AU/ACSC/0266/97-03

A SHOT TO THE SPACE BRAIN

THE VULNERABILITY OF COMMAND AND CONTROL OF NON-MILITARY SPACE SYSTEMS

A Research Paper

Presented To

The Research Department

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Maj Sue B. Carter

March 1997

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense.

Contents

Page

Illustrations

Page

Tables

Page

Preface

The mainstream military has begun to embrace the value of space systems since Desert Storm. One unfortunate aspect of the recent attention, however, is a tendency towards mystification of space capabilities. Between orbitology and kinetic energy weapon theories, the realities of space systems sometimes get lost. I wrote this paper to try to address the practical side of one of the more important trends impacting the military use of space: the increasing reliance on commercial and civil systems. In my paper, I have attempted to de-mystify the components of a space system and talk about realistic vulnerabilities. It is my hope that the reader feels more comfortable with the space systems supporting their efforts and is subsequently able to evaluate them from an informed perspective after reading this paper.

I received help from over a dozen people in the development of this work. Of particular note, I wish to thank Mr. Bob Menrab (Landsat), Mr. Louie Laurent (SPOT), and Mr. Tom Feenham and Mr. Dan Schowalter (both of Radarsat). In these men I found a common space operations understanding, regardless of program funding source. Their willingness to help with this project, despite their busy schedules, was both refreshing and laudable. May their power supplies never quit.

Abstract

The US military is becoming reliant on space systems. These systems provide us the essential information and communication means required to dominate the future battle-space. This reliance has extended beyond military programs, however, and now includes a reliance on commercial and civil systems. While this trend towards non-military systems is inevitable, does reliance on civil and commercial space systems create a unique center of gravity for the US military?

This paper evaluates this issue by first identifying the need to use non-military systems and then developing a theory for analysis of realistic vulnerabilities of space systems. The focal point for this analysis is the command and control segment for a particular program. Four specific civil and commercial systems (Landsat, SPOT, Radarsat, and INTELSAT) are evaluated in light of this analysis. What results is an identification of system reliability based on the program drivers for a specific space system. The bottom line is that commercial and civil systems are more likely to solve vulnerability problems rather than create them.

Chapter 1

Introduction

The use of space based assets in support of military operations has become commonplace since Desert Storm. There has been concern raised, however, on our reliance on space systems which are not in the direct control of the US military. This paper is written to provide basic background on realistic vulnerabilities for any space system and determine whether or not civil and commercial systems are at greater risk.

To this end, the approach taken here will be to first identify which systems the military relies upon and then determine the importance of these systems. The military use for these civil and commercial space systems can be categorized as either those systems which provide information regarding the battlespace (remote sensing) or those systems which convey information to the military commander (communications). These two broad categories have significant differences between them regarding service and system design. In each category, we've seen how important the systems have been in the past and the anticipated role in the future.

After establishing the military need for these systems, a basic theory on realistic vulnerabilities of space systems is proposed. Using a nodal analysis technique, operational space systems are broken down into three segments: Space, Control, and User. Each segment is evaluated for risks and vulnerabilities in light of various overall system

architectures. The end result is a focus on the command generation feature of the Control Segment as the critical node of any space system.

The final section of the paper looks at the what drives the development of protection for the Control Segment in the military, civil, and commercial systems. A discussion of standards and programmatics demonstrates the difference between defense, science, and profit motive. Four civil and commercial programs are briefly evaluated to establish a sense of how these systems approach vulnerability. Based primarily on interviews with ground station personnel, the major redundancies and infrastructure, as well as satellite self-protection are evaluated. The net result identifies that there are universal commonalties among space systems but the motive (defense, science, or profit) does have an impact on the extent to which vulnerabilities are protected. Observations at the macro-level are also provided to look at the issue of vulnerability from the perspective of the military customer versus the individual system.

Chapter 2

Importance of Civil and Commercial Space Systems

[Desert Storm] was the first space war.

—Merrill A. McPeak

The emergence of space-based assets as critical to the war fighter since Desert Storm has been well publicized. What is not well understood is the extent of non-military assets required to support the battlespace. Post Cold War budget realities combined with the expense related to building and operating space systems has driven the military user to get the information he needs any way he can find it. This chapter will review those non-traditional systems and discuss the increasing trend to rely on them. In addition, we'll discuss the need to understand vulnerabilities of the space-based assets.

Key Commercial/Non-Military Space Systems

Traditional assets providing military support from space are those controlled by Air Force Space Command and the National Reconnaissance Office. These systems were designed and built with military support in mind. Also supporting the military, at this time, is a host of systems that are either commercial or from the civil scientific community. Table 1 provides a brief summary of current and future systems of interest. Understanda-

bly, these systems were built for commercial or scientific purposes and not designed specifically for military requirements.

Of these systems, the military relies upon those in two categories, either remote sensing (RS) or communications (COMM). There is a tremendous difference between these two categories that must be understood in order to appreciate the relative interaction between the space system and the military user. "Remote sensing is the acquisition of data and derivative information about objects or materials (targets) located at the earth's surface or in the atmosphere by using sensors mounted on platforms located at a distance from the targets to make measurements (usually multispectral) of interactions between the targets and electromagnetic radiation."[1] Put simply, it includes those spacecraft with onboard sensors that look at everything in the electromagnetic spectrum from infrared, visible, radar, and multispectral perspectives (multispectral refers to more than one portion (or band) of the electromagnetic spectrum). The key is that there is a sensor onboard designed to gather specific data about the earth, process it, and send it down to a user or processing station. The satellite itself performs the value-added function of target acquisition and initial processing.

Communications satellites, from a simplistic perspective, are primarily transponders that take an uplink from one source and pass (downlink) that same information to a receiver. "Basically, a satellite communication system consists of one or more stations that transmit information to the satellite . . . the satellite serves as a relay which conveys this uplinked information via a downlink signal to an end user who may be located at the downlink receiver location, or the information may be forwarded via a terrestrial link."[2]

Table 1. Civil and Commercial Systems of Military Interest

SYSTEM	Type	Owned /Operated By	Data/Services Available Through	Services Provided	Comments
Landsat	RS	National Air and Space Agency	NASA	Multispectral Imagery (25m resolution)	Landsat 4 & 5 on-orbit, Landsat 7 to be launched 1997
SPOT	RS	CNES (France's Space Agency)	Spot Imaging Corp	Imagery (10m panchromatic resolution)	Spot 1 & 2 functional, Spot 3 recently lost
Radarsat	RS	Canadian Space Agency	CCRS	Synthetic Aperture Radar Data	1st asset launched in 1995
CRSS	RS	Lockheed-Martin	Space Imaging	1m panchromatic, 4m multispectral imagery	Future system, launch expected 97
Early Bird/Quick Bird	RS	EarthWatch	EarthWatch	Satellite imagery (3m/82m resolution) and maps	Launch in 97
IRS	RS	Indian Space Research Organization	EOSAT	5m panchromatic imagery, multispectral,stereo, and regional imagery	IRS-1C launched in 1996 by Russian Lavochkin Association launcher
ERS	RS	European Space Agency	SPOT Imaging for US customers	Synthetic Aperture Radar Data	ERS-1 and ERS-2 on orbit
Resource21	RS	Boeing Commercial Space Company, GDE Systems, and three agro-business groups	Unknown	Multispectral (resolution unknown)	Launch in 99, described as a commercial Landsat, its target customer is farming
Orbview	RS	OrbImage (Orbital Image Corporation)	OrbImage	1 and 2 m panchromatic, 8 m multispectral	Launch in 97
Geostationary Operational Environmental Satellite (GOES)	RS	National Oceanic and Atmospheric Administration (NOAA)	Data processed by NOA and rebroadcast via GOES to distributed users	Weather data	GOES operating for over 30 years. Satellites build and launched through partnership with NASA.
NOAA Polar Orbiter Advanced Television Infrared Observation Satellite (TIROS)	RS	National Oceanic and Atmospheric Administration (NOAA)	EROS Data Center	Atmospheric Data using infrared sensors such as the Advanced Very High Resolution Radiometer	Operating since 1978
TELSTAR	COMM	AT&T	AT&T (Loral SKYNET Satellite Services)	Communications Bandwidth	US Military has leased services for years
INTELSAT	COMM	International Consortium	COMSAT RSI	Communications Bandwidth/Transpon-ders	US Military has leased services for years
INMARSAT	COMM	International Consortium/INMARSAT	INMARSAT	Global Mobile Communications	US Military has leased services for years
IRIDIUM	COMM	IRIDIUM LLC/Motorola Satellite Communications Division	IRIDIUM LLC - a Private International Consortium	Wireless personal communications data	future

The original information goes through various modulation and compression techniques, but the end information is not altered (or should not be) by the satellite. The implication is that there is no specific value added by the spacecraft, its value is that it provides the conduit to get from transmitter to receiver.

From a user perspective, the remote sensing system is evaluated based on the type of information it provides to its customer. The communications system is usually evaluated based on the amount (and type) of data it can transmit, as well as to where the information can be transmitted to. When it comes to reliance on these systems, the difference is between information type and information availability. The one constant between remote sensing data and communication bandwidth is that the military user always wants "more."

Previous Uses of Civil and Commercial Systems

Desert Storm was the first well-publicized use of non-military systems. Shortly after the war, the Permanent Select Committee on Intelligence for the US House of Representatives held hearings on the use of Landsat and SPOT data during Desert Storm. Two key speakers were the Major General William James, Director of the Defense Mapping Agency and Mr. D. Brian Gordon of the Defense Intelligence Agency. In Mr. Gordon's words, "there were significant contributions by Landsat, by SPOT and AVHRR [The Advanced Very High Resolution Radiometer is a payload onboard a NOAA satellite], contribution to the success of Operation Desert Storm."[3] The primary value was wide area coverage provided by these systems, the timeliness of the data available to analysts, the multispectral dimension associated with the data, and the unclassified nature of the data. Per Mr. Gordon, "We had to have unclassified data in order to share certain

types of operational and targeting material with other countries' forces during that particular operation (Desert Storm)."[4] Examples of DIA uses included identification of oil fires, extent of an intentional oil slick, and materials in support of a practice attack. Additionally, data used from the SPOT satellite was loaded into a simulator called "Wings." With this simulator, the tactical commander could practice a run against an important manifold complex that was creating the intentional oil slick.[5]

The key to the use of these civilian systems was the hardware and processing performed by the DIA. As early as 1987, they began experimentation and exploitation of SPOT and Landsat. In the classified report on the value of this data, the following unclassified statement was made: "The dramatic increase in intelligence and defense uses of civil multispectral satellite data is the result of recent technology development in four critical areas: improved sensors with higher spatial resolutions, reliable high data-rate technology, new inexpensive computer hardware, and image processing software."[6]

To be most effective, it is important to be able to use both SPOT and Landsat in combination. Landsat has multispectral data over a broad area, SPOT has better resolution over a smaller area. Processing techniques provided a composite and useful image, printable on a standard color printer, which was not available elsewhere.[7]

At the Defense Mapping Agency (DMA), their enthusiasm for Landsat was tempered with some criticism that their standard film-based products were too slow and did not cover a great enough area. Per General James, DMA "makes some use of Landsat imagery to augment our imagery source materials and to produce interim products in uncharted areas pending the completion of standard topographic products."[8] In that particular hearing, DMA made a strong case for further support for the Landsat program,

but only if resolution was improved. Prior to Desert Storm, Landsat was under constant threat of cancellation for continued operating expenses. In fact, after the Desert Storm experience, a new generation of improved Landsat systems (Landsat 6 and 7) were approved for development.

