Newport, R. I.

PROTECTING CRITICAL SPACE SYSTEMS: A NATIONAL SECURITY ISSUE

by

William T. Cooney
CDR, USN

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Maritime Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:_____

13 May 2002

_____
Advisor: Captain Mark Seaman

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol:
C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):Protecting Critical Space Systems: A National Security Issue

9. Personal Authors: Commander William T. Cooney

10.Type of Report: FINAL

11. Date of Report: 13 May 2002

12.Page Count:28 **12A Paper Advisor (if any): Captain Mark Seaman**

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:

Commercial space capabilities, asymmetric attack, national security, space policy and doctrine, protection of commercial military space systems

15.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). The space 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 and military play in assuring our access?

Future projections point to force-on-force space confrontations with peer competitors and asymmetric attack by hostile groups, and individuals. Therefore, protection of commercial military space systems must be rooted in space law, space policy and doctrine with consideration to the and future strategic environment they will become. Key questions will address the impact on U.S. national security due to attacks on commercial and military space assets. What is the 'real' impact of commercial space on the U.S. economy and military capability? 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? Finally, what policy and process changes are needed to protect our national security?

16.Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461

20.Office Symbol: **C**

Security Classification of This Page **Unclassified**

Abstract of

Protecting Critical Space Systems: A National Security Issue

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). The space 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 and military play in assuring our access?

Future projections point to force-on-force space confrontations with peer competitors and asymmetric attack by hostile groups, and individuals. Therefore, protection of commercial and military space systems must be rooted in space law, space policy and doctrine with consideration to the future strategic environment they will become. Key questions will address the impact on U.S. national security due to attacks on commercial and military space assets. What is the 'real' impact of commercial space on the U.S. economy and military capability? 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? Finally, what policy and process changes are needed to protect our national security?

Background

"Space assets must be protected because the nation's enemies know how valuable those assets are and will try to find a way to deny their use. Besides protecting those assets, technology must be developed to keep enemies from using U.S. assets for their own purpose."[i]

— Ralph Eberhart
General, USAF

Invisible lines of satellite information are rapidly supplementing the sea-lanes, roads, and cables of today and yesterday. Television, voice, weather, images, location, and other data stream down to Earth from satellites orbiting above—all of which are operated by military, civil, or commercial entities. These satellites

perform functions similar to those of terrestrial public utilities, providing needed goods and services. Unlike their earthbound counterparts, which service only a neighborhood or city, these utilities are used on almost every continent by billions of people and may thus be appropriately labeled "global utilities[*]." They are critically important to the national security, economies, and safety of the user nations. In May 1998, 40–45 million pager subscribers lost service; some ATM and credit card machines could not process transactions; news bureaus could not transmit information; and many areas lost television service—all because of the loss of one satellite.[ii] Over the past years, the reliance on satellites for all types of global utilities has increased, and future loss of any of these satellites, whether through operator error or subversion, would have drastic implications.

Satellite services are invaluable to the United States and its allies. The use of space is one of this country's greatest strengths, but extensive reliance on global utilities also represents a substantial liability. Currently no physical system exists for protecting these global utilities. We can bring to bear economic, political, and other multilateral pressures on an offending nation or group, and we are party to treaties and agreements that prohibit certain activities—these have worked well in the past. But what if the threat comes from non-government organizations, terrorist groups, or an adversarial nation? Or what if we are unable to identify the sources of the offense? Treaties and sanctions may not prove so effective. We will need some other source of protection.

Because of the critical nature of these services, they should not be left without some form of security or escort. We provide protection for other potentially vulnerable goods and services traversing the seas or land. Specifically, the Navy has the ability and duty to escort and protect domestic and allied vessels through hostile seas, and the Army aids in disaster or famine relief in some countries and secures transit lines for most operations. In contrast, we provide space-based utilities no such security or assurance of safe passage or operation.

International laws and treaties—such as the various United Nations treaties—permit free travel in space, but history has demonstrated that international laws protecting the open seas can mean very little in a conflict. It

---

[*] Global Utility: Civil, military or commercial system-some or all of which are based in space-that provide communication, environmental, position, image, location, timing, or other vital technical service or data to global users.

is likely that in some future battle, space will become a battleground, as have all other mediums in the past. Yet, satellite systems of the United States and its allies are, for the most part, unprotected on the open seas of space. Unfortunately, we have no method of protecting them from attack.

