

MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963-A

①

AD-A156 970

COMMERCIAL/MILITARY COMMUNICATIONS
SATELLITE SYSTEMS INTEROPERABILITY

by

David Martin Skiver

B.S., United States Air Force Academy, 1977

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

1984

DTIC
ELECTE
JUL 15 1985
S G D

DTIC FILE COPY

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

85 06 24 098

UNCLASS

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM	
1. REPORT NUMBER AFIT/CI/NR 85-38T	2. GOVT ACCESSION NO. A11-A 156 470	3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle) Commercial/Military Communications Satellite Systems Interoperability		5. TYPE OF REPORT & PERIOD COVERED THESIS/DISSERTATION	
		6. PERFORMING ORG. REPORT NUMBER	
7. AUTHOR(s) David Martin Skiver		8. CONTRACT OR GRANT NUMBER(s)	
9. PERFORMING ORGANIZATION NAME AND ADDRESS AFIT STUDENT AT: University of Colorado		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS	
11. CONTROLLING OFFICE NAME AND ADDRESS AFIT/NR WPAFB OH 45433		12. REPORT DATE 1984	
		13. NUMBER OF PAGES 96	
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASS	
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE	
16. DISTRIBUTION STATEMENT (of this Report) APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED			
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report) }			
18. SUPPLEMENTARY NOTES APPROVED FOR PUBLIC RELEASE: IAW AFR 190-1X Lynn E. Wolaver, Dean for Research and Professional Development (4 Mar 86) AFIT, Wright-Patterson AFB OH			
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)			
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) ATTACHED			

DD FORM 1473

1 JAN 73

EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASS

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

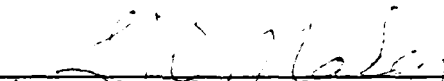
Skiver, David Martin (M.S., Telecommunications)

Commercial/Military Communications Satellite
Systems Interoperability

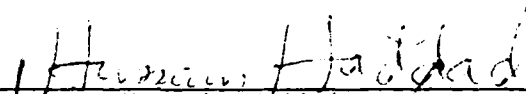
Thesis directed by Professor Samuel W. Maley

This thesis describes the Commercial Satellite Survivability (CSS) Task Force's recommendations for commercial-to-commercial and commercial-to-military satellite interoperability, commercial satellite security and survivability, and the legal/regulatory ramifications of commercial satellite vendors' cooperative efforts to provide a viable, nationwide, emergency satellite communications network. Once these proposals are described and summarized, this thesis then expounds upon each in an individual chapter in order to ascertain the magnitude of effort involved in each proposal, as well as its feasibility for implementation. Finally, conclusions are drawn and recommendations are proposed based upon the previous discussion.

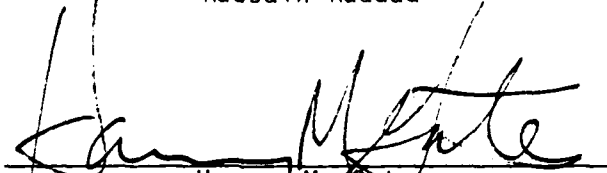
This Thesis for the Master of Science Degree by
David Martin Skiver
has been approved for the
Program in Telecommunications
by



Samuel W. Maley



Hussain Haddad



Harvey M. Gates

Accession For	<input checked="" type="checkbox"/>
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
and/or	
and	

A/1

Date 27 Nov 1977

Skiver, David Martin (M.S., Telecommunications)

Commercial/Military Communications Satellite
Systems Interoperability

Thesis directed by Professor Samuel W. Maley

This thesis describes the Commercial Satellite Survivability (CSS) Task Force's recommendations for commercial-to-commercial and commercial-to-military satellite interoperability, commercial satellite security and survivability, and the legal/regulatory ramifications of commercial satellite vendors' cooperative efforts to provide a viable, nationwide, emergency satellite communications network. Once these proposals are described and summarized, this thesis then expounds upon each in an individual chapter in order to ascertain the magnitude of effort involved in each proposal, as well as its feasibility for implementation. Finally, conclusions are drawn and recommendations are proposed based upon the previous discussion.

ACKNOWLEDGMENTS

This thesis could not have been written without the assistance and encouragement of many people. I would like to thank the members of my committee, Dr. Samuel Maley, Dr. Hussain Huddad, and Dr. Harvey Gates for their assistance and comments. A special thanks to the librarians of the U.S. Department of Commerce Boulder Laboratories Library for their assistance during my research, and to Mrs. Maureen Detmer who took the time from her busy schedule to professionally prepare this final copy.

Without the love and encouragement of my wife, Julieann, I seriously doubt I could have completed this thesis. She endured many evenings of thesis preparation, always thinking of me first, and herself second. My greatest thanks I would like to extend to my Lord Jesus Christ who gives us the wisdom and strength to persevere through any and all adversities.

CONTENTS

CHAPTER

I. INTRODUCTION.....	1
Notes.....	5
II. RECOMMENDATIONS OF THE COMMERCIAL SATELLITE SURVIVABILITY TASK FORCE.....	6
Commercial Satellite Communications Survivability Program and CSS Program Office.....	6
Contingency Plans and Emergency Procedures.....	8
Communications and TT&C Interoperability.....	9
System Security.....	12
System Survivability.....	13
Funding and Regulatory Issues.....	15
Notes.....	17
III. INTEROPERABILITY.....	18
Commercial Satellite Corporations.....	19
Military Satellite Systems.....	22
Technical Aspects of Interoperability.....	26
Seven-Level Model.....	26
Antenna Agility.....	30
Polarization Agility.....	31
Frequency Agility.....	32
T-1 Carrier.....	32
Military/Commercial Interoperability.....	33
Terrestrial/Satellite System Interface.....	34

CONTENTS (continued)

CHAPTER

III. (continued)

Telemetry and Control Interoperability..... 38

Notes..... 43

IV. SECURITY AND SURVIVABILITY..... 46

Electronic Intrusion..... 48

Encryption..... 48

Anti-Jam Techniques..... 53

Physical Protection - Non-Nuclear..... 54

Physical Protection - Nuclear..... 58

How Much is Enough?..... 64

Notes..... 66

V. LEGAL/REGULATORY ISSUES..... 70

History of Common Carrier Regulation..... 71

Today's Deregulation/Pro-Market Emphasis..... 74

Effects of Competitive Forces on the
CSS Task Force Proposals..... 77

Notes..... 80

VI. CONCLUSIONS/RECOMMENDATIONS..... 82

Proposal Prioritization..... 83

Cost Distribution..... 87

A Final Look..... 89

Summary..... 90

Notes..... 92

BIBLIOGRAPHY..... 93

FIGURES

Figure

1	MILSATCOM Evolution.....	22
2	INSAT Computer Software.....	41

DISCLAIMER

The opinions expressed are those of the author, and do not necessarily reflect the views of the United States Air Force, the Department of Defense, or any other government agency. No classified material was used in the production of this thesis. Review of this thesis by Department of Defense personnel does not necessarily constitute an endorsement.

CHAPTER I

INTRODUCTION

On September 13, 1982, President Reagan issued Executive Order 12382 entitled, "President's National Security Telecommunications Advisory Committee." According to this order, the NSTAC is to be comprised of not more than 30 members with knowledge and expertise in the telecommunications field and representing various elements of the nation's telecommunications industry. Its function is to provide the President with the necessary technical knowledge and advice from the perspective of the telecommunications industry regarding the feasibility of implementing measures to improve the telecommunications aspects of our national security, as well as identifying and solving problems which may affect the same. In addition, the NSTAC will conduct studies necessary to implement Presidential Directive 53, National Security Telecommunications Policy, and make the findings of such reports and periodic reviews known to the President and Secretary of Defense.¹

The NSTAC's first formal meeting took place on December 14, 1982, to recognize the need to make commercial communications satellites interoperable with military systems and each other, as well as "to emphasize commercial satellite communication survivability initiatives as a matter of priority."² Because of the fact that this nation

has no common, nationally owned communications satellite system, the NSTAC recognized the need to develop an interoperable, secure, survivable system from the fragmented satellite industry. In consonance with the recognition of this need, the NSTAC established the Commercial Satellite Survivability (CSS) Task Force to conduct a study with the following goals in mind:³

1. Enhance the interoperability and survivability of commercial satellite communications systems to provide responsive satellite networks for communications during emergency periods.
2. Protect the satellite command system to assure that only the intended signals are received and processed by the satellite.
3. Provide a capability for interoperability and survivability of TT&C functions so that a satellite system in need of TT&C assistance can call upon at least one alternate operator or common control center.
4. Reduce vulnerability of TT&C facilities and communications earth stations to disruption through sabotage or damage from hostile actions.
5. Assess the susceptibility of commercial communications satellites to nuclear effects and establish hardening guidelines for future programs.

Based on these goals, the CSS Task Force published a document entitled, "Commercial Satellite Communications Survivability Report, May 20, 1983." In this report the CSS Task Force made the following recommendations:⁴

1. ... the Government establish a commercial satellite communications survivability program with appropriate funding ...
2. ... the Government establish a CSS Program Office to coordinate the program ...
3. ... the CSS Program Office ... should ... develop emergency plans and procedures to assure ... the restoration of com-

planning, design, and development of equipment, software, etc., needed for implementation. Operational and maintenance costs associated with implementation on a continuing basis would also increase. Finally, there would be a decrease in earning/revenue potential, because for every pound of redundant, hardening, and other hardware required for security and survival aboard the spacecraft, a pound of revenue-producing equipment is lost due to the finite payload capacity of satellite launchers. The Task Force recommended the following financial incentives:

1. Some form of subsidy;
2. Launch incentives such as cost reduction and scheduling priority;
3. Investment Tax Credit;
4. Special transponder lease fees;
5. Rate base adjustment;
6. Warranty payback; and
7. Regulatory protection.

This paper will not explore these funding recommendations further.

In regard to the legal issues, the recommendations called for commercial companies to cooperate for planning, for exchanging operating and proprietary information, and for developing capabilities for interoperability. The Task Force realized that there are certain legal/regulatory limitations to these initiatives which must be explored and dealt with to ensure a smooth operation.

At this time, it is appropriate to explore in more detail the communications and TT&C interoperability recommendations.

study to determine its needs in this area as to such factors as geographic distribution, survivable storage facilities, manpower requirements, maintenance procedures, power needs, and transportation arrangements to ensure the most systematic, economically sound deployment of the mobile terminals.

As far as nuclear susceptibility and hardening is concerned, the Task Force recognized that although all commercial satellites are designed against the natural environment, virtually no protection is afforded against a nuclear threat. The potential for a "nuclear event" in space constitutes a sufficient threat to warrant hardening considerations; therefore, the Task Force recommended a study to:

1. Identify satellite susceptibilities and vulnerabilities;
2. Develop hardening guidelines;
3. Determine hardening impacts on such factors as cost, scheduling, and performance; and
4. Develop long-range plans and policies.

Funding and Regulatory Issues

Two major concerns raised by the Task Force were how the initiatives/recommendations were to be funded and what were the legal/regulatory impacts and antitrust issues arising from the cooperative efforts to implement the recommended emergency procedures among those supposedly competing with each other. The proposed recommendations would have significant impact on three financial aspects. The first would be increased acquisition costs for such things as one-time

first recommended the development of a capability to enhance satellite control system survivability by achieving command link protection. Secondly, a study to assess commercial satellite susceptibility to nuclear effects was proposed. The Task Force did not believe that a single solution for control/command link survivability was available in the near term, nor may a single solution be particularly desirable where survivability is concerned. The first step would be to encourage industry to voluntarily incorporate command link protection into their spacecraft systems, with government support via the National Security Agency (NSA). As a long-term initiative for both command link and communications survivability, the Task Force proposed the development of a transportable terminal which could be used to:

1. Enhance the restoration of critical communication links in emergencies;
2. Extend communications to emergency, isolated locations;
3. Provide for the interim restoral of system connectivity under stressed conditions; and
4. Support the other objectives of communications interoperability, communications security, and physical security.

These mobile facilities could be stored in secure and/or remote locations, and be relocated where and when necessary. The terminals would be comprised of all the communications/control equipment required for independent operation, including power and antenna systems, should the particular system being replaced have been completely destroyed. The Task Force recommended that the government conduct a

ical security of both satellite TT&C and communications earth stations. As a first step, they recommended that minimum security levels for such stations be established and a program implemented to meet those levels by identifying critical control and communication sites and determining what would be necessary to bring each site up to the required security level. This would be done in conjunction with the second step which would be for industry to conduct a site-by-site survey to assess security upgrade requirements, including consideration for sufficient backup power. The next step would be for the actual security upgrade, including the provision of critical supplies during times of emergencies. Finally, the government should be able and prepared to provide government security forces during times of national emergencies.

In the December 1983 report addendum, the Task Force specifically recommended against any initiative to locate commercial earth terminals on government property. Their argument was that to provide the best service at the lowest cost, the earth terminals should be located in close proximity to the communities to which they provide service. Locating such terminals on government property to provide non-government service would not be cost justified by the slight improvement in protection provided, especially since such action still does not ensure overall system integrity.

System Survivability

The recommendations given by the Task Force for commercial satellite communications system survivability were two-fold. They

long-term considerations would be more appropriately discussed in the system survivability section of this chapter.

System Security

The Task Force recommended the development of a capability which uses the Digital Encryption Standard (DES) algorithm for electronic security, as well as increased physical security of both satellite control facilities and earth stations. A distinction was made between information protection and encryption. Protection of "in-the-air" transmission of the entire band of channels is different from end-to-end circuit encryption. The Task Force recognized that such end-to-end encryption would be the responsibility of the individual users. On the other hand, protection of information over the satellite hop could and would be the responsibility of the satellite carriers and could be achieved with commercial equipment already available on the market. Of course, the government would have to identify which links required protection, but once this was done, the commercial carriers could implement the protection to meet the government's requirements.

The Task Force not only recognized the potential for unauthorized, even hostile interception of satellite transmissions, but also the potential threat, or at least the technical ability, to disrupt or destroy our national satellite capability by the physical attack of such persons as disgruntled employees, terrorists, or enemy agents. Thus, they concluded that a need exists to increase the phys-

The second action item identified by the Task Force to achieve communications interoperability would be the provision of a standard limited capacity communications capability at government specified earth stations. The recommended standard is a 24-voice channel T-1 modem and terminal. If a multi-destination capability was desired, it could be achieved by using one transmit and three receive paths at given carrier stations. The use of a single-channel per carrier (SCPC) system would provide lesser interconnection, but increased flexibility. It would, of course, be necessary for the government to identify the required services, such as voice, data, bandwidth, data rate, etc.