From a communications perspective, the use of commercial satellite communications (SATCOM) has been commonplace. Per Lt Col Rich Thomas of the Defense Information Systems Agency (DISA), the combatant commanders (CINCs) have always used leased commercial satellite bandwidth for specific communication requirements not satisfied by military systems such as the Defense Satellite Communication System (DSCS). Per a congressional study in 1993, over $160M was spent annually for commercial bandwidth.[9] During Desert Storm commercial assets were also used. Per Joint Pub 6-0, the initial communications infrastructure was insufficient for the total communications requirements.[10] This was quickly corrected with an influx of military and commercial systems that resulted in "more strategic connectivity (circuits, telephone trunks and radio links) in the AOR than in Europe."[11] From a SATCOM perspective there were 118 government terminals and 12 commercial terminals.[12]

Current Uses of Commercial and Civil Systems

Mr. Gordon best summarized both DIA's and the DOD's approach to the use of commercial and civil system: "We're quite pragmatic about the situation. When it comes to national defense, we're going to use everything, every possible source we can get."[13] Since the time of Desert Storm, the use of non-military systems has become a fact, not an option. Per John Morris, Principle Deputy for the Central Measurement and Signature

Intelligence (MASINT) Office (CMO), there is "a real policy on the use of commercial assets as well as traditional sources."[14] Per Mr. Morris, the CMO is currently working on developing the US Spectral Plan to include all government "stakeholders" within DOD and NASA. Of prime interest is the purchase of commercial spectral data and what quantity of data should be purchased. In addition to this policy development, they have received $14.2M for two to three prototype exploitation centers to take advantage of multi-hyperspectral data. One of these centers is planned to be located in a joint intelligence center. Per Mr. Morris, it is important to involve the military customer in the determining the full utility of the data and developing the infrastructure up front for good user relations. Of special note, the primary data source will be commercial assets "because they are ahead of the DOD (in multispectral)." [15]

From a military perspective, direction from the Chairman of the Joint Chiefs of Staff was provided on 23 September 1996 that expressly called for the use of commercial remote sensing data. In a memorandum for the Secretary of Defense on an Interagency evaluation of the Defense Science Board Task Force on Improved Applications of Intelligence to the Battlefield, the Chairman supported many recommendations regarding ways to "leverage current and emerging Information Age capabilities."[16] Of key interest is the specific Defense Science Board recommendation to "direct procurement and use of commercial/international imagery to fill gaps in theater surveillance needs to detect changes."[17] The report specifically calls out Project Eagle Vision to fulfill this requirement. Eagle Vision is a deployable satellite ground receiving and processing system under development by USAF/CV.[18] Its current focus is on broad area and multispectral imagery. Physically, it consists of a receiving antenna and two vans for data acquisition and data

integration, all deployable on one C-130. The project began post-Desert Storm and has made significant development progress during Joint Endeavor in the Balkans. In 1992, SPOT images were purchased by the USAF and used in Bosnia. This area was re-imaged in 1994, 1995, and 1996 (to provide winter depictions) and processed by the Eagle Vision project. The value again was broad area, unclassified, and current data available for the military intelligence and commanders in the field. Future plans for Eagle Vision include upgrading for Radarsat data, European Remote Sensing (ERS), and the Indian Remote Sensing (IRS) satellites.[19] In addition, the project office has received $12M from the National Reconnaissance Office to purchase a second system and to incorporate some national systems data as well as EarthWatch (Early Bird and Quick Bird), Commercial Remote Satellite System (CRSS), Orbview, and Resource 21 satellites in an upgraded Eagle Vision II system.[20] What this plan demonstrates is a substantial and continuing national commitment to exploit these commercial assets for real-time battlefield support.

From a communications perspective, the future of commercial/civil systems is embodied in the Global Broadcasting System (GBS) and the Commercial Satellite Communications Initiative (CSCI). GBS is a "system of systems" exploiting currently available direct broadcasting satellites to transmit military communication. The long-term goal is use a combination of commercial and DOD systems to provide the required communications support.[21] The CSCI program was the result of a 1993 congressional study on the use of commercial satellites for communication. It is a pilot program to lease full satellite transponders rather than individual leasing of bandwidth. Lt Col Thomas is in charge of the program for DISA and is using this initiative to offload "ancillary traffic" into commercial bundles.[22]

Compared to military systems, commercial systems offer a large capacity to all global locations. For example, DSCS has Super High Frequency (SHF) capacity in six transponders of one vehicle, only two of which are high power. INTELSAT has up to 40 transponders per spacecraft, with all of them high power. A high-power transponder (e.g., 40 watts) can be downlinked to a dish which is physically smaller (e.g., 10 feet) than lower-wattage transponders.[23]

The communication demands of the CINCs, especially overseas, is driving the DOD to use whatever assets can be bought. The Global Command and Control System (GCCS) is an example of one service that is becoming a bandwidth "hog." A solution to handling all the requirements, within fiscal realities, is what drove the CSCI program. Bundling up requirements into groups and leasing whole transponders is cheaper for the government but appears as a more direct expense to the CINC (via the Services) versus DSCS. Service costs are also driven by the requirement to have non-preemptable service. This means that if a satellite or satellite transponder fails, the non-preemptable circuits will have priority for restoration over other links. Since its inception in 1993, the CSCI program has put an additional $30-40M into commercial satellite systems.[24]

A Question of Vulnerability

The Institute for Strategic Studies has raised a key issue regarding military dependence upon civil and commercial space systems: How susceptible are these remote sensing and communication systems to attack? Central to this question is the concern that if the system was not designed for military support or is not protected or controlled by military assets, it may not be available when the military users really needs it. The rest of

this paper will address two issues: (1) what are the key vulnerabilities of space systems, in general, and (2) what have the commercial and civil programs done to protect their systems.

Notes

[1]Nicholas M. Short, *The LANDSAT Tutorial Workbook: Basics of Satellite Remote Sensing*. (Washington, D.C.: NASA Goddard Space Flight Center, 1982), 10.

[2]Bruno Pattan, *Satellite Systems: Principles and Technologies*. (New York, N.Y.: Van Nostrand Reinhold, 1993), 239-240.

[3]House and Senate, *Joint Hearing before the Committee on Science, Space, and Technology and the Permanent Select Committee on Intelligence*, 102nd Cong., 1st sess., 26 Jun 91, 28.

[4]Ibid.

[5]Ibid., 31.

[6]Defense Intelligence Agency, *Multispectral Applications: The Intelligence Value of the use of Landsat, SPOT, and Aircraft Multispectral Imagery (U)*. (Washington, D.C.: DIA, 1987), 1. (Secret) Information extracted is unclassified.

[7]House and Senate, *Joint Hearings*, 30.

[8]Ibid.,19.

[9]Lt Col Rich Thomas, Defense Information Systems Agency, interviewed by author 12 February 1997.

[10]Joint Pub 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, 30 May 1995, III-7.

[11]Ibid.

[12]Ibid.

[13]House and Senate, *Joint Hearings*, 47.

[14]Mr. John Morris, Principle Deputy of the Central Measurement and Signature Intelligence (MASINT) Office, interviewed by author 30 October 1996.

[15]Ibid.

[16]Gen John M. Shalikashvili, Chairman of the Joint Chiefs of Staff, Memorandum to the Secretary of Defense, subject: Report of the Interagency Implementation Group on the Recommendations of the Defense Science Board Task Force on Improved Applications of Intelligence to the Battlefield, 23 Sep 1996.

[17]Ibid., Enclosure, 5.

[18]Gen Richard E. Hawly, *Foreign Comparative Test Program Final Test Report Executive Summary for Eagle Vision Deployable Satellite Ground Receiving and Processing System* (APO AE 09094, Headquarters United States Air Forces in Europe, 14 December 1995), 1.

[19]Briefing, Electronic Systems Command/ICI, subject: Eagle Vision Program Status Briefing, January 1996.

Notes

[20]John K. Larabee, Director, International and Commercial Affairs, Office of Systems Applications, National Reconnaissance Office, to Scott Carson, Executive Vice President, Boeing Commercial Space Company, letter, subject: Eagle Vision II, 3 July 1996.

[21]William Perry, "Annual Report to the President and the Congress: Space Forces," in *Operational Structures Coursebook*, Air Command and Staff College, (Maxwell Air Force Base, AL: Air Education and Training Command, November 1996), 62.

[22]Thomas.

[23]Ibid.

[24]Ibid.

Chapter 3

Realistic Vulnerability of Space Systems

Many military space theorists focus on translating airpower theory into spacepower theory. Specifically, they write in terms of space control, counterspace operations, and space combat support.[1] While this may seem to be appealing in order to break down traditional thought processes regarding space, it primarily focuses on only on-orbit assets versus the entire space system. Like the airpower theorists who think only in terms of different types of airframes, space theorists who think only in terms of spacecraft are missing out on the full spectrum of military space theory. This chapter will provide a simplistic model for understanding basic space systems from a daily operational perspective and will use that model to identify the more realistic vulnerabilities of a space system.

Components of a Space System

No matter what program is evaluated, there are basically three components to any space system: The Space Segment, the Control Segment, and the User Segment. These three "segments" should be viewed as functions and not necessarily three discrete physical entities. While there are variations on how the three interact, you must have each of these for an operational system performing a specified mission. Figures 1 and 2

illustrate two of the variations for these systems. Both have the three segments but differ from the user perspective. In Figure 1, we have a centralized user who processes the mission data (or communications signal) and sends it on for secondary use. The second model (Figure 2) depicts a distributed architecture where many end users receive direct input from the spacecraft. Other variations which show different physical relationships will be depicted later in this chapter.

