AU/ACSC/035/1999-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

PROTECTING COMMERCIAL SPACE SYSTEMS:

A CRITICAL NATIONAL SECURITY ISSUE

by

Charles H. Cynamon, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major Daniel C. Blaettler

Maxwell Air Force Base, Alabama

April 1999

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. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Page

Tables

Page

Preface

First and foremost, I must acknowledge the unwavering support of my wife, Eileen, as I spouted endlessly about why I wanted to write a research paper when ACSC offers electives. My two sons, Jared and Sam, put up with my endless hours of "hogging" the computer searching the Internet for data. Without the patience and support of my family, this thesis would have been dead long before I ever wrote it.

This research topic began as a curious interest and blossomed into a consuming quest for interested listeners as I regaled them with the logic stream that evolved and I provide herein. Major Dan Blaettler, my faculty research advisor, provided some serious vector to my thrust. While Major Russ Dodd (Air Force Doctrine Center) provided the initial interest and guidance, the folks working on the National Defense Industry Association (NDIA) Summer Study and the Air Force Defensive Counter Space (DCS) Working Group provided much of the hard data for my analyses. I must personally thank Ms Karen Fiorillo, Mr Usto Schulz, Major Lisa Schulz-Latsis, and Major Win Idle. Mr Terry Hawkins at the Air University Library provided enthusiastic support as well. Finally, Major Jeff Spencer was key to my continued motivation at ACSC and was a sounding board as I bounced numerous ideas around for this paper for many months.

Abstract

Commercial space capabilities are expanding. As they expand, the capabilities will increase in their military utility. These capabilities include communications, remote sensing, navigation, and imagery. Spending in the commercial space industry between 1995 and 2010 will top $100 billion. With the rise in commercially available services and declining defense budgets, the DoD will inevitably migrate traditionally dedicated space capabilities to commercial systems (communications, remote sensing, and possibly navigation). Since their ultimate goal is profitability (and rightfully so), industry considers countermeasures costly and unnecessary against threats they deem not likely. With our economic well-being increasingly tied to space, what role should the US Government play in assuring our access?

In the days of pirates, naval forces were essential to protect trade routes for friendly commerce. Naval theorists, such as Alfred Thayer Mahan, and maritime law provide thought-provoking analogies for the need to protect lines of communication, control the medium, and protecting national sovereignty. In addition, future projections of the strategic environment point to force-on-force space confrontation with peer competitors and asymmetric attack by niche competitors, hostile groups, and individuals. Therefore, protection of commercial space assets must be rooted in space law, space policy and doctrine with consideration for the aforementioned future strategic environment.

Key questions will address the impact on U.S. national security due to attacks on commercial space assets. What is the 'real' impact of commercial space on the U.S. economy (not just spending)? How would loss of commercial space capabilities impact U.S. war fighting capability? What constitutes an attack on a commercial space system? How do we deter and detect an attack? How should the U.S. respond to such attacks, proportionally or massively? Finally, what policy and process changes are needed to protect our national security?

Chapter 1

Background

> *Space. The possibilities are endless – but there are dangers there. As we explore the fullest promise of space, we must also get ready to protect our interests and freedoms there.*
>
> — Howell M. Estes III
> General, USAF (Ret)

Maritime Analogy

Contemporary thought in the US Air Force views both air and space as mediums in which future wars will be fought for superiority. [1] In an effort to make a convincing argument to "sell" space control to a nation which generally views space as the "last peaceful frontier," the space community often turns to an analogy, which more appropriately compares control of space to that of sea.[2] The following analogy is becoming a rallying cry for the protection of commercial space systems:

> In the early nineteenth century, the US Navy patrolled the seas to protect US merchant shipping from piracy at sea. Today, commercial payloads in space face similar threats from rogue nations and terrorists and, thus, require the protection of our nation's armed forces.[3]

Although this analogy does capture the basic need for protecting commerce in space, it does not tell the whole story. History has revealed the need to protect our sea lines of communication, but today the space environment is equally vital to the continuing military security and economic

prosperity of our nation.[4] Aside from the obvious physical differences in the mediums of sea and space, our use of the two has evolved in quite different manners. In recognizing similarities and differences in how we govern and use the mediums themselves, we can enhance the previous analogy to describe the need to protect commercial space.

A closer look at nations' rights to use both sea and space mediums reveals one major similarity with respect to governing international law and treaties. Both mediums have evolved to the point where numerous nations recognize international agreements governing peacetime use. Realistically, in wartime, the belligerents will use both mediums as deemed necessary to achieve national objectives even if treaty violations result. Another similarity concerns the exclusivity of sea- and space-faring nations by their ability to access the medium. As one of the premier thinkers on naval theory, Alfred Thayer Mahan, pointed out, [5]

> "The seaboard of a country is one of its frontiers, and the easier the access offered by the frontier to the region beyond, in this case the sea, the greater will be the tendency of a people toward intercourse with the rest of the world by it… Numerous and deep harbors are a source of strength and wealth…they become a source of weakness in war, if not properly defended."

In a similar manner, one could describe space-faring nations as either those with spaceports or the resources to access foreign launch services. Therefore, the key is the capability to gain and protect one's access to the medium. Lastly, both mediums present the user grave threats and hazards. At sea, mariners face lawlessness, in the form of piracy, and natural dangers, most notably, weather. In space, unmanned vessels could also face similar forms of lawlessness and natural dangers such as collision with natural and man-made objects. Because these similarities exist, the basic premise of the analogy is valid. However, it is through the examination of the differences that the analogy is strengthened.

The first difference is the initial use of each environment for primarily economic or military purposes. To the United States, the maritime environment was mostly an economic environment

in the early years following our founding. Although it was a means for global presence and power projection for the British and Spanish, the sea was America's only mode of transportation for trade with the world's hub of economic activity, Europe. This inter-continental trade was vital to our national interest. Conversely, our national use of space sprang directly out of the Cold War. Initially, space was a politico-military environment in which we competed with the Soviet Union. The military and civil space complexes sowed the seeds for commercial industry. Another major difference is the definition of sovereignty. In the maritime environment, even though the "high seas" are free, there are portions of the physical medium that are considered national territory. In space, freedom of navigation is a right enjoyed in all areas of the medium; it is only the vessels themselves, which are considered sovereign. Finally, the level of technology required to exploit the environment differs. Most any sea-faring nation can construct even crude vessels to use the sea without external aid. However, only a small fraction of nations can currently launch spacecraft and even the crudest vessels exceed the technological capability for most non-space-faring nations.

While this author agrees with the basic premise behind the original analogy, our understanding of the similarities and differences offer additional insight which only serve to strengthen the earlier analogy. The proposed analogy would be expanded as follows:

> In the early days of this country, the sea was a vital national interest because it was our eastern frontier and this country's lifeline to foreign markets. US naval forces patrolled the seas to protect our sovereign use of the sea against pirates and natural hazards. Today, space has become a vital national interest because it is our vertical frontier and a key to our own economic growth as a lifeline to emerging markets overseas. While we vigilantly surveil the medium, we have only limited means to protect our sovereign use against natural hazards and man-made threats.

This paper will take a systematic approach to first prove the vital nature of commerce in space. Once this is achieved, the means to protect space systems will be addressed.

Thesis Statement

Many in the national security arena will agree with the statement that space is vital for our national security. Our desire to protect the nature of US military space capabilities since the early days of the Cold War is proof of this assertion. However, it is seemingly a leap to state commercial space systems, in particular, are equally vital to our national security. In order to state unequivocally the need to protect commercial space systems, it must be shown that the loss of these capabilities represents a critical national security issue. Part one of this thesis will conclusively argue, at the strategic level, through an evaluation of reliance, threats and consequences that commercial space systems are vital to our national security and therefore require protection. First, the case will be made that there is a growing reliance in this country on the capabilities of commercial systems and the trend projects further increases in our reliance. Next, the paper will describe the emerging threats and hazards to commercial systems, which includes the space, ground, link and information segments. Lastly, qualitative descriptions will be given of the dire consequences if an adversary should deliberately and systematically attack our commercial space systems. Part two will describe, at the operational level, this author's theory for space protection and recommend a course of action to work cooperatively with industry to minimize vulnerabilities.

Notes

[1] Air Force Doctrine Document 1, *Air Force Basic Doctrine*, September 1997.

[2] This analogy is frequently cited in an academic manner as a comparison due to the nature of the physical mediums and the types of international agreements that govern its peaceful use.

[3] This research project is sponsored by the HQ Air Force Doctrine Center. This analogy is paraphrased from the expanded description of the topic furnished by AFDC.

[4] The White House, *A National Security Strategy For a New Century*, October 1998, 25.