As far as TT&C interoperability is concerned, the Task Force stated both near- and far-term opportunities, and recognized that multiple solutions have a negative impact on control interoperability, thus requiring some standard design. At the present time, manufacturers are making control system interoperable within their own make, and users who are provided systems from the same manufacturer are in many cases negotiating support agreements already. The Task Force recommends for the near-term that this be expanded so that each system has at least one designated backup control facility. This would require the ability to provide real-time satellite control information and somehow still protect the propriety of such information. The coordination among "like system" users for backup support would require the NCM to assist in defining interoperability arrangements, provide information exchange between carriers, and procedural verification. The

greater variety of frequency plans available. One C-band system could readily use another C-band system's satellites with some required enhancements to improve antenna pointing, polarization, and frequency agility. The CSS Program Office, along with the NCM, would have to develop programs for such agility enhancements at selected carrier earth stations in order to achieve radio frequency interoperability for C-band systems, as well as prioritizing the order of enhancement for the earth stations selected.

Later, in the December 1983 report addendum, the Task Force recognized that with the potential proliferation of private Ku-band satellite systems which can be tied into the terrestrial networks, there existed a need to incorporate other than C-band systems into the emergency system. Such communication interoperability could be done at one of three levels. The first would be just the maintenance of a data base of such systems, and in times of disaster, communications would be interfaced into a surviving network station via some external means such as cable or courier. The second level would involve the designation of certain network stations as gateways and directly interfacing these stations into the surviving network by repointing the antenna or having a complete backup antenna system pointing at a different satellite. The third option would be to equip all network stations as gateways. Obviously, there is a trade-off between cost and interoperability in each option, with both increasing as the level increases.

the total national telecommunications network. The guidelines set forth in the plans would help in the development and testing of network restoral procedures for the satellite systems. An important aspect of this restoral capacity would be the development of a data base of the nation's commercial satellite capabilities to be maintained at the National Coordinating Center (NCC). Also required are emergency communication procedures for coordination between the NCC and the satellite control facilities and earth stations, a capability which would very well be an integral part of the NCC backup communications system. An intersite, universal satellite station orderwire would go far in making this coordination need a reality. Finally, each site should develop its own set of emergency procedures as required to respond to the needs of the NCC.

Communications and TT&C Interoperability

The Task Force recommended the development of a capability of not only having communications interoperability at crucial earth stations, but also of control interoperability between satellite systems to ensure continuity of control among the commercial satellite assets under emergency conditions. Two specific action items were initially developed to achieve communications interoperability. First, it was recognized that communication systems operating within a given frequency band could use other system's satellites within the same band. This is particularly so within the C-band as opposed to the Ku-band where interoperability could prove far more difficult because of the

... communications in support of command and control functions must operate efficiently to enable direction of surviving forces for counterattack. Therefore, these global command and control communications must be considered as prime targets. Of course, no single communications capability is adequately robust to withstand a direct attack. Therefore, it is necessary to capitalize on the aggregate capability that is afforded by intelligently combining the assets of existing and planned systems. 4

The Task Force believes that a CSS Program Office, in conjunction with a National Coordinating Mechanism (NCM), would be required to execute such an interoperability program in terms of systems engineering, development of hardware/software modifications, and equipment procurement. They also stated that the first steps the NCM should take are to determine the governmental needs in this area and develop contingency plans and emergency procedures to meet those needs. Once this is accomplished, the Task Force feels that first level enhancements in emergency control and communications interoperability could conceivably be accomplished within the first year of implementation.

Contingency Plans and Emergency Procedures

The Task Force stated that such plans and procedures are necessary to ensure a capability within government and industry to coordinate the restoration of commercial satellite communications services under various emergency conditions. The plans and procedures must, of course, be developed within the context of the mission of the NCM, as satellite communications is only one of several elements of

done. Unlike many other nations of the world, the United States does not have a Ministry of Telecommunications, or equivalent, which is responsible for all aspects of this nation's telecommunications policy and performance.

The coordination problems associated with developing interoperable communications systems within the United States environment is probably more complicated than within other countries. This is due to the autonomy of the many organizations involved. 2

A quick look at the structure of telecommunications within the United States will illustrate this point. The commercial telecommunications industry is privately owned and is not directly controlled by any government agency, but only regulated to ensure the interests of the majority of U.S. citizens are met. As far as the government agencies are concerned, those with the most direct influence on telecommunications policy include, but are not limited to, the FCC, National Telecommunications and Information Administration (NTIA), Congress, Department of State, Federal Courts, and Department of Defense.³ Even within the Department of Defense, due to the differing telecommunications needs of the various services, each is given some measure of autonomy in determining and procuring systems to meet those needs. It is a small wonder there is a great deal of effort predicted in establishing a unified approach to telecommunications interoperability.

However, just because a lot of effort and money will need to be expended, such effort should not detract from the importance of continuing on with the initiative, for under emergency/hostile conditions,

CHAPTER II

RECOMMENDATIONS OF THE COMMERCIAL SATELLITE SURVIVABILITY TASK FORCE

Chapter I listed the recommendations given by the CSS Task Force in their response to the NSTAC's tasking to study the problems involved with making commercial communications satellite systems interoperable with each other and military systems, as well as making them secure and survivable. This chapter will expound upon the recommendations stated in Chapter I by summarizing the report and its addendum. Unless otherwise noted, all information in this chapter is from the survivability report and addendum, in order to avoid unnecessarily repetitive footnoting.¹

Commercial Satellite Communications Survivability Program and CSS Program Office

The Commercial Satellite Survivability (CSS) Task Force found that for the successful implementation of its proposed actions it is essential that the government identify and develop an integrated and coherent effort to link the requirements of the DOD and other government agencies to an implementation management structure and to the commercial satellite industry. They felt it very important to have a coordinating program between government and industry to adequately plan and implement these actions, or else they just would not get

NOTES - CHAPTER I

¹Ronald Reagan, Executive Order 12382 of September 13, 1982, President's National Security Telecommunications Advisory Committee.

²Commercial Satellite Communications Survivability Report, May 20, 1983, Prepared by the CSS Task Force Resource Enhancements Working Group, p. ES-2.

³Ibid., pp. ES-4 - ES-5.

⁴Ibid., pp. ES-5 - ES-6.

⁵Ibid., p. J-1.

⁶Ibid., pp. 2-3.

⁷Ibid., pp. ES-10 - ES-12.

2. these satellite systems offer a quick means of restoring communications over extended distances, especially to isolated areas of the country, and
3. that these networks are vulnerable to a variety of hostile actions which tend to reduce their utility to provide service under emergency conditions.

This paper will look at the recommendations of the CSS Task Force and expound upon their potential, including problem areas where they might exist. In addition, this paper will address a fundamental question which arose during the Task Force's study and remains unanswered, specifically, what legal and/or regulatory impacts arise from the cooperative efforts required to plan and implement satellite emergency procedures? These topics will be covered in the following format:

1. Chapter II will present a more detailed summary of the findings of the CSS Task Force.
2. Chapter III will examine the proposal for communications and TT&C interoperability, both commercial-to-commercial and government-to-commercial.
3. Chapter IV will look at the security aspects, both electronic and physical (unclassified), as well as system survivability.
4. Chapter V will examine the legal/regulatory issues raised by the Task Force.
5. Chapter VI will draw conclusions and make recommendations warranted by the previous discussion.

mercial satellite communications services under ...
emergency conditions ...

4. The development of a capability for communications interoperability at critical earth stations ...
5. The development of a capability utilizing the Digital Encryption Standard (DES) algorithm to protect digital communications links, if ... required by the Government.
6. ... to enhance the survivability of satellite control systems ... to achieve command link protection.
7. The development of control interoperability between satellite systems ...
8. ... increase physical security of satellite control facilities and communications earth stations.
9. ... initiate a study which would assess the susceptibility of existing commercial satellite communications systems to nuclear effects and provide recommendations which would establish hardening guidelines for future commercial satellite programs.

The CSS Task Force included members from the following industries: RCA Astroelectronics, COMSAT General Corporation, GTE Corporation, American Satellite Company, Ford Aerospace and Communications Company, Southern Pacific Communications Company, AT&T Long Lines, and Western Union Corporation.⁵ The members of these various entities of the telecommunications industry gave the above recommendations based upon the following aspects of a stated problem:⁶

1. Satellite communications systems have been used by government and private agencies since the 1960's, and with the proliferation of companies providing such services, this usage will continue to grow in the 1980's.

NOTES - CHAPTER II

¹Commercial Satellite Communications Survivability Report, May 20, 1983, and Addendum, December 15, 1983. Prepared by the CSS Task Force Resource Enhancements Working Group.

²Gilbert E. LaVean, "Interoperability in Defense Communications," IEEE Transactions on Communications, Vol. COM-28, No. 9, September 1980, p. 1446.

³Dale N. Hatfield, Telecommunications Course: "Current Issues in Telecommunications Policy," University of Colorado, Boulder, CO, Summer 1983.

⁴LaVean, p. 1445.

CHAPTER III

INTEROPERABILITY

The purpose of this chapter is to more closely examine the magnitude of the CSS Task Force proposal for satellite communication system interoperability among commercial systems and between commercial and military systems. There are a multitude of vendors which provide both the space and earth segments of satellite communications links for commercial and defense use, and the coordination of technical and operational standards to provide for the proposed interoperability could prove to be quite a challenge, indeed. This chapter will also look at some of the technical aspects of making these systems interoperable, such as antenna configurations, polarization, frequency response, terminal equipment, configuration, and terrestrial/satellite system interface.

To accomplish the above-stated purpose, we will first survey the various commercial entities involved in providing satellite communications service on a commercial level. This will in no way be an exhaustive survey, for entire volumes have been devoted to such and it would be inappropriate to do so here. A quick look at those corporations which were involved in the CSS Task Force study and a listing of some of the others, as well as a few relevant statistics, will suffice to give an understanding of the complexity of the industry. Following

this, a condensed look at the Department of Defense satellite system will be given, including a few proposals into the 1990's. Finally, we will explore some of the technical aspects of making the systems interoperable. Again, this will not be exhaustive in nature; we will simply search for an understanding of some of the issues involved.

Commercial Satellite Corporations

The representative of the Communications Satellite Corporation (COMSAT) was also the CSS Task Force chairman. COMSAT was established in 1963 as the first U.S. commercial satellite company.¹ COMSAT owns and operates both domestic and international satellite communications systems, but due to the delicate nature of international affairs, such systems would not appropriately be involved in the CSS Task Force's proposal on interoperability. The COMSAT General Corporation operates and leases the capacity of two primary satellite systems, COMSTAR and MARISAT. COMSAT has five domestic earth stations in the following locations:²

1. Andover, Maine
2. Brewster, Washington
3. Etam, West Virginia
4. Jamesburg, California
5. Paumala, Hawaii

The American Satellite Company (AMSAT) has 20 percent ownership in the Westar satellite system (Westar I-IV). AMSAT also plans on launching two satellites of its own by 1986. It provides

five, seven, or ten meter earth stations on location, providing a 56 kbps or 1.544 Mbps capability.³ AT&T Long Lines owns the TELSTAR III system which has two satellites in orbit and one on-the-ground spare. Also part of the AT&T long-distance system are the COMSTAR (D1-D4) satellites which are co-owned by GTE.⁴ The GTE Satellite Corporation (GSAT) owns and operates the GSTAR satellite system with two satellites providing uniform coverage to the continental United States and spot beam coverage to Alaska and Hawaii. The GSTAR system also includes two earth stations which provide both communications interface and TT&C. A third satellite is planned for 1985.⁵

The Ford Aerospace and Communications Corporation is a major manufacturer of both communications satellites and earth stations.⁶ Hughes Communications, Inc. owns the Galaxy I, II, and III satellite system, which provides cable television (Galaxy I), video, voice, data, and facsimile services (Galaxy II and III). The Galaxy ground segment consists of two telemetry and command, transmit and receive earth stations in Brooklyn, New York and Fillmore, California, as well as an operations control center in El Segundo, California.⁷ RCA American Communications, Inc. is a major provider of satellite communications services to other users, both commercial and government agencies such as NASA and DoD. Among its assets are SATCOM I-V, SATCOM I-R and II-R, and major earth stations near New York City, Chicago, San Francisco, Los Angeles, Houston, Atlanta, and Miami.⁸

Satellite Business Systems (SBS) is a specialized common carrier providing integrated, all-digital, high-capacity satellite

networks for voice, video, data, and facsimile services. To accomplish this, SBS operates three advanced satellites, SBS-1, 2, and 3, operating in the Ku frequency band, as well as two TT&C earth stations in Colorado and Maryland.⁹ The Southern Pacific Satellite Company (SPSC) will operate the satellite network SPACENET which will consist of four satellites (three in orbit and one ground spare) to be launched in the 1984-85 time frame. TT&C earth stations are located in Woodbine, Maryland, and Livermore, California, with a satellite control center at McLean, Virginia. The SPACENET system will operate both in the C and Ku frequency band.¹⁰ The Western Union Telegraph Company provides service to its customers via the satellite system WESTARs I-V (C-band) providing cable television, video, voice, and data services. Western Union earth stations are located in the following cities:¹¹

1. Glenwood, New Jersey
2. Estill Fork, Alabama
3. Lake Geneva, Wisconsin
4. Steele Valley, California
5. Cedar Hill, Texas
6. Sky Valley, California
7. Issaquash, Washington

Other corporations with major satellite system services include, but are not limited to, the following:¹²

1. Advanced Business Communications, Inc.
2. Rainbow Satellite, Inc.

3. United States Satellite Systems, Inc.

4. The Direct Broadcast Satellite providers

Add to this approximately 500 companies providing hardware for satellite systems¹³ and 1200+ transmit and receive earth stations,¹⁴ and one can see that the goal of interoperability among commercial satellite systems is not one to be taken lightly.