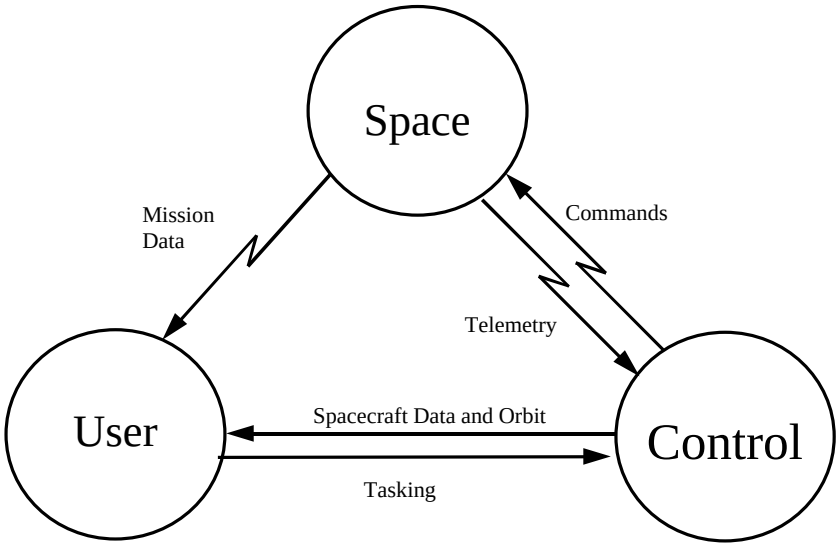

Figure 1. Centralized User Architecture

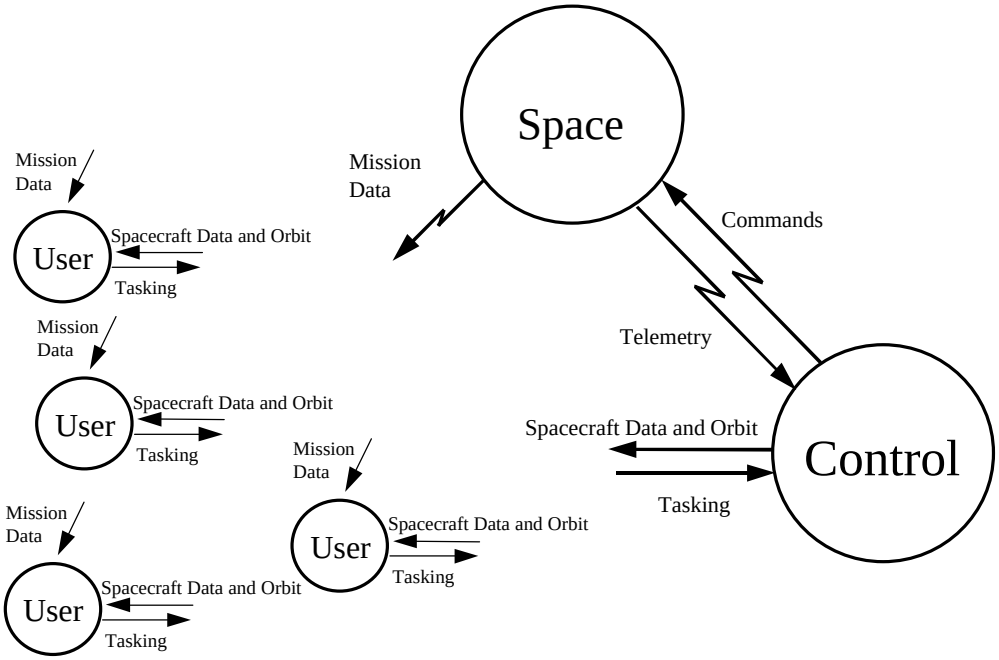

Figure 2. Distributed User Architecture

In order to systematically evaluate each of the three segments of a space system, a simplified nodal analysis technique will be used to first describe each segment and then identify vulnerabilities. "Nodal analysis is a technique used to model a system. . . . In military terms, nodal analysis helps us determine the most effective and efficient way to affect that system."[2] The technique breaks down a system into nodes for physical elements and links for the interaction between those elements.

The Space Segment

The most publicized portion of any program is the on-orbit asset. This piece costs the most, is the most complicated to build and deploy, and is typically both the source of capability and source of limitation in any space system. Although the types of satellites vary considerably, there are fundamental spacecraft principles that are applied in all program designs. Every satellite orbiting the earth performs the following functions:

payload and processing, telemetry tracking and control, satellite stabilization-attitude control, spacecraft power generation and storage, and spacecraft thermal management.[3] If any of these functions become inoperative, the satellite cannot perform its mission. Understandably, all modern spacecraft have redundancies in these areas to allow for normal on-orbit failures due to design or age. On occasion, the payload may have critical non-redundant parts. For example, an imaging system with a large telescope will have redundant electronics but only one set of optics. Figure 3 is a simplified nodal description of the Space Segment. Redundancies have not been shown for the sake of simplicity. The figure should give the reader a sense of what the main elements of a space system are but is not intended to provide a comprehensive physical description.

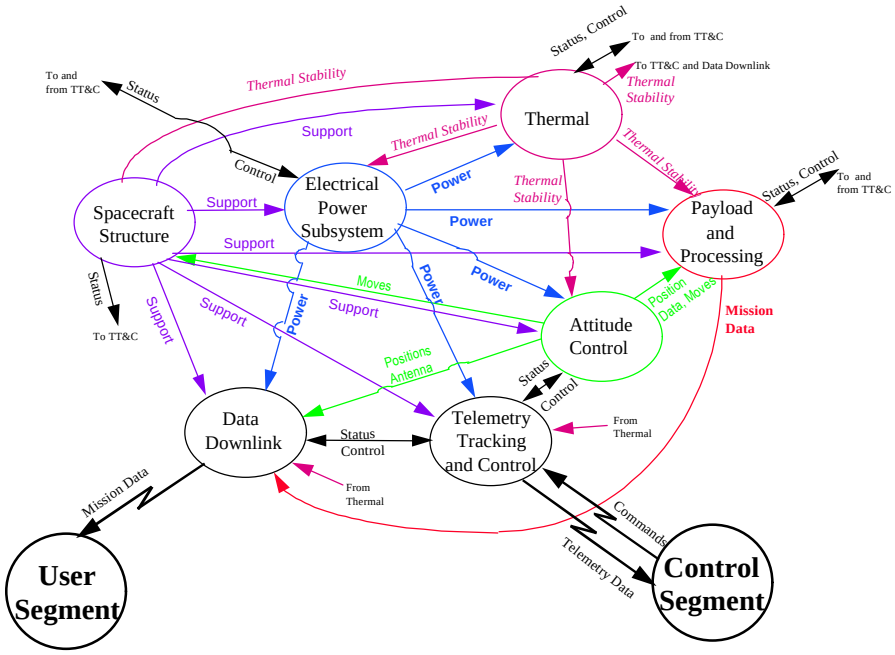

Figure 3. Space Segment

Once a satellite is in daily operation, each of the basic functions require some routine monitoring and intervention from ground control elements for normal operations and

maintenance. For example, a payload will often need a mission profile to determine where it is going to point its sensing devices. A communications satellite payload must be told where to downlink a received signal. An attitude control system must be adjusted for gravity gradient, magnetic field changes, solar radiation pressure, thermal differences, and aerodynamic pressure (low-earth orbit).[4] Solar-powered spacecraft (which represent all on-orbit assets except a few Former Soviet Union programs), may experience eclipses which require battery charging and discharging. Sun-synchronous satellites may require extensive thermal management to keep the vehicle at optimal temperatures. Each on-orbit asset has those "features" which require routine ground contact for mission. In most cases, routine mission operations may cease anywhere from minutes to hours without ground contact. This is not to imply that the spacecraft will fail in that short a period of time. In fact, almost all on-orbit assets have autonomous safekeeping to provide for more extended ground outages. Often this will involve a satellite autonomously re-orienting to a thermally benign and stable position which maximizes its ability to regain ground communication. Another common feature of safekeeping is power reduction (e.g., turn off all or part of the payload) to keep the health and safety systems going. Depending on satellite complexity, age, and orbital characteristics, this safekeeping can last anywhere from a couple of days to several months. During this time, however, mission is usually lost.

The Control Segment

Contact from the ground is through the program's control station. Ground stations come in many varieties but all perform similar functions: transmit commands and verify

satellite response, acquisition and processing of telemetry data, evaluation of health and "housekeeping" telemetry, command generation, signal generation and output, satellite tracking and orbit prediction, and mission commanding. In general, when referring to that information downlinked from a spacecraft which is associated with vehicle health and safety, the term *telemetry* is used. When the downlinked information is the product of the payload, it's considered *mission data* vice telemetry. The command and Control Segment will always receive and process telemetry, but not necessarily mission data. Mission data processing may be co-located with the command and Control Segment or it may be at a separate user receiving station.

Physical elements of the command and Control Segment are the antenna (e.g., pedestal, big parabolic dish), the low-noise receiver, the transmitting power amplifiers, the Radio Frequency (RF) conversion circuitry, signal generation or signal output equipment, and satellite tracking receivers.[5] Mission and vehicle control further requires telemetry processing, mission planning, spacecraft analysis, spacecraft databases, and operators. Finally, a key element is the command generation system which takes operator, database, spacecraft maintenance, and mission planning inputs to generate the legal commands to the spacecraft. Figure 4 is nodal depiction of the Control Segment. Again, the focus is more on physical functions and relations than specific pieces of hardware.

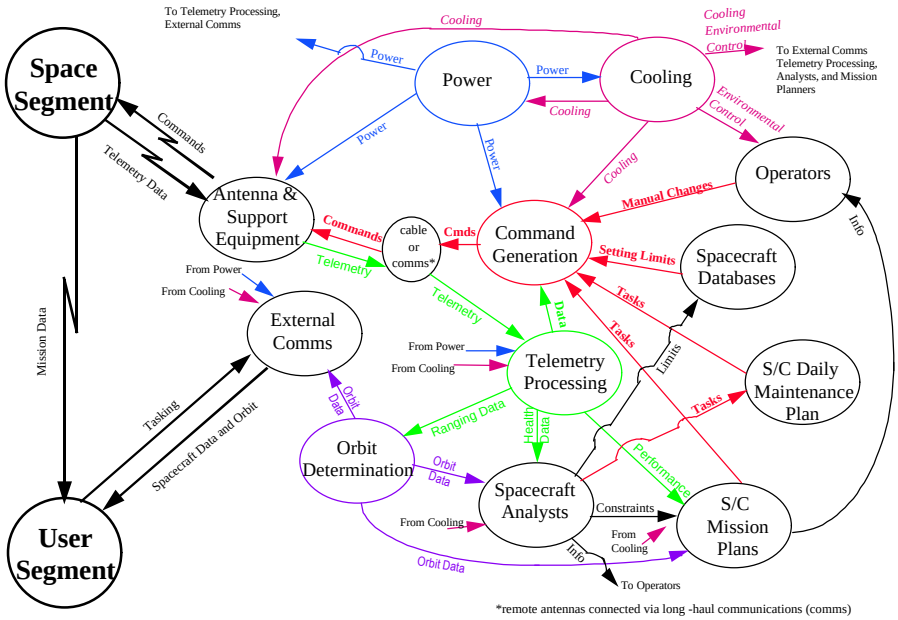

Figure 4. Control Segment

The particular design of the command and Control Segment is dependent on the spacecraft orbit and internationally assigned frequency. For geosynchronous and highly-elliptical orbits, only one control station uplink is usually required. For low-earth orbits, several uplink sites may be required to command the spacecraft, but generally only one source of command generation is required. The remote sites are sent the commands from the one location (via long haul communications) and then these are "bent piped" up to the satellite. These remote sites may or may not be dedicated to a particular program. Many satellite systems operate their telemetry tracking and control uplink in the "S-Band" frequency range so they can use the NASA deep space network as a backup system (e.g., Radarsat).[6] This particular band of the frequency range is internationally recognized for this function, is the NASA standard for their networks, and is very good for link margin to ensure commands will always get to the spacecraft. From a physical perspective, S-Band

systems are fairly obvious due to the large (often 10-meter) antennas required to transmit the uplink. While there may be more than one uplink site, however, the number of sites capable for command generation is usually limited to one or two. The rationale is based both on security, costs, and unity of effort. The ability to process telemetry and generate the correct command sequences requires communicating in a unique language. The satellite should only respond to the correct command sequence and, by limiting the control stations which can generate that "language," access affecting the health and safety of the vehicle is limited. Many modern spacecraft also have complex encryption schemes in addition to a limited number of command generation systems. While command generation is like a language, encryption is a password. If the control station's password does not match the satellite's, the vehicle will not accept the commands. Finally, duplication of the large analytical and mission planning effort required to maintain the satellite, as well as perform mission, is usually avoided. Besides the expense, unity of effort requires that only one location be responsible for daily adjustments to the spacecraft. A second site may be capable of performing these functions, but is usually an emergency backup for any one particular spacecraft. Simplistically, only one site can "drive the car," although a backup driver should be available. As explained in the Space Segment, correct and routine commanding from the ground is required in order to ensure the spacecraft continues is routine mission.

