects experienced by specific pieces of equipment, but also from the collateral effects such as scintillation and absorption, atmospheric ionization, electromagnetic pulse (EMP), and radiation.

Nuclear effects are nondiscriminatory and difficult to contain. Once a combatant chooses to explode a nuclear weapon for the purposes of disrupting the communications spectrum, then that same combatant must face the consequences of his own actions. While the greatest

concentration of effect might be against his target, the chances of his own communications capability being affected are high. Therefore, most would agree that the likelihood of using nuclear weapons effects as a means to disrupt satellite communications, short of the threshold of outright nuclear conflict, is low. Still, we must examine the threat and protect against it since military communications satellites may be called upon to operate in a nuclear-affected environment.

The effects of a nuclear blast on a communications satellite are a function of the blasts' yield, altitude, distance from the communication path and the time after the detonation.<sup>8</sup> Blasts may be classified as surface, air, or high altitude bursts (20 km or more above sea level), with the latter being the most devastating to the spacecraft segment of a system.<sup>9</sup> The geometry between the detonation site and the communication path also affects the degree of disturbance. In addition, the degree of signal attenuation "is not only affected by the distance from the blast site but also by the number of times that the propagation path intersects the disturbed regions of the ionosphere."<sup>10</sup>

Looking at the major effects of a nuclear explosion, it is difficult to determine where one starts and the other ends. Overlap does exist but an effort is made here to separate and discuss the various effects attributed to a nuclear detonation.

### Blast

Although it may be difficult to discern with which particular nuclear effect an adversary might be attacking a target, it is doubtful that he would intend blast as the primary method against a satellite. Generally, blast effects are directed at hard targets such as missile silos,

underground command centers, etc. Also, "satellites are typically thousands of kilometers apart, while the lethal range of even a one megaton explosion against a satellite hardened to a feasible level of hardness is under 100 km."<sup>11</sup> Satellites would more probably be targeted with the collateral effects of a nuclear detonation such as absorption and scintillation, atmospheric ionization, EMP, or radiation.

Blast destroys an object through the creation of over- pressure and shock and its force is directly related to the size of the weapon and the distance from detonation. It may range from a nominal per square inch (psi) measurement up to the point where significant structural damage would be done to the satellite.<sup>12</sup>

Should an adversary be willing to target a satellite(s) with the intention of destroying it with the blast from a warhead then little could be done to protect that satellite. A reasonable assessment would suggest that such a targeting strategy is unlikely. But, perhaps an adversary would want a particular satellite eliminated and was willing to commit a single warhead to that satellite. Then, in all likelihood, that satellite would be destroyed. The question here is whether it would be economically worth hardening each and every satellite, if it were technically feasible, so that it could withstand a small to medium size blast. The answer is probably not.

#### Absorption and Scintillation

There are many ways to deliberately disrupt or interfere with the communications links to and from a satellite. Perhaps a more efficient use of a nuclear warhead, as compared with direct blast damage, would be to attack satellite communications by exploding a nuclear device in



the upper atmosphere. In this way, one warhead's effects could spread over a very large area, disrupting all manner of communications. Such an explosion would cause the twin phenomena of signal absorption and scintillation.<sup>13</sup> As Stares describes:

Absorption could "black out" communication for up to an hour over a region a few hundred kilometers in diameter, while scintillation could cause severe disruption for much longer periods and over an even larger area.<sup>14</sup>

By spreading a few high altitude bursts over a continent, an enemy could disrupt the atmosphere to such a degree as to satisfactorily degrade satellite links.

"Absorption of electromagnetic energy is the primary cause for signal attenuation after a nuclear burst."<sup>15</sup> Essentially, the electron densities change within the atmosphere making it impenetrable or only partially penetrable by electromagnetic signals. Absorption is directly proportional to the electron density and inversely proportional to the square of the frequency, resulting in more significant signal attenuation for lower frequency communications.<sup>16</sup> Thus, we can conclude that the higher frequency ranges used in satellite communications (such as SHF and EHF) will be affected to a lesser degree and for a shorter time by absorption. The latter is true since the electron density has a natural tendency to return to normalcy after a nuclear event and will become transparent to the shorter wavelengths of SHF and EHF before the longer ones of UHF.

Signal scintillation is marked by both amplitude and phase variations in signal level due to propagation through the ionosphere. "These irregularities result from disturbances in the ion density that align themselves along the earth's magnetic lines of flux."<sup>17</sup> Natural

disturbances are roughly cylindrical in shape with diameters of 100 to 1000 feet and may affect an area of the ionosphere from 25 to 2000 miles in diameter.<sup>18</sup> Scintillation induced by nuclear weapons would be characteristically non-uniform. As one report describes:

Since the irregularities of electron density cannot be predicted, the effect of such irregularities on signal propagation can only be described by statistical parameters, such as rms amplitude and phase fluctuations and associated decorrelation times. The medium irregularities (often referred to as striations) that cause both amplitude and phase scintillations generally occur at heights from 200 to 600 km.<sup>19</sup>

While affecting the entire electromagnetic spectrum, scintillation would produce a dramatic enhancing and fading effect upon HF, VHF, and UHF transmissions. These effects may disrupt UHF communications for many hours, SHF for a few hours, and EHF momentarily.<sup>20</sup>

#### Atmospheric Ionization

Atmospheric ionization occurs as a result of the interaction of the atmosphere with the gamma rays, neutrons, or X-rays that are released at the onset of a nuclear detonation. Approximately 75% of the energy released by a nuclear detonation goes into ionizing the surrounding atmosphere.<sup>21</sup> Residual radiation that is released from beta particles, gamma rays, and positive ions from the weapon debris also contributes to atmospheric ionization. Even the ultraviolet component of thermal radiation increases the ionization surrounding the fireball.<sup>22</sup>

Atmospheric ionization primarily disturbs satellite communications by changing the propagation characteristics of the earth's ionosphere. Basically, this ionization changes the electron densities of the various layers of the atmosphere. As a paper for the Defense Nuclear Agency explains:

In general, the ionosphere can be considered to be a plasma that surrounds the earth and consists of randomly moving particles plus regular drifts of ionized formations. The electron density and time variation of the composite ionized medium determines its propagation properties. The maximum density is on the order of  $3 \times 10^6$  electrons per  $\text{cm}^3$  for the normal ionosphere and many orders of magnitude higher in the nuclear fireball.<sup>23</sup>

The plasma frequency can be used as a measure of the ability of a signal to propagate through the plasma. It is proportional to the square root of the electron density, which means that a signal propagates freely if it is higher than the plasma frequency. As a medium is disturbed and the plasma frequency rises, then a lower frequency signal will be either reflected or severely attenuated. This "attenuation or absorption of radio waves in a plasma is mainly due to losses caused by conversion of electron oscillation energy into heat on collision with other particles."<sup>24</sup> As an example, the plasma frequency is about 10 GHz for a density of  $10^{12}$  electrons per  $\text{cm}^3$ , which represents a relatively disturbed medium.<sup>25</sup>

Ionization creates the channel degradations which manifest themselves as dispersion effects, phase shifts (doppler), group time delay, beam spreading, and thermal noise. Dispersion effects seem to degrade wideband channels much more than narrowband ones.<sup>26</sup> Phase shifts bring changes in frequency due to the variation of phase path length. As communications signals are scattered they create multipath interference at the receiver. "This interference is accentuated by the fact that the received signal will undergo phase changes as it is being refracted."<sup>27</sup> These random changes in the received signal's phase induce added noise into the receiving equipment and,

consequently, reduce the signal to noise ratio. Also, these phase shifts affect wideband signals:

Not only is the signal to noise ratio reduced but for wide bandwidth communications systems the effective bandwidth could also be reduced. In a wide bandwidth system the phase of the various frequencies which make up the bandwidth may be randomly changed due to refraction and scattering. Since changes in the index of refraction ( $n$ ) over time will change the velocity at which the signal is propagated, a wideband signal passing through a region of fluctuating  $n$  will undergo a shift in frequency due to the Doppler effect; thereby causing interference with adjacent channels.<sup>28</sup>

The group time delay and its fluctuation disturb the signal in such a way as to make the use of high rate Time Division Multiple Access (TDMA) systems, with high data rates and pseudo-noise (PN) codes, difficult to implement. Beam spreading causes the antenna bandwidths to fatten as the angle-of-arrival of the wave is perturbed. A narrowbeam receiving antenna may suffer excessive losses as energy is diverted from the main beam. Finally, thermal noise from the hot fireball would be coupled into the receiver from the antenna raising the system noise temperature.<sup>29</sup>

#### Electromagnetic Pulse

Electromagnetic Pulse is one of the more familiar effects of a nuclear explosion. It is caused by the prompt release of high energy X-rays and gamma rays. Donadio explains this phenomenon:

When these high energy rays interact with the surrounding air molecules they produce radially moving electrons and positively charged ions through the Compton affect. These electrons are turned by the earth's magnetic field and create a transverse current density. This current produces a fast moving electromagnetic pulse which can attain a peak energy of about 50 Kv/m within 10 nS.<sup>30</sup>

This EMP can be coupled to the exposed antennas of a communications satellite. Once the antennas have collected the strong current then it may be transmitted to the receiving equipment via the various power and transmission lines. These transients may then cause disruption and/or destructive currents and voltages at the connection pins of the receiving equipment.<sup>31</sup>

Perhaps the most insidious aspect of EMP is how far reaching the effects may be felt. For example, communication equipment may be damaged or disrupted within a 2,000 mile radius depending upon the magnitude of the weapon and the height of burst. The entire United States would be blanketed with EMP if a nuclear weapon were detonated at an altitude of 500 km above the center of the country.<sup>32</sup> As it turns out, a high altitude burst is the most effective way to cover an area with EMP. In fact, the abbreviation HEMP is often used to designate a High Altitude Electromagnetic Pulse. As a further description:

A high altitude burst is the result of a weapon detonating 20 Km or more above sea level. When gamma rays which are emitted in a downward direction encounter regions of denser atmosphere (at about 20 Km) Compton electrons are produced. Detonation of a large yield nuclear weapon above 20 Km will produce the most severe EMP effects.<sup>33</sup>

Even though the primary EMP may be insignificant at great distances, a significant EMP effect can be induced in a satellite structure by the initial incident radiation pulse creating unwanted currents in the spacecraft.<sup>34</sup>

One thing that makes today's satellites more vulnerable is the susceptibility of solid state circuitry to HEMP damage. Though solid state electronics have brought the benefits of increased capability and

reduced size of communications systems, they are also 1,000 times more vulnerable than the old vacuum tube technology.<sup>35</sup>

### Radiation

Radiation is a more general term applied to all emissions and propagation of particles from a nuclear weapon. In this case, there is some overlap between what we mean by the original radiation and the subsequent effects associated with that radiation. As described earlier, since space is a vacuum, satellites would probably not be affected by the blast from an explosion but rather by the nuclear radiation. This radiation would travel many thousands of kilometers unimpeded by its medium, the atmosphere. "Depending on a satellite's proximity to the explosion, the radiation would damage it through thermomechanical shock, ionization burnout, or a system-generated electromagnetic pulse (SGEMP)."<sup>36</sup> This assumes, of course, that the satellite is unprotected from the radiation.

Thermomechanical shock occurs when the satellite becomes overheated after absorbing X-rays from the explosion. Generally, thermomechanical shock is preceded by ionization burnout in the same way that atmospheric signal absorption precedes scintillation effects. Ionization burnout occurs when X-rays penetrate the thin skin of a spacecraft and damage its electronic components. These two phenomena would be lethal to an unshielded satellite that was within a few hundred kilometers of a detonation. As addressed above, EMP becomes the real threat at distances greater than about 1,000 Km. SGEMP creates a positive photoelectric current after the bombarding X-rays have stripped electrons from the surface of the satellite. The resultant electrical

charge can ravage the satellites' internal components, causing malfunction and burnout of electronic parts.<sup>37</sup>

Prompt radiation consists of X-rays which account for 70% of the explosive energy and neutrons which account for 1%. A negligible portion (3/10%) of the prompt radiation are gamma rays.<sup>38</sup>

The follow-on effect to prompt radiation would be delayed radiation. "Delayed radiation is the result of energy being emitted in the form of beta and gamma radiation from the radioactive debris of the nuclear explosion."<sup>39</sup> This delayed radiation will cause a resulting increase in the ionization of the surrounding atmosphere. Like many of the other effects, its duration as well as the area affected are dependent upon the yield and burst altitude of the weapon.<sup>40</sup>

As stated earlier, satellites would more likely be affected by higher altitude bursts. The degree of the effects experienced by the satellite are very dependent upon the weapon's height of burst. For example, should the debris from a lower burst reach an altitude in excess of 40 miles, then:

[T]he electrically charged beta particles will spiral along the earth's geomagnetic field into the opposite magnetic hemisphere and irradiate the conjugate area of the ionosphere. The total level of ionization caused by the beta particles is equally distributed between the blast site and conjugate area. Meanwhile gamma rays are not restricted by the earth's magnetic lines of flux and will continue to spread about the blast site. The ionization caused by the gamma radiation is less intense than the beta particles and dissipates with increased altitude.<sup>41</sup>

The beta particles which spread along the earth's magnetic lines cause irregularities in the ionosphere. These irregularities then form arcs or tubes of varying electron densities, similar to the results exhibited by scintillation.<sup>42</sup>

Should the detonation occur above 70 miles then radioactive debris could be propelled hundreds of miles above the blast point. At these upper altitudes the electrically charged debris can create a disruptive geomagnetic field to stretch before it. "The debris may continue to expand for hundreds of miles before it is stopped by the pressure of the magnetic field." The beta particles which have been trapped by the earth's magnetic field will continue to irradiate the area around the blast site. Additionally while the total area affected is larger for a high altitude burst (40-70 miles), the consequent electron density of the lowest level of the ionosphere (approx. 70 km above sea level) region is less than would be the case if the burst altitude was lower, say between 10 to 40 miles.<sup>43</sup>

Satellites outside of the direct line of sight of a nuclear explosion can later suffer damage through radiation trapped within the earth's magnetic field. This effect was first observed in 1958 when the U.S. detonated in space three low-yield nuclear devices during a test program named Argus.<sup>44</sup> The Argus effect was graphically demonstrated again in 1962 when the effects of trapped radiation inadvertently damaged six satellites in another U.S. high-altitude nuclear test code-named Starfish Prime.<sup>45</sup>

Thermal radiation from the nuclear blast would be the primary cause for the increased atmospheric noise experienced by a communications satellite. As described:

The temperature generated around the fireball may remain in excess of 1,000 degrees K for several minutes. This may result in a significant contribution to the overall system temperature (noise level) of a low temperature satellite receiver particularly if the directive antenna is aimed at the region of the fireball.<sup>46</sup>



This increase in noise level would be a temporary disruption of satellite communications, but again it is just one of many effects contributing toward the same end result.