Military Satellite Systems

The military satellite communications (MIL-SATCOM) system architecture can be subdivided into three primary categories: wideband, mobile/tactical, and nuclear capable. The following figure illustrates not only these three categories, but also their evolution through the early 1990's.¹⁵

<u>User Groups</u>	<u>MILSATCOM Systems</u>		
	<u>Near-Term</u>	<u>Mid-Term</u>	<u>Far-Term</u>
Wideband	DSCS II	DSCS III	DSCS III(upgrade)
Mobile/Tactical	FLTSATCOM	LEASATCOM	TACSATCOM II
Nuclear-Capable	AFSATCOM	SSS	SSS(upgrade)

Figure 1. MILSATCOM Evolution

The MILSATCOM wideband capability is truly the DoD "common user" system for bulk satellite communication services. The Defense Satellite Communications System (DSCS) is the backbone of this capability, operating in the SHF band. DSCS II is being replaced by DSCS III which will provide a significantly improved anti-jam capac-

ity, as well as greater flexibility, in orbit life, and system control. The projected upgrade for the DSCS III will have EHF transponders for even better jam resistance and higher data rates.¹⁶

The DoD's tactical/mobile capability uses narrowband, small antenna UHF terminals with the GAPFILLER and FLTSAT spacecraft which are now being replaced by LEASAT satellites. In order to alleviate bandwidth and anti-jam deficiencies in the present UHF system, TACSAT II has been proposed for the early 1990's which will have EHF transponders, on-board processing, and antenna nulling for jam resistance.¹⁷ For the nuclear capable users, the UHF AFSATCOM system will evolve into the SHF Strategic Satellite System (SSS) which will also have greater jam resistance, as well as improved survivability via hardening and increased altitude (i.e., five times that of GSO). Thus not only will it be outside any realistic enemy striking range, it will also not be "stationary" with respect to the earth. This will not only require more sophisticated tracking and acquisition techniques for control purposes, but also for destruction purposes by a potential enemy. The SSS upgrade will also include an EHF capability.¹⁸ Since the DSCS system is the most similar system to the commercial carriers, it may very well be the first to be targeted for interoperability considerations with commercial systems. That being a possibility, let us take a closer look at this system.

DSCS supports more than just long-haul DoD common user voice and data services. In fact, this is only about one-third of the total DSCS traffic. The other two-thirds includes a "myriad of 'special'

users and 'special' dedicated subnetworks, such as Diplomatic Telecommunications Service, support to tactical Ground Mobile Forces (GMF) and wide-band (multimegabit) point-to-point data systems."¹⁹ Although in some aspects DSCS is similar to commercial wideband systems, in others it is quite different, for

DSCS requirements for control of satellite transmission facilities differ significantly from commercial equivalents in that unpredictable changes in traffic requirements must be implemented rapidly and reliably, and essential connectivity must be maintained at maximum supportable data rates under jamming conditions. In addition, DSCS must accommodate a wide variety of terminal sizes and dynamically changing terminal deployment. 20

It does not take much imagination to see the enormity of the problems facing interoperability not only on a technical, but also operational level.

Current projections for military usage of satellite systems for the 1980's indicate an increase in the number and variety of those using X-band communications and telemetry. Presently, such usage is confined primarily to long-haul, point-to-point communications, though it is becoming more and more apparent that the community of users will soon include both small tactical and shipboard terminals. "In response to this requirement for increased diversity, a third generation of DSCS satellites is under development."²¹ DSCS III satellites will not only be able to use the X-band for communications, but also for improved survivability in satellite control as well, for the

DSCS III satellites have X-band telemetry and control so that the control of the communications payload can be exercised through the DSCS earth stations. In addition, the DSCS III satellites are equipped with S-band telemetry and control for housekeeping functions and for the communications payload, hence providing backup to the X-band control ... 22

and improving overall control survivability.

In recognition of the critical importance of space in our national defense, the decision was made in the summer of 1982 to establish the United States Space Command, which in essence would be responsible for all Air Force and most DoD activities in space.²³ Working with the U.S. Space Command is the Air Force Satellite Control Facility (AFSCF), which

... is a USAF world-wide network composed of control center, called the Satellite Test Center (STC), located in Sunnyvale, California, seven geographically separated Remote Tracking Stations (RTS) ... and all of the equipment, subsystems, and computer programs required to track and control satellite during on-orbit, and recovery from space operations. The AFSCF is fundamentally a service organization which time-shares its resources among (sic) multiple satellite programs. ... The AFSCF ... supports programs by real time telemetry, reception/processing, tracking, command and control; and recovery of Department of Defense (DOD) space vehicles. 24

Such telemetry and command data is transmitted to the STC via the AFSCF communications system on a real-time basis to be further processed and recorded for distribution and display.²⁵ The AFSCF's survivability, workload handling capacity, and command and control capabilities will be increased and enhanced by the opening of the proposed Consolidated Space Operations Center (CSOC) in Colorado Springs, Colorado by mid-1986.²⁶ The CSOC will

... be a secure, dedicated space control center that will provide the Air Force enhanced command and control capability in the late 1980's and 1990's. ... the CSOC will include a Satellite Operations Center (SOC) and a Shuttle Operations and Planning Center. The SOC ... functionally identical to the Satellite Test Center (STC) ... will perform its command and control functions with a modernized data system. ... Also, in the event of a catastrophic failure, the SOC will provide austere backup support for ... the STC, and vice versa. ... 27

The building of the SOC satisfies many concerns about survivability for the command and control of DoD space programs. The following is a list of the Remote Tracking Station locations:²⁸

1. Oakhange, England
2. Thule, Greenland
3. Maha (Indian Ocean)
4. Guam
5. Hawaii
6. Sunnyvale, California
7. Vandenburg, California
8. New Hampshire

With the background just provided on commercial and military satellite communication and control systems, let us now look at some of the technical aspects of communications and TT&C interoperability.

Technical Aspects of Interoperability

Seven-Level Model

Mr. Gilbert E. LaVean of the Defense Communications Agency and member of the IEEE proposed a seven-level model of interoperability among satellite communication systems.²⁹ The first portion of this section will deal with this model and determine approximately where the CSS Task Force's proposal falls within that model.

Level One - Separate Systems:

At this level, a decision has been made that any form of interoperability is technically, financially, or otherwise infeasible,

and therefore managerially unwanted. The only "interoperability" permitted here is strictly by human interface.

Level Two - Shared Resources:

Within this level, all system resources are still technically completely separate. In other words, there is no electronic interface in level two; however, more human interface is permitted than in level one in that a memorandum of understanding has been reached by all parties concerned to share resources as required. This sharing would most likely be done on a non-interference basis with the owner of the facilities.

Level Three - Gateways:

In level three we find the first electronic interface permitted among equipment of different owners. In this level, certain terminals are designated as "gateways" to which interface devices are allowed to connect the different systems together with the agreement that subscribers may "talk" among systems as long as there is no adverse impact on any one system.

Level Four - Multiple Entry Points:

This level is similar to the previous with two major exceptions. Interoperability has reached level four when the number of gateways among systems ranges from twelve to twenty. The other factor which differentiates level four from level three is that an agreement has been reached on mission importance. For example, the parties agree that overall system security/survivability is important.

Level Five - Conformable/Compatible Systems:

At this level, we find the same mission mindedness of level four; however, there is no longer a need for gateway interface devices. Here, the systems are designed to interconnect without "little black boxes" to make them electrically compatible.

Level Six - Completely Interoperable Systems:

Here, the same interoperability exists as at level five, along with a willingness to accept a significant impact on the systems from the actions taken by subscribers and management. At this level, there is a recognition that under some circumstances, a set of users may require priority of the entire system, even at the expense of other users of the system.

Level Seven - Same System:

At this highest level of interoperability, common equipment and management control in essence make the network all one system. We come the closest to this in nations where all communications networks are state owned and operated, and measures have been taken to make the equipment interoperable to the point that much of the equipment is made by a common, perhaps government-owned, manufacturer.

After presenting his model, LeVean concludes the following:³⁰

1. There is a fairly well-established need for telecommunication interoperability within the United States which has not been met and may only get worse.
2. Due to the vastly differing needs of the various communities during peace time, it is not realistic to expect them to use the same equipment.

3. A high level of autonomy is desirable during peace time.
4. Since interoperability is only one of many potentially conflicting design criteria, keeping the number of interoperable modes down to only those absolutely necessary is highly desirable.
5. Interoperability goals must be measurable and established early.
6. A means must be established to ensure objectives are achieved and maintained throughout the system's life.

Many of the CSS Task Force's proposals fall into near- and far-term objectives. At the present time, they recognized that much of the nation's satellite telecommunications interoperability rises no higher than level two of merely agreeing to share resources, as required, and some are no higher than level one of almost no cooperation among system managers. They realized that to a large extent much of this lack of cooperation is due to legal and regulatory constraints placed on them to ensure competition and to restrict the concentration of undue economic power. With this in mind, they recommended further investigation into this area, a topic which will be dealt with separately in a later chapter of this paper.

Putting the potential legal obstacles aside for the sake of making valid recommendations, the Task Force's near-term proposals on interoperability would get the nation's satellite system through level two to levels three and four of LaVean's model by designating facilities as gateways to interface military and civilian satellite systems.

For long-term planning, compatible and sometimes common equipment is proposed on military installations to allow complete, unrestrained access to civilian satellite systems if the situation dictates. Thus, the long-term proposals of the Task Force would bring the system to levels five and six of LaVean's model. Implicit in the Task Force's discussion was the understanding that certain times of crisis would necessitate giving government precedence over the entire system, completely understanding that in times of national emergencies where survival may be at stake, the satellite interoperability level may have to temporarily be at level seven of LaVean's model. They, as did LaVean, recognized that this nation would have difficulty achieving level seven in times of severe national emergency unless levels five-six were maintained during peace time.

As stated earlier, the Task Force recognized that "all domestic commercial C-band satellite systems have similar frequency bandwidths and all have linear, orthogonal polarizations but with differing configurations."³¹ Therefore, interoperability among commercial carriers could be accomplished by increasing the systems' flexibility to do the following:³²

1. Point the earth station antennas to other satellites.
2. Adjust the polarization for both up and downlinks.
3. Adjust the frequency to available channels.

Antenna Agility

There are several limitations on the flexibility of repointing earth station antennas that must be overcome. One is the fact that

²⁰Ibid.

²¹Harry L. VanTrees, ed., Satellite Communications, (New York, NY: IEEE Press, 1979), p. 53.

²²Rosner, p. 1513.

²³"All About Space Command," Military Times News Magazine, November 1983, p. 8.

²⁴K.L. Konopasek and J. Kluetmeir, "The Air Force Satellite Control Facility," Proceedings, International Telemetry Conference, Vol. XVI, 1980, p. 13.

²⁵Ibid., p. 15.

²⁶Ibid., p. 18.

²⁷Margaret H. Moffat and Sidney Hollander, "Consolidated Space Operations Center," Proceedings, International Telemetry Conference, Vol. XVI, 1980, p. 125.

²⁸Konopasek, p. 19.

²⁹Gilbert E. LaVeau, "Interoperability in Defense Communications," IEEE Transactions on Communications, Vol. Com-28, No. 9, September 1980, p. 1448.

³⁰Ibid., pp. 1452-1453.

³¹Commercial Satellite Communications Survivability Report, May 20, 1983. Prepared by the CSS Task Force Resource Enhancements Working Group, p. A-3.

³²Ibid.

³³James Martin, Communications Satellite Systems, (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1978), p. 23.

³⁴VanTrees, p. 581.

³⁵Survivability Report

³⁶Kamile Feher, Digital Communications Satellite/Earth Station Engineering, (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1983), p. 18.

³⁷Survivability Report.

NOTES - CHAPTER III

¹Mark Kimmel, ed., The 1983 Satellite Directory, (Bethesda, MD: Phillips Publishing, Inc., 1983), p. 12.

²Ibid., pp. 12-13.

³Ibid., p. 11.

⁴Ibid., p. 6.

⁵Ibid., p. 15.

⁶Ibid., p. 111.

⁷Ibid., p. 18.

⁸Ibid., pp. 29-30.

⁹Ibid., pp. 39-40.

¹⁰Ibid., p. 42.

¹¹Ibid., pp. 55-56.

¹²Ibid., pp. 1-68.

¹³Ibid., pp. 71-201.

¹⁴Ibid., pp. 771-792.

¹⁵Allen D. Dayton and Pravid C. Jain, "MILSATCOM Architecture," IEEE Transactions on Communications, Vol. Com-28, No. 9, September 1980, p. 1457.

¹⁶Ibid., pp. 1456-1457.

¹⁷Ibid., p. 1456.

¹⁸Ibid., p. 1458.

¹⁹Roy Daniel Rosner, "An Integrated Distributed Control Structure for Global Communications," IEEE Transactions on Communications, Vol. Com-28, No. 9, September 1980, p. 1511.

in the TT&C function. This appears to be the best solution, as at the present time Hughes and RCA are the only suppliers of U.S. commercial satellites.⁵⁷ Other potential solutions include the following:⁵⁸

1. A centralized control facility -- commercial or government.
2. Cross-connecting all commercial systems.
3. Zone control facilities.
4. Dispersed mobile facilities.

Each of these solutions has advantages and disadvantages which we will not expand upon here, other than to say that each increases interoperability (advantage), but each would take a significant amount of money and policy/philosophy changing (disadvantage). Perhaps the dispersement of mobile facilities warrants the most consideration for another reason -- increased security and survivability -- a subject we will be covering next.

Operating System

- Executive Control
- File Management
- Task Management
- Interrupt Handling
- Program Compiler
- Utilities

Real-Time Software

- Telemetry
- Display
- Command
- Tracking
- Data base management
- Event recording
- Device drivers
- Antenna drive control

Analysis and Planning Software

- Executive
- Database control
- Orbit parameter control, determination, maneuver, etc.
- Tracking data edit
- Events prediction
- Ephemeris data generation
- Apogee burn maneuver
- Telemetry analysis
- Attitude verification
- Sensor intrusion

Figure 2. INSAT Computer Software

Obviously, not every corporation's TT&C function is exactly like INSAT's, but each must perform many of the same functions, and INSAT's does provide a good model for informational purposes. It is clear that the TT&C function is not simple at all, and neither would be any interoperability initiatives. Of course, most of the pre and post-orbit functions would not have to be performed, as one could assume that the satellite is already in orbit when a backup TT&C facility would be required. Although not always true, this would simplify matters greatly. As stated previously, companies who have equipment from the same manufacturer are already backing each other up

Many SGCSs work in conjunction with a Satellite Control Center (SCC). Among the functions of the SCC are central control for the SGCS network, real-time satellite monitoring, control and display (initiation and validation of all commands, processing telemetry data, display of control information and space status, and range measurements), analysis of orbit, operational and mission planning, permanent maintenance of historical records, and spacecraft evaluation and performance.⁵⁴ Obviously the SGCS and SCC could not perform their functions without the use of some fairly sophisticated computer hard and software. Using the INSAT system as a model, let us explore the TT&C computer functions.