The User Segment

This component of the Space System has the most variety from program to program. As mentioned earlier, the User Segment can be anything from a co-located processing

facility at the control station or it can be located at separate geographic locations. These separate locations may be capable of receiving the satellite data downlink directly or will get the data bent-pipe from the control station. Communications satellites, by their very nature, are designed to be located around the world, receiving the communications data from the satellite and passing it on either terrestrially or via another satellite "bounce." While user receiving stations may sometimes be confused with control stations, the critical difference is in command generation. User segments usually will not have the requisite transmitting power amplifiers and, by design, won't have the command generation equipment or analysis support to conduct health and safety operations.

What occurs at the User Segment is very much system dependent. For remote sensing systems, first-order processing and assessment of the data usually occurs at this location. Some satellites can directly broadcast a "finished" product, others require analysis before the data is usable. Communications systems, by design, are simply relaying data and analytical processing is not required. Equipment with appropriate communication protocols to demodulate the signal may be required, as well as data dissemination equipment. Figure 5 is a nodal analysis of the key physical functions and relations in a User Segment. Notable physical characteristic are: the receiving antenna (with demodulation equipment), antenna control, data processing, secondary analysis (or comm signal routing), and future mission task generation. Tasking is shown in its most basic form. Usually, tasking requires not only evaluation of previous collection versus user requirements, it also requires a lengthy bureaucratic process before task generation turns into a mission profile at the Control Segment. This process is mercifully ignored in the

figure as it is not particularly critical for this vulnerability analysis. The requisite infrastructure (power, cooling, and communications) is also depicted. Whereas command uplink sites are limited, user receiving sites can be a few as one and as many as hundreds or thousands (for direct broadcast systems).

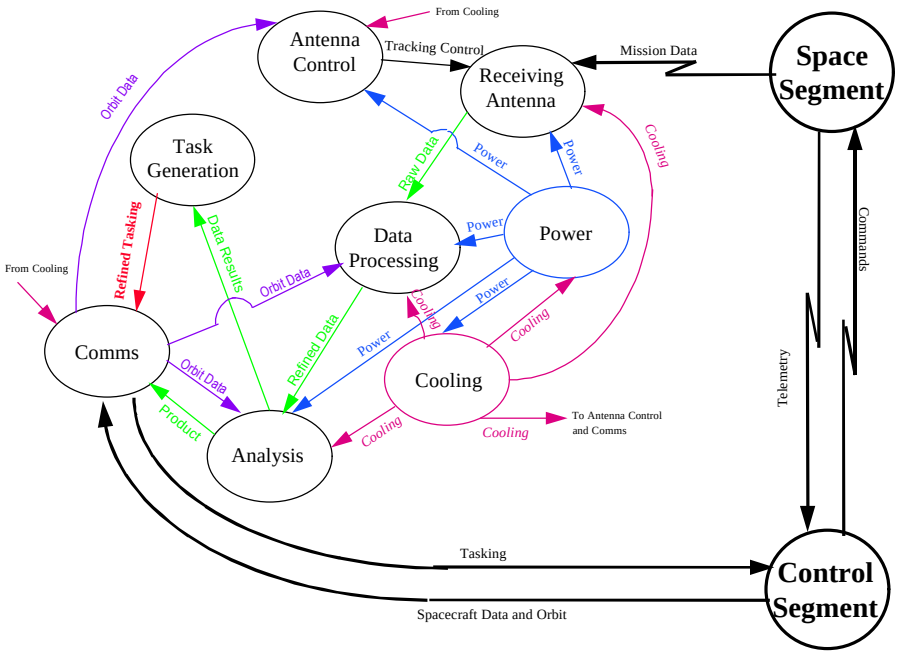

Figure 5. User Segment

Architecture Options

Figures 6–10 show a few of the ways that the ground elements of a space system (Control Segment and User Segment) may be organized. CS-I (Figure 6) shows a control facility with an adjacent antenna. This might be expected for a geosynchronous satellite. CS-II (Figure 7) is a control facility where the actual commands to the satellite are relayed via bent pipe commanding. This might be expected for a low-earth orbiting satellite. Global networks which support these remote antennas are fairly common (e.g., Air Force's Satellite Control Network, NASA's network). While this type of Control Seg-

ment architecture does have complex communications paths (terrestrial or satellite links) and alternate routing techniques, the physical functions provided at the remote stations are still fairly simple. The remote stations will take the commands generated at the central facility and uplink them to the on-orbit asset via the attached antenna. No analysis or independent command generation is performed.

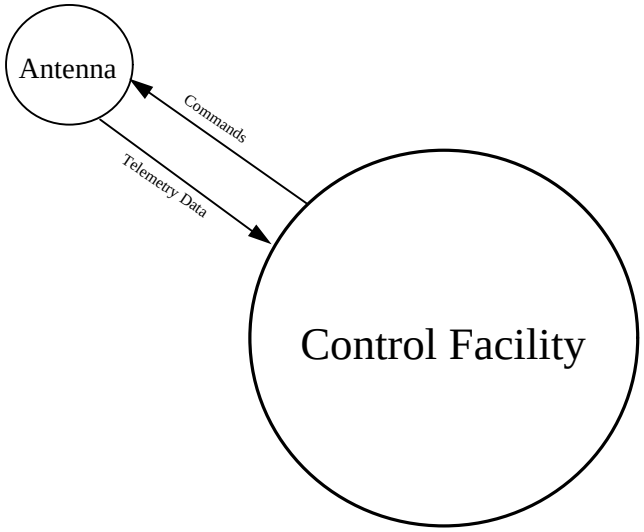

Figure 6. Architecture Options for Ground Elements: Collocated/Central Control Facility and Antenna (CS-I)

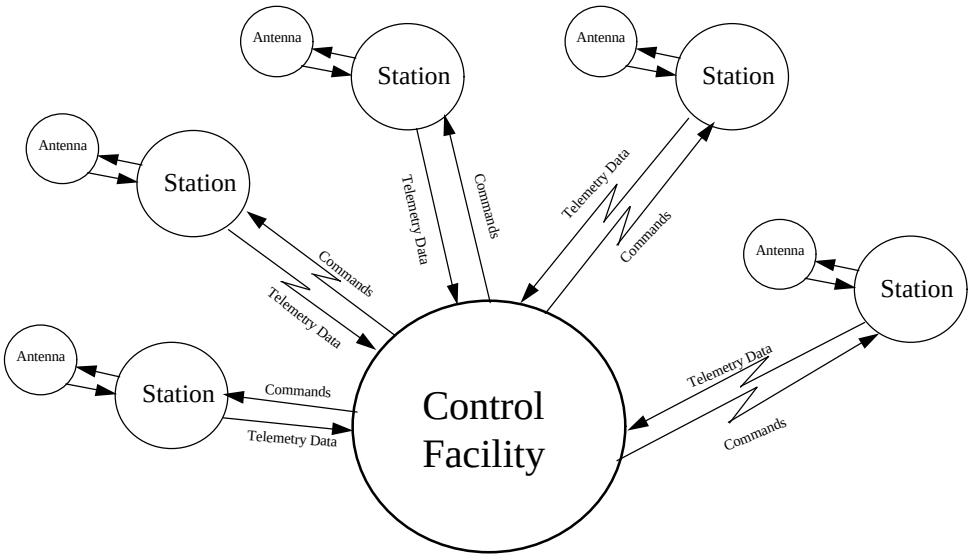

Figure 7. Architecture Options for Ground Elements: Central Control Facility with Remote Antennas via Global Network (CS-II)

Three architecture options are shown on the User Segment side. The first is the co-located control and User Segment (US-I, Figure 8). In this option (typical for a geosynchronous system), both satellite telemetry, mission data, and spacecraft commands can actually pass through the same antenna aperture (presuming it is designed to do so). This architecture provides direct access between the spacecraft analysts, mission planners, and mission data analysts. Although the bureaucratic tasking process is not likely to be circumvented, data quality feedback and system anomaly information is readily passed. US-II (Figure 9) shows the centralized user separate from the Control Segment. This would be more likely for a low-earth orbit asset. Finally, a newer trend in satellite systems is the distributed user architecture (Figure 10). In this instance, the mission data from the spacecraft must be either fairly refined to begin with or the data processing and analysis functions are relatively straightforward. The SPOT system for satellite imagery and the

Global Broadcasting System for future military communication requirements are two programs which use this approach.

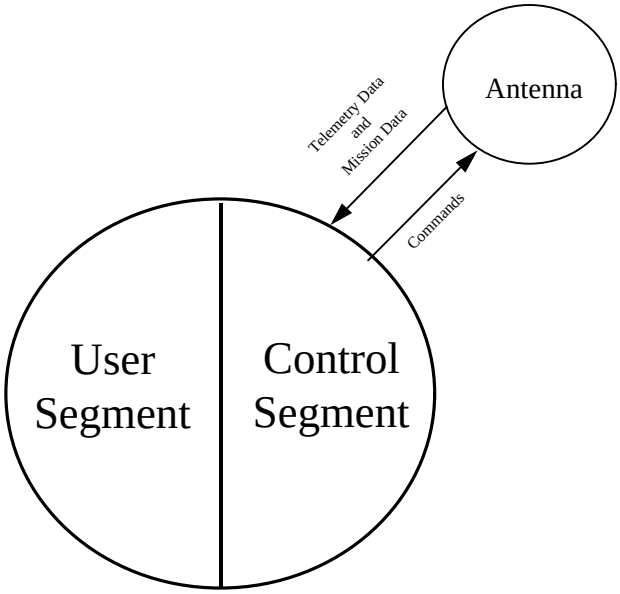

Figure 8. Architecture Options for Ground Elements: Collocated Control and User Segment (US-I)

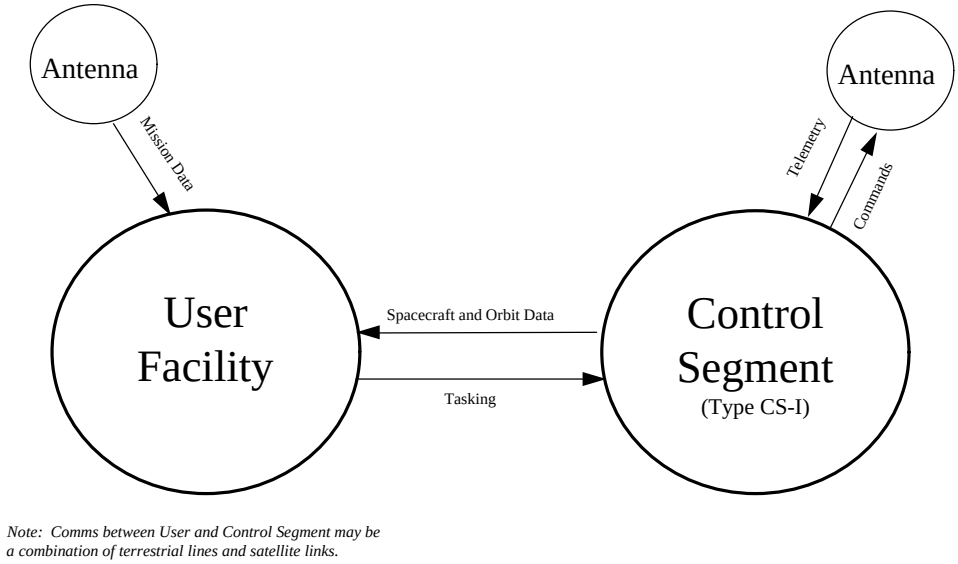

Figure 9. Architecture Options for Ground Elements: Separate Control and Centralized User Segment (US-II)