Notes

[5] Mahan, Alfred Thayer, "The Influence of Sea Power on World History: 1660-1783" (excerpt). *Air Command and Staff College War Theory Coursebook* (Academic Year 1999), 87-88.

Chapter 2

Reliance on Commercial Space Systems

"Space has emerged in this decade as a new global information utility with extensive political, diplomatic, military, and economic implications for the United States."

National Security Strategy
October 1998

Some Numbers to Ponder

Twenty-four, sixty-six, two hundred eighty-eight, twenty, one thousand one hundred…. What does all this add up to? Anyone following the space industry knows the answer is not 1498. These numbers characterize the realities of the commercial space industry. The 24-satellite Global Positioning System (GPS), originally a military system, now has as many civilian applications as military. The 66-satellite constellation of Motorola's Iridium is just coming on-line. This system promises voice, fax and data communications connectivity worldwide.[1] Teledesic is a 288-satellite system, which plans to offer direct-to-home (DTH) "Internet-in-the-sky" services to the public by 2003.[2] The sum of all investment currently taking place in this country adds up to an annual industry growth in excess of 20%. If one believes this to be a temporary condition, they are gravely mistaken. Waiting in the wings to join these constellations are projects, which plan for another 1,100 satellites by 2008, providing personal and broadband communications, remote sensing, and environmental sensing services.

The purpose here is to go beyond just numbers to show the reliance these space systems have begun to create in both our civil and military sectors. Within the civil sector of our society, space systems are creating services for both business and individual consumers. For the military, the competing demand for procurement resources to replace obsolescent vital surface war fighting capabilities will make the reliance on commercial space systems attractive. Regardless, commercial space systems are proliferating in number, but are they gaining acceptance by consumers?

Civil Demand

For the civil sector of our economy, the resounding response to the previous question is yes. We are living in a society with an insatiable appetite for technology. For business, this appetite is fueled by efficiency and profit motives. For individuals, time is precious and anything to save time and maximize its value spent is marketable. As is the case with most high-tech products, initial high cost of a new technology product usually drives early appeal to business. With the passage of time, the cost for the product moderates and appeal to the individual consumer explodes (e.g., personal computers). The proof is in the industry estimates for use of products and services (Figure 1).[3] Between 1997 and 2001 this sector of the industry is predicted to grow 163%. By extrapolating out to the end of the first decade in the 21st century, this sector of the industry would grow by an order of magnitude over today. The products and services portion of the satellite industry is growing almost six times faster than the design, manufacture and launch of space vehicles sector. Projections for DTH television users and mobile communications subscribers are fueling these estimates. DTH equipment costs have decreased since introduction.[4] And the initial $2.96/minute and $2,795 personal communications

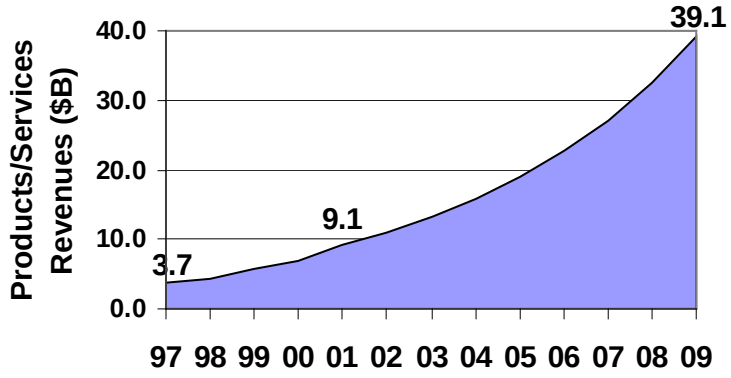

Figure 1. Products and Services Revenues[5]

system (PCS) phone[6] is likely to drop to capture more than just businesses and wealthier consumers. As a matter of fact, Teledesic is counting on the potential to connect not just offices and factories, but schools and homes as well.[7] The growing acceptance of a previously skeptical financial community further attests to investor confidence that the growth in commercial space is real, permanent, and probable. But, in reality, how does the investment in these space capabilities penetrate into the overall economy to affect our everyday lives?

Communications, navigation, and environmental and remote sensing are indispensable for our economy. These space capabilities impact our daily lives today but most of us don't recognize it. Communications satellites are an important part of the revolution in the telecommunications industry. Many Americans may not fully appreciate the significance of the "Live via satellite" caption on CNN, or 160 channels of digital TV. However, these are the icons of today which represent the *evolution of the revolution* from a single-channel transmission bounced off a Telstar satellite to multiple channels of integrated voice, data, fax and video transmissions via a broadband communications satellite. This is significant for the "connecting" of society. We are increasingly choosing to remotely transact business, to connect our computers to the Internet, to have an 18" satellite dish in lieu of cable TV (Figure 2), and to have the ability

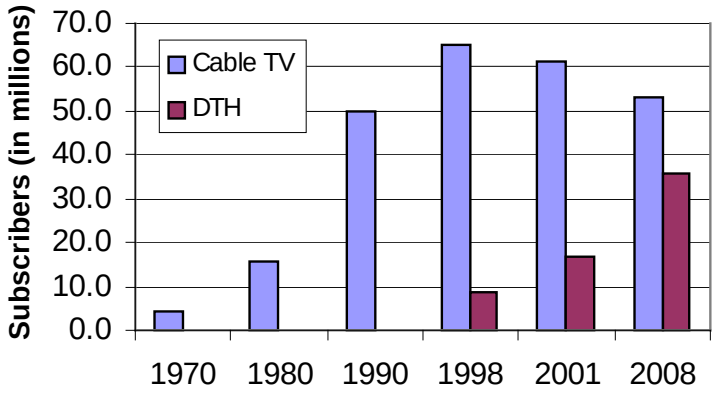

Figure 2. Cable TV and DTH Market Share Projections[8]

to contact anyone from anywhere with as small a phone as possible.[9] Likewise, the increasing use of navigation satellites such as GPS has entered our everyday lives. GPS will likely be the primary source for air traffic control for commercial airlines in the 21st century. We have already begun to produce automobiles with built-in GPS receivers for personal navigation.[10] Finally, sensing of our environment from space is crucial for predicting natural disasters and everyday weather, and for studying the earth's environment.[11] It's no exaggeration, the average person hardly realizes the extent they rely on commercial space systems. For most, the realization comes when the capability is lost, such as the failure of the Galaxy IV satellite in May 1998. The failure of that one satellite left about 80-90% of the 45 million pager customers in the US without service for 2-4 days and 5400 of 7700 Chevron gas stations without pay-at the-pump capability.[12] This failure left employees processing credit payments with the manual system they had long since forgotten.

Military Reliance

What the civil sector at large is now learning about the benefits of space capabilities, many in the military have known for years. The proclamation of the 1991 Gulf War by some as the

"First Space War" is, in essence, the acknowledgment of those benefits. The acceptance of space for a technology-bent organization like the US Armed Forces has actually been more of a struggle than for the general population. The space capabilities becoming available to the general public have been available to the military for years. To this point, the military has predominantly developed dedicated military space systems. However, this trend is rapidly changing as the current National Space Policy precludes the government from acquiring its own capabilities if suitable capability exists commercially.[13]

In addition to fostering economic growth in the space market, the National Space Policy recognizes the government cannot effectively compete with the commercial space market. The surge in commercial space capabilities coupled with post-Cold War declining defense budgets is forcing the DoD to weigh carefully which multi-billion dollar space systems it can afford to buy.[14] Dedicated military space systems are not likely to be procured when suitable commercial systems are available. Future investment in dedicated systems is likely to be in mission areas that provide capabilities uniquely military or to fill a critical redundancy such as: early warning (EW); navigation; intelligence, surveillance, and reconnaissance (ISR); and strategic communications. In reality, the military is already dependent on commercial space capabilities in force-enhancing missions such as non-strategic communications and remote sensing (Figure 3).[15] One need only look at our experience in the Gulf War to see the emerging trend. During Operations Desert Shield/Desert Storm, commercial satellites such as INTELSAT provided 45% of all communications between the theater and the CONUS.[16] The military strategic vision for the future is set forth in the Joint Vision 2010. Information superiority, as one of the key enablers for full spectrum dominance in the future, is "the capability to collect, process, and disseminate an uninterrupted flow of information."[17] Commercial space systems will be

essential for gaining and maintaining information superiority for all future military activities from major theater wars (MTWs) to small scale contingencies (SSCs). As shown, time will dictate the extent to which the military will be dependent on commercial space.