The INSAT computer software has three basic functional groupings. The operating system is provided by the manufacturer for executive control, support, and utility of computer operations. The real-time software conducts the real and near real-time operations of the SCC. Finally, the analysis and planning software controls the orbital mission and performance evaluation.⁵⁵ The following figure shows the relationship between the three INSAT computer software systems and expands upon their various functions.⁵⁶

control interoperability. "Satellites contain much instrumentation and continuously radio to earth details about the spacecraft subsystems. This information, along with measurements of the signals received from the transponders," is known as telemetry data.⁵⁰ The satellite ground control system (SGCS) in turn will use the telemetry data received to make control transmissions to the satellite as appropriate. This telemetry and command information is transmitted via a radio link with a data rate far less than that of the transponders, though the link reliability is higher. Since some of the command functions relate to pointing and/or despinning the antenna subsystem which must be sent even if it is not pointing toward earth, a separate, omnidirectional antenna is required on board the spacecraft.⁵¹

The major functions of the SGCS include controlling the satellite during the transfer and drift operations, maintenance of the satellite during on-station operation, and coordination among users.⁵² Satellite transfer and drift operations involve such factors as the determination and control of orbit and attitude, monitoring and control of subsystems, firing the apogee kick motor, various satellite maneuvers, and satellite positioning on station. Maintaining the satellite during on-station operations means station keeping, orbit determination, maintenance and control of orbit and attitude, and monitoring and controlling subsystem "health," as well as recordkeeping, planning, and analysis. The SGCS must also coordinate among such users as meteorological, broadcasting, and telecommunications payloads.⁵³

miniscule delay appears very significant, indeed, and must be accounted for in system design.

At the present time, satellite earth stations provide direct digital interface (DDI) or terminal interface equipment (TIE) to integrate terrestrial and satellite networks by compensating for the various differences between each. The major functions of the DDI include slip control, compensation for varying path length, data rate conversion, and format changes.⁴⁹ When the signal begins to lose its timing between the earth station and the satellite, the DDI will compensate by "slipping" standard 8000 bit frames back 125 microseconds, or multiples thereof, to preserve frame integrity. This technique requires buffer space for frame storage while slipping is occurring, as does compensating for path length variations. The buffer size varies as the telemetry data indicates the path length varies, thereby accommodating any changes. Data rate changes also are accommodated by a series of buffers with low-speed input and high-speed output buffers (and vice versa) to change the usually lower speed terrestrial data to the much higher speed satellite data capacity. Finally, the DDI will make the necessary format changes such as additional error control and addressing to compensate for the unique satellite characteristics.

Telemetry and Control Interoperability

To this point, we have discussed primarily communications interoperability in satellite systems. It is now appropriate to take a short look at some of the factors which are involved in telemetry and

long, adjusting it until it passes in its entirety through the transponder "window" at which time synchronization is achieved. The fifth technique, ranging and prediction, has the earth station using current telemetry data to predict the satellite's location and using this information to determine its burst time slot. Finally, coarse synchronization involves "rough guessing" on the part of the earth station as far as timing is concerned. It is not truly efficient, but it keeps the equipment less complex and is appropriate for some military and maritime uses.⁴⁶

Combining these various timing schemes into a coherently synchronized network is difficult in itself, but the difficulty is compounded by characteristics which are unique to satellite communications, specifically satellite drift and oscillation. This satellite motion is caused by forces of two types, those that cause the satellite to oscillate north and south of its original orbit and those that cause it to move east or west. The tidal forces of the sun and the moon cause the satellite to move north and south. Anomalies in the earth's gravitational pull cause the satellite to drift in an east/west direction toward a gravitational "valley" located approximately between 79°E and 101°W.⁴⁷ In a twelve-hour period, a satellite can move up to 50,000 feet before being repositioned. This change in distance equates to a timing difference of approximately 50 microseconds, which may appear insignificant, but, at a data rate of 60 Mbps, the time of transmission for 1 bit is 16.67 nanoseconds. At this rate, 3000 bits are transmitted in 50 microseconds.⁴⁸ Suddenly, that

node has its own highly accurate clock and keeps its own timing. This decentralized method is more reliable than the first, but even the most accurate clocks can lose synchronization periodically, which can be compensated by buffers. External timing, the third method, is basically a means in which all nodes reference a timing source outside the communications network. Mutual synchronization involves the periodic reset of each node's timing clock based on phase feedback received from surrounding nodes. Time reference distribution is a "step-up" in sophistication from the independent clock method in that the clocks themselves are reset instead of buffers. Finally, pulse stuffing involves the padding of asynchronous signals with "dummy" pulses to bring them up to a common data rate for transmission.

The six methods of satellite network synchronization for data transmission are random access, reference burst and self-locking, synchronization via M-sequences, window method, ranging and prediction, and coarse synchronization. In random access, each earth station simply accesses the satellite when it has data to transmit, and retransmits at random when conflicting with another earth station (i.e., ALOHA). With reference burst and self-locking, each station transmits a reference burst which is received by all other stations, and each station monitors its own burst to approximate its assigned time slot within a transmission frame. The M-sequences method, used in DSCS, uses wideband signals with excellent correlation properties for synchronization purposes. In the window method, an earth station transmits and retransmits a timing signal approximately 1 microsecond

minimal, on the order of a few milliseconds. Satellite systems, on the other hand, require 250 to 270 milliseconds propagation from transmitter to receiver via the satellite. This is doubled if the data communications protocol concerned requires a response back from the receiver acknowledging receipt of the message. To accommodate these time delays, an engineer should design delay constraints for data communications as follows: 200 milliseconds worst case response in terrestrial only systems, and 760 milliseconds when a satellite hop is included in the system.⁴⁴ Data communications protocols have been designed to accommodate these time delays to allow the integration of a satellite link into a data system. It would be inappropriate to study these in depth here, but it should be accounted for in the overall system interoperability design.

The other major technical difficulty which must be taken into account when designing for communications interoperability is synchronizing terrestrial and satellite networks. There are six basic methods of synchronization for both terrestrial and satellite networks.⁴⁵ The six fundamental techniques for synchronization for terrestrial data systems are master-slave, independent clock, external time reference, mutual synchronization, time reference distribution, and pulse stuffing. In master-slave, all nodes of the network have their synchronization clocks slaved to timing signals which are transmitted from a master clock. A backup clock is necessary to ensure continuity of synchronization should the primary master fail. The second technique, independent timing, is designed so that each

2. Surviving military systems could be using the UHF or X bands requiring a huge investment in earth station equipment for commercial interoperability.
3. Some of the military high data rate networks derive their timing from a cesium clock not used by commercial systems.
4. The military uses special jam resistant equipment.
5. Commercial channel and trunk data rates are usually a small subset of the military standard rates.

Even with these problems, the Task Force proposed two alternatives for military/commercial interoperability.⁴³ The first involved buying or leasing commercial equipment to be used at the military installations to communicate with each other via a commercial satellite. The second alternative is the natural next step after the first, which would be to obtain the necessary additional equipment for a military earth station to be able to not only use a commercial satellite, but to be able to communicate with a commercial earth station, as well.

Terrestrial/Satellite System Interface

Two major technical difficulties which must be overcome in interfacing satellite and terrestrial networks and which must be taken into account in planning for earth station interoperability are propagation delay and synchronization differentials. A direct effect of the difference in the distances involved between terrestrial and satellite networks is the electromagnetic wave propagation delay characteristics. In terrestrial systems this propagation delay is

communications interoperability among earth stations of different companies must be established. The Task Force found that "a promising candidate for this purpose would be a 24 voice channel bank for the T-1 digital system." This particular carrier is Bell T1 standard which has a data rate of 1.544 Mbps. This carrier can handle the 24-voice channels multiplexed together. This is accomplished by having each channel, in turn, insert seven bits of data and one signaling bit (eight bits total) into a 125 microsecond frame giving a total of 192 bits per frame, plus 1 bit for framing, thus transmitting 193 bits every 125 microseconds, which gives the data rate of 1.544 Mbps.⁴⁰

This particular technique is very common within the United States; thus it is the most likely candidate for an interoperability standard, which could be achieved with a 24-voice channel T-1 modem and terminals. Multidestination two-way transmission could be available if the satellite's high powered amplifiers permitted with up to three other destinations.⁴¹ Integrating the satellite and terrestrial networks was not addressed by the CSS Task Force, but will be here later in this chapter.

Military/Commercial Interoperability

As far as making military systems interoperable with those of commercial carriers is concerned, the Task Force was unable to come to grips with the following problems:⁴²

1. Much of the military satellite communications service is for overseas coverage, thereby indicating international ramifications on a commercial level.

tremely important. Unfortunately, not all manufacturers'/operators' specific polarization techniques are standardized. Some use horizontal polarization in the uplink, some use it in the downlink, and some, such as SATCOM, have a skewed polarization which is some twenty degrees off the horizontal or vertical.³⁷

To provide this polarization agility, adjustable three of four port antenna feeds are necessary for each antenna involved. Many earth stations already have this ability, but those that do not and are selected for interoperability would have to have them installed. For a ten-meter antenna, purchase and installation would run in the neighborhood of \$50,000.³⁸

Frequency Agility

As stated earlier, frequency assignment variations exist in the C-band, and even more so in the Ku-band. As a result, even though theoretically satellite communication systems using the same band could use each others satellite transponders, in practice there would need to be some frequency agility to reach the exact up and downlink frequencies. This would require a high-power amplifier with the necessary frequency agility and a high stability frequency synthesizer for both up and downlink frequency conversion at a total cost of about \$40,000.³⁹

T-1 Carrier

Once the earth station to satellite communications issues have been resolved, essentially making the satellite "transparent," then

some of the older earth stations have huge and very expensive antenna systems that may be physically extremely impractical to repoint.³³ Of course, many of today's high-performance earth stations have overcome this problem with wheel and track azimuth control which allows far more agility in antenna pointing. On the other hand, minimum cost earth stations can be repointed manually, so there is more than one way to overcome this particular problem.³⁴ Another problem would be obstacles, natural and man-made, obstructing the view to the alternate satellite. This is usually not a problem except for the smaller earth station within a metropolitan area. Prior planning would be required to ensure an earth station was not a backup for a satellite it could not "see."³⁵

Polarization Agility

The use of orthogonal polarization by satellite systems recognizes the unique characteristics of propagating electromagnetic energy which aligns itself along two planes 90 degrees apart. With proper filtering techniques, these two planes of energy can be isolated from each other in such a way that each can carry different information signals, on the same frequency, without interfering with each other, thereby doubling the carrying capacity of any given set of frequencies. This is particularly important because there are a finite number of Geostationary Orbit (GSO) positions, not because of "physical" space limitations, but frequency separation limitations.³⁶ Therefore, doubling the capacity with orthogonal polarization is ex-

- ³⁸ Ibid., p. A-4.
- ³⁹ Ibid.
- ⁴⁰ Andrew S. Tanenbaum, Computer Networks, (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1981), p. 105.
- ⁴¹ Survivability Report, p. A-5.
- ⁴² Ibid., pp. A-9 - A-10.
- ⁴³ Ibid., p. A-10.
- ⁴⁴ A.R.K. Sastry, "Performance Objectives for ISDNs," IEEE Communications Magazine, Vol. 22, No. 1, January 1984, p. 53.
- ⁴⁵ E.A. Harrington, "Issues in Terrestrial/Satellite Network Synchronization," IEEE National Telecommunications Conference Record, 1979, Washington, D.C., November 1979, pp. 52.2.1-4.
- ⁴⁶ Ibid., p. 52.2.4.
- ⁴⁷ Martin, p. 48.
- ⁴⁸ Harrington, p. 52.2.3.
- ⁴⁹ Kazumovi Inagek, et al, "International Connection of Plesiochronous Networks Via TDMA Satellite Link," IEEE Journal on Selected Areas in Communications, Vol. SAC-1, No. 1, January 1983, pp. 188-190.
- ⁵⁰ Martin, p. 72.
- ⁵¹ Ibid., p. 73.
- ⁵² Patrick J. Fisher, "Satellite Ground Control System For INSAT," Proceedings, International Telemetry Conference, Vol. XVI, 1980, p. 83.
- ⁵³ Ibid.
- ⁵⁴ Ibid., p. 84.
- ⁵⁵ Ibid., p. 85.
- ⁵⁶ Ibid., p. 94.
- ⁵⁷ Survivability Report, p. E-1.
- ⁵⁸ Ibid., p. E-2.

CHAPTER IV

SECURITY AND SURVIVABILITY

To this point, the discussion has included the possibility of emergencies and disasters of either natural or human origin. Satellite communications link destruction from either source needs to be planned for to ensure adequate communications for emergency relief and/or defense requirements. In this chapter, for the first time, we will examine the threat to satellite communications facilities, both earth and space segments, from only the human source. There are two primary man-made threats to the nation's satellite communications systems. The first involves electronic intrusion into the system; the second involves the physical destruction of the system.

Electronic intrusion into a satellite communications system can be either passive or active.¹ Passive intrusion would most likely take the form of some manner of eavesdropping to extract information of relative importance. Active electronic intrusion, on the other hand, can come in a variety of forms. One of these is an attempt at communications disruption or jamming. A second is some sort of attempt to alter the information for deception purposes. Another, in the case of satellite systems, would be attempts to send false control signals to the satellite to render it inoperative or unuseful in some way.

For the purposes of this paper, the physical threat will be divided into two parts: physical attacks on the earth stations and electromagnetic pulse (EMP) damage to both the earth stations and spacecraft as the result of a nuclear explosion. This treatment of the physical threat is the result of two assumptions. The first is that conventional (non-nuclear) attacks will only be made on earth stations and not satellites because present technology indicates almost zero chance of success of a non-nuclear attack on a GSO satellite, and even if the technology changes, there is little that can be done to thwart a physical attack of any kind in space. The second assumption is that the only protection which can be provided to a satellite communications system against a nuclear attack is the "hardening" of the electronic systems against the effects of the EMP and other forms of radiation of a nuclear blast which was not in close enough proximity to actually destroy the satellite or earth station.

The purpose of this chapter is to explore the man-made threats to satellite communications systems and discuss some of the techniques used to combat these threats. In so doing, we will first examine cryptography and anti-jam techniques used to combat the electronic intrusion. We will then look at some techniques which can be used for the physical protection from a conventional attack on an earth station. Next we will discuss the protection of the system from EMP and other radiation damage. Finally, we will briefly look at how much security and survivability protection is sufficient for commercial systems.