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. There are major differences in 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.[iii] Also, 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.

This paper will take a systematic approach to first prove the vital nature of space-based assets such as satellites. 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. Military space systems have always been vital to national security. Over the last decade commercial space systems have become equally vital to our national security. In order to state unequivocally the need to protect commercial along with military 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 military and commercial systems, which include 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.

Reliance on Military and 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

Utilities provided by satellites are numerous and varied (fig. 1).[iv] New commercial remote-imaging and communications satellites are being launched at an increasing pace. World reliance on satellite utilities increases every day and no doubt will continue to do so, with most projections indicating growth in communications satellites and a tripling of the number of satellites in service (fig. 2).[v]

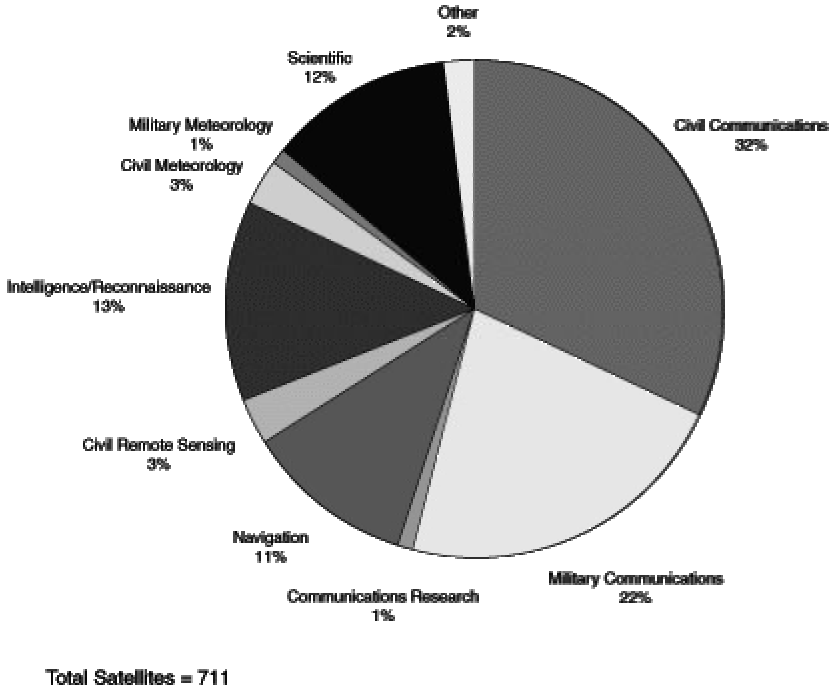

Figure 1. Satellites by mission (1996)

Let us consider one of the most important global utilities—the Global Positioning System (GPS). Although GPS provides precise positions for military, civil, and commercial purposes worldwide, it may be even more important as the "global clock."

Users everywhere rely on GPS as a means of "time transfer" to clock a multitude of products precisely, from communications circuits to bank transactions—all to within a few billionths of a second. To see how important this is, consider what happened when a real error occurred in 1996. A satellite controller at the Air Force's GPS control center accidentally put the wrong time into just one of GPS's 24 satellites. The erroneous time was broadcast for only six seconds before automatic systems detected it and shut the satellite signal down.

Nonetheless, over one hundred of the more than eight hundred cellular telephone networks on the US East Coast—which rely on precise GPS-provided timing—failed. Some took hours and even days to recover.[vi] GPS directly produces several tens of billions of dollars in revenue for the United States yearly. Indirectly, it produces many times this amount, so the economic implications are tremendous.

This kind of dependence on global utilities continues to grow. Almost two thousand satellites may provide service to the billions of people on Earth by 2010 (fig. 2), and none of them will have protection from an attack. We must develop a security system to ensure continued operation of these critical global utilities. War fighters and others depend on GPS to tell them where they are and what time it is. Missiles and bombs rely on targeting information provided by satellites. These end users could find themselves without service or with severely degraded capabilities due to an attack, potentially resulting in friendly casualties, political instability, or a risk to security.