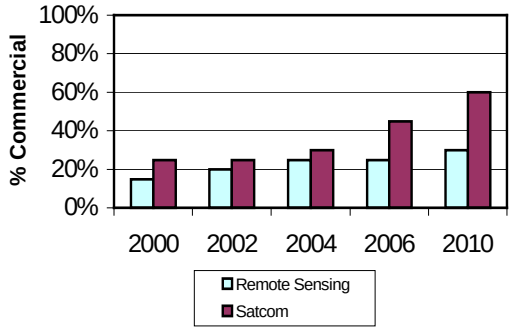

Figure 3. Growing Military Dependence on Commercial Assets

Summary

The road to this reliance has been short and welcoming to a technology-hungry society like the US. Our civilian and military leadership agrees US politics, economics, and armed forces are ever increasingly dependent on the informational functions provided by commercial space systems.[18] It behooves us to ask, "where are the potholes in this road?" or how will we protect this vital resource.

Notes

[1] "Space Almanac: Major Military Satellite Systems." *Air Force Magazine*, August 1998, 31.

[2] "Commercial Spacefarers." *Air Force Magazine*, December 1998, 44.

[3] Space Publications, *State of the Space Industry*, 1998, 8.

[4] DirecTV premiered in 1995 at home electronics stores for $499 for the basic dish/receiver equipment. Latest advertisements quote a price of $149.

[5] For a conservative estimate, calendar years 2002 through 2009 have been extrapolated with the average industry 20% annual growth rate. Note: the averaged rate of growth in this sector of the industry between 1997-2001 is expected to be between 22% and 35%.

Notes

[6] Motorola Inc quote for Iridium satellite phone, received 16 Feb 99. Based on a Satellite Portable (8817) phone, model #S8432A, with $200 cash back rebate. The quote for $2.96/minute is for satellite phone service. Not included are any other initiation or usage fees.

[7] "Commercial Spacefarers." *Air Force Magazine*, December 1998, 44.

[8] Charted data from two sources: (1) Space Publications. *State of the Space Industry*, 1998, 42, 49; and (2) US Census Bureau, *Statistical Abstract of the United States: 1998*, 1 Oct 1998, 578. Data up to and including 1997 is actual data. DTH projections based on DTH revenues projected through 2001 and extrapolated to 2008. Cable TV projected data based on extrapolation of 2% market share loss through 2008.

[9] Space Publications. *State of the Space Industry*, 1998, 42-51. The fixed satellite service (FSS) market is expected to grow 31% between 1997 and 2001. Financial and business transactions and cable and video transmissions subscribe to FSS. Mobile satellite services and direct-to-home services are expected to grow 784% and 156%, respectively, in the same period.

[10] Ibid., 54.

[11] Ibid., 16.

[12] The Oregonian. "*Satellite Loss Puts Millions Out of Touch,*" 21 May 1998. Of the pager service affected, all 10.4 million customers of the paging industry's leading provider, PageNet, were without service. Exhaustive research did not yield any official estimates for the loss. However, 10.4 million $10/month pager contracts without service could have cost PageNet about $3.5 million per day.

[13] The White House. *National Space Policy*, 19 September 1996, 8. "The US Government agencies shall purchase commercially available space goods and services to the fullest extent feasible …except for reasons of national security or public safety."

[14] Although the percentage of the space budget continues to grow, the overall defense budget is a zero-sum game. Gains to be made by expanding space systems come at the expense of other systems or operations and maintenance.

[15] National Defense Industry Association. Draft briefing. To CINCSPACE. Subject: Protection of commercial Space, December 1998, 6.

[16] NAIC, *Threats to US Military Access to Space* (Document # NAIC-1422-0984-98), 11.

[17] Department of Defense, *Joint Vision 2010*, 16.

[18] The White House. *National Security Strategy*, October 1998, 25. USSPACECOM. *Long Range Plan*, March 1998, p viii. These documents state the vital interests commercial space serves in political, economic, and military security of the US.

Chapter 3

Hazards, Threats, and Vulnerabilities

"Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways…"

— Presidential Decision Directive 63
22 May 1998

In this chapter, the goal is to show the vulnerability of commercial space systems to hazards and threats and to demonstrate the likelihood of occurrence of the threat in the future. A distinguishable difference exists between hazards associated with operating space systems versus threats to our space systems. First, we must examine this difference and then we may characterize the different types of both. Although hazards and threats are present, industry and government do not universally agree on the priority to which these risks should be addressed. Consequently, USSPACECOM commissioned a National Defense Industry Associated (NDIA) study to research industry's views on hazards and threats to commercial systems. Finally, threats will be addressed regarding what constitutes an attack and who might accomplish an attack.

Definitions and Types

The recent survey of the commercial space industry completed by the NDIA Summer Study in 1998 yielded suitable working definitions for hazards and threats. A **hazard** is best defined as *a natural environmental event or a man-made condition lacking intent*, whereas a **threat** is best

defined as *an intention specifically planned to deceive, deny, disrupt, degrade or destroy (D^5) or exploit*. The key difference obviously is in intent. When considering how space systems may be compromised, we must look at the various segments that comprise a space system: satellite(s), ground station(s), links, and the information or data. Each hazard or threat described below can have a singular effect on each segment or combined effects on multiple segments.

Hazards to space systems are characterized as occurring by accident either naturally, as a result of the space environment, or as a result of man-made conditions. Naturally occurring hazards are associated with phenomena such as solar cycles, satellite charging within the Van Allen radiation belts, gravity gradients, and collisions with celestial objects such as meteorites. Man-made hazards occur as a result of collisions with other space objects and unintentional interference such as radio frequency interference. Collisions could occur with other active satellites or orbital debris. Unintentional interference can degrade, disrupt or deny command and control of spacecraft and the payload information. At any point in a space system's lifecycle (from manufacture to launch and on-orbit operations), human errors or equipment failures can accidentally cause total or partial loss of mission capability.

Threats can also be characterized into types. The National Air Intelligence Center (NAIC)[1] and USSPACECOM[2] agree on the types of threats facing US access to space although their labels differ. For simplicity, the threats will be typified here by the method of attack: directed energy, direct ascent and physical attack, passive measures, exo-atmospheric nuclear blast, and information warfare.[3] Directed energy weapons could take the form of jamming; lasing; high power microwave; and non-nuclear, electromagnetic pulse (EMP). Directed energy weapons may be terrestrial or, eventually, space-based and would be used to deceive, deny, disrupt, degrade or destroy (D^5) any of the four segments of a space system. Direct ascent weapons

intentionally collide with satellites to achieve desired effects while ground stations are vulnerable to physical attack. Passive measures degrade the ability of a space system to complete its mission through concealment or deception.[4] The predictability of satellite orbits permits one to hide events and information from overhead collection systems. A nuclear detonation in space relies on the resultant EMP and electromagnetic interference (EMI) to achieve its desired negation effects, typically against satellites and their links. Finally, information warfare against any segment of the space system can be used to negate a space system through D[5] or to exploit for intelligence purposes (economic or military).

A qualitative assessment summarizes the vulnerabilities of each segment of the space system to each type of hazard and threat (Table 1). The prevalence with which hazards affect space systems provides a key indicator of why industry prioritizes hazards above threats.

	Satellite	**Ground Station**	**Link**	**Information**
Hazards				
Natural occurrences				
Man-made occurrences				
Threats				
Directed Energy				
Direct Ascent/ Physical attack				
Passive Measures				
Exo-atmospheric Nuclear Blast				
Information warfare				

Table 1. System Segment Vulnerability vs. Threat

Industry and Government Views

USCINCSPACE expressly commissioned the 1998 NDIA study to examine industry's views on the protection of commercial space assets. Specifically, USCINCSPACE posed two

questions: (1) "what does industry want?" and (2) "what is industry's position on protection?" The Threats and Sensors sub-panel queried major US companies in the commercial space industry for their views on hazards and threats. **Industry's top concern results from hazards such as on-orbit collisions and environmental phenomena, not threat of attack**.[5] According to industry, the government can best use its large space resource infrastructure to help by providing warning of these hazards. The NDIA study team opined industry would not actively pursue protection measures until after the first commercial spacecraft is destroyed.[6] The data suggests industry is not interested in addressing future threats they don't believe likely. Therefore, they see no added value to their bottom line in protecting against these threats.