Electronic Intrusion

The CSS Task Force recognized the need for information protection, or bulk encryption, of a satellite link. They differentiated this from end-to-end circuit encryption, stating the former is the responsibility of the commercial carrier while the latter is the responsibility of the end user(s).² Therefore, the purpose of bulk encrypting of the satellite link is not to protect the transmission of classified information, but to protect communications privacy while "in the air" over the satellite hop. This is obviously so, because one would not want to transmit classified information from one end of a circuit to another where the only encryption is in the satellite link, because the rest of the circuit would be "uncovered" and susceptible to interception by unauthorized personnel. Thus, the bulk encrypting would provide double security for already encrypted circuits, and information privacy for non-classified circuits, which is particularly important in a communications means such as satellite because of the broadcast nature of the medium where even with spotbeam coverage it would prove almost impossible to control access to the downlink transmission.

Encryption

The National Security Agency's (NSA) data encryption standard (DES) algorithm was recommended for the bulk encryption. The DES "is the standard cryptographic algorithm for use within the Federal Government for protecting non-classified transmission and storage of

computer data."³ This algorithm is normally implemented in the hardware, because even though there are some software implementations, they do not comply with the standard and are usually quite inefficient as compared to the hardware versions.⁴ The NSA has endorsed devices using the DES algorithm which will soon be available commercially at operational data rates from 1.544 Mbps to 6.5 Mbps. These particular units would be ideal for the task described.⁵ However, one should not necessarily limit the potential solutions to only one, for there are several techniques which could prove more desirable under certain circumstances.

Although many satellite systems use a digital means of transmission, there is still a projection for the use of analog through the 1990's. It has been generally assumed the only way to encrypt an analog signal was to "digitize" it and then encipher digitally, thus increasing the bandwidth utilization.⁶ However, a scrambling technique without bandwidth expansion exists for analog signals which "is based on the existence of a set of orthonormal band-limited functions (f_0, f_1, \dots) which may be used as a set of bases to 'support' the band-limited signal."⁷ Mixing the signal with one of the functions produces another signal which is limited to the same bandwidth. The larger the matrix of functions, the better the security, to a point.⁸

Digital signature is another method of encrypting a satellite link which is used for originator verification or authentication. Within "the enciphering and deciphering procedures ... a user can

'sign' his message with his own secret deciphering key and anyone can use the enciphering key to verify his signature."⁹ To establish sender authenticity, the digital signature must be able to be validated by the recipient, it must be impossible for anyone, including the recipient, to forge the signature, and should the sender disavow the signature it must be possible for a judge to settle a dispute arising between the sender and recipient.¹⁰

Proposals have also been made to combine multiplexing and/or forward error control (FEC) techniques with those of cryptography. As far as encrypted multiplexing is concerned,

Messages to different destinations multiplexed together in a seemingly random manner can be difficult to interpret without precise knowledge of the multiplexing procedure ... [which is] inherently secure against traffic analysis because messages to each destination cannot be singled out without the deciphering key. It is also more difficult to cryptanalyze messages between a particular source destination pair because all messages from the source must be recorded and analyzed. ¹¹

In combining FEC and cryptography, one could use such techniques as convolutional coding combined with an expansion function. By adding artificial noise to the channel, receivers will be able to decode the signal only if the expansion function is known. And, to a point, the noisier the channel, the more secure the overall system.¹²

One of the major problems involved in encryption is key distribution. In the past, key distribution has been accomplished by some secure means, such as a courier, and required secure storage. A compromise of the key by any of the users meant a compromise of the

whole system, and an alternate had to be redistributed if it had not been with the original. Several solutions have been proposed for the awkward key distribution function for satellite communications, two of which will be presented here. Both techniques assume the satellite is protected from undetected tampering.¹³

In the first technique proposed, a satellite onboard computer would store a set of identifiers, one identifier for each user. The satellite itself would act as the central authenticator. Via a "handshaking" process, users' mutual identifications are verified and a common key is then exchanged. Once this is accomplished, secure communications may commence. This technique would require a large memory onboard the spacecraft, which could be updated with a new set of identifiers in accordance with security standards.¹⁴

The second proposal involves a "trap-door" one-way function. Secret parameters needed to implement the inverse of the "trap-door" one-way function are stored in the satellite computer with an algorithm for inverting the function.¹⁵ In other words,

Instead of identical keys to encipher and decipher messages at the transmit and receive ends, two different keys, related by a so-called 'trap-door' one-way function are used. Calculation from one key to the other is simple with the 'trap-door' information, but extremely difficult without this information.¹⁶

In order to ensure security, this system must be able to detect attempts at transmission from an unauthorized earth station.¹⁷

These techniques substantially reduce the key distribution and management problems in large networks by the use of a single key to

decipher messages from all network sources. However, they are not without their disadvantages which include large onboard memory capacity for identifier storage and mathematical calculations, increased bandwidth, large key size, and, in the case of the "trap-door" process, questionable security if the key parameters of the function are chosen improperly.¹⁸

Encryption of telemetry and control communications between the satellite and control center is important to ensure unauthorized commands are not given to the satellite which could make it unusable in some way for communication purposes. Because of the small number of users (i.e., the satellite, the control center, and maybe a backup control center), elaborate methods for key distribution are not as necessary, thereby making the encryption techniques somewhat simpler. The Navy has experimented with telemetry encryption and found that

... while it has long been known that a high degree of security can be realized on a data stream by mixing it with a pseudo-random pattern of sufficient length, it has only recently been near practical to do so on ... telemetry. For a signal to be effectively enciphered, it must be in digital (PCM) form, and the pseudo-random sequence long with respect to the duration of the test. 19

Of course, encrypting telemetry and control, as well as regular communications, can provide additional problems. Greater control of access would be required to include security clearances for people who may otherwise not have needed them. More room/physical space would be required not only for the cryptographic equipment, but also to ensure proper separation of cryptographic from the other communica-

tions equipment. There is increased complexity in the handling of enciphered data, as well as in the work load for the operation and maintenance of cryptographic equipment.²⁰ However, once accomplished, the encryption of regular and telemetry/control communications will provide a security level otherwise completely unattainable.

Anti-Jam Techniques

For protecting satellite communications from jamming, three primary techniques are used by military users which may be applicable to commercial users, as well. The first two fall into the category called spread spectrum. Here, the signal uses the entire frequency range allotted to transmit its signal, thereby making it extremely difficult for an intruder to zero in on any given frequency with sufficient power to disrupt communications as a whole. "In military satellite communication systems, frequency hopping (FH) is generally the favored spread spectrum technique to combat intentional jamming. ..."²¹ As the name implies, the signal "hops" in an apparent random pattern from one frequency to another, thereby never giving the intruder an opportunity to disrupt the entire signal by jamming just one frequency. With the proper forward error control techniques, partial signal destruction at a given frequency can be compensated for with the signal being reconstructed at the distant end (bent pipe), or by the satellite onboard processor.²²

The second spread spectrum technique discussed here is a method in which pseudo-random noise is generated within the signal to

spread its power over the entire spectrum. By use of the proper filtering techniques at the distant end, the jammer's signal power will remain spread over the entire spectrum while the authorized signal's power is reconcentrated and easily extracted.²³ A third technique, quite different from the first two, is satellite antenna nulling.²⁴ This method is most appropriate in a satellite with a large number of spotbeam antennas used to tie in a large network of users. When one particular antenna detects an intruder signal, the antenna nulls out, thereby protecting the rest of the network from an isolated jammer. A drawback here is that the users of that particular antenna are out of communications until the jamming ceases.

With this brief discussion of electronic intrusion behind us, let us now look at the protection of earth stations from a conventional, physical attack.

Physical Protection - Non-Nuclear

Physical damage caused by a conventional attack as a result of deliberate acts of terrorism or sabotage against terminals and control facilities presents a threat that is a great concern to all. With the trend toward more remotely located, unmanned sites, the threat is even more magnified. Depending on the terrorists' goals, damage could be light, such as a bullet into an antenna feed horn, or heavy, resulting in the destruction of the receiver, transmitter, and/or computer control equipment. At the present time, the physical security measures in force will likely detect, but not significantly protect against

trained saboteurs or military/mob attack.²⁵ From this statement, one can conclude that there are two basic levels of physical protection from attack. The first step is to detect the intruder(s) and the second is to prevent their entry and preferably apprehend them prior to damage infliction.

There are a variety of systems used for remote intruder detection. Let us briefly examine a few of them here. Probably one of the best known is the use of close circuit television (CCTV). CCTV for perimeter assessment is good where visual observation is most appropriate. To be the most effective, CCTV perimeter assessment systems must be characterized by the following:²⁶

1. It should interface with the identification system so alarms will cause all the cameras in that perimeter zone to be switched to the assessment monitors within less than one second.
2. The picture must be of high enough resolution to allow the guard to identify the image of a 100-pound person.
3. The ability to maintain the system by quick exchange of module units is a must to minimize down time.
4. There must be 100 percent coverage of all areas within and between fences.

Another type of security system is one which detects ground vibrations. There are two fundamental categories of vibration detection sensors: artificial and natural. The artificial products are usually mounted on fences or walls (artificial structures). They have

two disadvantages. They do not react well to weak vibrations, and they are incapable of distinguishing between real and false alarms. The natural products are those buried in the soil, which react to higher levels of vibration, thus allowing some distinction between real and false alarms, but with such systems the recognition/detection of individual footsteps is very difficult.²⁷ Obviously, these two systems would only be used in conjunction with other means of detection.

One such additional means is "leaky" cable technology. Leaky cables, as used in intrusion detection, are in effect normal coaxial cables in which apertures are produced in the outer conductor in order to provide a controlled amount of radio frequency (RF) energy coupling.²⁸ When two parallel leaky cables are used, a pulse of RF energy is transmitted on one cable, with the target reflector being monitored by a receiver colocated with the transmitter. With such, human targets can be detected in the vicinity of the cables.²⁹ Another means of detection is a microwave intruder alarm. Microwave Doppler radar motion detection is a widely used and effective means of intruder detection. With such a system, "an alarm condition is identified when a significantly large return signal within the appropriate frequency range is presented for a period of time ... considered to be significant and consistent with the presence of a real intruder."³⁰ As one can see, combining any of the above techniques (and numerous others) will significantly improve the probability of intruder detection over the use of just a single sensor.

Of course, detection is just the first step. Actually stopping the intruder before major damage is accomplished is another. It is unrealistic to expect the commercial satellite industry to so protect each and every facility, manned and unmanned, with enough physical security to thwart every threat, no matter how great (i.e., a full frontal assault by a well-armed team of commandos). However, sufficient physical security to repel less than such an attack at the more critical facilities is not out of the question. In fact, many of the protective measures already discussed have been, or are in the process of being, implemented.³¹ Other security measures used to actually physically restrict entry are guards (and guard dogs); fences; barricades; windowless, concrete walls; etc. A badge identification system to ensure personnel identity would be appropriate at manned locations.³²

Particularly interesting are some experimental techniques for the detection of bulk explosives in letters, packages, briefcases, etc. The most successful to date involve radio frequency resonance absorption spectroscopy (RRAS) methods, of which there are four: nuclear magnetic resonance (NMR), nuclear quadrupole resonance (NQR), electron spin resonance (ESR), and microwave molecular absorption (MMA).³³ Each of these techniques is

... characterized by the selective absorption of energy from an electromagnetic field impinging upon the material of interest. This selective absorption results from resonances established by interactions between the electric or magnetic moments of components which exist in the material and other internal or external fields. 34

All of these techniques are good for the detection of some explosives, but none are good for the detection of all types. For example, NMR is the most versatile and can detect a wide range of explosive types, but EMR is good for little but the detection of black powder, and NQR is limited to sensing TNT and a few others.³⁵ Upon the refinement of this technology, the commercial satellite community may look to have such a system installed at their more crucial facilities to protect against the single saboteur.

Hopefully, in conjunction with the implementation of these types of technology and procedures, U.S. intelligence sources, both internal and external, would be able to anticipate the build-up of any kind of major terrorist efforts which would disrupt a significant portion of our commercial systems, and appropriately "beef up" security measures with both civil and federal forces. Unfortunately, conventional physical threats are not our only source of concern. A potentially more devastating threat to national communications systems, not to mention national survival, are the effects of a nuclear environment, the subject of the next section's discussion.

Physical Protection - Nuclear

What is nuclear electromagnetic pulse (EMP), why should we be concerned about it, and what can be done to protect against it? These are the questions this section will address. We need to have an understanding of EMP and its effects on satellite communications systems

should be required to provide non-discriminatory service.⁶

Once common carrier status was given to the telecommunications industry, the natural follow-on was common carrier regulation, primarily because of the monopoly power of the industry.

Firms in the communications carrier industry qualify as public utilities and thus reside in an environment of regulation. A monopoly franchise is tendered on the premise that competition is wasteful, costly, and inefficient. In return for a license to operate in exclusive territories, the telephone carrier is obligated to submit its expenses, revenues, profits, and service to public scrutiny and review. ... Regulatory agencies attempt to prevent the firm from employing its monopoly base to levy extortionate prices from the subscribing public. At the same time, the agency endeavors to allow the firm sufficient revenues to compete in the capital market.⁷

In spite of the U.S. Postal Service's insistence that the telegraph industry be nationalized and made part of that service, Congress preferred to keep the industry in private hands and required common carrier behavior from it.⁸ Although many court disputes were heard on the issue, eventually the courts found that the ensuing telephone industry also fell into the common carrier category.⁹ Even with the advent of radio into the telegraph and telephone industry, little changed as far as common carrier status was concerned, because in 1934 Congress passed the Communications Act which defined a common carrier as

...any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy ... but a person engaged in radio broadcasting shall not ... be deemed a common carrier.¹⁰
[Emphasis added.]