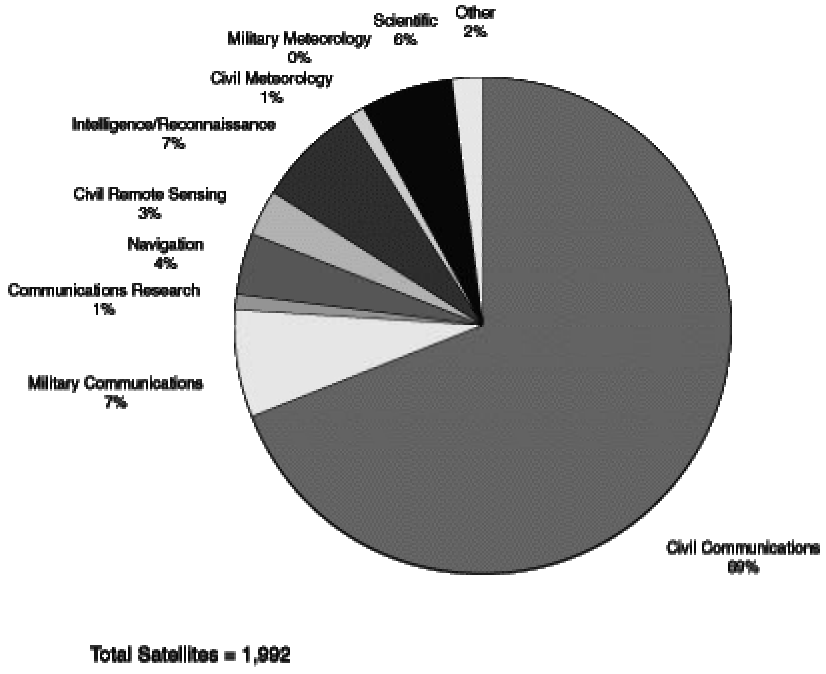

Figure 2. Satellites by Mission (2010)

The purpose here is 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 or aging vital war fighting capabilities will make the reliance on commercial space systems attractive.

Civil Demand

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. 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.[vii]

Sensing of our environment from space is crucial for predicting natural disasters and everyday weather, and for studying the earth's environment.[viii] The realization of how reliant we are 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.[ix]

Military Reliance

The proclamation of the 1991 Gulf War by some as the "First Space War" is, in essence, the acknowledgment of the benefits of space capabilities. The acceptance of space has actually been more of a struggle for a technology-bent organization like the US Armed Forces 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.[x]

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 declining post-Cold War defense budgets is forcing the DoD to weigh carefully which multi-billion dollar space systems it can afford to buy.[xi] 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).[xii] 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 continental United States (CONUS).[xiii] The military strategic vision for the future is set forth in the Joint Vision 2010. Information

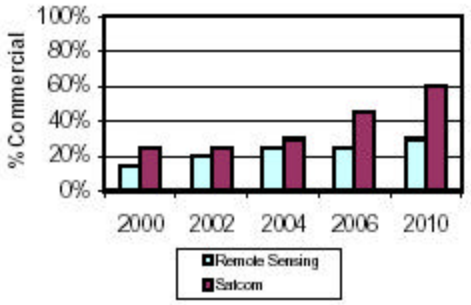

Figure 3. Growing Military Dependence on Commercial Assets

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."[xiv] 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-based utilities.

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 military and 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 with 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.[xv] Finally, threats will be addressed regarding what constitutes an attack and who might accomplish an attack.

Definitions and Types

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 intentional act specifically planned to deceive, deny, disrupt, degrade or destroy (D_5) or exploit.[xvi] 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.

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.[xvii] 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.[xviii] 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.[xix] 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 DS or to exploit it for intelligence purposes (economic or military).

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?" Industry's top concern results from hazards such as on-orbit collisions and environmental phenomena, not threat of attack.[xx] 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 that industry would not actively pursue protection measures until after the first commercial spacecraft is destroyed.[xxi] The data suggests industry is not interested in addressing potential future threats they don't believe likely to arise. Therefore, they see no added value to their bottom line in protecting against these threats.

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.[xxii] 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.[xxiii] 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 assets we must protect.

But since promulgation of that policy, government actions point to space systems threats that are real and must be considered in the interest of national security. Therefore, a space systems protection plan must be proactive and safeguard commercial as well as military systems.

Space Systems Attack

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.[xxiv] 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.

Russia remains a nation 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.[xxv] Although the Russian Duma has banned the use of ASAT weapons[xxvi], open source information suggests direct ascent and directed energy capabilities (including laser and electronic attack weapons) exist.[xxvii] 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.[xxviii] This list of peer competitors may appear short, but we must continually concern ourselves with the dilemma of proliferation.