Synchrotron radiation is a secondary source of atmospheric noise. This radiation results from the beta particles that are trapped along the earth's magnetic lines of flux. As the beta particles travel along they generate synchrotron radiation at right angles to their line of propagation. Its intensity is inversely proportional to the transmission frequency; causing the most significant deterioration to low frequency communications systems.<sup>47</sup>

#### Anti-Satellite Weapons

Anti-Satellite weapons serve the purpose of providing a more surgical-like way to attack an adversary's satellites. Except for the instance where ICBMs or other nuclear-tipped ballistic missiles are used as ASATs, this class of weapons, as a whole, has few collateral effects. The strategy behind using ASATs would follow the philosophy of quickly eliminating an opponent's critical C<sup>3</sup> nodes in order to create chaos in their attempt at commanding and controlling the launching of retaliatory measures. Attacking satellites seems a fairly "clean" way to disrupt an adversary's communications since, by virtue of their location in space, they can be attacked without damaging anything else. Also, they do not clearly fit into either a counter-value (normally associated with population centers) or counter-force (traditional military targets such as a missile silos) type of categorization and therefore might be a more socially acceptable target.

Through their technological efforts both the Soviet Union and the United States have shown a resolve to develop ASAT capability that would play an integral part in each power's overall defense posture. From their rudimentary beginnings in the 1960s these weapons have progressed to the point that they are viable threats to today's and tomorrow's satellites.

ASATs can be grouped into three main categories: 1) Nuclear weapons including Anti-Ballistic Missile Systems (ABMs), Intermediate Range Ballistic Missiles (IRBMs), Submarine Launched Ballistic Missiles (SLBMs), and Intercontinental Ballistic Missiles (ICBMs); 2) Kinetic energy weapons which disable their targets by the mechanical shock of impact and include space mines, co-orbiting killer satellites, and miniature homing vehicles; and 3) Directed Energy weapons which include lasers, particle beam weapons, and high-powered radio-frequency generators.

#### Nuclear

Unlike the previous section which discussed nuclear effects, here nuclear weapons are treated as an existing weapon type which could be reprogrammed to attack specific satellites directly. This would be a relatively inexpensive method of attacking satellites, but it suffers from the same problems as those alluded to earlier with the use of nuclear effects. That is, collateral damage to friendly satellites and the disruption of communications on earth, as well as the risk of escalating a conflict.<sup>48</sup>

Still, they must be considered as viable anti-satellite weapons. Any ICBM, IRBM, or SLBM could be modified to attack satellites by

reprogramming the missile's guidance logic and changing the fusing on the warhead to detonate at a given point in space.<sup>49</sup> ICBMs and SLBMs are capable of lofting warheads to apogee altitudes of over 1400 Km making them lethal to low-earth orbit satellites and capable of spreading their nuclear effects to damage higher altitude satellites.<sup>50</sup>

The Galosh ABM system of missile interceptors surrounding Moscow must also be credited with an ASAT capability. This system, designed to intercept attacking warheads outside of the earth's atmosphere, is being upgraded with new battle management radars and an improved version of the Galosh interceptor (designated SH-04).<sup>51</sup> In all probability, it is doubtful that the Soviets would use this system in an ASAT role since their own satellites and communications would be degraded and there would be fewer missiles to perform their primary mission, the protection of Moscow.

### Kinetic

Kinetic weapons more closely fit the mold of a traditional ASAT and are usually designed explicitly for this type of mission. They are guided or unguided projectiles that disable their targets by the mechanical shock of impact. As a class, they are more discriminating than nuclear weapons. Oftentimes they use the target satellite's orbital velocity (about four or five kilometers a second at perigee in low earth orbit) as a weapon against itself by creating a catastrophic collision with the attacking ASAT.<sup>52</sup>

The primary disadvantages of conventional kinetic energy weapons are that they require accurate pre-attack targeting information and often

must employ the use of sophisticated guidance and fusing mechanisms to execute an attack. Stares describes additional criteria:

Depending on the type of kinetic energy weapon, a propulsion system with enough fuel to maneuver close to the target satellite, especially one capable of evasive action, would also be required. And space-based ASATs would need a responsive command and control system to carry out an attack.<sup>53</sup>

In other words, a kinetic energy weapon generally employs technologies which make it more flexible for attacking satellites.

Kinetic energy ASATs could be any variety of devices ranging from conventional fragmentation charges that explode near the target to more sophisticated homing vehicles that smash into it.<sup>54</sup> Space mines, co-orbiting "killer" satellites, and direct ascent or homing vehicles are just a few of the many types of these weapons being developed.

Bulkeley and Spinardi, from their book Space Weapons, describe space mines as explosive satellites, "not unlike the current Soviet ASAT", that require pre-placement in orbits near their targets waiting to be detonated on command.<sup>55</sup> They could even be maneuverable, allowing them to stalk their prey when called upon.

Deploying space mines covertly, without raising suspicions, would be a difficult task. For mining to be effective, a mine would need to be assigned to each target satellite within a constellation. This type of deployment would be easily detected. In the geostationary arc there is an international convention requiring a minimum separation of 2 degrees to avoid signal interference.<sup>56</sup> Again, a violation of this convention would bring quick attention to such a craft. Of course, an enemy may be willing to arm an active satellite and use it in time of conflict to attack its celestial neighbors.

In a looser sense, some would say that the concept of a space mine would include space-based lasers or directed energy weapons or even mines that would jam or disrupt communications.<sup>57</sup> Each of these types of weapons will be addressed separately in future sections. Essentially, any mine that would deny an adversary use of his satellite's capabilities, at a reasonable cost of employment, might be developed for ASAT use.

An ASAT could employ a co-orbital mode of deployment where it is placed into the same orbit as its prey. In this way, it can maneuver toward the target when required. Variations to this method would be for the attacker to be placed into an orbit so that it only occasionally comes close to its target, or close enough so that its guidance and kill mechanism could be effective.<sup>58</sup>

Direct ascent exploding or homing vehicles are ASATs that use missiles or high-flying aircraft as launch platforms. A direct ascent system would use a ground-based interceptor that would be programmed to arrive at the same time and place as a passing target satellite. Through the use of a homing device an ASAT could track and attack a maneuverable target.

The Soviets possess a ground-based co-orbital ASAT interceptor which can also function as a direct ascent weapon. It was developed in the late 1960s and uses an ICBM booster to put a pellet-laden warhead into the same orbit as that of a targeted satellite. The ASAT vehicle would be launched from Tyuratam space center, in the central Soviet Union, as its target satellite passed overhead (within 5000 Km). "It would then close in on its target within two orbital revolutions, site it with

a radar homing sensor, and destroy the target by exploding the pellet-type warhead at close range."<sup>59</sup>

The U.S. has tested a direct ascent system using an F-15 aircraft to launch an ASAT at low orbit satellites. This system suffers from many drawbacks including the fact that it would have to be deployed in the southern hemisphere where it could reach the perigee of the Soviet satellites. It does, however, have a relatively quick launch capability.

Similar to the Soviet system, the U.S. Army tested its Homing Overlay Experiment (HOE) in June of 1984. It used an old Minuteman I booster with a nonnuclear device to intercept a ballistic missile warhead at an altitude of 150 kilometers.<sup>60</sup> The experiment was designed to test the ability of a pellet impact system to destroy very hard re-entry vehicles. Should its long-wave infrared (LWIR) sensors be resistant to countermeasures, then it could demonstrate a large kill radius against relatively soft satellites.<sup>61</sup>

### Directed Energy

Some of the most sophisticated technological efforts have gone into developing directed energy (DEW) or beam weapons. This classification would include lasers, particle beam weapons, and high-powered radio-frequency generators. Once they become technically feasible and deployable, they could prove to be formidable ASAT weapons. Their effects travel so fast that no warning or evasive action could be undertaken by the target satellite.<sup>62</sup>

Their deficiencies stem from a trade-off in basing modes. If they are to be deployed within the atmosphere on land, ships, or aircraft, then their effectiveness could be seriously attenuated by such atmospheric

conditions as clouds or precipitation. Of course, these systems would be less constrained by weight and size requirements than a space-based mode. To deploy them as space battle stations would remedy the problem of atmospheric interference, but many new challenges would arise. For example, their design, maintenance, command and control, etc. would all have to be tailored for a spaceborne platform.<sup>63</sup> Then, the predatory cycle starts again since these platforms would be targets and therefore should also be made survivable.

An electron particle-beam weapon based within the atmosphere suffers dramatic loss in beam power through the effort of penetrating the air. Up to 50% loss of beam energy within 200 meters could be expended through the effort to penetrate and also through electron scattering. Even the earth's magnetic field would work against a charged particle-beam weapon by deflecting the beam.<sup>64</sup> One remedy to the latter problem might be to use a neutral particle beam.<sup>65</sup>

Lasers are coherent beams of electromagnetic radiation in which the electromagnetic waves oscillate in step. Numerous laser sources exist, each with its own characteristics. Used as an ASAT and given the ability to concentrate enough power, a laser could damage a satellite by overheating its surface, by "blinding" key on-board sensors, or by puncturing the outer surface of the spacecraft to expose internal equipment.<sup>66</sup>

The Soviet Union continues to test high energy lasers as both ballistic missile defense and, presumably, ASAT weapons. USAF Gen. John Piotrowski confirmed that the Soviets could damage our satellites when he stated:

Twin ground-based lasers at Sary Shagan in the south-central

Soviet Union are capable of killing U.S. satellites below 400 km (248 mi.) in low Earth orbit and damaging satellites up to 1,200 km (744 mi.) in space. The lasers also can cause inband damage to sensors and solar panels on satellites in geosynchronous orbit at 35,880 km (22,245 mi.) if transmitted over certain frequencies.<sup>67</sup>

In addition to the lasers at Sary Shagan, another completely new laser facility seems to be under construction at Dushanbe in the Tadzhik Socialist People's Republic near the Afghanistan border (1987).<sup>68</sup> But, the Soviet's efforts have not been limited to ground-based systems. The March 1990 issue of Signal magazine reports that a defecting Soviet scientist claims that Moscow already has deployed laser weapons in space capable of attacking U.S. satellites and possibly ballistic missiles.<sup>69</sup>

At this point, the greatest danger posed by these weapons seems to be their ability to damage or blind our own satellites' sensors. Little doubt exists, though, that they are actively researching ways to make their lasers more powerful.

Our Department of Defense has developed and constructed a large deuterium fluoride laser at White Sands Proving Ground in New Mexico.<sup>70</sup> In addition, the Strategic Defense Initiative has spawned many new programs which, while designed for ballistic missile defense, could be used for ASAT purposes. One such project using lasers is called the Relay Mirror Experiment. It is designed to demonstrate the ability to bounce a ground-based laser beam off of a mirrored satellite, then hit and destroy a missile in space.<sup>71</sup>

Particle beam weapons consist of large accelerators which propel charged or neutral particles at great speeds to their target. These weapons seem to be more susceptible to atmospheric interference than lasers. Yet, unlike today's lasers, "a particle beam could immediately



penetrate the surface of a satellite and disable its internal components through thermal and radiation damage."<sup>72</sup>

Radio frequency weapons could make up another sector of directed energy ASATs. It is predicted that the Soviet Union could test a ground based radio frequency weapon capable of damaging satellites in the 1990s.<sup>73</sup>

### Direct Electronic Measures

Direct electronic measures constitute another method for disrupting an adversary's satellite communications. These are intentional electronic methods designed to create nondestructive interference and include such techniques as jamming and spoofing. Collectively these techniques are known as electronic countermeasures (ECM).

The inherent benefit with using these types of techniques is that they are comparatively non-escalatory. They do not create permanent damage, and are also often difficult to verify that they are being used. Therefore, it is presumed that such methods could possibly be the first used during the early phases of a conflict.

The fact that the U.S. recognizes this threat to its military communications satellites was acknowledged in 1978 by Air Force General Alton Slay. He declared that "the Soviet Union has electronic warfare facilities which could be employed against certain U.S. satellites."<sup>74</sup> In principle, any radio transmitter broadcasting from the right position with the requisite power and at the appropriate frequency could interfere with a satellite's communications links. Stares records that no incidents of deliberate interference with U.S. satellites have been officially acknowledged.<sup>75</sup>

The benefits of wide coverage area and easy access that a satellite communications system affords may be used against that same system. Since a communications satellites' footprint normally covers a large earth surface area, providing coverage for its subscribers, it also provides an equally large area for access by those wishing to disrupt its links.<sup>76</sup> A quote from Stares' book suggests, "Jamming sources might include shipborne facilities, ground-based facilities in Cuba, or jammers covertly operated inside U.S. territory."<sup>77</sup>

### Jamming

This ECM technique is conducted by an enemy to prevent communications by swamping a system with radiated power. Essentially it "entails transmitting a competing signal with sufficient power to an enemy receiver so as to drown out the meaningful reception of other signals."<sup>78</sup> A jammer may choose to spread his jamming power over the entire frequency bandwidth of the target signal or concentrate it on specific channels. The former case describes barrage jamming while the latter is called spot jamming.

When considering satellite communications, a jammer may choose to attack either the uplink or the downlink. Uplink jamming is probably the most feasible threat against communications satellites since most satellite receive antennas view hostile territory. In the same way that a large ground station can radiate high power, a jammer of similar scale would be able to radiate an equal or greater amount of interfering power. By using very high power gyrotron tubes at higher microwave frequencies, a jammer may create extremely high jammer EIRPs

(Effective isotropically radiated power).<sup>79</sup> Tozer describes other effects an uplink jammer can have:

An uplink jammer will affect the signal directly, resulting in reduced SNR, and as the transponder is power-limiting, it can capture the downlink power. This results in an absolute reduction in the wanted downlink EIRP, plus additional Small Signal Suppression of up to 6 dB. The effect is that the transponder communications throughput is greatly reduced, and normal traffic may become virtually impossible.<sup>80</sup>

Again, a higher altitude satellite, for example in geosynchronous orbit, would be more susceptible to uplink jamming than would a low earth orbit satellite. A low earth orbit satellite would have a smaller coverage area and therefore smaller access area for a jammer which means a shorter jamming period, also.