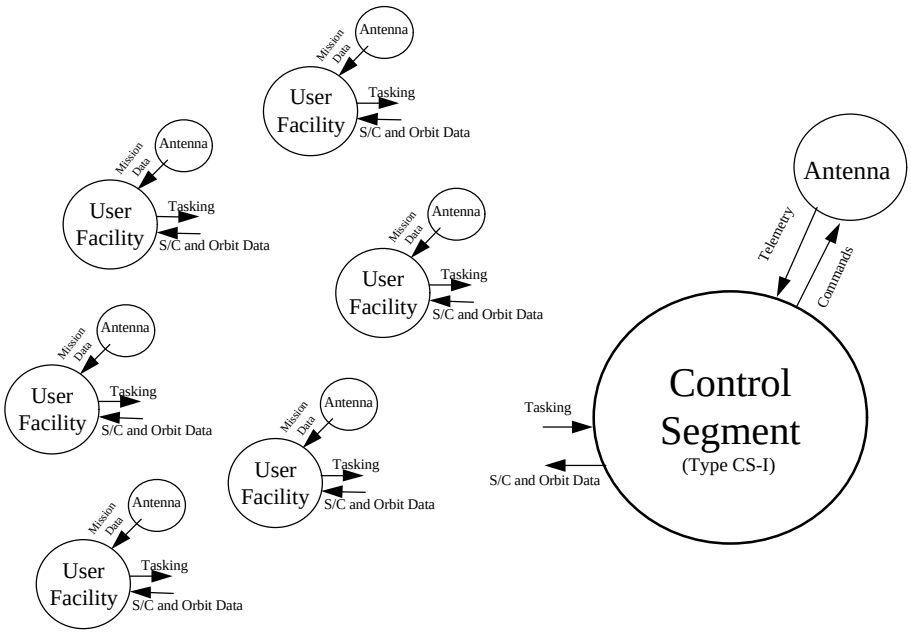

Figure 10. Architecture Options for Ground Elements: Separate Control and Distributed User Segment (US-III)

In all cases, the ground element architecture is a function of satellite orbit, system mission, and user requirements. The nodal descriptions and architectural depiction are not intended to be all-encompassing or even particularly precise. Instead, this combination of nodes and architecture should provide a rough model of what is critical in a space system. Based on this model, the system can then be evaluated for vulnerabilities.

Determination of Center of Gravity and Critical Node for Space Systems

To identify a system's vulnerabilities is to search for its center(s) of gravity. Clausewitz said the center of gravity is "the hub of all power and movement, on which everything depends."[7] With this definition alone, it would appear that the spacecraft is the center of gravity and "the point against which all our energies should be directed."[8] The on-orbit asset is the basis of existence for a space system because it performs the mission.

In his report, "The New Sword: A Theory of Space Combat Power," Lt Col Mantz provides a detailed description of how external sources can disrupt on-orbit functions.[9] As evidenced by his paper, direct attack against a satellite is neither a simple nor inexpensive undertaking. The spacecraft itself may be broken by simply throwing a rock at it. However, lifting that rock into orbit requires both the technology to lift the "weapon" and the precision to actually hit the target. In addition, remote disruption of a satellite's uplink or downlink also requires high-power amplifiers or exotic directed-energy weapons. Further, there is a common practice of using uplink encryption which makes direct interference much more difficult. While many of the hostile options are possible, the amount of investment and effort required makes this type of attack both difficult to perform and difficult to conceal. Beyond the issue of vulnerability, risk to the attacker should also be evaluated. Certainly the physical risk of attacking an on-orbit asset is small. The political risk, however, is exceptional. Concealment of a missile launch is just not possible with today's on-orbit assets. Development, testing, and employment of high-energy systems is difficult to hide. The physical size of the associated device and level of technology required limits the number of potential players significantly. One note should be made on the popular "put a nuclear device in orbit and take out the spacecraft" theory. Certainly this is viable from a technology perspective for some adversaries but, if the enemy blinds us they may also blind themselves. One cannot discount this approach as a possibility, but would an enemy be *likely* to employ this option? This option is an example of one which is recognized to exist but should not be used as a basis to ignore more

realistic, and subtle, alternatives. Direct attack of the center of gravity is possible, but not always practical. This is where nodal analysis comes into play.

Nodal analysis identifies the centers of gravity but recognizes that direct attack may not be possible or desirable. It evaluates the entire system and looks for a way to achieve the desired affect against the center of gravity by attacking a critical node. A critical node is one which, when affected, produces "cascading effects" that cause the system to change as desired.[10] The interdepencies of a space system make nodal analysis particularly applicable. To determine the critical node of a system requires evaluation of the links more than the physical elements.[11] Understanding the relationship between the physical elements allows determination of what cascading effects are created when a node is removed or altered.

Based on the simplistic space system model, alternatives to direct attack are to either eliminate the User Segment or eliminate the Control Segment. Table 2 shows a high-level segment versus vulnerability and risk assessment based on either centralized or distributed user architecture. Looking first at the User Segment, we can glean a few key facts. First, the User Segment is vulnerable to practical weapon systems. A truck full of explosives can take out an antenna, the infrastructure, or data processing. No current satellite system provides extensive physical security beyond armed guards and entry control. As evidenced by terrorist experiences such as the bombing of the Khobar Towers in Dharain, Saudi Arabia, this level of security is insufficient to prevent damage by a determined foe. Further, placement on US soil is also not a guarantee of protection (witness the Oklahoma bombing). Other options include a handheld missile through the antenna (not easily

replaced) or disruption of the commercial power supply. Often, power supplies are backed up by generators, but this is not always the case. In the macro sense, however, complete elimination of the User Segment is not always possible. With distributed architecture, the data can be recorded and dumped to an alternate facility (a common feature). Even more important, the actual center of gravity (the spacecraft) is still producing its product.

Table 2. Segment Impact versus Risk and Vulnerability

User Architecture	Segment to Eliminate	Impact to Mission	Vulnerability*	Physical Risk**	Political Risk**
Centralized	Space	Stop	Low	Low	High
	User	Stop	High	Moderate	Moderate
	Control	Stop	High	Moderate	Moderate
Distributed	Space	Stop	Low	Low	High
	User	Disrupt	High	Low	Moderate
	Control	Stop	High	Moderate	Moderate

** To attack*
*** To attacker*

The Control Segment is also a soft target. It has the same physical vulnerabilities as the User Segment. Evaluation of the Control Segment (Figure 4) shows that it is the command generation node that is the most critical node in this segment. Depending on orbit characteristics, elimination of the antenna is only important if there is only one antenna to communicate with the spacecraft. This is not the case for those systems on a global grid. While there may be more than one antenna, however, there is usually only one spot where the analysis, plans, and protocols come together to create the commands which control the spacecraft. Using the J.F.C. Fuller concept of brain versus body warfare,[12] the command generation node represents the brain of the space system. It

receives all the inputs and directs the actions of the system. The spacecraft will only do what it is told, it is the "arms and legs." It is for this reason that the elimination of the command generation node represents the "shot to the (space) brain."

Evaluation of the Control Segment at the macro level further supports this concept. First, the Control Segment architecture is not distributive. For unity of effort, cost, and security reasons, the ability to command the spacecraft is usually limited to one or two sites. In fact, the "second" site may be capable of performing only spacecraft health and safety support. Second, eliminating the Control Segment directly impacts the Space Segment. As mentioned above, the cascading effect of stopping commands from getting to a spacecraft directly impacts its ability to perform its mission. If the Control Segment is taken out for an extended period of time, depending on orbit characteristics and spacecraft design, the entire satellite could become irretrievable. Unexpected entry into autonomous safekeeping may result in eventual low-power shutdown of the spacecraft's ability to receive commands. Long-term orbital motion could eventually overwhelm the attitude control system, also making re-establishment of contact difficult, if not impossible. There is no magic formula to say how long before a spacecraft is totally lost (versus just losing the mission). It is a multivariate problem that requires specific program evaluation.

While both ground elements (control and user) provide practical alternatives to direct assault on the spacecraft, the Control Segment is the most likely system to produce the desired affects. It not only disrupts the immediate mission, but recovery is much more complicated due to the cascading effects on the on-orbit asset and the less-distributive nature on the control function. As expressed in Table 2, while each segment of the space

system can be attacked, evaluation of the vulnerability of the system verses the risk to the attacker demonstrates that the indirect approach is the best alternative. Based on the nodal analysis described above, the conclusion is that a "shot to the (space) brain" (i.e., the command generation node of the Control Segment) is the most practical way to take out a space system.

Table 3 takes this analysis a step further by assigning risk categories based on Control Segment features versus likely impact. This table will be used as a guide to evaluate the risk for continued service for specific programs. The next chapter will discuss what drives the design of the Control Segment, as well as provide details on four programs currently (or in the near future) providing service to the military.

Table 3. Risk Categorization

Category	Impact	Example
NONE	Mission disruption unlikely or very transient	A control segment with geographically separate redundant access to on-orbit assets. On-orbit assets with robust autonomous safekeeping
LIMITED	Mission disruption in the short term but eventual recovery of services likely	A control segment with internal redundancies combined with a robust on-orbit safekeeping system
MODERATE	Mission disruption in the short term with recovery of services in jeopardy	A control segment with limited redundancies as well as limited autonomous safekeeping on-orbit
SEVERE	Mission loss as well as total loss of asset likely	A unique control segment with little redundancies or a on-orbit asset with no autonomous safekeeping

Notes

[1]Michael R. Mantz, *The New Sword: A Theory of Space Combat Power*, Air University Research Report AU-ARI-94-6 (Maxwell AFB, AL., Air University Press, May 1995), 9.

[2]Kurt Daniels, "Nodal Analysis ToolBook", Air Command and Staff College Hypertext Multimedia ToolBook, War/Theater Level Studies Department, 1996, n.p., available on-line on the Air Command and Staff College network, November 1996.

[3]Pattan, vi-vii.

[4]Pattan, 148.

[5]Pattan, 263.

[6]Dan Schowalter, Canadian Space Agency Manager of Spacecraft Operations for Radarsat, interviewed by Author, 14 February 1997.

[7]Carl von Clausewitz, On War, ed. and trans. Micheal Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 595-596.

[8]Ibid.

[9]Mantz, 67.

[10]Daniels, "critical node" page.

[11]Daniels, "critical node" page.

[12]J. F. C. Fuller, "Tank Warfare," in *The Art of War in World History*, ed. Gerard Challiand, (Berkeley and Los Angeles, C.A.: University of California Press, 1994), 923.