According to the Reuters News Agency in February 1999, hackers hijacked a British Skynet military communications satellite.[xxix] In the published news report, the hackers blackmailed the British government and refused to stop interfering with the satellite until a ransom was paid. We should be particularly concerned because this is a military satellite, presumably protected with encrypted links. Even if this story cannot be

confirmed, this scenario should serve as a wake-up call for policy-makers about the vulnerability of space-based satellite systems.

Consequences

"Look at the global war on terrorism, General Tommy Franks and his forces are using ten times [the bandwidth] we used in *Desert Storm* and four times what we used in *Allied Force*. I see that continuing to climb over time."

— Ralph Eberhart
General, USAF

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 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.[xxx] With regard to commercial space systems, this chapter will answer the "so what" question. What are the consequences of not protecting commercial space-based sytems?

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' capabilities. But we must be concerned with the potential for a "Space Pearl Harbor," whether perpetrated by another state or a terrorist intending to cripple our economy. In this scenario, n adversary could attack our commercial space systems (a decisive point) to damage our economy (a center of gravity) via our financial markets. If US intervention can be prevented, our adversary's goals, of devastating the US economy, are more likely to be achieved.

Military Implications

For the military, it's a forgone conclusion that commercial space systems 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 order 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 commercial capability, such 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 a peacetime environment, the military relies on commercial products and services, such as imagery and communications.[xxxi] As important as these commercial capabilities are for training and exercises, they are vital for conducting operational planning and implementing military operations as directed by the Secretary of Defense (SECDEF). 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 that diminishing military effectiveness directly equates to an increase 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 hinges on the ability to prove commercial and military 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 and military space systems pose 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.

Recommendations and Conclusions

"Space is the inescapable challenge to all advanced nations of the earth. Our goal is nothing less than to establish the United States as the preeminent space-faring nation."

- President George Bush
20 July 1989

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.

Though the Navy is considered by most to assure access to the sea, the US Coast Guard (USCG) 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.[xxxii] 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 1 compares the four broad roles proposed for a space protection force with those of the USCG.[xxxiii] 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 exercises • Wartime support for USN	• Peacetime planning and exercise • Crisis response

Table 1. 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 (AOR), not just a function. Responding to the new organizational structure of commands, the merger of Space Command and Strategic Command would complement both commands' offensive and defensive relationships. PDD-63 directs the Department of Defense to participate in the National Infrastructure Protection Center (NIPC). The NIPC provides indications and warnings, assesses threats, and enforces laws.[xxxiv] To complement commercial space protection under the NIPC, a recommended organizational structure incorporating DoD protection systems and command relationships is shown below (Figure 4).

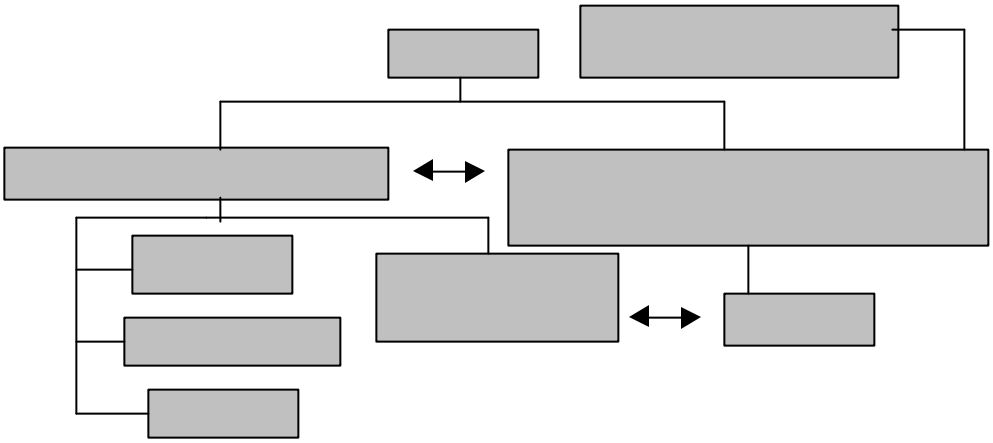

Figure 4. Proposed Organization Structure

The DoD has responded to PDD-63 by establishing JTF Computer Network Defense (JTF-CND) for protection of DoD's critical information infrastructure. Since spaced based commercial systems are 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 that 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 systems as another key element of our critical information infrastructure. 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 would 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.