Downlink jamming would be more difficult to perform but it offers equally lucrative benefits to an adversary. This type of jamming would need to be performed from an altitude overlooking the ground station by an aircraft or some sort of space platform, making the jammer vulnerable to physical attack. By performing downlink jamming on a communications link both the actual communications traffic and the telemetry data from the satellite could be disrupted. Telemetry data might include such information as satellite temperature levels, battery power, fuel consumption, attitude, etc.<sup>81</sup>

In the future, as crosslinks (direct links between satellites) become more prevalent, they too will be subject to ECM.

### Spoofing

Spoofing is a more sophisticated method of interfering with a satellite link. It entails feeding false commands and information to the satellite in order to impede its mission or render it inoperable. This

means that an attacker must have detailed knowledge of the satellite system to be able to insert such commands covertly. Along with this knowledge, he must also be able to construct/create or have access to adequate hardware and software to transmit such commands to a satellite.

Generally, spoofing would be used against the satellite's command link. Should an adversary choose this method of attack, then he could affect the satellite's sensors, thermal controls, or propulsion system. "Spoofing is perhaps the most discreet and undetectable way of interfering with satellites."<sup>82</sup>

### Conclusions

While nuclear effects, anti-satellite weapons, and direct electronic measures may be the major foreseeable threats to military communications satellites, only the imagination limits the potential plethora of methods to disrupt satellite communications. As long as the military continues to rely heavily on these systems to carry their vital command and control information, then they will remain lucrative targets for an adversary.

To protect these crucial assets, an accurate assessment must be conducted of existing and potential threats. Next, feasible schemes must be developed to resist or thwart these threats.

## NOTES - CHAPTER III

<sup>1</sup>Paul B. Stares, Space and National Security, (Washington, D.C.: The Brookings Institution, 1987), p. 74.

<sup>2</sup>Stares, p. 74.

<sup>3</sup>Charles W. Cook, "The U.S. Air Force Space Program," as found in National Security Issues Symposium, 1984: Space, National Security and C<sup>3</sup>I, Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the MITRE Corporation, Oct 25-26, 1984 (Boston: MITRE Document M85-3, 1984), p. 41.

<sup>4</sup>Colin S. Gray, American Military Space Policy: Information Systems, Weapon Systems and Arms Control (Cambridge, MA: Abt Books, 1982), p. 46.

<sup>5</sup>William P. Murdock, Jr., "Alternative Force Structuring Strategies for Military Satellite Communication Systems", Thesis submitted to the Air Force Institute of Technology, Wright-Patterson AFB, OH, Dec 1987, p. 1.

<sup>6</sup>Murdock, p. 1.

<sup>7</sup>Murdock, p. 1.

<sup>8</sup>Guiseppe Donadio, "Comparative Analysis of Passive Communications Satellites Employing the SHF and HF Spectrum for Use in a Strategic Role", Thesis submitted to the Naval Postgraduate School, Monterey, CA, Mar 1988, p. 19.

<sup>9</sup>Donadio, p. 18.

<sup>10</sup>Donadio, p. 19.

<sup>11</sup>Michael M. May, "Safeguarding Our Space Assets", in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Regime (Lanham, MD: The Aspen Institute for Humanistic Studies and the University Press of America, 1987), p. 77.

<sup>12</sup>Joseph A. Poliakon, "System Issues and Considerations Associated with Design of Ground Mobile Strategic Satellite Communication Terminals", in Conference Record from IEEE Military Communications Conference, Oct 31 - Nov 2, 1983, Washington, D.C., p. 254.

<sup>13</sup>Stares, p. 81.

<sup>14</sup>Stares, p. 81.

<sup>15</sup>Donadio, p. 31.

<sup>16</sup>Donadio, p. 31.

<sup>17</sup>Donadio, p. 21.

<sup>18</sup>Donadio, p. 21.

<sup>19</sup>"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process", Report prepared by Computer Sciences Corporation for the Defense Nuclear Agency, Jun 4, 1976, p. 5-72.

<sup>20</sup>T. C. Tozer, "An Introduction to Military Satellite Communications," Memorandum No. 3976 of the Royal Signal & Radar Establishment, Malvern, England, Apr 1987, p. 21.

<sup>21</sup>Donadio, p. 21.

<sup>22</sup>Donadio, p. 21.

<sup>23</sup>"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process", p. 5-71.

<sup>24</sup>"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process", p. 5-72.

<sup>25</sup>"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process", p. 5-72.

<sup>26</sup>"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process", p. 5-72.

<sup>27</sup>Donadio, p. 31.

<sup>28</sup>Donadio, p. 31.

<sup>29</sup>"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process", p. 5-72.

<sup>30</sup>Donadio, p. 17.

<sup>31</sup>Donadio, p. 18.

<sup>32</sup>Donadio, p. 8.

<sup>33</sup>Tozer, p. 21.

<sup>34</sup>Donadio, p. 8.

<sup>35</sup>Donadio, p. 8.

<sup>36</sup>Stares, p. 74.

<sup>37</sup>Stares, p. 74-5.

<sup>38</sup>Donadio, p. 22.

<sup>39</sup>Donadio, p. 25.

<sup>40</sup>Donadio, p. 25.

<sup>41</sup>Donadio, p. 25

<sup>42</sup>Donadio, p. 26.

<sup>43</sup>Donadio, p. 26-7.

<sup>44</sup>Stares, p. 75.

<sup>45</sup>Stares, p. 75.

<sup>46</sup>Donadio, p. 29.

<sup>47</sup>Donadio, p. 29.

<sup>48</sup>Stares, p. 77.

<sup>49</sup>Stares, p. 96.

<sup>50</sup>Ashton B. Carter, "The Current and Future Military Uses of Space", in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime (Lanham, MD: The Aspen Strategy Group and University Press of America, 1987), p. 51.

<sup>51</sup>Stares, p. 96.

<sup>52</sup>Stares, p. 75.

<sup>53</sup>Stares, p. 77.

<sup>54</sup>Stares, p. 75.

<sup>55</sup>Rip Bulkeley and Graham Spinardi, Space Weapons: Deterrence or Delusion? (Totowa, NJ: Barnes & Noble Books, 1986), p. 52.

<sup>56</sup>Bulkeley and Spinardi, p. 52.

<sup>57</sup>Carter, pp. 60-1.

<sup>58</sup>Stares, p. 76.

<sup>59</sup>William J. Perry, Brent Scowcroft, Joseph S. Nye, Jr., and James A. Shear, "Anti-Satellite Weapons and U.S. Military Space Policy: An Introduction", in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime (Lanham, MD: The Aspen Strategy Group and University Press of America, 1987), p. 7.

<sup>60</sup>Perry, Scowcroft, Nye, and Shear, p. 9.

<sup>61</sup>Gray, p. 47.

<sup>62</sup>Bulkeley and Spinardi, p. 52.

<sup>63</sup>Stares, p. 77.

<sup>64</sup>Gray, p. 46.

<sup>65</sup>Stares, p. 76.

<sup>66</sup>Stares, p. 75-6.

<sup>67</sup>Murdock, p. 4.

<sup>68</sup>Stares, p. 97.

<sup>69</sup>Leonard H. Perroots, "Soviet Beam Weapons are Near Tactical Maturity", Signal, Mar 1990, p. 38.

<sup>70</sup>Carter, p. 52.

<sup>71</sup>Victoria Gits, "Ball Project Part of 'Star Wars' Test", Daily Camera, Sec A., p. 1.

<sup>72</sup>Stares, p. 76.

<sup>73</sup>Perroots, p. 39.

<sup>74</sup>Stares, p. 97-8.

<sup>75</sup>Stares, p. 98.

<sup>76</sup>Harris A. Stover, "Engineering Aids for the Design of Survivable Defense Communications Transmission Capability," Technical Note No. 11-82 (Defense Communications Agency, Jan 1984), pp. 16.

<sup>77</sup>Stares, p. 98.

<sup>78</sup>Stares, p. 81.

<sup>79</sup>Tozer, p. 22.

<sup>80</sup>Tozer, p. 22.

<sup>81</sup>Stares, p. 81.



<sup>82</sup>Stares, p. 82.

## CHAPTER IV

### TECHNOLOGICAL MEANS AND METHODS FOR MITIGATING, ELIMINATING, AND DEFEATING THE THREATS

After having reviewed the unique requirements of military communications satellites and the existing and potential threats against them, it is now time to examine methods for protecting these valuable assets.

As viable threats become reality, we are made acutely aware that these critical C<sup>3</sup> nodes will be targeted and, if need be, attacked. Today's military communications satellites incorporate certain survivability features and as we move toward newer generations of constellations there will be a greater push in this direction. In a critical analysis, much more could be done to enhance these systems' survivability. Ashton B. Carter, an expert on space arms control, agrees:

The survivability features of satellites in orbit today are not a good indication of what is possible at relatively modest additional cost. No arms control provisions can protect a satellite whose designers have left it open to "cheap shots." Adequate satellite survivability programs are not an alternative to, but a necessary precondition for, effective arms control.<sup>1</sup>

Carter's commentary appeared in 1987 and his analysis is just as accurate today. By "cheap shots", he means a relatively low-cost method to attack a satellite that might make such an attack economically attractive and viable to an adversary.

As alluded to earlier, planning survivability features for satellites involves a certain amount of forecasting. This forecasting should be based on intelligence analysis that is as accurate as possible. A certain degree of anticipation of evolving threats is required so that survivability features can be "in place" as the threat actually materializes. This is necessary since changing the physical features of a satellite after launch would be nearly impossible, and probably economically prohibitive.

A multitude of factors should be considered when deciding upon which kinds of survivability features to incorporate into a military communications satellite. Besides the overriding cost factors, there are operational tradeoffs to many of the proposed technical features. A satellite planner may choose to consider four general principles offered by Stares when making such decisions:

First, protective measures tend to work synergistically. Increasing ground-segment redundancy and satellite autonomy is a case in point. . . . Second, the space system is only as survivable as its weakest link. It is pointless to protect one part of the system while leaving the others comparatively vulnerable. Third, satellite survivability measures should be kept in proportion to the value of the satellite's mission. Some satellites are more important than others in time of war and should be protected accordingly. Fourth, satellite survivability measures should be kept in proportion to the threat. Hardening satellites against, say, nuclear effects is only meaningful up to a certain threshold, after which it is better to rely on reconstitutable spares or non-space-based alternatives.<sup>2</sup>

As will be seen later, the rule of synergism carries throughout. For example, through the use of higher frequencies (in the EHF range), communications may be more resistant to nuclear effects and the increased bandwidth would make it easier to incorporate spread spectrum techniques. The portion of the satellite system being considered here is the spacecraft portion. Communications satellites carry a high target value due to their scope of influence and

pervasiveness and should warrant an equally high protection factor. The degree of protection to be incorporated must be decided, not by today's threats, but those that demonstrate a likelihood of emerging during the lifetime of the spacecraft.

Two divergent philosophies have emerged for enhancing the survivability of the space portion of a satellite communications system. Should the U.S. choose to follow its present course of using fewer, more expensive, more capable, multi-mission satellites, then preparations should be made for making each of these spacecrafts as survivable as possible. Such precautions are an insurance toward protecting our defense and monetary investments. An alternative approach would be to borrow from the Soviets' philosophy of employing many, low-cost, single-mission satellites. Using the same monetary resources required for the smaller constellation, a simpler, more proliferated system could be built. In such a system less reliance would be placed on each, individual spacecraft and an adversary would have to neutralize many more targets to degrade the overall communications system. This philosophy would include the use of on-orbit and quick launch spares.

There are advocates for both approaches and judgement will not be made here as to which is "better". Each has its merits and advantages depending upon one's perspective. The first section of this chapter will address ways to enhance the survivability of individual satellites. The assumption here is that all economically feasible means could be brought to bear to diminish the threats against each satellite. The second section examines proliferation schemes and specifically the idea of Multiple Satellite Systems (MSS). Survivability is improved by increasing the number of space platforms and hence, the number of

targets that an enemy must to destroy in order to significantly degrade the communications network.

### Individual Survivability Improvements

Many features may be incorporated into a satellite's design to help enhance survivability. In this discussion an effort will be made to match survivability measures with the corresponding threats that were identified in Chapter #3. The three major threat areas addressed were nuclear effects (blast, absorption and scintillation, atmospheric ionization, EMP, and radiation), ASATs (nuclear, kinetic, and directed energy), and direct electronic measures (jamming and spoofing). Oftentimes, a survivability features' effects may spill over from combating one threat to help diminish a separate one. One example, as noted above, is the move toward higher frequency bands such as EHF.

### Nuclear Hardening

This category encompasses all precautions taken to protect a satellite from the effects of a nuclear explosion. These effects span the gamut from blast to radiation.

For all practical purposes, only limited blast resistance can be incorporated into a satellite without exacting severe weight restrictions. Blast damage in open space is really of minimal concern unless the satellite is targeted directly. In such a case, protection may be a lost cause anyway. The development of harder and lighter weight materials hold promise for making a satellite more blast resistant.

Generally, nuclear hardening refers to protections not directly related to blast effects, but rather the effects of long-range prompt and

delayed radiation. These include methods to prevent radiation and EMP from damaging the spacecraft's sensitive electronics. As examples, the outer surface of the satellite can be constructed of special metals and materials which reduce conductivity to System Generated EMP (SGEMP). The inner electrical components (many of which are transistors) can be shielded by protective enclosures known as Faraday cages. Electrical cables can be wrapped in copper foil or materials of lower atomic number to reduce the available electrons. Finally, the electronic components themselves can be made more resistant to large electrical surges and other radiation effects.<sup>3</sup> The drawbacks to these hardening measures are that they are expensive and add additional weight requirements to the spacecraft.

EMP is especially dangerous to electronic circuitry and may be conveyed into the spacecraft through the antenna systems. In addition to shielding, many other techniques are available for protection. These include filtering, surge arrestors/suppression, electrical bonding, cable/wire bundling, chokes, spare gaps, zener diodes, circuit design, and grounding which all serve to shield against or limit EMP induced currents and voltages.<sup>4 & 5</sup>

The vast majority of today's military satellites use the UHF and SHF bands for their communications links. In the future, many factors will drive a move toward EHF communications. One of these is that such high frequencies are less disturbed by nuclear effects-related interferences than the lower bands.<sup>6</sup> At these frequencies, disruption from scintillation and absorption would last only a few minutes instead of many hours.<sup>7</sup> The drawbacks would be increased attenuation by

atmospheric conditions such as rain or dust. This could affect the normal, day-to-day operations of the system.