Obviously, the key business consideration for industry is profit and rate of return especially for an emerging sector in the global economy. As was shown in the previous chapter, the products and services portion of the industry is growing rapidly making profit by selling products and services to external customers. In 2001, estimated revenues for products and services will reach $9 billion in comparison to the total industry revenue projection of $117 billion.[7] The $108 billion difference between these estimated revenues is internal industry investment to establish and maintain infrastructure, telecommunications and support services. The start-up and operations and maintenance costs with this industry are significant, hence, the profit margins are not large. Industry regards hazards as the risks of doing business, but countering unproven threats reduces already slim profit margins that might undo the recent progress in attracting investors. Industry is only willing to accept help in minimizing the effects of space hazards if no governmental regulation is imposed. Consequently, the primary hedge against hazards is accomplished by obtaining insurance against the various types of losses. The insurance portion of the commercial space industry has been profitable in recent years because hazards, though

potentially devastating, are rare. However, on-orbit claims are expected to increase as the heavens become proliferated with additional constellations.[8]

On the government side, threats and hazards have been of concern since the early days of the space program. As testament to the concern for hazards, the space operations center at USSPACECOM maintains a catalog of every man-made satellite launched since Sputnik I in 1957 as well as space debris large enough to cause damage to spacecraft.[9] Until the break-up of the Soviet Union, mutual deterrence and treaties countered threats since the predominant use of space was strategic (warning, communications and intelligence). Hazards to orbiting satellites remain a concern for the government, however, the Gulf War demonstrated a new center of gravity for an expeditionary force like the US military. Threatening our lines of communication and limiting our situational awareness can severely hamper our ability to respond to crises. The US government's commitment to our military freedom of action in the space environment is clearly stated in such documents as the National Space Policy (NSP), the National Security Strategy (NSS), the national Military Strategy (NMS), and various joint and service doctrine documents.[10] Although focusing on minimizing threats to our critical information infrastructure, The Clinton Administration's Policy on Critical Infrastructure Protection (PDD-63) does not specifically mention space as one of the aspects we must protect. A promising step in the right direction occurred in October 1998, the House National Security Committee expressed its concern for civilian systems during Assistant Secretary of the Air Force Keith Hall's testimony regarding the threats to space systems.[11] In summary, the government's views on space and information protection yields the following:

(1) The Clinton Administration is showing concern for threats to critical information systems (PDD-63) and, separately, the need to control space (NSP and NSS);

(2) Congressional interest (House and Senate) is expanding with regard to space control and the protection of space systems; and

(3) The USSPACECOM has a vision for the systems needed to protect military space systems (Long Range Plan) while contemplating commercial systems protection as well (NDIA Study).

By synthesis, these government actions point to space systems threats that are real and must be considered in the interest of national security.

One must concede commercial industry's lack of concern for threats at this point in time is a rational and logical choice. This reality exists for primarily fiscal reasons. To admit the existence of threats would dampen investment and consumer confidence in this blossoming industry. However, industry's views are a temporary condition. Once threats to their systems manifest themselves, industry will seek government support for protection. As an analogy, consider numerous examples of American citizens travelling abroad to potentially openly hostile states. Even though the State Department advises travelers of the threats beforehand, the first instinct of these people is to blame the US government when threats actually arise. The same principle applies here. The US government is concerned about threats to all of its national interests. Therefore, a space systems protection plan must be proactive and safeguard commercial systems as well.

Space Systems Attack

Because an attack on a commercial space system would lead us into uncharted territory, this author believes the response would be predicated on the actor(s) perpetrating the event, and their motives. In other words, the decision to label an event as restricting our free passage in space and therefore an attack would be a political decision.[12] Our current National Space Policy,

predicated on peaceful use of space, condemns a space attack because it threatens our sovereign use of space and interferes with our fundamental right to acquire data from space. [13] An adversary will view space as one of our strengths to attack. Therefore, we must examine the types of actors and the various methods by which we could expect each to threaten our commercial space systems within the next decade.

World actors in conflict are classified as states, non-governmental organizations (NGOs), and individuals.[14] State actors can be further sub-divided into potential peer or niche competitors.[15] A peer competitor will be capable of directly challenging our vital interests through force-on-force engagements in space while also developing innovative asymmetric strategies for countering space systems. Russia remains a nation already with significant military capabilities such as anti-satellite (ASAT) weapons while China is an example of a nation capable of emerging to peer status in the early 21st century. [16] Although the Russian Duma has banned the use of ASAT weapons[17], the open source information suggests direct ascent and directed energy (including laser and electronic attack weapons) capabilities exist.[18] Just as we fear the proliferation of weapons of mass destruction (WMD) due to the economic troubles in Russia, so should we be concerned with the sale of Russian ASAT weapons and technologies. Moreover, we should not discount the potential for China to develop its own ASAT capability. With a robust launch capability and ballistic missile technology, China could possibly use ballistic missiles to boost ASAT weapons into orbit. Further, China is known to be developing its directed energy capabilities and has also shown great interest in laser technology.[19] This list of peer competitors may appear short, but we must continually concern ourselves with the dilemma of proliferation.

Unlike the peer competitor, a niche competitor will likely challenge our cost tolerance by employing asymmetric strategies such as information warfare or passive measures. Iran, Turkey, and Indonesia have jammed satellites in the past according to US Space Command reports.[20] However, one cannot rule out the possibility of non-space faring competitors like North Korea, in pursuit of nuclear capability, from developing a capability to explode a nuclear devise in low-earth orbit. It is logical to conclude potential niche competitors learned what Desert Storm taught Iraq. The ability for the US to successfully mobilize, deploy, employ, sustain, and re-deploy forces is a function of the information we have about the situation. With our growing reliance on commercial space systems, future competitors (peer and niche) will naturally see these systems as a viable center of gravity to attack.

PDD-63 makes clear the Clinton Administration's concern for the safety of our critical information infrastructure against terrorists, criminals and hackers. These actors would not be capable of constructing and concealing complex technological threat systems. However, these groups and individuals do recognize commercial space systems represent a target to damage our national security and prestige to achieve their goals. One need only consider a situation emerging as this thesis was written. According to the Reuters News Agency, hackers "high-jacked" a British Skynet military communications satellite.[21] In the published news report, the hackers are blackmailing the British government and refuse to stop interfering with the satellite until a ransom is paid. We should be particularly concerned because this is a military satellite and presumably protected with encrypted links. Even if these reports are proven to be unfounded, this scenario should serve as a wake-up call for our vulnerable commercial systems.

Against the array of space threats presented earlier, Table 2 summarizes the various actors against the possibility of possessing the specified threat capability.[22]

	Directed Energy	Direct Ascent/ Physical attack	Passive measures	Exoatmospheric Nuclear Blast	Information warfare
Peer Competitors					
Niche Competitors					
Terrorist/Criminal Organizations					
Hackers					

Table 2. Actors vs. Threats

Whether industry chooses to accept it, the fact remains space systems, especially commercial space systems, are vulnerable to these threats. The obvious question is "what is the impact of these threats?" The next chapter will address the effect of the loss of commercial space capability on our national security by answering a corollary question, "can we afford the cost of ignoring these threats?".

Notes

[1] NAIC, *Threats to US Military Access to Space* (Document # NAIC-1422-0984-98).

[2] USSPACECOM, *Long Range Plan: Implementing USSPACECOM Vision for 2020*, March 1998, 4.

[3] Ibid., 4.

[4] Ibid.

[5] National Defense Industry Association. Draft briefing. To CINCSPACE. Subject: Protection of commercial Space, December 1998, 18.

[6] Ibid., 38. Two telling quotes from interviews with international service providers are: (1) "The threat can be 1000 times worse than the daily hazard, it just won't be believed till it happens" and (2) "It's sort of like the crossing guard; there isn't one until someone gets run over."

[7] Space Publications, *State of the Space Industry*, 1998, 8.

[8] Ibid., 59.

[9] Air University. *AU-18 Space Handbook: A War Fighter's Guide to Space Vol 1*, December 1993, 98.

[10] Joint Pub 3-14 is in draft. This publication expresses CJCS' views on joint tactics, techniques, and procedures for space operations. Additionally, Air Force Doctrine Document (AFDD) 1 and AFDD 2-2 specify the need to protect our freedom of action in space while denying the same to an adversary.

[11] On 29 October 1998, Rep. Curt Weldon (R-PA) expressed concern over the vulnerability of US national security if civilian satellite systems were targeted by a foreign adversary. Air Force Space Command. *Legislative Update*, 6 October 1998, 1.

Notes

[12] United States Space Command. *Long Range Plan*, p138. The LRP acknowledges a need to identify "US reaction to attack on satellites." This is one of their "Out of Our Lane" items. Additionally, USSPACECOM also sees the need to "clarify the policy on sovereignty of space systems" especially as it pertains to commercial systems

[13] The National Space Policy considers interference with "right of passage" as "an infringement on sovereign rights." The White House. *National Space Policy*, 19 September 1996, 2.

[14] Papp, Daniel S., *Contemporary International Relations: Framework for Understanding*. 4th ed. New York: Macmillan College Publishing Company, 1994. Papp also identifies international governmental organizations (IGOs) as a type of actor. However, IGOs are not considered because they are essentially a collection of individual states.

[15] Barnett, Col Jeffrey R., *Future War: An Assessment of Aerospace Campaigns in 2010*. (Air University Press), 1996. Col Barrett considers the aerospace aspects of future campaigns against state actors. In his book, Col Barnett defines a peer competitor as a "state capable of fielding multiple types and large numbers of both emerging and present weapons, then developing innovative concepts of operations (CONOPS) to realize the full potential of this mix." He defines a niche competitor as "a state that combines limited numbers of emerging weapons with a robust inventory of current weapons, then develops an innovative concept of operations to best employ this mix."