Chapter 4

Current Commercial and Civil Systems

The focus of this chapter is to review current practices regarding command and control sites for commercial and civil programs. This analysis will include a discussion of the doctrine or guidance available, as well as programmatic drivers for development of the control site. Details regarding SPOT, Radarsat, Landsat, and INTELSAT will be discussed in light of the nodal analysis developed in Chapter 3. Final observations will be provided regarding general vulnerabilities from a macro perspective.

Standards and Guidance

No domestic or international standards exist regarding the development or architecture of a command and control site. A review of available literature did reveal a draft American Institute of Aeronautics and Astronautics (AIAA) standard on control sites, but found this limited in scope. Per discussion with Jim French who is responsible for the draft, the new standard addresses issues of interoperability (e.g., power supply, data formats) and not reliability concerns. For military, civil, and commercial systems, the guidance for what is required at the control site is program unique. For example, the Air Force's Remote Tracking System and Network are guided by a Systems Operational Requirements Document (SORD) which provides basic security and reliability guidance

for that particular system.[1] There is no one particular document which drives control site architecture for all US military satellite systems. There are, however, two Air Force Instructions on electrical services for facilities which support satellite command and control. These are AFI 32-1062[2] and 32-1063[3] and they require an emergency backup power supply called a UPS (Uninterruptable Power Supply). Per AFI 32-1063, other aspects of special-purpose facilities (such as satellite command and control) are handled within initial program requirements definitions.

For US civil system, such as Landsat, there is specific NASA guidance which applies to all of its systems. Simplistically, NASA breaks down their space programs into two classes. Class A programs are the large programs whose failure could result in loss of human life (e.g., the Shuttle). Class B programs are those smaller endeavors whose failure could result in loss of science (e.g., Solar and Heliospheric Observatory, SOHO).[4] Class A systems require fairly extensive redundancies in infrastructure whereas Class B systems are allowed to have "single string" command and control setups. From the NASA perspective, a loss of the Shuttle is a direct loss of life whereas a loss of a weather satellite will not directly result in loss of life. From a military perspective, this means that GOES (weather data) and Landsat are both Class B systems.

Programmatics

If there are no universally accepted standards regarding control sites, then how a site is designed is driven by programmatics. For the purposes of this paper, the term "programmatics" incorporates system requirements, risk tradeoffs, and funding levels which shape how a system is designed and operated. While all space system designers

would naturally prefer the most reliable architecture possible, fiscal realities require tradeoffs between the system requirements and reasonable risks. It is in the area of programmatics that a comparison of "mindsets" amongst the three categories of systems (military, civil, and commercial) is most revealing. At issue is what drives the system design in the first place and what is the penalty for non-performance.

The military mindset, from a simplistic perspective, is to ensure that the space system provides the required services regardless of conditions (hostile or peacetime). To that end, some programs are driven by satellite hardening and ground station survivability requirements that have Cold War origins. The impact of this tradeoff can be seen in some of the capabilities available. Cost is significantly increased and performance is often limited. For example, the MILSTAR program is a highly reliable, survivable, communications system, but is not the practical solution for large bandwidth requirements of a multinational peacekeeping mission. Is an extremely reliable, survivable system necessary for the military? Absolutely. At the end of the day, a baseline command and control capability must be available to ensure some level of access between higher headquarters and forces in the field. Is it practical or required to expect all military communications to go through such a system? Not in a fiscally and time-constrained world. The practical solution is to have a combination of both highly reliable, survivable communications links, as well as large-bandwidth systems. On a day-to-day basis, the performance of the on-orbit asset is based on how well it provided its service and how available the system was to its military customers. Accountability for gaps in service are a function of system importance to the particular customer. For example, a gap in GPS service over the Antarctica is not likely to cause a big issue. A gap in GPS service over Bosnia will receive

high-level attention and investigation. In times of war, non-performance by the military system could result in loss of life. In all cases, the feedback is from military members to military members. A direct relationship that could impact future program decisions.

The civil mindset is to provide the best service it can within the budget it has justified. The NASA concept of "loss of life" versus "loss of science" is the single most important driving factor for reliability and survivability issues. For example, although all NASA satellite systems are required to have uplink encryption for their spacecraft, the first step most Class B program managers take is to obtain a waiver to that requirement.[5] A NASA science asset is only as valuable as the data and dissemination of the data that it produces. From their perspective, the program funds are best spent on the on-orbit capabilities and user throughput. Furthermore, the typical autonomous safekeeping mode of the spacecraft is only 24-48 hours before the satellite is at risk for permanent loss.[6] This drives down on-orbit costs, as well. Regarding accountability, the science and weather community view the value of the product in terms of data quality and availability. The global weather system is a combination of military and civil systems, so actual gaps in world coverage are less likely. When they do occur, feedback from the customer is direct (the National Weather Service) and immediate, but not punitive. Gaps in the unique science data provided by the non-weather systems has historically been par for the course for the scientific community. Feedback is not direct because Congress is the one who foots the overall program bill but they are not direct users of the program's data. Data customers pay for data media not operations and maintenance costs.[7] Data customer feedback is also not likely to be in "real-time" and will not be punitive. A tradition of non-performance, on the other hand, would eventually result in a program review or

cancellation by Congress. The future Landsat 7 system, however, will have a more "real-time" mission and will thus receive more direct and immediate feedback for non-performance.[8]

On both the military and civil side, the daily impact for non-performance is generally a feedback issue. Direct accountability for those who designed the system is not likely. Direct accountability for those who operate the system is more realistic but less likely to be punitive because the "operators" are limited to operating a system within the budget provided. The commercial sector, however, is a completely different mindset.

The commercial mindset is driven by the profit-motive. Failure to provide "data continuity" is directly related to profit and is a major issue for commercial programs.[9] Interviews with representatives from both SPOT and Radarsat (CCRS) both emphasized the issue of data continuity. Survivability in a hostile environment is not a cost driver for the on-orbit asset, but ensuring that the data can reach the user is critical. The key for the commercial industry is to develop a system in a unique or lucrative market niche and then keep costs down in order to maintain profit. The regulator on cost cutting is in the penalty for non-performance. The accountability for non-performance is direct and immediate. Failure to deliver data means loss of revenue. Consistent failure to deliver data will result in a loss of credibility and ultimate loss of business. Failure to make a profit will also result in loss of a satellite program.

Control Segment Information on Specific On-Orbit Systems

In conducting research on current civil and commercial satellite programs it was clear that the program emphasis lay in the on-orbit assets and the user services provided. Most

open-source literature provides details (and sometimes samples) of the product, as well as a few details on the satellite orbit and coverage areas. Personal interviews were required in order to find specific information regarding the Control Segment for these programs. Information was obtained on Landsat, SPOT, Radarsat, and INTELSAT.

Landsat

The Landsat program is a series of remote sensing satellites, in sun-synchronous orbit, with a Multi-Spectral Sensor and Thematic Mapper.[10] The program has been operating for over twenty years and has been used for agricultural, pollution monitoring, academia, and governmental missions. Landsat 5, launched in 1984, is still the workhorse of the program due to a failed launch attempt of Landsat 6 in the early 1990s. Landsat 7 is due for launch in 1997 and has improved capabilities based, to a great extent, on the demonstrated utility of the system in Desert Storm (see Chapter 2). Prior to Desert Storm, the program was plagued with a series of programmatic crises. At one point the money for continued daily operations was removed from the NASA budget.[11] The successful use of the multispectral data for mapping and other unclassified data sharing with multinational partners turned around the Landsat program in the early 1990s and resulted in the funding of two new systems (Landsat 6 and 7).

Landsat 7 has a brand new Control Segment call the Mission Operations Center (MOC) at NASA's Goddard Spaceflight Center in Maryland.[12] This is where basic command generation will occur. Uplinks to the satellite will be through the five ground stations associated with the Mission to Planet Earth. One of these is specifically the Landsat Ground Station in Sioux Falls, SD.[13] These ground stations receive the commands from the MOC via NASA's Space Network (including TDRSS) and relay the

commands to the spacecraft. Consistent with NASA Class B guidance, there is no command generation capability. From an infrastructure perspective, all the ground stations, as well as the MOC, have a redundant uninterruptable power supply systems, standard facility security, and controlled access to operations. The MOC is located on Goddard Spaceflight Center which is a large complex of buildings just outside of Washington, DC. From a security perspective, access to Goddard has control points of entry and identification of which building performs what particular function is not intuitive. There are no large, obvious, "golf ball" targets. If a potential adversary was able to determine where operations were being conducted, the actual building, however, is a soft target. The uplink to the spacecraft has received a waiver for encryption, but it does employ a reliable error-correcting encoding structure for commanding. The spacecraft has a safehold feature which will allow mission to continue for up to 24 hours and the satellite to remain unattended for up to 48 hours.

Based on the nodal analysis discussion in Chapter 3, Landsat exhibits a moderate level of vulnerability in its architecture. The lack of command generation redundancy combined with a relatively short safehold feature on-orbit leaves the system at serious risk if the MOC is attacked. On the other hand, the redundancies in the infrastructure provide a level of protection from natural disasters or external attack on the commercial power supply. Further, a determined attack against the MOC requires entry onto the Goddard Facility and foreknowledge of the exact facility location. Open-source literature does not pinpoint the MOC's location. Finally, the distributive nature of the ground stations means that if one uplink antenna was removed, four others would be available to accomplish the required commanding.

SPOT

SPOT is a satellite system designed by the Centre National d'Etudes Spatiales (CNES) in France. CNES operates the current two active satellites and the SPOT Imaging Corporation provides worldwide data services. SPOT provides high resolution, stereo imaging in either a panchromatic (black and white) with 10-meter resolution picture or a 20-meter multispectral color composite image.[14] SPOT recently lost its premier SPOT 3 spacecraft due to a sudden, catastrophic failure. The automatic safekeeping mechanism apparently failed as well and did not save the vehicle. It was declared lost after a few days.[15] The experiences of SPOT 3 underscore the critical nature of the autonomous safekeeping function in on-orbit assets (see Chapter 3). Figure 11 shows the ground station worldwide layout. The two sites in black, Toulouse, France and Kiruna, Sweden are the principal Control Segment locations, as well as the primary receiving stations.[16] Per Mr. Louie Laurent, the CNES Air Attaché, there is a third ground station in Pretoria (South Africa). In case of emergency there is two more stations in the CNES 2 GHz network that can be activated in Kourou (French Guyana) and Kergelen (Indian Ocean). Toulouse is the primary SPOT Control Center. [17] Regarding infrastructure redundancies, "all the equipment are (sic) running in 'hot' redundancy and the ground station(s) are equipped with backup electrical unit(s)".[18] CNES developed its own standards for ground station development. As mentioned earlier, the SPOT system does have a "safeguard mode" in case something goes wrong.