The choice of modulation/demodulation schemes can have a direct impact upon how vulnerable a channel will be in a nuclear environment. Tests have determined that coherent modulation schemes are considerably more vulnerable to scintillation effects due to the problems in maintaining phase lock. A report for the Defense Nuclear Agency recommends non-coherent frequency-shift keying (FSK) as opposed to phase-shift keying (PSK) for transmissions in a nuclear-disturbed environment.<sup>8</sup>

Another method for enhancing transmission through a nuclear disturbed environment is to employ a stressed mode of communications. This implies having the users drop to a slower data rate such as 75 or 2,400 BPS.<sup>9</sup>

Paul, Meader, Lyons, and Ayers conducted a transmission analysis of a simulated slow-fading, nuclear-disturbed channel using the Defense Nuclear Agency's (DNA) nuclear-scintillated channel model. Their goal was to determine performance tradeoffs for using interleaver storage, forward error correction (FEC), and spatial diversity on the link signal-to-noise ratio for differential binary phase shift keying in the slow-fading environment.<sup>10</sup>

As background, an adversary may choose to detonate a high-altitude nuclear blast to disturb the propagation characteristics of the atmosphere. Such a burst can cause non-uniform ionization and other physical alterations in the composition of the transmission medium that diffract and disperse the carrier beam. This results in multipath fades and other severe distortions in the received signal. The transmission

characteristics of the nuclear channel vary gradually over time from the instant of the explosion. Immediately following the blast, a period (on the order of minutes) exists where satellite links experience fast-fading and coherent bandwidth limitations. "These fast-fading effects can be accomodated by proper waveform design that ensures that the signal coherent bandwidth is less than the channel bandwidth and that the required signal coherence interval is less than that provided by the channel."<sup>11</sup>

Fast-fading is followed by a period characterized by very slow (relative to the modulation symbol interval) correlated Rayleigh fading. This period, which can last for hours, sees deep fades for untreated channels which result in long bursts of errors for high-data-rate signals. "Unlike fast-fading, the waveform design alone is insufficient to mitigate the effects of fading, and therefore alternate means must be found."<sup>12</sup>

Slow-fading is best combatted by encoding the transmitted data symbols using forward error correction (FEC) techniques and then interleaving them in time. At the receiver, the samples of the received signal are deinterleaved so that independent symbol errors are presented to the decoder. With sufficient interleaver memory size to produce independent symbol errors, the decoded error rate can be predicted. The problem is that the interleaver memory may not be large enough to accomodate high data rates together with long decorrelation times. Also, excessive transmission delays would be a problem, especially for voice channels. The remedy suggested by the authors is to use spatial (or antenna) diversity and Reed-Solomon coding to compensate for inadequate interleaving memory.<sup>13</sup>



Much of the technology for minimizing nuclear effects can be borrowed from terrestrial systems. These methods are relatively mature since the existence and knowledge of these effects has been around since the 1940s and 1950s. They simply need to be adapted for use on satellites where the basic concerns of size and weight are key. Also, these techniques offer some basic protection from other threats. For example, Stares suggests that some of the techniques for hardening against nuclear effects would also help protect satellites from particle beam weapons.<sup>14</sup>

#### Protection Against ASATs

To protect a satellite against an ASAT is to protect it against an intentional and determined menace. Generally, ASATs are designed to attack a single satellite; one-on-one. The exception would be laser and particle beam weapons. These should be able to attack multiple satellites if they can command enough power for multiple attacks.

The three major ASAT threats to communications satellites are nuclear weapons (ABMs, ICBMs, IRBMs, and SLBMs), kinetic weapons (fragmentation, space mines, co-orbiting "killer" satellites, direct-ascent, and homing weapons), and directed energy weapons (lasers, particle beam weapons, and high-powered radio-frequency generators).

Protecting satellites against ASATs requires both passive and active measures. Passive measures, such as those presented for nuclear effects, are built-in features that, by their nature, increase the odds of the satellite's survival. Active measures imply that the satellite reacts in some way to the attack so as to save itself. For example, a satellite's sensors might alert the spacecraft that it is receiving ever-

increasing radar-type reflections, meaning that something is using radar to track it. It might process this information and initiate a maneuver or evasive action to propel itself out of the attacker's path or deploy a decoy for the ASAT to strike. There are many types of passive and active measures a satellite may employ.

As illustrated by this hypothetical scenario, an ASAT must first find the target that it is to attack. Therefore, a promising survivability measure would be to reduce the likelihood of detection. Similar to our "stealthy" aircraft, satellites could be designed with low radar cross sections. To create this effect, they might replace the large solar panels with small nuclear generators and coat the outside of the spacecraft with radar-absorbing materials and paints. These work together to mask the satellite from targeting sensors. Since most communications satellites rest in the relatively high geosynchronous orbit such techniques would make them harder to detect and identify. Also, this tactic would be especially effective for hiding spare satellites in high-altitude orbits.<sup>15</sup>

In fact, using high-altitude orbits or placing satellites in widely separated orbital planes creates a twofold effect. First, an assailant's attack time would be increased and second, his targeting vastly complicated as compared with a geosynchronous target.<sup>16</sup>

Protecting satellites from the harms of laser weapons takes many forms. Special ablative materials such as those using graphite derivatives could be used to minimize the thermal effect of lasers. These would be designed to protect the "skin" of the satellite. To negate a satellite's ability to warn itself, an adversary might choose to attack the sensors on a satellite via laser. These sensors are an integral part of the satellite's overall survivability package and therefore special warrant

protection, also. These sensors could be shielded by special shutters or filters that operate on warning of laser illumination.<sup>17</sup>

Much has been written about the evolving threat of lasers in recent years, partially because of the Strategic Defence Initiative (SDI). The consensus seems to be that in the near term laser weapons pose little threat to a properly protected satellite in geosynchronous or higher orbits. Nye describes the futuristic laser capability of a SDI battle station versus a geosynchronous satellite:

High-orbiting satellites facing directed energy attack have the great advantage of the vastness of space on their side. Consider, for example, the ASAT potential of a 20-megawatt hydrogen fluoride laser "battle station" with 10-meter perfect optics based in LEO. This is about the laser brightness that the Strategic Defense Initiative Organization (SDIO) would consider a good start for the BMD role. This laser could dispose of hundreds of ICBM boosters at a range of hundreds of kilometers or a few thousand kilometers within the space of a minute, unless successfully countermeasured. If this laser's beam were directed at a satellite in GEO (36,000 km distant), the received energy flux would be about 100 times what that satellite would be receiving from the sun. The effect of such illumination on the thermal balance, power system, sensors, and antennas of a present-day satellite would be serious, but properly designed spacecraft for many missions could be made to withstand such illumination for hundreds of seconds, if not indefinitely. A determined satellite hardening effort could make spacecraft resilient to much stronger illumination. Hundreds of seconds of lasing time might consume the entire store of fuel aboard the laser, making this attack a costly one-on-one affair. Alternatively, the target satellite could use this long illumination time to deploy shielding, to deceive the laser's pointing sensor, to counterattack, or to alert others to the attack.<sup>18</sup>

May's assessment states that ground-based lasers with the power and optics required to damage a high-altitude satellite will not be operational for at ten years (from 1987). He adds that such a facility would be difficult to hide (we know about the Sary Shagan and Dushanbe facilities) and would need to be installed in a region relatively free from cloud cover most of the time.<sup>19</sup>

If an adversary chose to design, develop, and construct space-based lasers, then even high-orbit satellites would be in danger. May speculates that such weapons could be deadly to any satellite with state-of-the-art survivability features as long as the ASAT weapon could be maneuvered within 100 to 1000 km of its target. Still, such a weapon could not "sweep the sky clear of satellites" in a short time unless they were deployed one-on-one. An adversary must answer the question as to whether such space-based laser ASATs could be constructed less expensively than their intended targets.<sup>20</sup> Also, as escalation increased, these space laser platforms might become targets in their own right.

The ability to maneuver in space would greatly enhance a satellite's chances of avoiding attack. Even if a laser ASAT "locked-on" to a satellite, with such an emergency propulsion system, the targeted satellite could maneuver away from the laser beam before the laser could concentrate enough damaging energy on the satellite. Also, a ground-launched, direct-ascent ASAT would take hours to reach satellites at geosynchronous altitudes. During that time, the threat could be recognized and evasive action could be taken.<sup>21</sup> This, of course, puts the burden on our ability to detect such attacks and react to them.

A drawback to incorporating a maneuver capability for a satellite is that the fuel and propulsion system required would extract a weight penalty which otherwise could be used for payload enhancement.

As mentioned above, special sensors which detect radar and laser illumination could be used to alert the satellite of impending attack. They could also detect efforts at interference or the approach of hostile

satellites. Because of their integral role in the survivability of the satellite, these sensors must be protected. As stated above, sensors outfitted with shutters and wavelength-selective filters would be more resistive to laser attacks. Another technique is to use warning sensors that observe infrared light at wavelengths to which the earth's atmosphere is opaque. In this way, ground-based lasers could not blind the sensors. Also, one way to use shutter protection would be to use low-sensitivity sensors that survey a region before the main sensor. Should it detect damaging laser energy, then it could activate a shutter over the main sensor's aperture.<sup>22</sup>

One way to frustrate the attack of an approaching ASAT might be to dispense a decoy. The decoy would only need to be able to fool a simple homing sensor on the ASAT itself. But, a decoy designed to mimic an ordinary satellite for long periods of spacetracking observation would need to "stationkeep" and emit signals just like the real satellites.<sup>23</sup> It would be much easier for the decoys to mimic satellites that are themselves "stealthy".

If an ASAT employs radar to track its target, then radar jamming or infrared flares might be viable options to deceive or deflect the ASAT's guidance system or warhead.<sup>24</sup>

#### Electronic Counter Counter-Measures

In the classical sense, electronic counter counter-measures (ECCM) are those means taken to counter an adversary's intentional electronic counter measures (ECM). ECMs are methods for disrupting or denying the "friendly" use of the electro-magnetic spectrum. For this particular discussion, ECM will refer to both direct intentional measures

(such as jamming) and also nuclear effects (such as scintillation) which can create the same types of disruptive effects. The reason for grouping the two together is that certain ECCM techniques can be effective against both intentional and nuclear-collateral effects.

Although the measures included here may not have been intentionally developed to combat ECM only, each shows potential for mitigating its effects. For example, code division multiple access (CDMA) is one of many ways for providing multiple ground terminal access to a single satellite; it provides a means for sharing the satellites' capabilities among several terrestrial terminals. In an ECCM sense, it also works to prevent intrusion and jamming of the satellite's links.

Each of the ECCM techniques chosen for this discussion could be examined in greater detail, but the effort here is to address several and give a brief overview of how they work to counter ECM efforts. Many of the sources listed in the bibliography have excellent descriptions of these techniques for those interested in further detail.

The techniques showing the most promise in fighting ECM include using higher frequencies such as EHF, employing narrowbeam or adaptive nulling steerable antennas, on-board processing, spread spectrum techniques (both direct sequence and frequency hopping), CDMA, and error correction coding.

As noted earlier, there are many advantages to using the EHF band for satellite communications, including EHF's greater immunity to and shorter time for being affected after a nuclear explosion (as compared to UHF or SHF). EHF provides additional advantages, many of which facilitate ECCM techniques. First, higher frequency communications have a higher limit to their data-carrying capacity than

lower frequency waves.<sup>25</sup> The wider bandwidths translate to more space for error correcting coding and encryption techniques without sacrificing as much space for "information". They facilitate such anti-jam (AJ) techniques as spreading the message over the entire bandwidth (either frequency hopping or direct sequence), again without extracting too much of a penalty from the channel's information-carrying capacity. And, ground terminals also benefit from EHF's wider bandwidths by employing low-probability-of-intercept techniques. This facilitates covert operation; especially important for tactical forces. Finally, transmitting antennas for EHF would be smaller without sacrificing performance, since the effectiveness of a transmit dish is determined by the ratio of its size to the wavelength of the radio waves it is transmitting.<sup>26</sup> This is important not only for the satellite developer, but it means smaller terminals for tactical and airborne platforms. While the difference in sizes may only mean a slight weight advantage, this would still mean that the excess weight saved by using the smaller dish on a satellite could be used for other payload or survivability enhancements.

To illustrate the effectiveness of an EHF system over attempted jamming, Leahy conducted a simulation where he compared typical MILSATCOM links in the UHF (300 MHz), SHF (8 GHz), and EHF (20/44 GHz) ranges. Using a standard set of assumptions, both uplink and downlink budgets were developed showing a jammer's diminishing effect over the higher frequency systems. See Tables 1 and 2. The link budget assumptions included: 1) a low data rate system (2.4 kbps to 75 bps), 2) both clear sky and jamming environments, 3) any existing technologies employed by each of these systems to diminish jamming

Table 1. Uplink Budgets for Three MILSATCOM Systems

Item	Symbol	Parameter		
Payload Receive Frequency		300 MHz	8 GHz	44 GHz
Gain/ $H_{3dB}$	$G_R$	18 dB/18°	41 dB/1.5°	44 dB/1.0°
Payload Antenna	DIA	156 in.	72 in.	20 in.
Noise Temperature	$T_s$	630°K	1000°K	2000°K
Receive Figure of Merit	$G_R/T$	-10 dBk	11 dBk	11 dBk
Thermal Noise Density	$N_0$	-200.6 dBW/Hz	-198.6 dBW/Hz	-195.6 dBW/Hz
Terminal Antenna Gain/ $H_{3dB}$	$G_T$	6 dB	25 dB/9°	34 dB/3°
Terminal Antenna Diameter		25 in.	12 in.	6 in.
Terminal Transmitter Power	$P_T$	20 watts	10 watts	5 watts
Terminal EIRP		19 dBW	35 dBW	41 dBW
Path Loss at Nadir	$L_p$	-173 dB	-202 dB	-216 dB
Losses - Antenna Pointing, Implementation, Etc.	$L$	2 dB	3 dB	4 dB
Received Power	$P_R$	-138 dBW	-129 dBW	-135 dBW
$C/N_0$ Clear Sky	$C/N_0$	62.6 dB Hz	69.6 dB Hz	60.6 dB Hz
Available Transponder Bandwidth	BW	500 kHz	60 MHz	2 GHz
Noise Density with Jammer: $(N_0)_J = EIRP_J - BW + G_R - L_p + A_N$	$(N_0)_J$	$EIRP_J - 212$ dBW/Hz	$EIRP_J - 269$ dBW/Hz	$EIRP_J - 295$ dBW/Hz
Payload Antenna Spatial Rejection	$A_N$	0 dB	-30 dB	-30 dB
$C/(N_0)_J = P_R - (N_0)_J$	$C/(N_0)_J$	$74 - EIRP_J$	$140 - EIRP_J$	$160 - EIRP_J$
$E_b/N_0$ ( $M_{ary}$ , FSK, Coding)	$E_b/N_0$	10 dB	10 dB	10 dB
$J/S = BW - \text{Data Rate} - E_b/N_0 + A_N - L$	$J/S$	26 dB (75 bps)	61 dB (2.4 kbps)	75 dB (2.4 kbps)

Source: Peter Leahy, "MILCOM 83 Small AJ Satcom Terminal Considerations", in Conference Record from IEEE Military Communications Conference (Washington, D.C.: Oct 31 - Nov 2, 1983), p. 230.