[16] NAIC, *Threats to US Military Access to Space* (Document # NAIC-1422-0984-98), p5-16. This document describes physical and electronic threats to all four segments of space systems. The threats are posed primarily by Russian capability developed during the Cold War and still exist today as well as emerging Chinese capability.

[17] DeBlois, Lt Col Bruce M., "*Space Sanctuary: A Viable National Strategy*," Airpower Journal, Winter 1998, 47.

[18] NAIC, *Threats to US Military Access to Space* (Document # NAIC-1422-0984-98), p5-16.

[19] Wall, Robert. "*Intelligence Lacking On Satellite Threats"* Aviation Week & Space Technology, 1 March 1999, 54. According to this article, "The Pentagon said late last year that China is working on directed energy anti-satellite technology."

[20] Ibid. Gen Myers, USCINCSPACE, is quoted in this article.

[21] Reuters News, "*Hackers Reportedly Seize British Military Satellite*," 28 February 1999.

[22] Data presented in table 2 is the author's analysis of Col Barrett's descriptions of capabilities for typical peer and niche competitors in 2010. NGO and hacker data is author's analysis of Clinton Administration PDD-63 concerns for critical information infrastructure against terrorist and individual activities. Further statement of the concern for cyber-terrorism was expressed by President Clinton on 22 Jan 99 at a speech given to the National Academy of Sciences. President Clinton has proposed a 40% increase in spending for the cyber threat (over 1997 levels). "…terrorists, recognizing they cannot defeat the United States with military force, are seeking new tools of destruction." Montgomery Advertiser, 23 Jan 99, p 9A. "Clinton proposes more anti-terrorism funds."

Chapter 4

Consequences

> *…just as by the year 1500 it was apparent that the European experience of power would be its domination of the global seas, it does not take much to see that the American experience of power will rest on the domination of space.*[1]
>
> — George and Meredith Friedman
> The Future of War

Without doubt, the US is becoming more and more reliant on commercial space systems for economic and military purposes. Additionally, differing perceptions between government and industry exist with respect to the likelihood of threats to commercial space systems. Furthermore, one should conclude there are a feasible and real threats to space systems because those with the best access to threat data (i.e., USSPACECOM) are planning to spend millions of dollars over the next 20 years to protect military systems.[2] With regard to commercial space systems, this chapter will answer the "so what" question. What are the consequences of not protecting commercial space? Assuming George and Meredith Friedman and the Toflers[3] are correct about the importance of space to the maintenance of America's dominance, what are the impacts on our future national security?

Economic Implications

No data exists to quantitatively prove the potential catastrophe awaiting our economy, and consequently our national security, should an adversary deliberately and systematically negate

our commercial space systems.[4] However, consider the sectors of the economy PDD-63 states are at risk via asymmetric attack on critical information infrastructures: telecommunications, energy and utilities, transportation, and banking and finance (Figure 4).[5] As stated in the first chapter, it is imprudent to simply consider the need to protect commercial space based solely on our annual investment in the commercial space industry.[6] We need to ensure the means to conduct business in the various economic sectors mentioned in PDD-63 (and any others not explicitly mentioned in the PDD) are safeguarded without unduly hampering the flow of commerce.

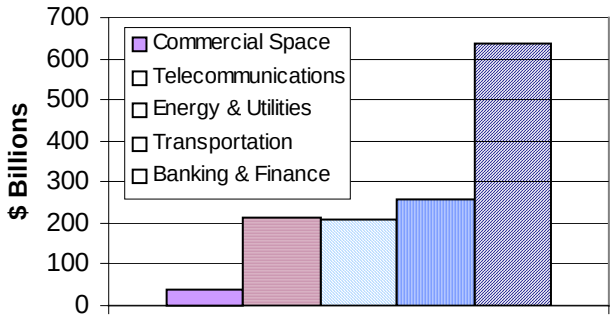

Figure 4. FY 1997 US GDP Expenditures

Qualitative assessment convinces us the economic implications of losing commercial space capability are real and too painful to bear. The May 1998 failure of the Galaxy IV satellite should stand as testament of the havoc an adversary might create. The more our economy becomes dependent on the information and services provided by these systems, the more significant the impacts are sure to be. The loss of a single Iridium satellite will not be catastrophic, not even significant. Many of these big low earth orbit (LEO) systems will provide on-orbit spares to enable near real-time switchover to the spare. However, we must be concerned with the potential for an "Informational Pearl Harbor" whether perpetrated by another

state or a terrorist intending to cripple our economy in the furtherance of their own interests. In this scenario, a peer competitor could attack our commercial space systems (a decisive point) to damage our economy (a center of gravity) via our financial markets. By devastating the US economy, an adversary might employ this diversionary tactic to turn our national focus inward. If US intervention can be prevented, our adversary's goals are more likely to be achieved. A secondary benefit would be the negation of US military effectiveness in countering our adversary's aggression.

One might argue, an "Informational Pearl Harbor" is a worst case scenario we cannot afford to defend against. Unfortunately, the threat of an asymmetrical attack on the US is growing. The drug trafficking war on our southwestern border is analogous to the threats against our commercial systems. We know we can never completely negate the flow of drugs with surveillance and response alone. However, like the drug threat, we must take the necessary steps to reduce the threat to an acceptable level by using all of the tools at our disposal to identify, classify and, if possible, negate the sources before they manifest themselves.

Military Implications

For the military, it's a forgone conclusion commercial space will be key to providing fully mission-capable operational forces. Because our operational forces are now predominantly stationed in the continental United States (CONUS), we must be expeditionary in our ability to meet America's global commitments. We must be ready to operate in an environment with little or no existing communications infrastructure, areas where little mapping has occurred, and vast expanses where continuous overhead intelligence collection will be key to real-time situational awareness. Among other burdens this reality incurs, it places a premium on such commercial capability as satellite communications to connect our forces with their logistics pipelines in the

US or to connect our combatant commanders with their CONUS-based staffs and in-theater component commanders. Even in today's peacetime environment, the military relies on commercial products and services, such as imagery and communications.[7] As important as these commercial capabilities are for training and exercises, they are vital for conducting operational planning and implementing military operational as directed by the National Command Authority. The military implications should these commercial capabilities not be available is rather simple. The military mantra is "train like we fight." The sudden loss of critical information to support war planning and execution will significantly diminish our military effectiveness. One should not and could not say this alone would spell defeat. However, there is no doubt a diminishing of military effectiveness directly equates to the number of body bags for US forces.

A Critical National Security Issue

As set forth in the first chapter, the case to be made for the protection of commercial space systems hinged on the ability to prove commercial space systems are critical to national security. The three elements required to prove this point do exist. First, commercial space reliance is rapidly increasing, economically and militarily. Second, although industry is primarily concerned with hazards facing their systems, viable and serious threats to these systems exist and cannot be ignored. Third, the consequences associated with the loss of commercial space systems poses a severe blow not only to the commercial space industry but to various other sectors of the US economy. Additionally, commercial space systems are force-enhancers for today's armed forces. The loss of these systems would seriously jeopardize our ability to effectively wage wars with minimal loss of life. These factors force us to conclude this is a critical national security issue just as many in high-level government positions are now realizing.

The second part of this paper will address recommendations to adequately protect these commercial systems without undermining the commercial space industry as a whole.

Notes

[1] Friedman, George and Meredith, *The Future of War: Power, Technology, and American World Dominance in the Twenty-First Century* (New York: St Martin's Press, 1996), 420.

[2] United States Space Command. *Long Range Plan*, p33-38. This section of the LRP contains CINCSPACE's plan to develop a protection capability for detecting and reporting, withstanding and defending, reconstituting and repairing, assessing mission impact, and identifying and classifying the source.

[3] Tofler, Alvin and Heidi, *War and Anti-War*. The Toflers contend the ways in which nations make wealth characterize the nature of war.

[4] This author conducted an exhaustive search for data to estimate the "true" cost of losing commercial space systems. The intent was to quantify the extent to which commercial space has embedded itself into our nation's economy beyond simply estimating the revenues for the commercial space industry. The true cost would consider the potential losses to the financial, retailing, telecommunications, and transportation industries as well as the government.

[5] US Department of Commerce Bureau of Economic Analysis. *Gross Domestic Product by Industry*. On-line Internet, 26 January 1999. (www.bea.doc.gov/bea/dn2/gpoc.htm).

[6] Space and Missile Systems Center. *Commercial Space Opportunities Study*, 1998. Source data from Merrill Lynch graphs the dollar growth of the US commercial space industry to be $40 billion (1997) going up to $170 billion (2007).