History of Common Carrier Regulation

When Congress enacted the Communications Act of 1934, it borrowed the concept of common carriage from the transportation field to describe and regulate companies providing communications services to the public.² However, the idea of telecommunications as a common carrier dates back well before 1934. In 1847, the original telegraph line between Washington, D.C. and Baltimore was sold to private interests, thereby laying the foundation of privately owned telecommunications common carriage.³

By 1851 there were fifty telegraph companies, most of them licensed under the Morse patent. In 1856 a large number of companies were merged into the Western Union Company, which in 1866 absorbed two other large companies. In 1861 Western Union spanned the continent from coast to coast.⁴

It was not long before the special characteristics of a common carrier were imposed upon the American telegraph companies. To encourage system growth, in 1866 Congress included the telegraph companies in the Post Roads Act which gave them privileges such as allowing them to run their lines freely along post roads and public lands, as well as the free use of trees from public property for poles. In order to be eligible for such privileges, these companies had to provide service as a common carrier (i.e., providing service to all comers without discrimination).⁵ In 1893, the Supreme Court reinforced the idea of the telecommunications industry as a common carrier when it ruled that telegraph companies resemble railroads and other common carriers, as they are instruments of commerce and therefore

CHAPTER V

LEGAL/REGULATORY ISSUES

"What legal or regulatory impacts arise from cooperative efforts to plan and implement satellite emergency procedures?"¹ This is the question asked by the CSS Task Force as they recognized that there are certain limitations by law/FCC regulation which could inhibit progress toward a viable emergency satellite communications system. The purpose of this section is to briefly explore the regulatory environment of communications common carriers as it pertains to satellite communications and to see how this regulatory environment applies to the programs recommended by the CSS Task Force.

To accomplish this purpose, we will first look at a short history of common carrier regulation. This will provide the background necessary to understand today's regulation emphasis. With the background provided, we will then examine the deregulation, procompetition approach to the common carrier market of the present day, and specifically the post-AT&T divestiture environment. Finally, we will attempt to tie in the nature of today's regulatory climate with the proposals of the CSS Task Force in order to ascertain what effects, if any, there may be.

⁵⁷Ibid., p. 415.

⁵⁸Charles J. Rugg, "AFSCF Planning Toward the 1990's," Proceedings: International Telemetry Conference, Vol. XVI, 1980, p. 152.

³⁴ Ibid.

³⁵ Ibid.

³⁶ L. W. Ricketts, EMP Radiation and Protective Techniques, (New York, NY: John Wiley & Sons, 1976), p. 5.

³⁷ Ibid., p. 7.

³⁸ Ibid., pp. 7-8.

³⁹ Survivability Report, p. G-2.

⁴⁰ Norman J. Rudie, Principles and Techniques of Radiation Hardening, Vol. 1, (North Hollywood, CA: Western Periodicals Company, 1980), p. 1.18.

⁴¹ Ibid., p. 1.21.

⁴² Survivability Report, p. G-1.

⁴³ Ibid., p. G-2.

⁴⁴ Ibid.

⁴⁵ Rudie, Vol. 13, p. i.

⁴⁶ Ibid., pp. 24.1-24.8.

⁴⁷ Ibid., pp. 24.1-24.3.

⁴⁸ Ibid., p. 24.5.

⁴⁹ Ibid., p. 24.6.

⁵⁰ Ibid.

⁵¹ Ibid., p. 24.12.

⁵² Ibid., p. 24.17.

⁵³ Ibid., pp. 24.17-24.18.

⁵⁴ Ibid., p. 24.18.

⁵⁵ Survivability Report, p. G-2.

⁵⁶ Stephen F. Rurak, "Ground Mobile Forces Tactical Satellite Terminals," Proceedings: International Telemetry Conference, Vol. XVI, 1980, p. 413.

¹⁸Lee, p. 767.

¹⁹James L. Rieger, "Impact of the Introduction of Telemetry Scrambling at Navy RDT&E Ranges," Proceedings: International Telemetering Conference, Vol. XVI, 1980, p. 187.

²⁰Ibid., p. 188.

²¹S. M. Sussman and P. Kotiveeria, "Partial Processing Satellite Relays for Frequency-Hop Antijam Communications," IEEE Transactions on Communications, Vol. Com-30, No. 8, August 1982, p. 1929.

²²Ibid., pp. 1929-1930.

²³Hussain Haddad, Telecommunications Course: "Satellite Communications Systems," University of Colorado, Boulder, CO, Spring 1983.

²⁴Survivability Report, p. D-1.

²⁵Ibid., p. F-1.

²⁶James W. Owen, "The Use of CCTV for Perimeter Assessment," Proceedings: 1982 Carnahan Conference on Security Technology, Lexington, KY, May 1982, p. 167.

²⁷Borivoj Taborin and Zoran Taborin, "Application of a Ground Vibration Detector Security System," Proceedings: 1982 Carnahan Conference on Security Technology, Lexington, KY, May 1982, p. 157.

²⁸R. K. Harman and John E. Siedlarz, "Advancements in Leaky Cable Technology for Intrusion Detection," Proceedings: 1982 Carnahan Conference on Security Technology, Lexington, KY, May 1982, p. 115.

²⁹Ibid., p. 118.

³⁰Fabian Monds, et al., "Microprocess Target Assessment for Microwave Intruder Alarms," Proceedings: 1982 Carnahan Conference on Security Technology, Lexington, KY, May 1982, p. 105.

³¹Survivability Report, p. F-2.

³²Ibid.

³³J. Derwin King, et al., "Advances in Magnetic Resonance for the Detection of Bulk Explosives," Proceedings: 1980 International Conference on Security Through Science and Technology, Berlin, September 1980, p. 181.

NOTES - CHAPTER IV

¹Dorothy E.R. Denning, Cryptography and Data Security, (Reading, MA: Addison-Wesley Publishing Company, 1982), p. 4.

²Commercial Satellite Communications Survivability Report, May 20, 1983. Prepared by the CSS Task Force Resource Enhancements Working Group, p. 34.

³Computer Science & Technology: Maintenance Testing for the Data Encryption Standard. NBS Special Publication 500-61, 1980, p. 1.

⁴Ibid., p. 6.

⁵Survivability Report, p. B-1.

⁶Lin-Nan Lee, "Cryptographic Techniques for Satellite Networks," AIAA 8th Communications Satellite Systems Conference, April 1980, p. 766.

⁷Ibid.

⁸Ibid.

⁹Ibid., p. 768.

¹⁰Denning, p. 14.

¹¹Lee, pp. 768-769.

¹²Ibid., p. 770.

¹³I. Ingemarsson and C. K. Wong, "Encryption and Authentication in On-Board Processing Satellite Communication Systems," IEEE Transactions on Communications, Vol. Com-29, No. 11, November 1981, p. 1684.

¹⁴Ibid.

¹⁵Ibid., p. 1685.

¹⁶Lee, p. 767.

¹⁷Ingemarsson, p. 1685.

To adequately protect against EMP and other radiation, much can be done in the design phase of the systems with little impact on cost. Proper grounding, filters, etc. could be added to a satellite, for example, without adding much weight to the overall system, weight being the most influential factor in satellite costs. Of course, shielding is most applicable to the earth stations because of the weight factor, but even then, only those stations in closest proximity to known nuclear targets may require extensive shielding.

Probably the greatest protection which can be given all these systems is to make as many as possible interoperable (discussed earlier). With the great proliferation of earth stations and satellites, if each could use or tie into the others system, then their sheer numbers and wide distribution would go a long way in protecting the nation's overall satellite communications system.

These initiatives, as with all the others discussed, would, of course, require a great deal of cooperative effort among commercial companies and between commerce and the government. This cooperation has legal and regulatory ramifications which will be discussed next.

How Much is Enough?

Just how much protection for our commercial systems is sufficient? As far as encryption is concerned, perhaps very little is required because of the fact that classified/sensitive circuits need to be encrypted anyway. Although the double protection of link encryption would be nice, it may not be absolutely necessary. Encryption of the command data link may be a different story, because the falsification of such data could possibly render the satellite temporarily or permanently useless, and since such encryption involves so few users, it should probably be done. Protection against jamming is important to a degree, so perhaps the most important/used systems should employ it. But since the chances of an enemy jamming all our systems at once are not good, the money spent to build jam resistance in all systems could probably be better spent elsewhere.

As far as physical security of the earth stations is concerned, some means of adequately detecting intruders should be used at most, if not all, the important, centralized facilities. In addition, a means of physically restricting entrance to all but perhaps the most insistent intruders should be employed. As we saw earlier, many of the protective techniques are already being employed to some extent or another. Here, as in all other protective measures, industry, with government assistance, must ascertain the threat to its particular facilities and comparably protect them.

damaged equipment by spares which are kept in places where EMP protection is provided, preferably secret locations.⁵⁵ This concept would have limited application for the space segment, but has great potential for earth stations. For the communications link,

... the U.S. Army has developed a family of small, mobile, relatively low cost, Satellite Communications Terminals. Designated as AN/TSC-85 and AN/TSC-93, the Ground Terminals provide Satellite Communication links using the SHF Band. The terminals have a similar design resulting in a high degree of commonality allowing for lower logistics and operational costs. A special signal processing equipment permits nodal (multi-point) and non-nodal (point-to-point) communications. Both terminals are designed to operate from a standard, field power generator as well as from a variety of other sources. The terminals can establish communications within thirty minutes of arrival on site.⁵⁶

This system has a 24-channel capacity with high data rates.⁵⁷ Although not necessarily designed for interoperability, this mobile satellite system demonstrates many of the features necessary for reconstitution, such as high mobility, multi-channel capacity, high data rates, self-supporting power, quick set up, etc. So does the Air Force's mobile answer for control and tracking, the Ground Station Link Survivability System (GSLS) which is a

... transportable, mobile RTS [remote tracking station] replacement ... [which] would provide a substantial increase in the survivability of the AFSCF ... should one of the existing RTS's be destroyed ... the GSLS prototype transportable RTS would be available for reconstruction of the station.⁵⁸

The above two systems demonstrate the ability to support an earth station reconstitution effort. The technology is available, and, were interoperability considerations taken into account, such mobile facilities could provide back up for many earth stations, commercial and military.

attenuating all others is an effective means of shielding components from undesirable RF energy.⁵⁰

Surge suppressors are devices designed to limit the amount of voltage to critical electronic components, and include such devices as dielectric and semi-conductor breakdown devices, and non-linear resistors (varistors).⁵¹ As far as component selection is concerned, "... a semiconductor device acts like a filter. Fast devices respond to more of the EMP environment than do slow devices. The speed of the device should, therefore, be as slow as possible."⁵²

System hardness can be promoted by designing circuits which are unresponsive to signal transitions on the order of nanoseconds, because EMP cable currents are typically of very high frequencies. In a computer system, a circumvention routine may be required which would sense a potential EMP disruption and discontinue digital processing until the danger has passed, thereby cutting out EMP-induced logic errors. Another circuit design which increases system hardness involves the inclusion of differential amplifiers and transformers on multipoint signal and return lines. Since EMP circuit excitation is similar on each line, devices which respond only to signal differentials among lines will reject significant portions of the EMP signal.⁵³ Finally, the better the equipotential ground, the better the protection of electronic components against the EMP.⁵⁴

Reconstitution of communications equipment is an entirely different concept of protection against the effects of a nuclear blast than hardening. Basically, reconstitution involves the replacement of

1. Shielding
2. Electrical bonding
3. Cable/wire bundling
4. Filtering
5. Surge suppression
6. Component selection
7. Circuit design
8. Grounding

Shielding is a very effective method of hardening. For EMP shielding, a dielectric with a conductive coating or strips is good protection. If a solid material is not possible, a wire mesh will provide some protection. A honeycombed paneling of conductive material is very good if weight is not a consideration (i.e., earth stations) because each honeycomb cell acts as a waveguide to dissipate EMP energy.⁴⁷ Electrical bonding is basically the electrical connection of two metal parts to reduce the contact impedance, which in turn prevents RF potential build up due to EMP induced currents, thereby reducing the damage potential, as well.⁴⁸

Cables/wires in a bundle originating and terminating in widely different parts of the system can result in a single EMP point of entry into the entire system. Therefore, it is important for hardening considerations to ensure that all cables/wires within the same bundle connect similar parts of the system in order to isolate their inductive qualities to a given subsystem rather than the whole system.⁴⁹ Filters which pass only a given band of frequencies while

which can damage the earth segment of a satellite link. EMP produced by a nuclear blast outside the atmosphere (exoatmospheric burst) produces a so-called high altitude burst EMP. The electrons freed by the burst are trapped by the geomagnetic field of the earth and are dissipated in approximately 100 meters after colliding into atoms of air.⁴⁰ Thus, exoatmospheric bursts provide little to no EMP hazard to earth stations. On the other hand, the other radiation produced by an exoatmospheric burst such as gamma rays, x-rays, neutrons, and beta particles⁴¹ can prove quite devastating to the spacecraft. This was shown to be true in the early 1960's, where a number of satellites did suffer damage from exoatmospheric nuclear tests prior to the banning of such tests.⁴² As a result of the test evidence, and the very real threat of an unstable global environment in which many third world countries have or will soon have the ability to test nuclear devices in space with no treaty restrictions, many are looking for a means of protecting our satellite communications systems.⁴³

There are two primary means of protecting satellite systems from the effects of a nuclear blast: hardening and equipment reconstitution.⁴⁴ Hardening is the actual designing and building into electronics the equipment necessary to protect against the effects of EMP. The two types of EMP, that generated in the atmosphere and that generated within the system's components as a result of other forms of nuclear radiation (system generated EMP),⁴⁵ can be protected against to some degree by one of the following, or combinations thereof:⁴⁶

to effectively protect against those effects. Therefore, a brief look at the answers to the above questions will follow, beginning with what EMP is.

The basic mechanism of EMP generation involves a process of energy transformation. In essence, a small fraction of nuclear energy is transformed into energy of the RF electromagnetic spectrum via several intermediary steps, the first of which is release of gamma rays during a nuclear explosion. The second step involves the interaction of these gamma rays with the atmosphere which produces electrons and positive ions. This flow of electrons produces a current which radiates electromagnetic energy, or EMP.³⁶

Severe EMP exposure can extend for great ranges. Also, EMP is not necessarily accompanied to any noticeable degree by other nuclear effects. Therefore, both military and civilian systems which may not be expected to be nuclear targets can still experience the results of EMP exposure from attacks on distant targets.³⁷ These results include the burn out of electronic components associated with large antenna systems or exposed conductors (i.e., power lines). EMP can also massively disrupt control circuits or digital processing, many times without permanent damage.³⁸ The use of solid state technology prevalent in today's generation of satellite systems makes them even more vulnerable to the effects of EMP.³⁹

Both ends of a satellite communications link are susceptible to EMP and other nuclear radiation damage. The EMP generation as described above results from a nuclear explosion within the atmosphere

With this definition, Congress included radio services into the common carrier field when used in telegraph and telephone services. Thus, this decision opened common carrier status to satellite communications systems not used for broadcasting.