Table 2. Downlink Budgets for Three MILSATCOM Systems

Item	Symbol	Parameter		
Frequency		300 MHz	8 GHz	20 GHz
Payload Trans Antenna Gain/ $\theta_{3dB}$	$G_T$	18 dB/18°	41 dB/1.5°	38 dB/2°
Payload Antenna Diameter	DIA	156 in.	72 in.	20 in.
Transmitter Power	$P_T$	10 watts	20 watts	20 watts
Payload EIRP		28 dBW	54 dBW	51 dBW
Receive Antenna Gain/ $\theta_{3dB}$	$G_R$	6 dB	25 dB/9°	27 dB/7°
Receive Antenna Diameter		25 in.	12 in.	6 in.
Noise Temperature	$T_S$	794°K	1000°K	1580°K
Receive Figure of Merit	$G_R/T$	-21 dBk	-8 dBk	-5 dBk
Thermal Noise Density	$N_0$	-199.6 dBW/Hz	-198.6 dBW/Hz	-196.6 dBW/Hz
Path Loss at Nadir	$L_P$	-173 dB	-202 dB	-210 dB
Losses - Antenna Pointing, Implementation, etc.	$L$	2 dB	3 dB	4 dB
Received Power	$P_R$	-141 dBW	-126 dBW	-136 dBW
$C/N_0$ Clear Sky	$C/N_0$	58.6 dB Hz	72.6 dB Hz	60.6 dB Hz
Available Bandwidth	BW	500 kHz	60 Mhz	1 GHz
Noise Density with Jammer: $(N_0)_J = EIRP_J - BW - G_R - L_J - A_N$	$(N_0)_J$	$EIRP_J - 167$ dBW/Hz	$EIRP_J - 228$ dBW/Hz	$EIRP_J - 245$ dBW/Hz
Terminal Antenna Spatial Rejection	$A_N$	0 dB	-30 dB	-30 dB
Path Loss for Downlink Jammer (30 miles)	$L_J$	-116 dB	-145 dB	-152 dB
$C/(N_0)_J = P_R - (N_0)_J$	$C/(N_0)_J$	$26 - EIRP_J$	$105 - EIRP_J$	$109 - EIRP_J$

Source: Peter Leahy, "MILCOM 83 Small AJ Satcom Terminal Considerations", in Conference Record from IEEE Military Communications Conference (Washington, D.C.: Oct 31 - Nov 2, 1983), p. 231.

were compensated for, 4) the assumed transponder bandwidths were - 500 kHz for UHF, 60 MHz for SHF, and 2 GHz for EHF, and 5) that the payload despreads the signal, i.e. a processing payload is required.<sup>27</sup>

In looking at the equation entitled "Noise Density with Jammer", it is easy to see that more is taken away from the EIRP (effective isotropically radiated power) of the jammer as frequency increases (Uplink budget: -212 dBW/Hz for UHF, -269 dBW/Hz for SHF, and -295 dBW/Hz for EHF). This means that the noise density created by the jammer and experienced at the receive antenna would be less for EHF than either SHF or UHF.

The other main feature of EHF, besides wider bandwidth, is its ability to generate narrow beam or spot beams to serve narrow regions on the earth's surface.<sup>28</sup> This too adds to its low-probability-of-intercept and the narrow spot beams for a fixed physical aperture "allow either narrow spot beams or active antenna nulling to achieve spatial rejection."<sup>29</sup>

As with most techniques, there are some disadvantages to moving to the higher frequencies. The principal difficulty in going to EHF is the increased terminal costs caused by the cost and complexity of the EHF microwave power amplifiers. "While considerable technical progress has been made in this area, conversion efficiency drops at higher frequencies."<sup>30</sup> EHF also suffers from greater attenuation and dispersion caused by rain, dust, and foliage.

Another type of technology needs to be incorporated into the spacecraft design to take full advantage of the narrow EHF beam. Mentioned above, null steering antennas permit the electronic interference to be "nulled out", while still permitting reception of

message traffic. Sophisticated antenna arrays will be required for uplink reception. These would provide jammer rejection together with high gain and perhaps frequency re-use.

Tozer recommends a Multiple Beam Antenna (MBA) system which would consist of an array of spot beam antennas. Selection of the appropriate earth coverage area could be achieved by employing a number of feeds sharing a common dish reflector or a waveguide lens structure. By selecting one element at a time, an MBA would yield only limited jammer rejection. But, combining the signals from two or more elements would improve jammer rejection of specific interference sources. In fact, by using several antenna elements, together with both phase and amplitude control and combination, considerable flexibility would be permitted by the nulling antenna, allowing simultaneous nulling of several interference sources. In general,  $N$  sources may be nulled by  $N + 1$  antenna elements.<sup>31</sup> Besides the benefit of flexible coverage, a MBA should also offer high gain.

As developments in phased array technology continue, it is anticipated that these types of antennas will be used for spacecraft of the future. A phased array antenna consists of an array of elements, each with suitably controlled amplitude and phase combining, which could replace a reflecting dish or lens aperture.<sup>32</sup>

An illustration of nulling is provided in Figure 1. Here, "the output from a spot-beam antenna, with a narrow beamwidth, is subtracted from that of an earth cover antenna with a wide beamwidth."<sup>33</sup> In focusing on just the amplitude, it can be seen how a narrow and unique null might be produced.

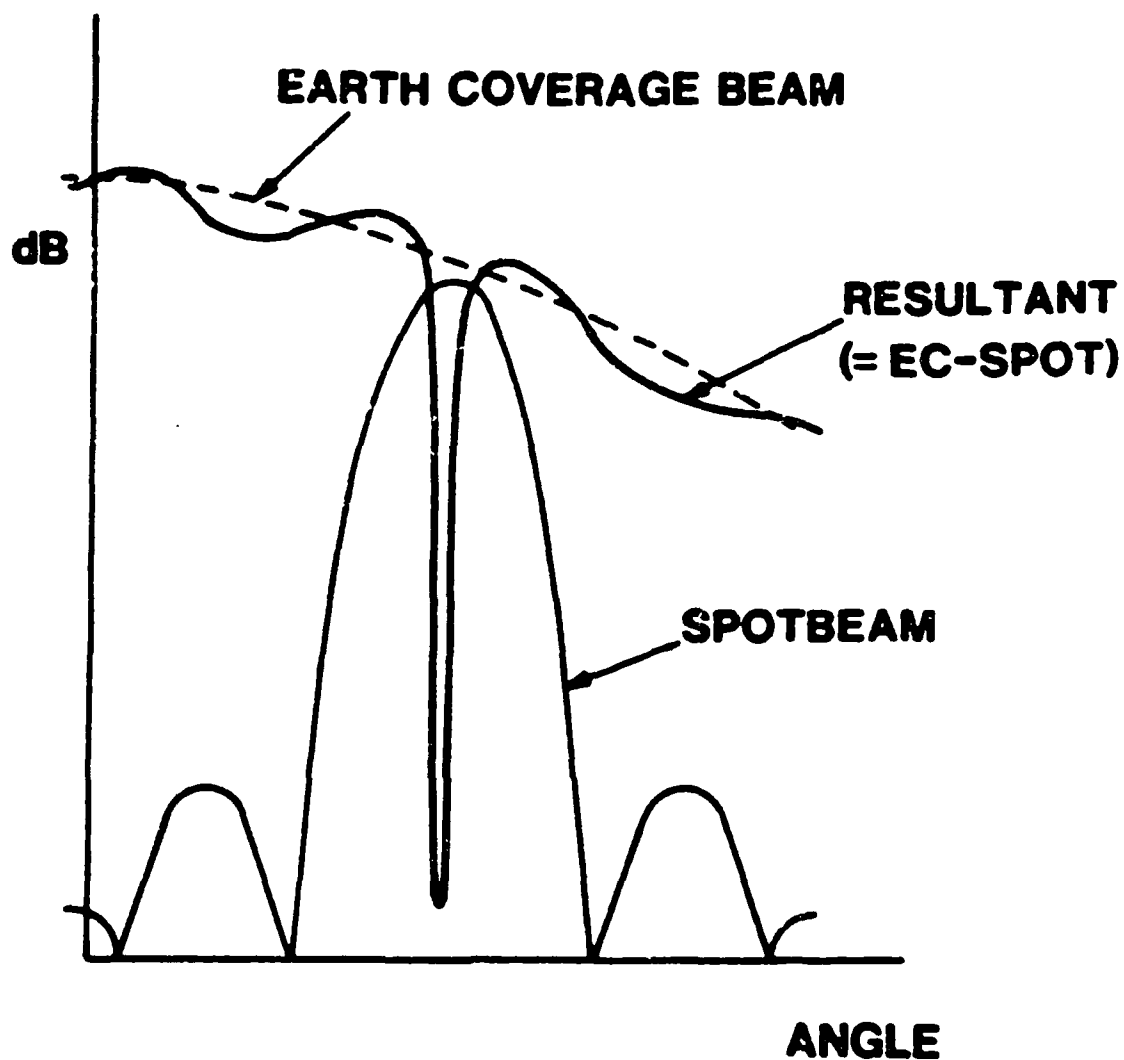


Figure 1. Illustration of Antenna Null Realization

Source: T.C. Tozer, "An Introduction to Military Satellite Communications," Memorandum No. 3976 of the Royal Signal & Radar Establishment, Malvern, England, Apr 1987, p. 24.

There is a price for such sophisticated antennas and the complexity that they add to the spacecraft. Insertion loss would inevitably affect even wanted users and such a system would have to meet the demands

for maintenance of performance over wide bandwidths and environmental temperature ranges. Efficient control could be administered either by remote telecommand or locally through on-board adaptive algorithms (these would discriminate against jamming or interference).<sup>34</sup>

To accommodate such complexity, a greater degree of on-board signal processing will be required. This would make the satellite more autonomous and therefore reduce its reliance on command links and with it the opportunities for jamming and spoofing. Placing more sophistication with the satellite has many benefits for tactical terminals, especially where size and weight requirements are paramount.<sup>35</sup> On-board processing also greatly facilitates the use of spread spectrum modulation.

Spread spectrum modulation is an AJ technique which relies on the friendly user spreading his signal with a spreading function across the available bandwidth. This spreading function cannot be replicated by an enemy. The receiver performs the inverse despreading operation and the original signal is recovered through a narrow bandpass filter. This process weakens an uncorrelated interference such as jamming by spreading it. Once the signal is spread, the bulk of the interference is then removed by the narrow bandpass filter. Processing Gain (PG) is the advantage given to the friendly signal over the interference. It can broadly be expressed as the ratio of the spread bandwidth over the signal bandwidth.<sup>36</sup> Following the sequential explanation from top to bottom in Fig 2 gives a basic description of spread spectrum.

There are two basic forms of spread spectrum. The first is direct-sequence pseudonoise (PN) which spreads messages over the entire bandwidth. The second, frequency hopping (FH), is a process of

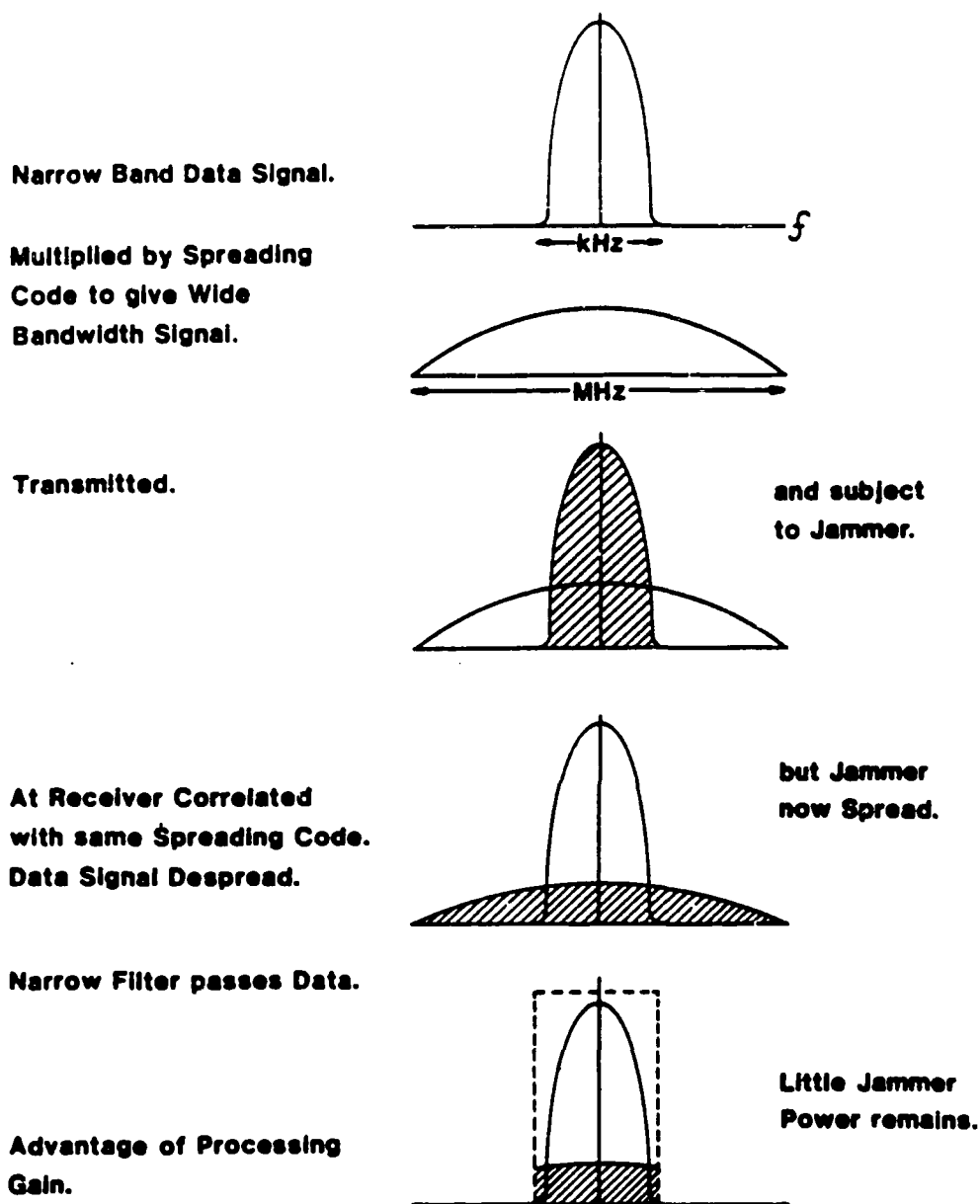


Figure 2. Jamming Protection Through Spread Spectrum

Source: T.C. Tozer, "An Introduction to Military Satellite Communications," Memorandum No. 3976 of the Royal Signal & Radar Establishment, Malvern, England, Apr 1987, p. 26.

randomly changing the transmission frequency in a way known only to the satellite and the friendly ground stations.