[7] The National Imagery and Mapping Agency (NIMA) signed two contracts with commercial imaging providers for services in 1998 to meet service demands. (SIGNAL Magazine, December 1998, p7) This author, while assigned to HQ Air Force Space Command, represented Air Mobility Command's SATCOM requirements. Because AMC has not had high priority to satisfy their connectivity needs exclusively with military SATCOM, they must compensate with commercial SATCOM capabilities such as Inmarsat.

Chapter 5

Recommendations

> *"The influence of the government will be felt in its most legitimate manner in maintaining an armed navy, of a size commensurate with the growth of its shipping and the importance of the interests connected with it."* [1]
>
> — Alfred Thayer Mahan

Mahan reminds us of the proper role for government to play in assuring our commercial and national security interests are protected. In Mahan's time, the emerging medium of commerce was the sea. Today, space systems have become an element of our critical information infrastructure, and we need a vision for how best to protect these systems. In pursuit of this vision, policies and processes must be developed and implemented. This is but a starting point as there are various aspects of the protection equation this country is only now beginning to analyze.

A New Vision

The current USSPACECOM Long Range Plan is predicated on a path leading towards a FAA-in-space framework for global traffic control. Throughout, the author has employed an updated maritime analogy is an alternative vision for the foundation of commercial space protection. Though the Navy is considered by to assure access to the sea, the US Coast Guard is a better model. The USCG's mission combines national security and commercial concerns with law enforcement activities.

The USCG is tasked by Title 14 USC 2 to perform the following four broad functions: maritime safety, maritime law enforcement, maritime environmental protection, and national security.[2,3] By analogy, the space arena needs an organization with similar functions to properly assure safety, enforce laws, protect the environment, and conduct national security operations. This organization could evolve to be a multi-national organization since space law is founded primarily on international treaties and agreements. However, the US must take the first step toward protecting space systems since we are the most capable nation and the most vulnerable. Table 3 compares the four broad roles proposed for a space protection force with those of the USCG. The four space protection roles with their associated tasks provide CINCSPACE with the means to deter aggression in peacetime and assure access to space in wartime.

	Coast Guard Roles	Space Protection Roles
Safety of the Medium	• Aids to navigation • Commercial vessel safety • Search and rescue • Waterways management • Port safety and security	• Hazard warnings • Tracking/ID/Catalog maintenance • Search • Domestic launch facilities safety and security
Law Enforcement	• Interdict smugglers • Enforce economic exclusion zone • Inspect vessels for compliance with laws • Assist other law enforcement agencies	• Surveillance and reconnaissance • Detection and assessment • Deterrence and response • Assist other law enforcement agencies
Environmental Monitoring	• Prevent/clean up after discharge of hazardous materials • Represent US interests at national and international forums	• Exoatmospheric nuclear detection and warning • Represent US interests at national and international forums
National Security	• Peacetime planning and exercise • Wartime support for USN	• Peacetime planning and exercise • Crisis response

Table 3. Commercial Space Protection Model

Policy Recommendations

As the world's foremost space warfighting organization, USSPACECOM controls the systems and expertise to be a global space police force. The role of USCINCSPACE needs to be expanded from "the single focal point for ***military*** space" to the single focal point for national

security in space. This change coincides with emerging thought in the space warfighting community of space as an area of responsibility not just a function. The recent PDD-63 directs the Department of Defense to participate in the National Information Protection Center (NIPC). The NIPC will provide indications and warning, assess threats, and enforce laws. To complement commercial space protection under the newly created NIPC, a recommended organizational structure incorporating DoD protection systems and command relationships is shown below (Figure 5).[4]

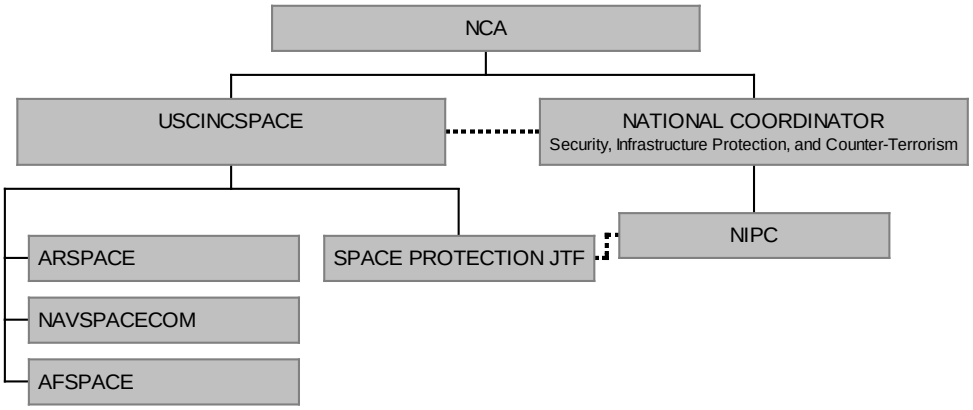

Figure 5. Proposed Organizational Structure

The DoD has responded to the PDD by establishing JTF Computer Network Defense (JTF-CND) for protection of DoD's critical information infrastructure. Arguably a portion of the critical information infrastructure, one could make the case that space protection should be considered as part of the JTF-CND. The counterpoint response is CINCSPACE is tasked as the responsible CINC for space protection. Following this logic, a Space Protection JTF under the operational control of USCINCSPACE would bring the needed resources and expertise to the NIPC to integrate military and commercial space as another key element of our critical information infrastructure.[5] This JTF would have its own Joint Staff for intelligence, operations

and planning while sharing USSPACECOM's Joint Staff for all other functions. The commander will require:

(1) Operational control of space surveillance and dedicated space protection forces,

(2) Statutory authority to participate in US space law enforcement activities,

(3) A means to establish an interagency working group for interaction with industry and other government departments for planning and operations, and

(4) Agreements with the NIPC for information sharing and complementary activities.

As the vision evolves to reality, the US Government should pursue international recognition of this joint task force and perhaps advocate a multi-national command to enforce internationally recognized space laws globally.

Commercial space is vulnerable now. We must enact policies and set up organizations immediately to commence our efforts to diminish our vulnerability. The proposed JTF will act as a constructive forum for discussions and planning with industry and other government entities. Process and material changes to create a space protection capability will occur once appropriate requirements are validated and an architecture is developed through the National Security Space Architect (NSSA) office.

Process and Material Recommendations

Countering hazards and threats against space systems would be the mission of the Space Protection JTF. Per joint doctrine, joint planning incorporates adaptive planning concepts for phased transition from peacetime activities to military force should deterrence fail. Against the threats identified in chapter 3, the first step in the space protection process is deterring actors from threatening our space systems. If deterrence fails, we must be prepared to detect, assess, and respond to the attack. Although we cannot deter hazards, an effective space protection

architecture will provide a margin of safety through warning and reduced impact caused by hazards. The USSPACECOM Long Range Plan divides the protection mission into five steps. Table 4 below maps the steps of the proposed process in contrast to the USSPACECOM plan.

Proposed Process	USSPACECOM Long Range Plan
Deter	Not addressed
Detect	Detect and report threats to owners Identify/locate/classify source with high confidence
Assess	Assess mission impact/disseminate
Respond	Withstand and defend against threats Reconstitute and repair space services

Table 4. Protection Process Comparison

The USSPACECOM Long Range Plan falls short of effective planning for deterring aggression against our space systems. The plan fails to explicitly recognize deterrence as the first step in the space protection mission. Not unlike geographic combatant commanders, USSPACECOM's first mission is to deter aggression within its area of responsibility. Most important to the space protection mission is the ability to surveil the entire medium to achieve total situational awareness. This cornerstone capability is vital as a deterrent to persuade would-be aggressors that any actions against our space systems will not go undetected and, consequently, will not go unpunished. The credibility of the deterrent is backed by the power of the world's dominant terrestrial force.

Today's space surveillance capability provides the US space program with only relative superiority over all other space-faring nations. The various surveillance sensor capabilities may be capable of detecting satellite anomalies but not their source. The CINCSPACE's vision is to develop a near real-time (NRT) space battle management system from LEO out to GEO. The Long Range Plan outlines a series of advanced technology upgrades to the space surveillance network as well as revamping the battle management command, control, and communications

structure to attain the stated vision. Disappointingly, USSPACECOM still grades itself "yellow" in the space surveillance segment by 2020 (only partially meeting goals).[6] Because surveillance will form the core of any other missions we will do in space, the future consequence is unacceptable and completely avoidable. Many of the requisite technologies are in development at the Air Force Research Lab (Phillips Research Site, Kirtland AFB NM). The Air Force must continue to fund these Science and Technology efforts and demonstrate warfighting capability through Space Battle Lab initiatives and future Expeditionary Force Experiments (EFXs).