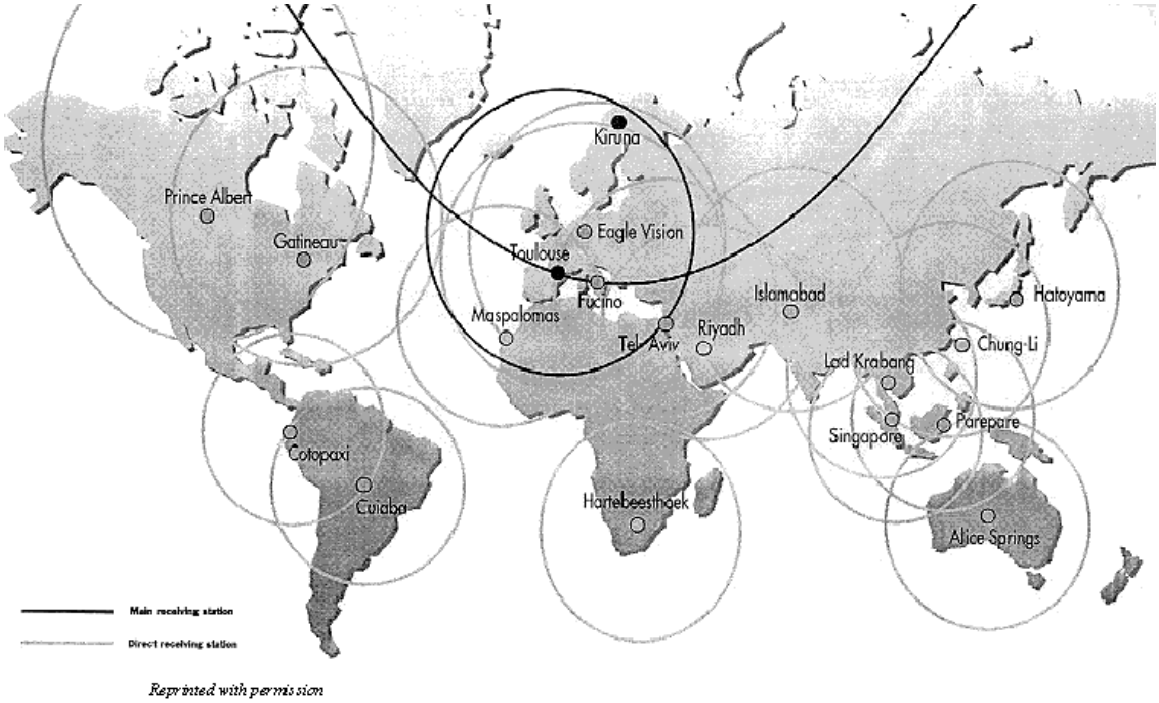

Figure 11. SPOT Receiving Stations

Based on the nodal analysis of Chapter 3, it would appear the SPOT system has limited vulnerability to hostile attack. Although the individual sites are soft targets, they have the requisite infrastructure redundancies. Even more critical is the existence of a completely redundant command and control capability which means that a total loss of mission is not likely. The existence, although questionable, of the safeguard mode means that the satellite will be available in the event that there is a ground station disruption.

Radarsat

Radarsat is a Canadian venture into remote sensing using a Synthetic Aperture Radar (SAR). This is an active sensor based on radar technology that provides detailed images of the earth even in the presence of darkness and cloud cover.[19] The program is considered "quasi-commercial" because the product is sold through a commercial business, but the system was built and is operated by the Canadian Space Agency (CSA).[20] It is also

considered an international program because NASA provided the launch vehicle and launch operations. Ball Corporation of the United States is the manufacturer of Radarsat.

Radarsat has one primary ground control site at Saint-Hubert in Quebec. This is a Canadian Space Agency (CSA) facility which is operated by a mix of government and contractor employees. Radarsat has two principal S-Band uplink sites and access to NASA's Deep Space Network (three more uplinks) for emergencies. With a low-earth orbit and limited ground stations, the system is designed to operate fairly autonomously. The spacecraft is a three-axis sun-synchronous system. The two stations see seven or eight passes of the spacecraft a day for 15 minutes each pass. This results in about 80 minutes of actual control commanding time a day. Mission profiles are for 24 hours. As with other programs, there is a "skyhold mode" for autonomous safekeeping in the event of attitude control problems. This mode has the requisite power-down and thermal and momentum management to ensure the spacecraft is relatively safe for an extended period of time (weeks versus days). [21] In part due to the robust nature of their spacecraft, the focus of the system reliability issues for the Control Segment has been on mission availability. As a relatively new program, the on-orbit asset has had a few problems which required an upload of new mission software in October 1995. A new version of attitude control flight software is expected in the next few months. Despite this, the autonomous features of the spacecraft have been remarkably stable.[22]

Regarding standards, CSA does use NASA's Consultative Committee for Space Data Systems (CCSDS) standards for data, but they developed their own requirements for the ground stations. They conducted a whole system availability analysis and the result is extensive redundancy for their commanding strings. Their focus is day-to-day operations

and they do not have a disaster recovery plan (although one is in the works).[23] From a day-to-day perspective, their biggest concern is power. They have a distributed UPS architecture and a separate generator on their antenna. They are not an isolated facility and believe they have appropriate access to emergency services. From a weather perspective, they do not experience climate extremes (e.g., heavy snow, tornado, or hurricane) but they do a have concerns with earthquakes. An earthquake registering 6.5 on the Richter scale is experienced approximately every 75 years. To that end, they have a building designed to support a magnitude 7.5 earthquake. They don't pay for any other type of disaster avoidance because, like all programs, they have a budget to worry about. Although they do not have a specific disaster recovery plan, the spacecraft operations manager, Mr. Dan Schowalter, was well aware of all the various vulnerabilities and had a draft plan in work.

Regarding physical security, the building has standard controlled access with an unarmed security guard at the single entrance. Interior rooms for command and control have two separate push-lock systems to further restrict access. The building is in an office park (versus government compound) and has a large 10-meter dish (without a radome) sitting next to it. Security cameras are placed in the building and around the antenna. Mr. Schowalter acknowledged that the antenna itself is fairly vulnerable, but the existence of a separate uplink site was a risk mitigator.

Based on the nodal analysis of Chapter 3, Radarsat is at limited to moderate risk from a vulnerability perspective. The office park location of the single source for command generation provides very limited protection but the on-orbit asset is exceptionally robust. The facility has the appropriate power and redundancy infrastructure, but a determined

attacker could disrupt mission for several days (after the mission profile expired) using a low-tech attack.

INTELSAT

INTELSAT is the "world's largest commercial satellite communications services provider."[24] There are 23 satellites in orbit providing voice/data and video communications worldwide. It is an international, profit-based consortium which has been in place since 1964. Companies and countries become "signatories" to the INTELSAT agreement and then operate the services in a particular area. Manufactures of the satellite include Loral, Hughes, and Lockheed-Martin. This means that not all of the on-orbit assets are of the same design. For example, the Hughes-built INTELSAT 6 is a spin-stabilized spacecraft whereas the others are three-axis stabilized. There are six major INTELSAT TT&C facilities: Italy, Germany, Australia, China, and two in the US (Maryland and Hawaii).[25] This is a geosynchronous satellite system with constant access for each satellite to at least two ground stations. This requirement to ensure access to two ground stations provides a baseline reliability that ensures minimum commanding. Per the US National Policy on Application of Communication Services to US Civil and Commercial Systems, all uplink commanding is encrypted.[26] Another programmatic approach towards reliability is in their service hierarchy. Customers can buy "non-preemptable" service from INTELSAT.[27] This means that is if a particular spacecraft was unavailable, non-preemptable service would be quickly routed via other assets. The DOD pays for this more-expensive non-preemptable service to ensure that our critical communications. From a user perspective the actual number of earth stations are unknown. In fact, the INTELSAT Internet web

page provides detailed instructions on what is required to build, test, and register receiving stations.

Although the individual uplink control stations are no more robust than any other Control Segment, the ground station architecture is exceptionally redundant.[28] Specifically, INTELSAT has a main control center in Washington DC as well as the six ground stations. Each control station is internally redundant. All ground stations are manned but commands are usually only sent from the main control center. Each ground station, however, has the capability to command with a limited number of command sets. In addition, INTELSAT has a fully redundant control center at a separate geographic location in Washington DC. This redundant center is exercised every six month where actual operations are conducted from the backup location.[29] The existence of complete redundant command and control sites combined with the plethora of on-orbit assets and downlink receiving stations makes INTELSAT very reliable. Based on Chapter 3's nodal analysis, INTELSAT service is at "limited to none" risk for a hostile attack due to the redundancy in their Control Segment architecture.

Observations at the Macro Level

This analysis has focused in on individual systems and their vulnerability to hostile attack. This is not the only perspective, however, that should be considered. Another perspective is that of the military customer. While individual system support to the military customer can be disrupted, at issue is whether or not this service represents a critical node or center of gravity for the individual user. Figure 12 shows two types of services in a notional depiction. The bottom line is clear: although removal of an

individual source would likely have an effect, the greater the number of independent sources providing similar information the more likely the required service will be provided. There is no one source that, if eliminated, would result in total loss of service. Further, the fact that this single node does not exist means that the need to eliminate one source is not as great. Although it certainly would have great harassment value, the tactical value of eliminating a source may not be worth the political and military risk to make the attack. In essence, commercial and civil systems increase security for continued service because they prevent creation of a critical node.

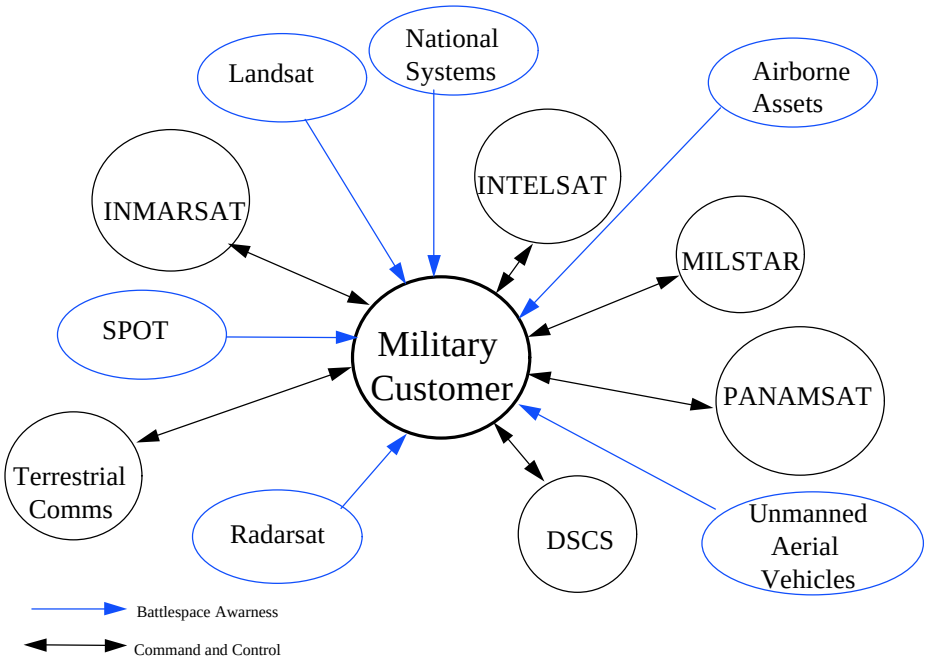

Figure 12. Remote Sensing and Communication Support

Notes

[1]BGen William E. Jones, Air Force Satellite Control Network (AFSCN) Remote Tracking Station (RTS) System Operational Requirements Document (SORD) #019-89-I/II/III (Rev 1), 22 October 1992.

[2]Air Force Instruction (AFI) 32-1062, *Power Supplies*, 10 May 1992, 6.

[3]Air Force Instruction (AFI) 32-1063, *Electrical Power Systems*, 31 March 1994, 6.

Notes

[4]Bob Menrab, Landsat Ground Systems Manager, interviewed by author 11 December 1996.