"Direct Sequence involves a linear modulation of the signal with a pseudo-random biphasic code, typically at several Mchip/s; thus the spectral width might be increased from (say) 10 kHz to 20 MHz (main lobe)."<sup>37</sup> The identical operation is performed at the despreading receiver with the same spreading code, suitably synchronized in time and code phase. Phase shift keying (PSK) is normally used for PN spread spectrum on satellites.<sup>38</sup> By using these example parameters, a processing gain of 33 dB could be achieved. Because technology limits the code chip rates to a few 10s of MHz, the PG is similarly restricted.<sup>39</sup>

Frequency Hopping requires the carrier frequency to jump in discrete time hops over a wide bandwidth. The receiver recovers the signal by hopping its local oscillator in synchrony with the established code. At the transmitter, frequency shift keying (FSK) is used to modulate the combined PN sequence and information onto the radio frequency carrier. Because a narrow band jammer can normally only concentrate on a few distinct frequencies, statistically he affects only a small proportion of the hops. Error correction coding with interleaving at the receiver then provides for reconstruction of the message. Even if the jammer spreads his power over a wide bandwidth, his affect against any individual hop is reduced. FH yields similar processing gain results to DS. "Hopping rates may range from 10 Hop/s to 20 kHop/s: the rate does not primarily affect the PG, which is determined by the frequency range (i.e. overall hopping BW)."<sup>40</sup>

For satellites, the benefits derived from spread spectrum technology can be applied to their multiple access schemes. The

military has adopted code division multiple access for many of its systems. In this method, "many stations simultaneously transmit orthogonally coded spread-spectrum signals that occupy the same frequency band. Decoding ("despreading") systems receive the combined transmissions from many stations and recover one of them.<sup>41</sup> Essentially, each uplink station is identified by a unique separable address code embedded within the carrier waveform. The transmitting station uses the entire satellite bandwidth and transmits through the satellite whenever desired (random access). Each active station's transmission is combined and superimposed on the downlink from the satellite. Carrier separation is achieved at an earth station by identifying the proper pseudo-random sequence (address) associated with the desired station.<sup>42</sup> "Subject to transponder power limitations and the practical constraints of the codes in use, stations having traffic can access a transponder on demand without coordinating their frequency (as in FDMA) or their time slot (as in TDMA) with any central authority."<sup>43</sup>

With direct sequence CDMA, a station's address is modulated directly on the carrier. Frequency hopped CDMA uses the digital address to continually change the frequency of the carrier.<sup>44</sup>

In addition to its anti-jam capability, CDMA affords its users the ability to minimize interference and combat unauthorized reception. By its nature, CDMA provides graceful degradation as the number of users increases and conversely, excess capacity provides excess margin when the number of users decreases. Pratt and Bostian point out CDMA's applicability for the military:

CDMA is more suited for a military tactical communications



environment where many small groups of mobile stations communicate briefly at irregular intervals than to a commercial environment where large volumes of traffic pass continuously between a small number of fixed locations.<sup>45</sup>

CDMA systems are often called spread spectrum multiple access (SSMA) systems since they involve spreading the carrier spectrum. Military systems are generally called SSMA since this spreading of the carrier spectrum brings inherent anti-jam advantages associated with military usage.<sup>46</sup>

Spread spectrum also adds to the overall complexity and price of a system. Solving the synchronization problems over the long links between transmitter-to-satellite-to-receiver are difficult. For example, "a 10 Mchip/s DS system requires sync to a fraction of a chip, i.e. a few nS."<sup>47</sup> FH systems are more robust and may maintain synchronization by using the time of day from a conventional crystal clock. As mentioned earlier, FH systems are also preferred for their FSK modulation technique since it may fare better in a nuclear environment than the PSK used in DS systems. On-board processing, which also increases complexity and price, would be needed to support a despreading receiver on the satellite in order to maintain performance under heavy jamming.

The future use of laser crosslinks will present a difficult jamming task for an adversary. Besides providing huge carrying capacity between satellites, such high frequencies make for pin-point beams. A jammer would have to be spaceborne and physically intercept the beam to disrupt the communications between satellites.

Error correction coding is another technique which aids in successful transmission through both a nuclear affected environment and through interference or jamming. Error coding trades information

rate capacity with information error rejection. "This is achieved by adding to the transmitted symbols a set of symbols which do not carry information, but which are derived from the nonredundant set of symbols in such a way that they can detect and also correct errors in the information carrying symbols."<sup>48</sup> Working in conjunction with other methods such as interleaving, forward error correction proves especially beneficial to link maintenance.

### Proliferation And Multiple Satellite Systems

The majority of this chapter has focused on methods for enhancing the survivability of individual spacecraft. This is a logical progression given the United States' history of reliance on fewer, more expensive, multi-mission, and highly complex satellites. Proposals for proliferated satellite networks represent a major, alternative shift from this philosophy. By launching a multitude of spacecraft for a satellite constellation, each satellite's effective importance to the network would be lower, thus making it a less valued target. Additionally, an attacker would need to neutralize many more targets in order to inflict the same degree of system impact as compared to destroying one satellite in a non-proliferated network. Given budgeting constraints, this implies that each satellite would need to be less expensive so that overall system costs would approximate those for a non-proliferated network.

Included in this discussion are the ideas of redundancy and deploying spare satellites. This is a similar scenario except that these spares would not be active until called upon. From a cost perspective, spares would still need to be budgeted for, just as if they were active in the constellation. They could be placed into orbits relatively

inaccessible to enemy ASATs (super-synchronous) or stored in protective shelters until needed. Should the decision be made to leave them on the earth, then a requirement for a quick, "hot" launch capability would be necessary, including spare boosters and launch facility.

Regardless of the mode, the primary impetus behind employing a multi-satellite system (MSS) or deploying spare satellites would be to force an attacker to expend more resources countering an increased number of hardened or redundant targets and also to lengthen the period in which the orbital segment remains operational.<sup>49</sup> This latter requirement would be very important when considering our own C<sup>3</sup> capabilities.

As such a system has yet to be deployed, many different proposals for a MSS have been postulated. Short descriptions of three different proposals are presented.

Harkening back to the days of Echo satellites and recognizing the potential threats against today's satellites, Donadio presented a proposal advocating a move toward simpler, passive satellites. Such a constellation would employ many passive satellites where all of the actual communications and TT&C processing would take place at the ground stations. The proliferated satellites could best be described as simple reflectors operating in a network using either HF or SHF. Such a network of passive satellites would offer many advantages: 1) increased reliability due to the lack of electronic and moving parts, 2) jamming resistance due to frequency agility over a large transmission bandwidth, 3) lower costs, 4) imperviousness to HEMP, 5) lower susceptibility to active countermeasures, and 6) lighter weight which could translate to a savings in launch delivery cost and a wider selection of potential launch

vehicles.<sup>50</sup> The benefits derived from having minimal processing equipment on the spacecraft also create serious problems with satellite management and control. For example, how do you maintain proper orbital stability and earth coverage? What about the "missed opportunities" from not using on-board processing or crosslink capability between satellites? A spaceborne store-and-forward system would be difficult to implement with such a system and an argument could be made that too much reliance was being shifted back to ground stations.

The more common description of a MSS constellation would include from 120 to 240 active satellites at altitudes of approximately 740 km or from 300-400 nautical miles.<sup>51</sup> These satellites would form the space portion of a global packet switched network supporting thousands of earth terminals. The MSS satellites will be highly crosslinked providing increased redundancy and dynamic communications networking. Each satellite would contain an on-board processor, memory, transceiver, electronically steerable antennas, and the software required to operate as a store-and-forward switch. The satellites would be able to support advanced link and network protocols, as well as variable data rates. The on-board processing capability could also be used for satellite attitude control and antenna pointing.<sup>52</sup>

The challenges to production of such a system are numerous. The constant changes in the network topology, the large propagation delays on the links, and limitations on power consumption are just a few of the problems to be solved. To add complexity, the MSS constellation will permit a high degree of autonomy for its satellites. Each satellite would assume the burden of monitoring its own position and imparting this position data to its neighboring satellites (meaning less reliance upon

ground TT&C). This requires complex communications algorithms at both the network and data link layers to be developed. "Establishing, scheduling, maintaining, and terminating a useful set of communications links from the vast number of links available is a tremendous technical challenge."<sup>53</sup> Another problem to be conquered is the routing scheme for such a packet switched network. Each satellite in the MSS would be capable of performing autonomous scheduling and routing algorithms. This would enhance the overall survivability of the system since no single point would be used to control scheduling and assignment of routing paths. However, it is a difficult task to schedule communications links and packet routes in a multi-node system when each of the nodes is moving.<sup>54</sup> Finally, since these satellites will support C<sup>3</sup> traffic, they will have to be able to handle both data and voice (much more difficult) in a store-and-forward manner.

A similar proposal (Sharifi and Arozullah) would employ an architecture with three (two operational and one spare) geosynchronous satellites and a large number of simple, low altitude satellites. The geosynchronous satellites are called central satellite stations (CSS) and are capable of some signal processing. The low altitude satellites would be capable of no processing. In essence, responsibility for network coordination, communications processing, and TT&C have been shifted from the ground segment to the CSSs. The authors include a detailed discussion of multiple access techniques, satellite architecture, and very small aperture terminal usage for the ground stations.<sup>55</sup> See Figure 3 for a conceptual drawing of the CSSs and their connectivity to the low earth orbit satellites and the ground stations. From a survivability perspective, such a system seems to have certain glaring weaknesses.

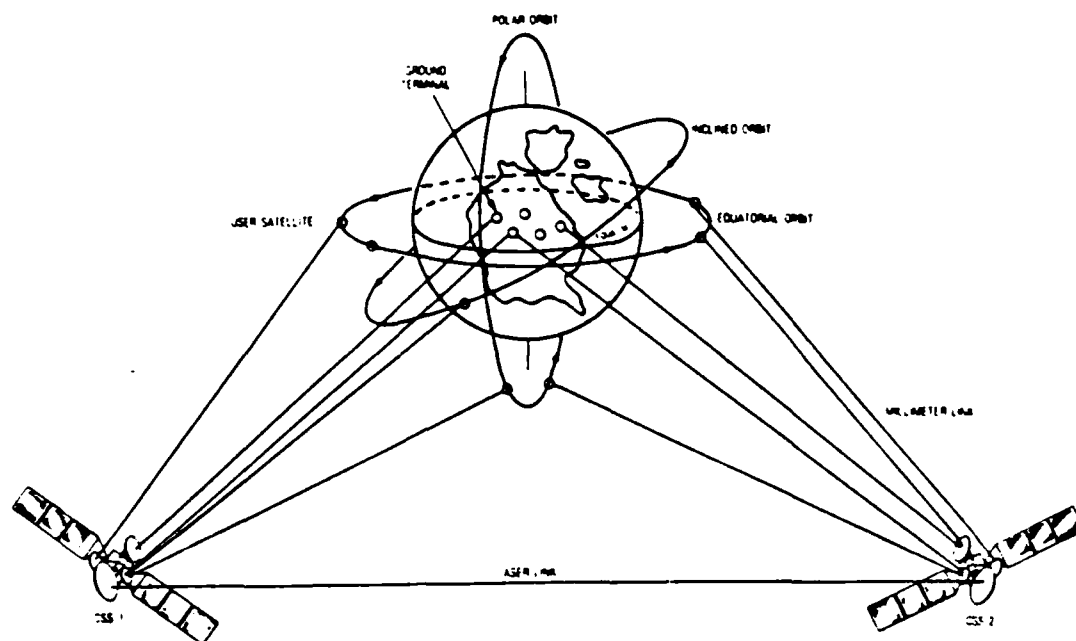


Figure 3. Multiple Satellite Network with Two Central Stations with On-Board Processing M User Satellites and L Small Ground Terminals

Source: Hossein M. Sharifi and Mohammed Arozullah, "A Centralized Multiple Satellite Network for Real Time Global Space, Land, and Mobile Communications", in Conference Record from IEEE Military Communications Conference (Washington, D.C.: Oct 19-22, 1987), p. 40.3.2.

While the CSSs solve many network control problems that would plague such a system, they also figure too prominently in the constellation. Too much processing capability is focused in one spot, making the constellation too reliant upon the CSSs. An adversary could do great damage to the network by attacking just one of the CSSs and could

totally neutralize it by destroying just three targets (the three CSSs). Also, while decreased sophistication of the low earth orbit satellites would bring down the cost per satellite (allowing for purchase of many satellites), the CSSs' and their complexity would likely carry a high price tag. Again, this would make the CSSs more lucrative targets.

Of the three options presented, the one most feasible from a survivability perspective would be an active constellation of many low earth orbiting satellites. This proposal is also the one being developed by both the Defense Advanced Research Projects Agency and the Rome Air Development Center and sponsored by the Strategic Defense Initiative Organization.<sup>56</sup>

## NOTES - CHAPTER IV

<sup>1</sup>Ashton B. Carter, "The Current and Future Military Uses of Space", in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Regime (Lanham, MD: The Aspen Institute for Humanistic Studies and the University Press of America, Inc., 1987), p. 64.

<sup>2</sup>Paul B. Stares, Space and National Security, (Washington, D.C.: The Brookings Institution, 1987), p. 83-4.

<sup>3</sup>Stares, p. 79.

<sup>4</sup>Joseph A. Poliakon, "System Issues and Considerations Associated with Design of Ground Mobile Strategic Satellite Communication Terminals", in Conference Record from IEEE Military Communications Conference, Oct 31 - Nov 2, 1983, Washington, D.C., p. 254.

<sup>5</sup>Timothy Curtis Gill and Robert Leigh Trapp, "A Model for Evaluating Communications Satellite Interoperability", Thesis submitted to the University of Colorado for the Air Force Institute of Technology, Wright-Patterson AFB, OH, Oct 1985, p. 96.