The second step in the process is not simply to detect the threat when inflicted upon the space system, but to classify the threat, identify the source, and provide timely notification. This capability will require on-board sensors to geo-locate the source and disseminate information in NRT to a space operations center. Upon detecting the threat, a mechanism must be inherent in the system to assess the impact of the threat, the third step. On-board processing and artificial intelligence will be key to accurate assessment. Finally, the system must be capable of responding effectively to the threat and reconstituting itself to regain normal operations (step four). This will require on-board systems to control active protection mechanisms, passive countermeasures (such as entering a safe mode), or maneuvering away from the threat. When the sensed threat has dissipated, the system must return to normal operations quickly and autonomously to minimize service interruption to users.[7] A modular, integrated active countermeasures and detection/location suite needs to be developed that would be readily adaptable to each of the industry's standard satellite buses planned for future payloads.

Prioritization and Timing

One may look at the CINCSPACE Long Range Plan and ask if it's really possible to achieve a space control capability in the next 20 years. Even after all the suggested modernization,

CINCSPACE rates key sub-areas of the space control mission of space surveillance and protection as "yellow" in 2020. Although the material solutions to achieve this process seem enormous, we can strive to achieve the protection vision incrementally. The organizational and policy changes should be considered as soon as possible. Establishment of a dedicated body toward the protection of space systems and the resources provided to it will dictate the timeline for any real capability. Inherent in the Space Protection JTF is an initial level of deterrence by showing would-be adversaries our intentions for the future. For the mid-term, the deterrent capability of an advanced technology space surveillance system should not be underrated. All other aspects of space control, including protection, are moot until we can achieve the adequate level of situational awareness. Since industry prioritizes hazards ahead of threats, an advanced space surveillance system with a battle management system tying industry's space operations centers to warn of hazards is an area for common understanding to begin future discussions regarding threat protection.

We are now at an important crossroads. Based on the recent PDD-63 and a new National Security Strategy, the Chairman of the Joints Chiefs of Staff (CJCS) will review and possibly revise the National Military Strategy (NMS) to include critical information infrastructure protection and other changes in the strategic environment. The NMS is a key input to the Secretary of Defense for his Defense Planning Guidance (DPG) in April 2000 for the FY2002 Service Program Objective Memorandums (POMs). The Air Force would then consider the resources needed to develop, build, and field the systems required for space systems protection in their FY2002 POM due in June 2000. This flow of events will provide DoD with resources beginning in FY2002 and result in the first real capability around 2010, after an 8-10 year acquisition program cycle (Figure 6).

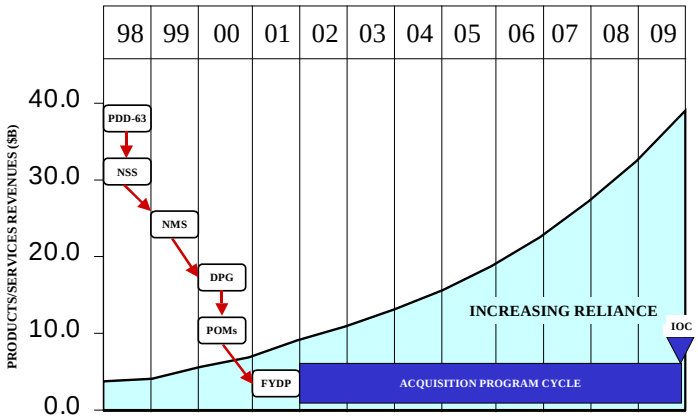

Figure 6. Schedule of Events vs. Reliance[8]

Follow-on capability to attain a robust system of integrated sensor/countermeasures suites could overlap and be available for a second or third generation of systems from now. The critical path to any capability will always run through the initial decision. It's important to point out that the window of vulnerability for our commercial space systems will continue to widen the longer it takes to commit to their protection.

Areas for Further Study

In the course of this research, four crucial areas emerged which require further study. First, the extent to which commercial space systems have become embedded within our national economy must be quantified. Industry has tied its opposition to protective measures to the "market won't bear it" view. Consumers, who are the American public at large, will not understand the extent of the problem until it can be quantified. The Office of Air and Space Commercialization at the Department of Commerce, in cooperation with the Space protection JTF, should be designated the lead agency to accomplish this task. To put this matter into perspective, consumers have been educated on the Y2K issue and few dispute the billions of dollars we are allocating to avert that crises.

A second area for further study regards intelligence requirements to identify and track the threats challenging our space systems. Various sources within the DoD cite intelligence as a serious shortfall for tracking the emerging threats to our space systems.[9] As pointed out earlier in this paper, we must be as concerned with proliferation of multi-use technology suitable for ASAT as we are for WMD technology proliferation.

Third, the Space Protection JTF should begin dialogue with the commercial industry on incentives to offset the costs of implementing a space protection architecture. Of the many ways to accomplish this, two stand out. One is to provide direct tax incentives to the companies who voluntarily incorporate attack detection sensors to their payloads and route data to USSPACECOM's Space Operations Center. A second method engages the space insurance sector of the industry. The government can provide similar tax incentives as reimbursement to the insurers who provide incentives to the satellite builders to work within the space protection architecture. These incentives could come in the form of policy rebates for protective equipment, analogous to the savings automobile insurers provide for air bags or alarms. As ASAT threats emerge, insurers will logically want to investigate the nature of on-orbit failures to verify the source.

Finally, USSPACECOM needs to reconsider its roadmap for the space surveillance network (SSN). As the keystone capability for the space control mission, the SSN must be fully capable to perform the defensive counterspace (DCS) mission. If we lack confidence in our surveillance systems to defend our space systems, how would we build target folders, determine aimpoints, and assess battle damage to perform the OCS function? Furthermore, would a future geographic CINC launch a major terrestrial campaign without *positive* assurance we've negated the adversary's space-based eyes and ears? Therefore, we need to determine the "delta" capabilities

and cost required to boost the advanced SSN advocated in the USSPACECOM Long Range Plan from yellow (meets partial goals) to green (meets all goals). This fully capable SSN should be one of the top items on the CINC's integrated priority list for the upcoming POM cycle.

Notes

[1] Mahan, Alfred Thayer, "The Influence of Sea Power on World History: 1660-1783" (excerpt). *Air Command and Staff College War Theory Coursebook* (Academic Year 1999), 109.

[2] Stubbs, Captain Bruce B., "The Coast Guard's National Security Role in the 21st Century." *Air Command and Staff College Operational Forces Coursebook* (Academic Year 1999), 35.

[3] The USCG is not a Title 10 Service, thus Posse Comitatus is not a consideration.

[4] The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism will report to the President through the Assistant to the President for National Security Affairs. A liaison from CINCSPACE to the National Coordinator would be appropriate as well as approval for the proposed JTF/CC to have direct liaison authority with the NIPC.

[5] The JTF proposed here should be structured like the two current Joint Inter-Agency Tasks Forces (JIATF East and JIATF West) performing law enforcement activities to counter drug smuggling as a national security concern.

[6] USSPACECOM. *Long Range Plan*, 1998, 19-47. These sections of the LRP assess the technology requirements to attain CINCSPACE's goals for space surveillance and protection, respectively.

[7]. Ibid., 31 and 36.

[8] The reliance data (an area graph version of Figure 1) is overlaid on the schedule of events to illustrate the growing window of vulnerability due to increased reliance without protection mechanisms in place.

[9] Wall, Robert. *"Intelligence Lacking On Satellite Threats"* Aviation Week & Space Technology, 1 March 1999, 54.

6

Conclusion

At the Crossroad?

General Estes, in his Nov 1997 "Air Force at a Crossroad" speech as CINCSPACE, foresaw the approaching crossroad for Air Force stewardship of space:[1]

> "But this [limitless] potential [of space] will never be realized unless we begin as an Air Force to change our culture to fully accept the responsibility for the role of space and its importance to the future national security interests of our country. This has been a problem in the past, we've never really embraced space in the Air Force. That's the crossroad."

Today, we find ourselves precisely at this crossroad. While members of the US Congress are questioning the USAF's ability to be a good steward for space[2], there is rising speculation USSPACECOM could follow in USSOCOM's footsteps. SOCOM, although a functional combatant command, has organizing, training, and equipping functions like the Services. Proponents of this organizational model see this as an intermediate step en route to an eventual separate space force. The USAF must restore confidence in America's elected leadership by tackling an issue of importance to US national security and following through. The question is which issue has this potential?