From the onset of satellite communications in the early 1960's, the question was not whether said systems were common carriers, but who should control them.

The overseas carriers sought satellite ownership and argued that potential economies of scale could be affected by treating satellites as an extension of existing carrier submarine facilities ... the carriers proposed a joint venture whereby satellite ownership would be assigned exclusively to the overseas communication carriers ... AT&T observed: "The policy we advance need not disturb the existing pattern of regulation or affect the competitive position of the carriers." 11

In other words, the carriers wanted to lock out competition of their submarine systems by restricting ownership of the satellite systems. Needless to say, this proposal did not go over well with those who were not overseas carriers, specifically the aerospace industry. The manufacturers of the space and earth equipment thought "that any distinction between common carriers and equipment manufacturers would be largely one of form rather than of substance."¹² And that "most of the carriers likely to be seriously interested in participating in a joint venture to establish a communications satellite system are strongly identified with equipment manufacturing."¹³ It was not long before Congress got involved in the controversy. As early as 1961, the U.S. Subcommittee on Antitrust and Monopoly of the Committee on the Judiciary considered the establishment of a single, commercial

satellite system, a monopoly.¹⁴ The Satellite Act of 1962 was Congress' attempt to compromise between the carriers and manufacturers by creating the Communication Satellite Corporation (COMSAT), which was to be half owned by the overseas carriers and half by non-overseas carrier interests. The Act states that no individual supplier could own more than 10 percent of COMSAT's stock.¹⁵

The proverbial water began to muddy with the onset of domestic satellite communication systems. In 1970, President Nixon's Task Force on the domestic satellite issue rejected the "natural monopoly" argument that COMSAT should own all domestic systems, and asserted that any firm should be allowed to establish a domestic satellite system, private or public, specialized or general.¹⁶ This finding opened the door to the competitive forces that exist in the domestic satellite market today -- the same forces dealt with by the CSS Task Force in 1983.

Today's Deregulation/Pro-Market Emphasis

The Federal Communications Commission is an independent regulatory agency. One of its purposes is to regulate communications common carriers to ensure that the public interest is met.¹⁷ However, in recent years there has been a trend toward deregulating the telecommunications field, including common carrier service. Probably the first FCC action which began the competitive race in the long-distance common carrier field was its Above 890 decision of 1959, which permitted the establishment of private microwave systems with a frequency

allocation above the 890 MHz range.¹⁸ The first company to take advantage of this decision was Microwave Communications, Inc. (MCI), who was given permission to build a private microwave network between Chicago and St. Louis in 1969.¹⁹ After many similar applications from MCI and others, "the FCC concluded that a general policy permitting new entrants and competition in the 'specialized' communications market would serve the public interest."²⁰ As far as competition in the area of communications satellites by non-government common carriers is concerned,

... the FCC in 1972 determined that there was considerable uncertainty about the viability and effectiveness of satellites for voice communications, that operational experience was needed to resolve the uncertainty, and that multiple entry by competing carriers was probably the best way to demonstrate fully this new transmission technology.²¹

The next step to competition was MCI's provision of its "Execunet" service in 1977 which was essentially regular long-distance service to its customers at cheaper rates than AT&T, thereby competing against AT&T in not only the specialized private service, but also in normal public long-distance. AT&T complained to the FCC, who upheld the complaint, stating that it had never intended for competition in normal long-distance service. A Columbia Circuit Court reversed the FCC decision, thereby allowing competition in the total long-distance market.²²

In 1983, Judge Harold Green approved the AT&T divestiture agreement with the U.S. Department of Justice.²³ In light of this divestiture,

... what was formerly one integrated, regulated monopoly system is now divided into three separate businesses: (1) customer premises equipment, including telephones, key systems, private branch exchange equipment (PBXs), and inside wire; (2) local exchange service, including the cable and central office switching equipment connecting a customer to the telephone network; and (3) the long-distance or toll network. The FCC and the judiciary found competition desirable and beneficial to customers in both the customer premise and toll business. 24

The FCC's Computer Inquiries I and II made further attempts to delineate those areas which should fall into the regulated monopoly jurisdiction and those that should fall into the free marketplace of competition. In Computer Inquiry I, the FCC considered computer to communications network interface and concluded that most combinations of communications and computer services were not common carriers which were subject to the provisions of the Communications Act of 1934. This decision permitted communications carriers to provide computer services on an unregulated basis as long as they did so through fully separate and segregated subsidiaries. Unfortunately for AT&T, the provisions of its 1956 consent decree did not allow them to compete in the computer market.²⁵

In 1980, the Commission took another look at the issue in its Computer Inquiry II. In so doing, it devised a solution which allowed AT&T to enter the competitive market of computers by also mandating the creation of a fully separate subsidiary to carry its competitive activities such as the provision of enhanced services and customer premises equipment.²⁶ Combine these two decisions with the divestiture of AT&T, and one can clearly see that the competitive/dereg-

ulatory emphasis of today's communications regulatory actors rings loud and clear. Just how will this almost obsession of deregulation and increased competition among commercial communications carriers affect attempts by the satellite industry to cooperate in the provision of a viable emergency communications satellite system? Will such emphasis have any effect at all? Since it has not yet been attempted, one cannot say for sure exactly what the answers to these questions are, especially since decisions which were initially thought to be illegal (i.e., MCI's provision of the Execunet service) were ultimately found not to be so. The communications regulatory environment is too volatile to state with 100 percent assurance that cooperative attempts by the satellite industry would have any legal ramifications. However, this should not prohibit one from exploring the issue further, and with the background previously provided as a foundation of understanding, that is now what we will attempt to do.

Effects of Competitive Forces on the CSS Task Force Proposals

With the introduction of deregulation, and the reliance on competitive market forces in the telecommunications satellite field, the government has to rely on the antitrust laws alone to protect market efficiency. "Where competition exists, antitrust remedies are an appropriate bar to intercompetitor collusion and should be used."²⁷ Therefore, it is these laws and how they affect the cooperative efforts of the satellite industry which we must explore.

The U.S. history has been riddled with incidences where the U.S. government, as the customer, has induced this kind of cooperation among a large number of contractors/commercial entities. Many anti-trust questions arise from this form of inducement.

What can ... orthodox applications of antitrust principles tell us of the competition implications where government is a giant and seemingly irrational customer, seeking a high technology custom weapon system from one or more suppliers who themselves are contractually bound up in a venture, which may last to 20 years, with scores of other companies in the same or related industries? How can traditional antitrust principles apply when the customer not only consents to the pooling, but has actively encouraged, or literally has compelled it as a condition of contract approval and award? 28

In the past, the courts have adopted a doctrine of antitrust immunity for such government/commercial joint ventures, actually stating that "legal means may be employed for an illegal end."²⁹ However, in the procompetition, anti-monopoly environment the telecommunications field finds itself in today, one may not be able to depend upon such court findings for any like ventures in the near future. A question arises as to why joint ventures cause antitrust concern.

There are three anticompetitive effects of the type of cooperative efforts put forth by the CSS Task Force. The first is the fact that such efforts could reduce potential competition in the overall market. The very fact that the government brings certain corporations together as a team could have a chilling effect on others entering the market. The second possible consequence, especially in long-term agreements, is the fact that competitive forces may break down altogether among companies brought together in the joint venture.

A third possibility is that certain types of joint ventures may have the potential of foreclosing competition at either the supplier or customer level.³⁰

The last question to be answered is whether or not the proposals of the CSS Task Force would produce the effects stated above. The answer would have to be a definite maybe. After a hard look at the proposals, one would have to conclude that there is a great potential for antitrust violation if they were implemented incorrectly. And here lies the key. It is not the proposals of interoperability, security, survivability, etc. which are monopolistic in nature, but the manner in which they will be implemented which could very conceivably restrain trade in the communications satellite market. Therefore, in deciding how these proposals will be implemented, the government and industry must ensure all are treated equitably and fairly, including the suppliers and customers, and that sufficient "arms length" distance is maintained among the competitors. In so doing, all will have gone a long way in ensuring that the worthy goals of the CSS Task Force do not break the laws of the land.

NOTES - CHAPTER V

¹Commercial Satellite Communications Survivability Report, May 20, 1983. Prepared by the CSS Task Force Resource Enhancements Working Group, p. 38.

²Mark A. Hall, "Common Carriers Under the Communications Act," The University of Chicago Law Review, Vol. 48, No. 2, Spring 1981, p. 409.

³Ithiel de Sola Pool, Technologies of Freedom, (Cambridge, MA: Harvard University Press, 1983), p. 95.

⁴Ibid.

⁵Ibid.

⁶Ibid., pp. 95-96.

⁷Manley R. Irwin, The Telecommunications Industry: Integration vs. Competition, (New York, NY: Praeger Publishers, 1971), p. 24.

⁸Pool, p. 97.

⁹Ibid., p. 103.

¹⁰Communications Act of 1934: As Amended and Other Provisions of the Law, United States Federal Communications Commission, January 1983, p. 3.

¹¹Irwin, p. 97.

¹²Ibid., p. 98.

¹³Ibid.

¹⁴Antitrust Problems of the Space Satellite Communications System, (Washington, D.C.: U.S. Government Printing Office, 1962), p. 1.

¹⁵Irwin, p. 101.

¹⁶Ibid., p. 106.

¹⁷Dale N. Hatfield, Telecommunications Course: "Current Issues in Telecommunications Policy," University of Colorado, Boulder, CO, Summer 1983.

¹⁸J. Michael Brown, et al., "An Analysis of Current Communications Initiatives in the FCC and Congress," William Mitchell Law Review, Vol. 10, No. 3, 1984, p. 462.

¹⁹Ibid.

²⁰Ibid.

²¹Ibid., p. 464.

²²Ibid., pp. 465-466.

²³Ibid., pp. 459-460.

²⁴Robert I. Alton, "Deregulation and the AT&T Divestiture: A Competitor's Perspective," William Mitchell Law Review, Vol. 10, No. 3, 1984, pp. 501-502.

²⁵Donald I. Baker and Beverly G. Baker, "Antitrust and Communications Deregulation," The Antitrust Bulletin, Vol. XXVIII, No. 1, Spring 1983, p. 5.

²⁶Ibid., pp. 5-6.

²⁷Ibid., p. 9.

²⁸Don T. Hibner, Jr., "Antitrust Considerations of Joint Ventures, Teaming Agreements, Co-production and Leader-Follower Agreements," Antitrust Law Journal, Vol. 51, Issue 4, Fall 1982, p. 706.

²⁹Ibid., p. 707.

³⁰Ibid., p. 715.

CHAPTER VI

CONCLUSIONS/RECOMMENDATIONS

The survival of a minimum national communications capability is critical to disaster response and/or post-nuclear attack reconstruction, and,

... commercial satellites play an ever-increasing role in national telecommunications for government, private and commercial interests. Satellite communications systems have a strong role to play in the day-to-day operations of our Nation's telecommunications. They offer a means to quickly restore communications to isolated sections of the country. Under the most stressful conditions of a national emergency, satellite communications systems would aid the maintenance and recovery of the economic, political and social structure of the United States. 1

It is not difficult to see that the proposals of the CSS Task Force will go a long way in enhancing this nation's communications readiness posture. At the present time, the myriad of equipment and system providers within the competitive satellite market have provided adequate, individual systems for commercial use. However, as we have seen, in the case of a national emergency, great doubt exists as to the viability of our national satellite communications network. The systems are fragmented, and for the most part unable to "talk" to each other to any great degree, thereby placing serious doubts for the establishment of a workable nationwide network in a crisis environment. These systems are also vulnerable to electronic intrusion of all

forms, physical attacks, and the effects of nuclear blasts which do not actually physically destroy the system. Yes, the Task Force's proposals will indeed rectify many of these vulnerabilities.

However, as with almost everything else in life, a proper balance must be maintained. In this case, the balance must be made between the increased readiness which will result from the proposals and the huge costs involved with their implementation. As a result of this need to maintain a balance, a two-step process should be implemented to determine funding needs. The first step should be to prioritize the proposals from the most to the least important as to their ability to enhance communications readiness. This is important because with a finite number of dollars to implement these proposals, it is important to have them prioritized to know how to allocate the limited resources. Secondly, once the proposals are prioritized, there exists a need to determine who is best able to fund them, government or industry. We will now take a closer look at each of these two steps.

Proposal Prioritization

Prioritizing the proposals is the best method to determine how to allocate this nation's limited resources toward their implementation. The following is a proposed priority list from most to least important:

1. Creation of the National Coordinating Center (NCC)
2. Development of Plans and Procedures

3. Interoperability implementation for satellite communication and control links
4. Nuclear hardening of satellites and earth stations
5. Electronic security of command and communications links
6. Physical security of earth stations.

The creation of the NCC was accomplished on January 3, 1984.²

Its mission statement is as follows:

The mission of the National Coordinating Center is to ensure that the critical telecommunications needs of the Federal Government can be and are satisfied in any emergency or crisis situation.³

Such a coordinating mechanism ranks highest on the priority list because, first of all, without such overseeing of the operation, probably few if any of the Task Force's recommendations would get implemented. Some centralized agency must oversee the entire program from beginning to end. Also, plans and procedures must be formulated (the second priority), and the NCC is the most likely body to coordinate the effort. Developing plans and procedures is rated second because without them, any attempts at tying together a nationwide communications network during the post attack/crisis phase would prove vastly time consuming at best, and fruitless at worst. This is so even if all the other proposals have been implemented, because without prearranged procedures, individual carriers would not know how to tie their systems together under stress, thereby rendering such efforts almost futile.

Once the NCC is established, and plans and procedures developed, the next step is satellite command and communications link interoperability. The reason this should be next on the priority list is really very fundamental. The more earth stations and spacecraft, both military and commercial, that can interact together, the less able a potential enemy will be in "zeroing in" on a few key systems and neutralizing our communications command and control capability. The chances of any enemy destroying every U.S. satellite system are much less than destroying a few key systems; therefore, if complete interoperability can be achieved, or almost so, then readiness, as well as complete system integrity, would be greatly enhanced even without implementing the initiatives lower on the priority list.

Nuclear hardening of the satellites and earth stations is probably the next important initiative because it is the type of attack which can be launched against the United States with little or no control of our own. In other words, a potential enemy need not be within our borders to launch this attack. Also, this is the only realistic attack which presently can be launched against the space segment of the system. And, with the fact that the Third World is presently developing this capability, and that they are not under treaty ban of exoatmospheric nuclear testing, such an attack could be mounted against our satellites under the guise of testing, a real possibility in today's unstable world. Of course, all government-owned systems should be hardened, but this may not be necessary for all commercial systems. Probably just the key earth stations would

need hardening. We could rely on the vast proliferation of smaller earth stations in widespread areas to ensure that some will survive. As far as the spacecraft is concerned, perhaps hardening only part of the inventory would work, as long as which ones were hardened and which were not was kept a secret. In that way, an enemy would not know which needed to be "zeroed in" on and destroyed because they were hardened, thereby increasing the probability that some would survive.