<sup>6</sup>Fred E. Bond, "Long Range MILSATCOM Architecture", in Conference Record from IEEE Military Communications Conference, Oct 17-20, 1982, Boston, p. 11.1-4.

<sup>7</sup>Stares, p. 82.

<sup>8</sup>"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process", Report prepared by Computer Sciences Corporation for the Defense Nuclear Agency, Jun 4, 1976, p. 5-72.

<sup>9</sup>Bond, p. 11.1-4.

<sup>10</sup>Heywood I. Paul, Charles B. Meader, Daniel A. Lyons, and David R. Ayers, "Forward Error Correction and Spatial Diversity Techniques for High-Data-Rate MILSATCOM over a Slow-Fading, Nuclear-Disturbed Channel", in Conference Record from IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., p. 11.4.1.

<sup>11</sup>Paul, Meader, Lyons, and Ayers, p. 11.4.1.

<sup>12</sup>Paul, Meader, Lyons, and Ayers, p. 11.4.1.

<sup>13</sup>Paul, Meader, Lyons, and Ayers, p. 11.4.1.



<sup>14</sup>Stares, p. 79.

<sup>15</sup>Stares, p. 78.

<sup>16</sup>William J. Perry, Brent Scowcroft, Joseph S. Nye, Jr., and James A. Shear, "Anti-Satellite Weapons and U.S. Military Space Policy: An Introduction", in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime (Lanham, MD: The Aspen Strategy Group and University Press of America, 1987), p. 13.

<sup>17</sup>Stares, p. 79.

<sup>18</sup>Carter, p. 63.

<sup>19</sup>Michael M. May, "Safeguarding Our Space Assets", in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Regime (Lanham, MD: The Aspen Institute for Humanistic Studies and the University Press of America, 1987), p. 78-9.

<sup>20</sup>May, p. 79.

<sup>21</sup>May, p. 80.

<sup>22</sup>Carter, p. 52.

<sup>23</sup>Carter, p. 60.

<sup>24</sup>Stares, p. 79.

<sup>25</sup>Carter, p. 39.

<sup>26</sup>Carter, p. 39.

<sup>27</sup>Peter Leahy, "MILCOM 83 Small AJ Satcom Terminal Considerations", in Conference Record from IEEE Military Communications Conference (Washington, D.C.: Oct 31 - Nov 2, 1983), p. 229.

<sup>28</sup>Dr. Thomas P. Quinn, "A Defense Department Perspective," from National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation, Oct 25-26, 1984 (Boston: MITRE Document M85-3, 1984), pp. 36.

<sup>29</sup>Leahy, p. 233.

<sup>30</sup>Leahy, p. 233.

<sup>31</sup>T. C. Tozer, "An Introduction to Military Satellite Communications," Memorandum No. 3976 of the Royal Signal & Radar Establishment, Malvern, England, Apr 1987, p. 23.

<sup>32</sup>Tozer, p. 28.

- 33Tozer, p. 23.
- 34Tozer, p. 25.
- 35Tozer, p. 28.
- 36Tozer, p. 25.
- 37Tozer, p. 25.
- 38Gill and Trapp, p. 74.
- 39Tozer, p. 25.
- 40Tozer, p. 25.
- 41Timothy Pratt and Charles W. Bostian, Satellite Communications (New York: John Wiley & Sons, 1986), p. 224.
- 42Robert M. Gagliardi, Satellite Communications (Belmont, CA: Lifetime Learning Publications, 1984), p. 267.
- 43Pratt and Bostian, p. 251.
- 44Gagliardi, p. 267.
- 45Pratt and Bostian, p. 251.
- 46Gagliardi, p. 268.
- 47Tozer, p. 27.
- 48R. Skaug and J. F. Hjelmstad, Spread Spectrum in Communication (London: Peter Peregrinus Ltd, 1985), p. 7.
- 49Stares, p. 80.
- 50Guiseppe Donadio, "Comparative Analysis of Passive Communications Satellites Employing the SHF and HF Spectrum for Use in a Strategic Role", Thesis submitted to the Naval Postgraduate School, Monterey, CA, Mar 1988, p. 1.
- 51Richard Binder and Dennis Perry, "The Multiple Satellite System - Low-Altitude Survivable Communications", in Conference Record from IEEE Military Communications Conference (Washington, D.C.: Oct 19-22, 1987), p. 30.3.1.
- 52Nachum Shacham, "Protocols for Multi-Satellite Networks", in Conference Record from IEEE Military Communications Conference (San Diego: Oct 23-26, 1988), p. 26.3.1.
- 53Brian Kaldenbach, David R. Geissler, and Edward W. Ver Hoef, "A System Simulator for Low Orbit Satellite Communication Network", in

Conference Record from IEEE Military Communications Conference (Washington, D.C.: Oct 19-22, 1987), p. 14.5.2.

<sup>54</sup>Kaldenbach, Geissler, and Ver Hoef, p. 14.5.2.

<sup>55</sup>Hossein M. Sharifi and Mahammed Arozullah, "A Centralized Multiple Satellite Network for Real Time Global Space, Land, and Mobile Communications", in Conference Record from IEEE Military Communications Conference (Washington, D.C.: Oct 19-22, 1987), p. 40.3.1.

<sup>56</sup>Kaldenbach, Geissler, and Ver Hoef, p. 14.5.1.

## CHAPTER V

### CONCLUSIONS

The survival of our military communications satellites plays a critical role in our ability to communicate during national emergencies or during trans and post-attack periods. These satellites form an integral cog in our national defense's telecommunications infrastructure. It is their unique requirement of being able to provide connectivity during times of stress or tension that differentiates them from commercial satellites. Long recognized as key elements in the command and control structure of the United States, technology advances now make it possible to launch attacks upon these satellites. Space conflict is no longer science fiction; but something that must be anticipated and for which we must be prepared.

Just as we have developed methods to attack satellites, so the Soviets have invested heavily in this capability. Our satellites are now vulnerable to many different types of threats and these threats will only continue to become more sophisticated and more capable. Likewise, we must develop methods for safeguarding our satellites and their capabilities. These survivability enhancements should be an integral design consideration from conception to deployment of our military communications satellites.

The survivability enhancement measures addressed in Chapter IV are listed in this table along with the corresponding threat that they are

poddesigned to combat. Certain measures appear as effective methods against multiple types of threats.

Table 3. Summary Table of Survivability Measures

<u>THREAT</u>	<u>SURVIVABILITY MEASURE</u>
Nuclear Effects	<ul style="list-style-type: none"> <li>-Outer surface constructed of special metals and materials to reduce SGEMP</li> <li>-Faraday cages used to shield inner electrical components</li> <li>-Cables can be wrapped in copper foil or materials of lower atomic number to reduce the available electrons</li> <li>-Electronic components should be made resistant to large electrical surges and other radiation effects</li> <li>-Shielding, filtering, electrical bonding, chokes, spare gaps, zener diodes, surge arrestors, surge suppressors, cable/wire bundling, circuit design, and grounding can all be used to shield against or limit EMP induced currents and voltages</li> <li>-Use of upper frequency bands, especially EHF</li> <li>-Stressed mode of operation where a user falls back to a slower data rate such as 75 or 2,400 BPS</li> <li>-Use FEC encoding with Reed-Solomon codes, spatial diversity, and interleaving to mitigate errors for a nuclear-affected, slow-fading channel</li> </ul>
ASATs	<ul style="list-style-type: none"> <li>-Employ stealth technologies to reduce the satellite's radar cross-section and thus its chances of being detected. These include:               <ol style="list-style-type: none"> <li>1) Using small nuclear generators instead of large solar panels</li> <li>2) Coat the outside of the satellite with radar absorbing materials and paints</li> </ol> </li> <li>-Deploy satellites in high altitude (super-synchronous) orbits or widely separated orbital planes. This decreases effects of land-based directed energy weapons and increases the warning time of an attack.</li> <li>-Incorporate certain ablative materials (generally graphite derivatives) into the spacecraft's exterior to shield against laser thermal effect</li> </ul>

Table 3. Continued

- Use special shutters and filters to prevent laser blinding of on-board sensors
- Provide for spacecraft maneuverability
- Use sensors to warn the spacecraft of radar illumination or potential ASAT attack. Sensors could also be used to initiate evasive action through maneuverability
- Employ on-board processing to process warning information and to initiate evasive maneuvering
- Sensors should be sensitive to frequencies that are opaque to the earth's atmosphere to lessen their susceptibility to blinding from ground-based lasers
- Use low-sensitivity sensors that scan areas before the main sensor. Should damaging laser energy be detected, then a shutter could be drawn over the main shutter's aperture
- Satellite might dispense decoys or infrared flares to disrupt an ASAT's homing mechanism
- On-board radar jamming capability might be useful to jam an ASAT's radar homing capability

#### ECM Techniques

- Use of EHF provides:
  - 1) Greater information-carrying capacity,
  - 2) Makes room for error correction coding and encryption,
  - 3) Wide channel to use spread spectrum over,
  - 4) Exploitation of low-probability-of-intercept techniques,
  - 5) Smaller antenna dishes,
  - 6) Exploitation of narrow beamwidths brings abilities to strike narrow portions of earth and employ spatial rejection. Also makes use of null steering antennas easiers.
- Use of null steering antennas
- Employ on-board processing to:
  - 1) Operate null steering antennas,
  - 2) Make satellite more autonomous by processing its own TT&C,
  - 3) Facilitate use of spread spectrum tech,
  - 4) Facilitate use of CDMA,
  - 5) Facilitate on-board routing of circuits to crosslinks or downlinks, &
  - 6) Steer laser crosslinks.
- Use spread spectrum technology
- Use CDMA
- Use laser crosslinks
- Use error correction coding and interleaving

Another method of enhancing the survivability of a satellite communications constellation would be to use a proliferated employment plan. This would require an adversary to destroy many more targets to achieve the same degrading effect as destroying only one satellite in a non-proliferated system.

## BIBLIOGRAPHY

### Books

Bulkeley, Rip, and Graham Spinardi. Space Weapons: Deterrence or Delusion? Totowa, NJ: Barnes & Noble Books, 1986.

Carter, Ashton B. "The Current and Future Military Uses of Space." in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: The Aspen Strategy Group and University Press of America, 1987, pp. 29- 69.

Gagliardi, Robert M. Satellite Communications. Belmont, CA: Lifetime Learning Publications, 1984.

Gray, Colin S. American Space Policy: Information Systems, Weapon Systems and Arms Control. Cambridge, MA: Abt Books, 1982.

May, Michael M. "Safeguarding Our Space Assets." in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: Aspen Strategy Group and University Press of America, 1987, pp. 71 - 85.

Perry, William J., Brent Scowcroft, Joseph S. Nye, Jr., and James A. Shear. "Anti-Satellite Weapons and U.S. Military Space Policy: An Introduction" in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: Aspen Strategy Group and University Press of America, 1987, pp. 1 - 28.

Pratt, Timothy, and Charles W. Bostian. Satellite Communications. New York: John Wiley & Sons, 1986.

Roddy, D. Satellite Communications. Englewood Cliffs, NJ Prentice Hall, 1989.

Skaug, R., and J. F. Hjelmstad. Spread Spectrum in Communication. London: Peter Peregrinus Ltd, 1985.

Stares, Paul B. The Militarization of Space. Ithaca, NY: Cornell University Press, 1985.

Stares, Paul B. Space and National Security. Washington, D.C.: The Brookings Institution, 1987.

Van Trees, Harry L. ed. Satellite Communications. New York: IEEE Press, 1979.



## Conference Proceedings

Binder, Richard, and Dennis Perry. "The Multiple Satellite System - Low-Altitude Survivable Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 30.3.1. - 30.3.6.

Bond, Fred E. "Long Range MILSATCOM Architecture." IEEE Military Communications Conference, Oct 17-20, 1982, Boston, Conference Record, pp. 11.1.1 - 11.1.5.

Boyd, R. W., S. L. Adams, M. I. Spellman, and L. V. Lucas. "Survivable Space Networks: The Physical Layer." IEEE Military Communications Conference, Oct 23-26, 1988, San Diego, Conference Record, pp. 26.6.1 - 26.6.6.

Cook, Charles W. "The U.S. Air Force Space Program." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, MITRE Document M85-3, pp. 39 - 42.

Cooper, Robert S. "Space Challenges." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, MITRE Document M85-3, pp. 65 - 72.

Day, M. H., and C. M. Lockhart. "Survivable Network Planning at AT&T Bell Laboratories." IEEE Military Communications Conference, Oct 5-9, 1986, Monterey, CA, Conference Record, pp. 24.1.1 - 24.1.4.

Frankel, Michael S. "Survivable Command, Control, and Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 30.1.1 - 30.1.4.

Hoernig, O. W., Jr., and D. R. Sood. "Command System Protection for Commercial Communication Satellites." IEEE Military Communications Conference, Oct 5-9, 1986, Monterey, CA, Conference Record, pp. 3.5.1 - 3.5.6.

Kaldenbach, Brian, David R. Geissler, and Edward W. Ver Hoef. "A System Simulator for Low Orbit Satellite Communication Network." IEEE Military Communications Conference, Oct 19-22, 1987,

Washington, D.C., Conference Record, pp. 14.5.1- 14.5.5.

Leahy, Peter. "Small AJ Satcom Terminal Considerations." IEEE Military Communications Conference, Oct 31 - Nov 2, 1983, Washington, D.C., Conference Record, pp. 229-233.

Paul, Heywood I., Charles B. Meader, Daniel A. Lyons, and David R. Ayers. "Forward Error Correction and Spatial Diversity Techniques for High-Data Rate MILSATCOM over a Slow-Fading Nuclear-Disturbed Channel." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 11.4.1 - 11.4.5.

Poliakon, Joseph A. "System Issues and Considerations Associated with Design of Ground Mobile Strategic Satellite Communication Terminals." IEEE Military Communications Conference, Oct 31 - Nov 2, 1983, Washington, D.C., Conference Record, pp. 253-258.

Quinn, Thomas P. "A Defense Department Perspective." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>2</sup>, MITRE Document M85-3, pp. 35 - 38.

Shacham, Nachum. "Protocols for Multi-Satellite Networks." IEEE Military Communications Conference, Oct 23-26, 1988, San Diego, Conference Record, pp. 26.3.1 - 26.3.5.

Sharifi, Hossein M., and Mahammed Arozullah. "A Centralized Multiple Satellite Network for Real Time Global Space, Land, and Mobile Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 40.3.1 - 40.3.5.

#### Government Documents

Donadio, Giuseppe. "Comparative Analysis of Passive Communications Satellites Employing the SHF and HF Spectrum for Use in a Strategic Role." Thesis submitted to the Naval Postgraduate School, Monterey, CA, Mar 1988.