The current rift between the USAF and Congress is over ballistic missile defense (BMD) and space control. BMD issues are complex; money and technology are considered the drivers to the actual fielding of capability. Space control is the other hot button issue with

Congressional members. Like BMD, offensive counter-space (OCS) carries excess space law, policy, and treaty baggage as well. First and foremost, we must subdivide the issue of space protection from space control because, inevitably, space control discussions lead to a polarizing debate regarding the weaponization of space. Although this debate is healthy for the maturation of space, it is imperative we embark on the path toward a space protection capability in the FY02 POM. Defensive counter-space (DCS) by itself does not evoke the emotional debates of OCS and BMD. Because this thesis shows the potential for grave danger to our national security, we cannot continue to neglect space protection. Technological, political, and resource roadblocks barring the development and fielding of surveillance, countermeasures, and battle management systems are fewer in number and severity relative to those facing BMD and OCS.[3] In reality, many of the systems needed for the protection mission are prerequisite enablers for the BMD and OCS missions.

Today's domestic environment is increasingly driven by concern about America's "cyber-safety." The Air Force should tackle the commercial protection issue and restore lost confidence in its ability to be the country's predominant space organization for national security. As compared to the enormous investment required for BMD and OCS, a small investment in multi-use science and technology for space protection will yield a big payoff.

The Air Force is truly at the crossroad General Estes espoused. As we stand here at the fork in the road, we have a clear choice between two paths. The first path is a winding, twisting and all-consuming quest for space-based weapons. This path is fraught with technical, cost and schedule risks with little guarantee of success before the threats described become real problems for our national security. Alternatively, the second path, although less politically expedient at the moment, is a gentle and smooth path to defense via deterrence and assured access to space.

The second path eventually reunites with the first but after its initial dangers and uncertainties have been resolved. Will we choose the path safest for retaining Air Force stewardship of space or the course that better protects our national security?

The Real Penalty for Failure

Eliot Cohen and John Gooch, in *Military Misfortunes*[4], theorize about why failure in war occurs. They believe there are three "simple" types of failure: failure to learn, failure to anticipate, and failure to adapt. Individually, these three failures are not catastrophic. When all three types of failures manifest themselves simultaneously, a recipe for disaster is brewing. If we remain passive reactionaries, these lessons may become applicable to the space protection issue.

Our country is becoming inextricably tied to commercial space systems for our economic and military benefit. There are dangers looming on the horizon in the form of threats. As Sun Tzu states, "know thyself and thy enemy." We cannot afford to re-learn the timeless lesson that one's source of strength is a target for one's adversaries. Likewise, as we recognize changes to our strategic environment and how we create wealth, we must not fail to anticipate the challenges in protecting our centers of gravity. Finally, we must adapt our thinking and defenses to the changes and challenges we face. Currently, we've begun a process of awareness in this country. Increased awareness and action is critical, even if it's initially a means of deterrence or limited defense. America can ill afford the potential disaster should we fail to heed Cohen and Gooch's advice.

Notes

[1] Estes, General Howell M. III, Commander-in-Chief United States Space Command. Address. Air Force Association Symposium, Los Angeles, CA, 14 November 1997.

Notes

[2] Air Force Space Command. *Legislative Update*, 17 February 1999. Sen Bob Smith (R-NH) has been critical of the USAF's handling of the SBIRS Low project and lack of any space control systems. Consequently, he plans to make the issue of a separate Space Force a key issue in his potential bid for the presidency in 2000. Defending the USAF's stewardship of space in a 4 Feb 99 address to the Air Force Association, General Myers (CINCSPACE) stated resources and technology are the "obstacles to achieving military space power."

[3] Fielding of ballistic missile defense and OCS systems may require changes to the Anti-Ballistic Missile (ABM) Treaty and Outer Space Treaty, respectively.

[4] Cohen, Eliot A. and John Gooch, *Military Misfortunes: The Anatomy of Failure in War*. New York: Vintage Books, 1991, p25-28.

Appendix A

Appendix A List of Acronyms

AFRL	Air Force Research Laboratory
AMC	Air Mobility Command
CINCSPACE	Commander-in-Chief US Space Command
CJCS	Chairman of the Joint Chiefs of Staff
CONOPS	Concept of Operations
CONUS	Continental United States
D^5	Deceive, Deny, Disrupt, Degrade, Destroy
DCS	Defensive Counter-space
DoD	Department of Defense
DPG	Defense Planning Guidance
DTH	Direct-to-Home
EW	Early Warning
FAA	Federal Aviation Agency
GDP	Gross Domestic Product
GEO	Geosynchronous Orbit
GPS	Global Positioning System
IGO	International Governmental Organization
ISR	Intelligence, Surveillance, and Reconnaissance
JIATF	Joint Interagency Task Force
JTF	Joint Task Force
LEO	Low Earth Orbit
NCA	National Command Authority
NDIA	National Defense Industry Association
NGO	Non-Governmental Organization
NIMA	National Imagery and Mapping Agency

NIPC	National Infrastructure Protection Center
NMS	National Military Strategy
NRT	Near Real-time
NSS	National Security Strategy
OCS	Offensive Counter-space
PDD	Presidential Decision Directive
POM	Program Objective Memorandum
SATCOM	Satellite Communications
US	United States
USCG	United States Coast Guard
USG	United States Government
USSPACECOM	United States Space Command
WMD	Weapons of mass destruction

Bibliography

AFDD 1, *Air Force Basic Doctrine*, September 1997.

AFDD 2-2, *Space Operations*, 23 August 1998.

Air University 18 (AU-18), *Space Handbook: A War Fighter's Guide to Space*. 2 vols., December 1993.

Barnett, Jeffrey R., *Future War: An Assessment of Aerospace Campaigns in 2010.* (Air University Press), 1996.

Caton, Maj Jeffrey L., *Rapid Space Force Reconstitution: Mandate For United States Security*. (Air University Press), 1994.

DeBlois, Maj Bruce M. "Ascendant Realms: Characteristics of Airpower and Space Power." *The Paths of Heaven.* (Air University Press), 1997, 529-578.

Friedman, George and Meredith, *The Future of War: Power, Technology and American World Dominance in the Twenty-First Century*. New York: Crown Publishers, Inc., 1996.

Giffen, Col Robert B., *US Space System Survivability* (National Defense University Press), 1982.

Goodrich, Jonathan N., *The Commercialization of Outer Space*. New York: Quorum Books, 1989.

Hust, Maj Gerald R., *Taking Down Telecommunications.* (Air University Press), 1994.

Hutcherson, Lt Col Norman B., *Command & Control Warfare: Putting Another Tool in the War-Fighter's Data Base.* (Air University Press), 1994.

Institute of Air & Space Law, http://www.iasl.mcgill.ca/.

International Space Brokers, http://www.isbworld.com/gateway.htm.

Joint Publication 3-14, *Joint Doctrine; Tactics, Techniques, and Procedures (TTP) for Space Operations*, first draft.

Kennedy, Capt Fred, Capt Rory Welch, and Capt Bryon Fessler. "A Failure of Vision: Retrospective." *Airpower Journal*, no. 2 (Summer 1998): 84-94.

Launchspace, http://www.launchspace.com/ref/msl/browse/mission/index.html.

Lupton, Lt Col David, *On Space Warfare* (Air University Press), 1988.

Mahan, Alfred Thayer, "The Influence of Sea Power on World History: 1660-1783" (excerpt). *Air Command and Staff College War Theory Coursebook,* Academic Year 1999.

Mantz, Col Michael R., *The New Sword: A Theory of Space Combat Power* (Air

NASA Office of Commercial Programs, *Commercial Use of Space: A New Economic Strength for America*, 1992.

National Science and Technology Council, *National Space Policy* (U), 19 September 1996. (Unclassified version)

National Security Space Architecture (NSSA) homepage; on-line, Internet, November 1998, available from http://www.irmspace.tasc.com/mindex.htm.

Office of Air and Space Commercialization, http://cher.edu.doc.gov/oasc.htm.

Petersen, Maj Steven R., *Space Control and the Role of Antisatellite Weapons.* (Air University Press), 1991.

Quoted in Defense Daily, "Satellites Could Be Vulnerable, NRO Chief Says," 1 October 1998 in Headquarters Air Force Space Command, *Legislative Update*, 6 October 1998.
Space Publications, *State of the Space Industry*, 1998.
The White House, *A National Security Strategy For A New Century*. May 1997.
The White House, *A National Security Strategy For A New Century*. October 1998.
United Nations Home Page, http://www.un.org/.
United States Space Command, *Long Range Plan*, 1997.
University Press), 1995.
USSPACECOM/J3, *Commercial Space Asset Protection, National Defense Industry Association (NDIA) Summer Study*, October 1998.
Weidenheimer, Lt Col Randall S. "Increasing the Weaponization of Space: A Prescription For Further Progress." Occasional Paper No. 8. Maxwell AFB, Ala.: Center for Strategy and Technology and Air War College, 1998.
Ziegler, Maj David W., *Safe Heavens: Military Strategy and Space Sanctuary Thought.* (Air University Press), 1998.