[5]Ibid.

[6]Ibid.

[7]Keith D. Walyus, Project Operations Director for Solar and Heliospheric Observatory, interviewed by author, 11 December 1996.

[8]Menrab.

[9]Colleen Hanley, SPOT Image Marketing and Communications Specialist, interviewed by author, 30 October 1996.

[10]"Welcome to the LANDSAT Program," *Landsat Program*, 13 November 1996, available from http://geo.arc.nasa.gove/sge/landsat/landsat.html.

[11]National Aeronautics and Space Administration, National Oceanic, and Atmospheric Administration, and the U.S. Geological Survey, "Landsat Program Management Plan," *Landsat Program*, on-line, Internet, 13 November 1996, available from http://geo.arc.nasa.gov/sge/landsat/mgmtplan.html

[12]"Landsat Mission Operations Center," *Landsat Program*, 13 November 1996, available from http://geo.arc.nasa.gov/sge/landsat/L7moc.html.

[13]Menrab.

[14]"SPOT System: Payload", *SPOT Image*, on-line, Internet, 12 February 1997, available from http://www.spot.com/anglaise/system.satel/ss_paylo.html.

[15]"Spot 3 Satellite Stops Working," *Space News*, 18-24 November 1996, 24.

[16]Material provided by Colleen Hamley, SPOT Image Corporation, November 1996.

[17]SPOT User's Handbook, *Reference Manual*, vol 1, (Reston V.A.: SPOT Image Corporation, May 1989) 4-12.

[18]Louis Laurent, CNES air attaché to U.S., e-mail to author, subject: Question on SPOT System, 3 January 1997.

[19]"RADARSAT Specification Sheet", *RADARSAT*, on-line, Internet, 22 October 1996, available http://radarsat.space.gc.ca/ENG/RADARSAT/specification_sheet.html.

[20]Schowalter.

[21]Ibid.

[22]Ibid.

[23]Ibid.

[24]"INTELSAT Overview," *Discover INTELSAT*, on-line, Internet, 12 February 1997, available from http://www.intelsat.int/cmc/info/intelsat.htm#WhatIsIntelsat.html.

[25]Pattan, 202.

[26]Dr. Al Dayton, COMSAT RSI, interviewed by author, 14 February 1997.

[27]Thomas.

[28]Joseph Jankowski, INTELSAT Manager for Sales Support, interviewed by author, 12 March 1997.

[29]Neil Hauser, Scitor Corporation, e-mail to author, subject: INTELSAT's approach to risk reduction, 15 December 1996.

Chapter 5

Conclusions

The move to increased reliance on commercial and civil assets is a fact. National policy, fiscal realities, and mission requirements will drive the need to use whatever means are available to increase battlespace awareness. The CSCI program and Eagle Vision are two examples of how the military commander will be directly reliant on these systems for future engagements.

Does the reliance on civil and military systems create a special vulnerability? Based on the small sampling taken, it would seem that the profit motive for the commercial side might be sufficient to protect against realistic threats. In both cases (SPOT and INTELSAT), complete redundancy of the control station significantly improved the reliability of these systems. The civil (Landsat) and quasi-commercial (Radarsat) ventures did not fare as well. In both cases, elimination of the single control station would take the systems out of mission for an extended period of time. Further, the cascading effect on the Landsat system would likely lose the asset if commanding was not reestablished within 48 hours. It would appear that the civil systems lack not only the profit motive of the commercial sector but also the strong requirements driver of the military systems. At the macro level, however, the addition of these systems does create a difficulty for an adversary. Even if these civil systems are more vulnerable, they still provide an alternate

source of friendly information. The increase in the number of systems reduces the risk to any one source.

As a cautionary note, however, a military commander who becomes reliant on a particular system would be well advised to seek an evaluation of the entire space system (not just the on-orbit asset) to determine if there is reasonable security. The commander should deal with this question at both the system and macro level. At the macro level, he should evaluate what systems he requires (including military, civil, and commercial). Only the commander can determine which of those systems are most critical to his operation. If he has identified that a particular asset is the sole source of information or communications flow, then he must take steps to identify it as a friendly center of gravity and look for alternative sources or ways to increase reliability. At the system level, he needs to understand that many of the individual systems have at least limited risk for disruption to mission. Actual details on the current vulnerability of any particular system may not be readily available. The military commander must realize that he needs to have this information and should task through the J-2 or J-6 organizations to seek further data for planning.

This paper provides a framework for understanding what the vulnerabilities of space systems are and what types of vulnerabilities exist with current civil and commercial programs today. Reliance on these systems should not be feared so long as steps are taken to avoid creation of friendly centers of gravity. These systems are force multipliers which provide necessary information with a reasonable amount of risk.

Bibliography

Air Force Instruction (AFI) 32-1062. *Power Supplies*, 10 May 1992.

Air Force Instruction (AFI) 32-1063. *Electrical Power Systems*. 31 March 1994.

Briefing. Electronic Systems Command/ICI. Subject: Eagle Vision Program Status Briefing, January 1996.

Clausewitz, Carl Von. *On War*. Edited and translated by Micheal Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1976.

Daniels, Kurt. "Nodal Analysis ToolBook." Air Command and Staff College Hypertext Multimedia ToolBook. War/Theater Level Studies Department, 1996. Available on-line on the Air Command and Staff College network, November 1996.

Defense Intelligence Agency. *Multispectral Applications: The Intelligence Value of the use of LANDSAT, SPOT, and Aircraft Multispectral Imagery* (U). Washington D.C.: Defense Intelligence Agency, 1 September 1987. (Secret) Information extracted is unclassified.

"EarthWatch Satellites." *Earth Watch Satellites*. On-line. Internet. 18 February 1997. Available from http://www.digitalglobe.com/company/satellites.html.

French, Jim. "Space Systems: Ground Support Equipment - General Requirements (ISO 14625)." Draft. Washington D.C.: American Institute of Aeronautics and Astronautics, 1996.

Fuller, J.F.C. "Tank Warfare." In *The Art of War in World History*. Edited by Gerard Challiand. Berkeley and Los Angeles, C.A.: University of California Press, 1994.

Government Accounting Office. *Space Operations: NASA's Communications Support for Earth Orbiting Spacecraft*. Government Accounting Office Report GAO/IMTEC-89-41. Washington D.C.: U.S. Government Accounting Office, April 1989.

Hauser, Neil, Scitor Corporation. E-mail to author. Subject: INTELSAT's approach to risk reduction. 15 December 1996.

Hawly, Gen Richard E. *Foreign Comparative Test Program Final Test Report Executive Summary for Eagle Vision Deployable Satellite Ground Receiving and Processing System*. APO AE 09094: Headquarters United States Air Forces in Europe, 14 December 1995.

Headquarters Air Force Space Command/XPCD, *Air Force Satellite Control Network (AFSCN) Network Control Segment (NCS) System Operational Requirements Document (SORD) #018-89-I/II/III (Rev 1)*, 16 June 1992.

Hughes, David. "RADARSAT Delivers First SAR Image." *Aviation Week & Space Technology*, no 144 (1 Jan 1996): p 27.

"INTELSAT Overview." *Discover INTELSAT*. On-line. Internet. 12 February 1997. Available from http://www.intelsat.int/cmc/info/intelsat.htm#WhatIsIntelsat.html.

"IRS 1C—In a Class of Its Own," 28 December 1995. *Recent News*. On-line. Internet. 5 March 1997. Available from: http://marge.genie.uottawa.ca/mandalm/space/recent_news/irs-1c2.html

Joint Pub 6-0. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*. 30 May 1995.

Jones, BGen William E., *Air Force Satellite Control Network (AFSCN) Remote Tracking Station (RTS) System Operational Requirements Document (SORD) #019-89-I/II/III (Rev 1)*, 22 October 1990.

"Landsat Mission Operations Center." *Landsat Program.* On-line. Internet. 13 November 1996. Available from http://geo.arc.nasa.gov/sge/landsat/L7moc.html.

Larabee, John K., Director, International and Commercial Affairs (Office of Systems Applications) National Reconnaissance Office. To Scott Carson, Executive Vice President, Boeing Commercial Space Company. Letter. Subject: Eagle Vision II, 3 July 1996.

Laurent, Louis, CNES air attaché to U.S.. E-mail to author. Subject: Question on SPOT System. 3 January 1997.

Mantz, Michael R. *The New Sword: A Theory of Space Combat Power* (AU-ARI-94-6), Maxwell AFB, AL: Air University Press, May 1995.

National Aeronautics and Space Administration, National Oceanic and Atmospheric Administration, and the U.S. Geological Survey. "Landsat Program Management Plan." *Landsat Program*. On-line. Internet, 13 November 1996. Available from http://geo.arc.nasa.gov/sge/landsat/mgmtplan.html.

Office of Technology Assessment, U.S. Congress. *Civilian Satellite Remote Sensing: A Strategic Approach*. Washington D.C.: U.S. Government Printing Office, September 1994.

"OrbImage announces new Orbview Remote Sensing Satellite," 28 September 1995. *ORBVIEW Press Release*. On-line. Internet. Available from http://www.orbimage.com.news/ov5295.htm.

Pace, Scott. "Remote Sensing and Global Competitiveness" Lecture. Santa Monica: RAND, 1993.

Pattan, Bruno. *Satellite Systems: Principles and Technologies*. New York, N.Y.: Van Nostrand Reinhold, 1993.

Perry, William. "Annual Report to the President and the Congress: Space Forces." In *Operational Structures Coursebook*. Air Command and Staff College. Maxwell Air Force Base, AL.: Air Education and Training Command, November 1996.

"RADARSAT Specification Sheet." *RADARSAT*. On-line. Internet. 22 October 1996. Available http://radarsat.space.gc.ca/ENG/RADARSAT/specification_sheet.html.

Richharria, Madhavendra. *Satellite Communication Systems: Design Principles*. Houndmills, Hampshire: The MacMillian Press Ltd., 1995.

"Satellite System Architecture," *Space Imaging EOSAT*. On-line. Internet. 5 March 1997. Available from http://www.spaceimage.com/home/satellit.html.

Shalikashvili, Gen John M., Chairman of the Joint Chiefs of Staff. To the Secretary of Defense. Memorandum. Subject: Report of the Interagency Implementation Group on the Recommendations of the Defense Science Board Task Force on Improved Applications of Intelligence to the Battlefield, 23 Sep 1996.

Short, Nicholas M. *The LANDSAT Tutorial Workbook: Basics of Satellite Remote Sensing*. Washington D.C.: National Aeronautics and Space Administration, 1982.

"SPOT System: Payload." *SPOT Image*. On-line. Internet. 12 February 1997. Available from http://www.spot.com/anglaise/system.satel/ss_paylo.html.

"SPOT 3 Satellite Stops Working." *Space News*. 18-24 November 1996, 24.

SPOT User's Handbook. *Reference Manual*. vol 1, Reston VA.: SPOT Imaging Corporation, May 1989.

US House and Senate. *Joint Hearing before the Committee on Science, Space, and Technology and the Permanent Select Committee on Intelligence*, 102nd Cong., 1st sess., 26 June 1991.

"Welcome to the LANDSAT Program." *Landsat Program*. On-line. Internet. 13 November 1996. Available from http://geo.arc.nasa.gove/sge/landsat/landsat.html.