Once hardened, electronic security of the satellite system would come next on the priority list because, although electronic security is important, end-to-end circuit encryption should be used where sensitive or classified information is being transmitted. And, although jamming can render a communications system all but useless, it could prove very difficult for a potential enemy to jam all of the U.S. systems, especially the military systems already designed for jam resistance. However, electronic security is higher on the priority list than physical security of the earth stations because again, an electronic attack on our satellite system can be launched outside our national borders, whereas by definition a physical attack on the U.S. earth stations must fall within its borders. And, with the advent of more sophisticated processors on board the spacecraft, the earth stations are becoming smaller and less expensive, thereby increasing their proliferation which in turn decreases their vulnerability to attack by their sheer numbers and ease of replacement.

AD-A156 978

COMMERCIAL/MILITARY COMMUNICATIONS SATELLITE SYSTEMS
INTEROPERABILITY(U) AIR FORCE INST OF TECH
WRIGHT-PATTERSON AFB OH D H SKIVER 1984

2/2

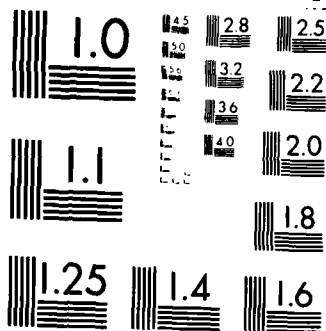
UNCLASSIFIED

AFIT/CI/NR-85-38T

F/G 22/2

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

Cost Distribution

The purpose of this section is not to do a detailed analysis of cost distribution and funding proposals for the recommendations of the CSS Task Force. Instead, we will try to outline some broad categories on a continuum of complete commercial funding to complete governmental funding. In presenting these categories, we will not attempt to place every aspect of the proposals within a specific category, but rather give one or two examples that may fall within each category. To attempt more detail than this is beyond the scope of this paper.

The first category is those initiatives which may be voluntarily implemented by the satellite industry with no governmental assistance. In other words, either through good public relations or even some measure of profitability, the industry would find it in its best interest to implement certain of the Task Force's proposals. One such proposal could be certain physical security measures for its earth stations. Many companies may very well find that protecting their assets is in their interest, at least to some degree. Another could be link encryption. Competitors could find that there may be a real commercial need to provide such a service and some big customers other than the Federal government may be willing to pay for it. Some measure of interoperability could also prove profitable in the long run with the proposed worldwide integrated system digital network (ISDN) where interoperability is almost a must.

Some standards of interoperability and hardness may be imposed upon industry by regulation without undue financial hardship. As we saw earlier, if taken into account during the design phase of the system, many of the techniques for hardening against EMP and other nuclear blast effects could be implemented within the electronics at little additional cost. It would be simply a matter of designing the system to take into account the potential for voltage surges and the like within the subsystems. The same could be said about some interoperability standards, simply a matter of doing things differently.

One step up from this category is even more stringent, potentially more costly standards being imposed upon those companies with government contracts which exceed "X" amount of dollars. Again, within limits, those corporations that hold large government contracts may find meeting more stringent standards in their self interest, and even profitable because of the amount of income they are receiving from the Federal government. It has been the experience of this author that government contractors may be willing to reduce profits or even take minor losses in one area to maintain larger profit margins in other areas. This is good public affairs which in turn helps keep those larger contracts coming.

The next category includes those standards of interoperability, survivability, security, etc. which may be implemented by the industry with nonfiscal government compensation or shared industry/government funding. An example of this would be launch schedule prioritizing. Payloads which met the proposed standards via private

funds could be given priority over those payloads which do not meet the standards, or do so at the expense of the taxpayer. Tax credits are another method of partial funding by the government for the industry's investment toward an emergency satellite communications system.

The final category is those measures which are so costly that industry could never find it within its interest to comply without adequate economic reimbursement. One must always remember that to stay in business, these carriers must be able to compete with alternative forms of communications such as microwave, cable, and optical fiber. To make a blanket policy that all satellite carriers' equipment must meet every one of these standards before it can be assigned an orbital slot could very well drive all but the largest out of business. The front-end costs of such a venture are enormous as is, and to pile on high additional costs which will not increase profits, or may even decrease them, could prove fatal to such a valuable national industry. If the U.S. government, for example, wants sufficient backup mobile replacements for earth stations, then the funding for such would probably have to come from the public sector.

A Final Look

It is not difficult to see, based upon the discussions presented in this paper, that to have a viable, national telecommunications system, the U.S. government will have to develop a closer partnership with the industry that provides that system. If we want a

system of communications, both satellite and terrestrial, which is available and responsive during and after a national crisis, and one which will allow other national industries to adequately interact with each other and the rest of the world, then some affirmative action must be taken. Somehow we cannot allow our obsession with deregulation and procompetition to so compartmentalize our telecommunications system that any hope for post-crisis communications is lost, and that other industries require the use of a dozen different communications systems to survive in the world's economy day by day. Both could, in the long run, prove disastrous to our national security.

On the other hand, too much government intervention into the industry, and too many standards could very well stifle innovation, which could prove even more dangerous than the alternatives above. Yes, again a balance must be maintained between too little and too much intervention and standardization within the industry. But isn't that what a true partnership is all about -- finding that compromise which will adequately fulfill both the requirements of sufficient but not stifling standardization? The real question then is whether or not this nation has the capacity and the will to see such a partnership through to its most optimal solution. This author believes so, but only time and commitment will tell us for sure.

Summary

This paper first introduced the CSS Task Force and provided a summary of its recommendations for interoperability, security, and

survivability. Then each of the proposals was studied and presented in more detail to examine the magnitude of effort involved and to determine its relevance to the industry's efforts to provide a viable emergency satellite system. We then looked at the legal regulatory issues pertaining to the cooperative efforts of the industry and government to carry out the Task Force's recommendations. Finally, we drew some conclusions and made some recommendations based upon the previously provided information.

NOTES - CHAPTER VI

¹Commercial Satellite Communications Survivability Report, May 20, 1983. Prepared by the CSS Task Force Resource Enhancements Working Group, p. ES-1.

²National Coordinating Center Operating Charter, December 20, 1983. As seen in Anthony E. Paulson, The Impact of the AT&T Divestiture on the Strategic Air Command, Thesis submitted to the University of Colorado, Boulder, CO, 1984, p. 2.

³Ibid., p. 3.

BIBLIOGRAPHY

Books

- Denning, Dorothy E. R. Cryptography and Data Security. Reading, MA: Addison-Wesley Publishing Company, 1982.
- Feher, Kamilo. Digital Communications: Satellite/Earth Station Engineering. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1983.
- Irwin, Manley R. The Telecommunications Industry: Integration vs. Competition. New York, NY: Praeger Publishers, 1971.
- Kimmel, Mark ed. The 1983 Satellite Directory. Bethesda, MD: Phillips Publishing, Inc., 1983.
- Martin, James. Communications Satellite Systems. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1978.
- Pool, Ithiel de Sola. Technologies of Freedom. Cambridge, MA: Harvard University Press, 1983.
- Ricketts, L. W. EMP Radiation and Protective Techniques. New York, NY: John Wiley & Sons, 1976.
- Rudie, Norman J. Principles and Techniques of Radiation Hardening. North Hollywood, CA: Western Periodicals Company, 1980.
- Tanenbaum, Andrew S. Computer Networks. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1981.
- Van Trees, Harry L. ed. Satellite Communications. New York, NY: IEEE Press, 1979.

Conference Proceedings

- Brandon, William T. and Strohl, Mary Jane. "A General Purpose Military Satellite Communications System Concept." Proceedings, International Telemetry Conference, Vol. XVI, 1980, pp. 399-401.
- Fisher, Patrick J. "Satellite Ground Control System for INSAT." Proceedings, International Telemetry Conference, Vol. XVI, 1980, pp. 83-95.

- Harman, R. K. and Siedlarz, John E. "Advancements in Leaky Cable Technology for Intrusion Detection." Proceedings: 1982 Carnahan Conference on Security Technology, Lexington, KY, May 1982, pp. 115-121.
- Harrington, E. A. "Issues in Terrestrial/Satellite Network Synchronization." IEEE National Telecommunications Conference Record, 1979, Washington, D.C., November 1979, pp. 52.2.1.5 - 52.2.1.9.
- King, J. Derwin, et al. "Advances in Magnetic Resonance for the Detection of Bulk Explosives." Proceedings: 1980 International Conference on Security Through Science and Engineering, Berlin, September 1980, pp. 181-188.
- Konopasek, K. L. and Kluetmeir, J. "The Air Force Satellite Control Facility." Proceedings, International Telemetry Conference, Vol. XVI, 1980, pp. 13-20.
- Lee, Lin-Nan. "Cryptographic Techniques for Satellite Networks." AIAA 8th Communications Satellite Systems Conference, April 20-24, 1980, pp. 766-773.
- McCoy, Lois Clark. "Emergency Response Communication Satellite Systems of the '80's." AIAA 8th Communications Satellite Systems Conference, April 20-24, 1980, pp. 347-352.
- Moffat, Margaret H. and Hollander, Sidney. "Consolidated Space Operations Center." Proceedings, International Telemetry Conference, Vol. XVI, 1980, pp. 125-135.
- Monds, Fabian, et al. "Microprocess Target Assessment for Microwave Intruder Alarms." Proceedings: 1982 Carnahan Conference on Security Technology, Lexington, KY, May 1982, pp. 105-108.
- Nakamura, Makoto, et al. "Future Advanced Satellite Communications Systems with Integrated Transponders." AIAA 9th Communications Satellite Systems Conference, March 7-11, 1982, pp. 227-233.
- Owen, James W. "The Use of CCTV for Perimeter Assessment." Proceedings: 1982 Carnahan Conference on Security Technology, Lexington, KY, May 1982, pp. 167-174.
- Rieger, James L. "Impact of the Introduction of Telemetry Scrambling at Navy RDT&E Ranges." Proceedings, International Telemetry Conference, Vol. XVI, 1980, pp. 187-188.
- Ruddy, J. M. and White, B. E. "Application of Advanced On-Board Processing to Satellite Communications -- Cost/Performance Implications for Technology Development." Proceedings, International Telemetry Conference, Vol. XVI, 1980, pp. 53-59.

- Rugg, Charles J. "AFSCF Planning Toward the 1990's." Proceedings, International Telemetry Conference, Vol. XVI, 1980, pp. 151-155.
- Rurak, Stephen F. "Ground Mobile Forces Tactical Satellite Terminals." Proceedings, International Telemetry Conference, Vol. XVI, 1980, pp. 413-418.
- Taborin, Borivoj, and Taborin, Zoran. "Application of a Ground Vibration Detector Security System." Proceedings: 1982 Carnahan Conference on Security Technology, Lexington, KY, May 1982, pp. 157-161.

Government Documents

- Antitrust Problems of the Space Satellite Communications System. Washington, D.C.: U.S. Government Printing Office, 1962.
- Commercial Satellite Communications Survivability Report, May 20, 1983 and Addendum, December 15, 1983. Prepared by the CSS Task Force Resource Enhancements Working Group.
- Communications Act of 1934 as Amended and Other Selected Provisions of Law. United States Federal Communications Commission, January 1983.
- Computer Science & Technology: Maintenance Testing for the Data Encryption Standard. NBS Special Publication 500-61, 1980.
- National Coordinating Center Operating Charter, December 20, 1983. As seen in Paulson, Anthony E. The Impact of the AT&T Divestiture on the Strategic Air Command. Thesis submitted to the University of Colorado, Boulder, CO, 1984.

Periodicals

- "All About Space Command." Military Times News Magazine, November 1983, pp. 8-19.
- Alton, Robert D. "Deregulation and the AT&T Divestiture: A Competitor's Perspective." William Mitchell Law Review, Vol. 10, No. 3, 1984, pp. 501-506.
- Baker, Donald I. and Baker, Beverly G. "Antitrust and Communications Deregulation." The Antitrust Bulletin, Vol. XXVIII, No. 1, Spring 1983, pp. 1-38.

- Brown, J. Michael, et al. "An Analysis of Current Communications Initiatives in the FCC and Congress." William Mitchell Law Review, Vol. 10, No. 3, 1984, pp. 459-488.
- Dayton, Allen D. and Jain, Pravin C. "MILSATCOM Architecture." IEEE Transactions on Communications, Vol. COM-28, No. 9, September 1980, pp. 1456-1459.
- Hall, Mark A. "Common Carriers Under the Communications Act." The University of Chicago Law Review, Vol. 48, No. 2, Spring 1981, pp. 409-438.
- Hibner, Don T., Jr. "Antitrust Considerations of Joint Ventures, Teaming Agreements, Co-production and Leader-Follower Agreements." Antitrust Law Journal, Vol. 51, Issue 4, Fall 1982, pp. 705-724.
- Inagek, Kazumovi, et al. "International Connection of Plesiochronous Networks Via TDMA Satellite Link." IEEE Journal on Selected Areas in Communications, Vol. SAC-1, No. 1, January 1983, pp. 188-198.
- Ingemarsson, I. and Wong, C. K. "Encryption and Authentication in On-Board Processing Satellite Communication Systems." IEEE Transactions on Communications, Vol. COM-29, No. 11, November 1981, pp. 1684-1687.
- LaVean, Gilbert E. "Interoperability in Defense Communications." IEEE Transactions on Communications, Vol. COM-28, No. 9, September 1980, pp. 1445-1455.
- Rosner, Roy Daniel. "An Integrated Distributed Control Structure for Global Communications." IEEE Transactions on Communications, Vol. COM-28, No. 9, September 1980, pp. 1505-1515.
- Sastry, A. R. K. "Performance Objectives for ISDN's." IEEE Communications Magazine, Vol. 22, No. 1, January 1984, pp. 49-55.
- Sussman, S. M. and Kotiveeria, P. "Partial Processing Satellite Relays for Frequency-Hop Antijam Communications." IEEE Transactions on Communications, Vol. COM-30, No. 8, August 1983, pp. 1929-1937.

END

FILMED

8-85

DTIC