Gill, Timothy Curtis, and Robert Leigh Trapp. "A Model for Evaluating Communications Satellite Interoperability." Thesis submitted to the University of Colorado for the Air Force Institute of Technology, Wright-Patterson AFB, OH, Oct 1985.

"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process." Report prepared by Computer Sciences Corporation for the Defense Nuclear Agency, Jun 4, 1976.

Murdock, William P., Jr. "Alternative Force Structuring Strategies for Military Satellite Communication Systems." Thesis submitted to the Air Force Institute of Technology, Wright-Patterson AFB, OH, Dec 1987.

Phillips, Barbara A. "A Prototype Knowledge-Based System to Aid Space System Restoration Management." Thesis submitted to the Air Force Institute of Technology, Dec 1986.

Stover, Harris A. "Engineering Aids for the Design of Survivable Defense Communications Transmission Capability." Technical Note 11-82. Defense Communications Agency, Jan 1984.

Townley, Ralph K., David W. Brown, Martin O. Bernet, and Bernard L. Pankowski. "Selected Issues in DCS Integration." Technical paper prepared by Computer Sciences Corporation for the Defense Communications Agency, Aug 1987.

Tozer, T. C. "An Introduction to Military Satellite Communications." Memorandum No. 3976 of the Royal Signals & Radar Establishment. Malvern, England, Apr 1987.

#### Periodicals

Gits, Victoria. "Ball Project Part of 'Star Wars' Test." Daily Camera, Feb 15, 1990, Sec A, pp. 1 and 11.

Hughes, David. "Milstar Terminal Capability Demonstrated as Congress Debates Program Budget." Aviation Week & Space Technology, Oct 30, 1989, pp. 49-50.

Klass, Philip J. "Gains in Satellite Technology Shape Trends in C<sup>3</sup> Development." Aviation Week & Space Technology, Mar 20, 1989, pp. 251-253.

Perroots, Leonard H. "Soviet Beam Weapons are Near Tactical Maturity." Signal, Mar 1990, pp. 37-39.

## APPENDIX

To augment the narrative, certain existing and emerging system's survivability enhancements are offered as examples. Since all of the chosen examples are military systems, much of the information about them is classified. Still, some of the descriptions are open or enough is known about them for accurate speculation to be conducted. The first example is the Defense Satellite Communications System (DSCS) III which is a follow-on to DSCS II. The second is not a communications satellite system at all, but a navigational system called the Global Positioning System (GPS) or NAVSTAR. It is included since there is open information about this system and many of its survivability enhancements would be the same type used on a communications satellite. The third and final system is the MILSTAR (Military Strategic and Tactical Relay System) system. This satellite system has been under development for over fifteen years and was designed to enhance the overall C<sup>3</sup> capability of the Department of Defense.

### DSCS III

DSCS III was designed as an upgrade to the aging DSCS II satellites. It provides more jamming protection and more flexible transmission and coverage than its predecessor. In addition to SHF capability (7-8 GHz), it also carries a transponder capable of EHF transmissions (30 GHz up and 20 GHz down). (This information was

printed in 1982 and seems to conflict with more recent articles which do not attribute EHF capability to the DSCS III). DSCS III will incorporate wideband spread spectrum and antenna nulling for significant jamming protection.<sup>1</sup>

The spacecraft will also have multibeam antennas, encrypted telemetry, and hardened design.<sup>2</sup>

### NAVSTAR

The NAVSTAR system was designed to provide extremely accurate global positioning information to any authorized user. Although not a communications system, it does provide a good, unclassified source of information on what types of survivability enhancements have been incorporated into recent spacecraft.

Ashton Carter claims that the following survivability enhancements have been incorporated into the GPS satellites:

These satellites have: crosslinks with antenna nulls directed toward earthbound jammers, mobile ground segments, special data coding to get through the ionosphere when its free-electron density distribution is altered by nuclear bursts, irregular orbit phasing to complicate the orbital mechanics for interceptors, radiation hardening, and other features that increase the attack price of the constellation.<sup>4</sup>

Even though the primary function of this constellation is to provide navigational information, it still must relay this information through communications links. Therefore, it must similarly protect these communications links. The following table provides an excellent summary of the comparison between attack method and the corresponding protective measure incorporated into the global positioning system.

Table 4. NAVSTAR Survivability Features

Attack Method	Protective Measures
Intercept	Graceful degradation Many planes Irregular phasing On-orbit spares Nuclear hardening Propulsion module (?)
Laser	Resistant to warming
Mines	Unique orbit
Ground segment destruction	Crosslinks Mobile ground stations Satellite autonomy
Electronic attack	NDS receiver on airborne command posts Encryption via pseudorandom noise sequence (PRN) Uplink antijam via coding and crosslinks Downlink antijam via PRN, nulling antennas, and spatial diversity Crosslink antijam via frequency hopping and antenna nulls
Nuclear effects	Radiation hardened satellites Automatic restart after transient upset EMP hardening of receivers for nuclear users Compression and coding for NDS downlink data Spatial diversity

Source: Ashton B. Carter, "The Current and Future Military Uses of Space", in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Regime (Lanham, MD: The Aspen Institute for Humanistic Studies and the University Press of America, Inc., 1987), p. 65.

### MILSTAR

The MILSTAR constellation, should it survive Congressional budget cuts, will prove to be our most complex space communications venture. It is designed to provide secure communications during and after a nuclear attack. According to an Aviation Week & Space Technology

article, "The Pentagon has identified Milstar as its top priority program in command, control, and communications (C<sup>3</sup>), and Defense Dept. officials continue to reiterate their support for the program."<sup>3</sup> In another Aviation Week & Space Technology article, MILSTAR is said to be the DoD's first operational space communications system to operate in the EHF range.<sup>4</sup> (This lends doubt to the idea that DSCS III has an EHF capability). The advantages to the use of EHF are addressed in the text of the thesis. MILSTAR will provide our strategic and tactical forces with an extremely survivable narrowband capability. This survivability will be provided through extensive antijam measures facilitated by on-board signal processing, satellite crosslinks, antenna nulling, hardening, and autonomous operation.<sup>5</sup> MILSTAR will also incorporate "an advanced frequency-hopping technique to minimize the risk of outage from enemy jamming."<sup>6</sup>

The MILSTAR constellation will have satellites in both geosynchronous and highly elliptical inclined orbits. The constellation will be highly internettted with both ground and satellite crosslinks.

## NOTES - APPENDIX

<sup>1</sup>Fred E. Bond, "Long Range MILSATCOM Architecture", in Conference Record from IEEE Military Communications Conference, Oct 17-20, 1982, Boston, p. 11.1-4.

<sup>2</sup>Harry L. Van Trees, ed., Satellite Communications (New York: IEEE Press, 1979), pp. 53, 56, and 60.

<sup>3</sup>David Hughes, "Milstar Terminal Capability Demonstrated as Congress Debates Program Budget", Aviation Week & Space Technology, Oct 30, 1989, p. 49.

<sup>4</sup>Philip J. Klass, "Gains in Satellite Technology Shape Trends in C<sup>3</sup> Development", Aviation Week & Space Technology, Mar 20, 1989, p. 251.

<sup>5</sup>Dr. Thomas P. Quinn, "A Defense Department Perspective," from National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the MITRE Corporation, Oct 25-26, 1984 (Boston: MITRE Document M85-3, 1984), pp. 36.

<sup>6</sup>Klass, p. 251.



## BIBLIOGRAPHY

### Books

Bulkeley, Rip, and Graham Spinardi. Space Weapons: Deterrence or Delusion? Totowa, NJ: Barnes & Noble Books, 1986.

Carter, Ashton B. "The Current and Future Military Uses of Space." in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: The Aspen Strategy Group and University Press of America, 1987, pp. 29- 69.

Gagliardi, Robert M. Satellite Communications. Belmont, CA: Lifetime Learning Publications, 1984.

Gray, Colin S. American Space Policy: Information Systems, Weapon Systems and Arms Control. Cambridge, MA: Abt Books, 1982.

May, Michael M. "Safeguarding Our Space Assets." in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: Aspen Strategy Group and University Press of America, 1987, pp. 71 - 85.

Perry, William J., Brent Scowcroft, Joseph S. Nye, Jr., and James A. Shear. "Anti-Satellite Weapons and U.S. Military Space Policy: An Introduction" in Seeking Stability in Space: Anti-Satellite Weapons and the Evolving Space Regime. Lanham, MD: Aspen Strategy Group and University Press of America, 1987, pp. 1 - 28.

Pratt, Timothy, and Charles W. Bostian. Satellite Communications. New York: John Wiley & Sons, 1986.

Roddy, D. Satellite Communications. Englewood Cliffs, NJ Prentice Hall, 1989.

Skaug, R., and J. F. Hjelmstad. Spread Spectrum in Communication. London: Peter Peregrinus Ltd, 1985.

Stares, Paul B. The Militarization of Space. Ithaca, NY: Cornell University Press, 1985.

Stares, Paul B. Space and National Security. Washington, D.C.: The Brookings Institution, 1987.

Van Trees, Harry L. ed. Satellite Communications. New York: IEEE Press, 1979.

## Conference Proceedings

- Binder, Richard, and Dennis Perry. "The Multiple Satellite System - Low-Altitude Survivable Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 30.3.1. - 30.3.6.
- Bond, Fred E. "Long Range MILSATCOM Architecture." IEEE Military Communications Conference, Oct 17-20, 1982, Boston, Conference Record, pp. 11.1.1 - 11.1.5.
- Boyd, R. W., S. L. Adams, M. I. Spellman, and L. V. Lucas. "Survivable Space Networks: The Physical Layer." IEEE Military Communications Conference, Oct 23-26, 1988, San Diego, Conference Record, pp. 26.6.1 - 26.6.6.
- Cook, Charles W. "The U.S. Air Force Space Program." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, MITRE Document M85-3, pp. 39 - 42.
- Cooper, Robert S. "Space Challenges." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, MITRE Document M85-3, pp. 65 - 72.
- Day, M. H., and C. M. Lockhart. "Survivable Network Planning at AT&T Bell Laboratories." IEEE Military Communications Conference, Oct 5-9, 1986, Monterey, CA, Conference Record, pp. 24.1.1 - 24.1.4.
- Frankel, Michael S. "Survivable Command, Control, and Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 30.1.1 - 30.1.4.
- Hoernig, O. W., Jr., and D. R. Sood. "Command System Protection for Commercial Communication Satellites." IEEE Military Communications Conference, Oct 5-9, 1986, Monterey, CA, Conference Record, pp. 3.5.1 - 3.5.6.
- Kaldenbach, Brian, David R. Geissler, and Edward W. Ver Hoef. "A System Simulator for Low Orbit Satellite Communication Network." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 14.5.1- 14.5.5.
- Leahy, Peter. "Small AJ Satcom Terminal Considerations." IEEE Military Communications Conference, Oct 31 - Nov 2, 1983, Washington, D.C., Conference Record, pp. 229-233.

Paul, Heywood I., Charles B. Meader, Daniel A. Lyons, and David R. Ayers. "Forward Error Correction and Spatial Diversity Techniques for High-Data Rate MILSATCOM over a Slow-Fading Nuclear-Disturbed Channel." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 11.4.1 - 11.4.5.

Poliakon, Joseph A. "System Issues and Considerations Associated with Design of Ground Mobile Strategic Satellite Communication Terminals." IEEE Military Communications Conference, Oct 31 - Nov 2, 1983, Washington, D.C., Conference Record, pp. 253-258.

Quinn, Thomas P. "A Defense Department Perspective." Proc. of a Symposium sponsored by the USAF Electronic Systems Division and the Mitre Corporation. Oct 25-26, 1984, Boston, National Security Issues Symposium, 1984: Space, National Security, and C<sup>3</sup>I, MITRE Document M85-3, pp. 35 - 38.

Shacham, Nachum. "Protocols for Multi-Satellite Networks." IEEE Military Communications Conference, Oct 23-26, 1988, San Diego, Conference Record, pp. 26.3.1 - 26.3.5.

Sharifi, Hossein M., and Mahammed Arozullah. "A Centralized Multiple Satellite Network for Real Time Global Space, Land, and Mobile Communications." IEEE Military Communications Conference, Oct 19-22, 1987, Washington, D.C., Conference Record, pp. 40.3.1 - 40.3.5.

#### Government Documents

Donadio, Giuseppe. "Comparative Analysis of Passive Communications Satellites Employing the SHF and HF Spectrum for Use in a Strategic Role." Thesis submitted to the Naval Postgraduate School, Monterey, CA, Mar 1988.

Gill, Timothy Curtis, and Robert Leigh Trapp. "A Model for Evaluating Communications Satellite Interoperability." Thesis submitted to the University of Colorado for the Air Force Institute of Technology, Wright-Patterson AFB, OH, Oct 1985.

"Investigation of the Vulnerability/Survivability of Systems Supporting the NCA Decision Process." Report prepared by Computer Sciences Corporation for the Defense Nuclear Agency, Jun 4, 1976.

Murdock, William P., Jr. "Alternative Force Structuring Strategies for Military Satellite Communication Systems." Thesis submitted to the Air Force Institute of Technology, Wright-Patterson AFB, OH, Dec 1987.

Phillips, Barbara A. "A Prototype Knowledge-Based System to Aid Space System Restoration Management." Thesis submitted to the Air Force Institute of Technology, Dec 1986.

Stover, Harris A. "Engineering Aids for the Design of Survivable Defense Communications Transmission Capability." Technical Note 11-82. Defense Communications Agency, Jan 1984.

Townley, Ralph K., David W. Brown, Martin O. Bernet, and Bernard L. Pankowski. "Selected Issues in DCS Integration." Technical paper prepared by Computer Sciences Corporation for the Defense Communications Agency, Aug 1987.

Tozer, T. C. "An Introduction to Military Satellite Communications." Memorandum No. 3976 of the Royal Signals & Radar Establishment. Malvern, England, Apr 1987.

#### Periodicals

Gits, Victoria. "Ball Project Part of 'Star Wars' Test." Daily Camera, Feb 15, 1990, Sec A, pp. 1 and 11.

Hughes, David. "Milstar Terminal Capability Demonstrated as Congress Debates Program Budget." Aviation Week & Space Technology, Oct 30, 1989, pp. 49-50.

Klass, Philip J. "Gains in Satellite Technology Shape Trends in C<sup>3</sup> Development." Aviation Week & Space Technology, Mar 20, 1989, pp. 251-253.

Perroots, Leonard H. "Soviet Beam Weapons are Near Tactical Maturity." Signal, Mar 1990, pp. 37-39.