Commercial space-based systems are vulnerable now. We must enact policies and set up organizations immediately to commence our efforts to diminish our vulnerability. The proposed JTF would 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 could occur once appropriate requirements are validated and 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 use of 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.[xxxv] 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 sources 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. 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.

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 near real time (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, 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.

Conclusion

The time has come to address, among warfighters and national policy makers, the emergence of space as a center of gravity for DoD and the nation. We must commit enough planning and resources to protect and enhance our access to, and use of, space. Although international treaties and legalities constrain some of the LRP's initiatives and concepts, our abilities in space will keep evolving as we address these legal, political, and international concerns. Our dominance of space depends not only on new systems but on the emerging synergy of space capabilities, CONOPS, organizational change, and effective and innovative ways to train and lead.

ENDNOTES

[i] "US Space Commander Charts Future Course." *Space Daily, 8 February 1998.*
[ii] Carlson, LT GEN Bruce, "*Protecting Global Utilities,"* Aerospace Power Journal, Summer 2000, 37.
[iii] Air Force Doctrine Document 1, *Air Force Basic Doctrine*, September 1997.
[iv] Carlson, LT GEN Bruce, "*Protecting Global Utilities,"* Aerospace Power Journal, Summer 2000, 38.
[v] Ibid., 39.
[vi] The Oregonian. *"Satellite Loss Puts Millions Out of Touch,"* 21 May 1998.
[vii] Space Publications. *State of the Space Industry*, 1998, 42-51.
[viii] Ibid., 16.
[ix] The Oregonian. *"Satellite Loss Puts Millions Out of Touch,"* 21 May 1998.
[x] The White House. *National Space Policy*, 19 September 1996, 8.
[xi] "Space Almanac: Major Military Satellite Systems." *Air Force Magazine*, August 1998, 31.
[xii] National Defense Industry Association. Draft briefing. To CINCSPACE. Subject: Protection of commercial Space, December 1998, 6.
[xiii] NAIC, *Threats to US Military Access to Space* (Document # NAIC-1422-0984-98), 11.
[xiv] Department of Defense, *Joint Vision 2010*, 16.
[xv] National Defense Industry Association. To CINCSPACE. Subject:Protection of Commercial Space, December 1998, 11.
[xvi] Ibid., 15.
[xvii] USSPACECOM, Long Range Plan: Implementing USSPACECOM Vision for 2020, March 1998, 4.
[xviii] National Defense Industrial Association. To CINCSPACE. Subject:Protection of Commercial Space, December 1998, 15.
[xix] USSPACECOM, Long Range Plan: Implementing USSPACECOM Vision for 2020, March 1998, 4.
[xx] National Defense Industrial Association. To CINCSPACE. Subject:Protection of Commercial Space, December 1998, 18.
[xxi] 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."
[xxii] Air University. AU-18 Space Handbook: A War Fighter's Guide to Space Vol 1, December 1993, 98.
[xxiii] Joint Pub 3-14. 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.
[xxiv] 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.
[xxv] 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.
[xxvi] DeBlois, Lt Col Bruce M., "*Space Sanctuary: A Viable National Strategy*," Airpower Journal, Winter 1998, 47.
[xxvii] NAIC, *Threats to US Military Access to Space* (Document # NAIC-1422-0984-98), p5-16.
[xxviii] 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."
[xxix] Reuters News, "*Hackers Reportedly Seize British Military Satellite*," 28 February 1999.
[xxx] 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.
[xxxi] 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).
[xxxii] Coast Guard 2020, (www.uscg.mil/COMMANDANT/COMDNT.HTML)
[xxxiii] Ibid.
[xxxiv] National Infrastructure Protection Center Homepage, (www.nipc.gov).
[xxxv] USSPACECOM. *Long Range Plan*, 1998, 19-47.

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.

Carlson, LTGEN Bruce, "Protecting Global Utilities." Aerospace Power Journal. (Summer 2000).

"Coast Guard 2020," 2002. <http://www.uscg.mil/COMMANDANT/COMDNT.HTML>

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

Franse, LtCol martin E. B. , "Back to the Future: Space Power Theory and A. T. Mahan." Aerospace Power Chronicles (4 August 2000) <http://airpower.maxwell.af.mil>

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

Hyten, LtCol John E., "A Sea of Peace or a Theater of War. Dealing with the Inevitable Conflict in Space." Aerospace Power Chronicles (January 2001).

Johnson, Bryan T., " The New Space Race: Challenges for U.S. national Security an Free Enterprise." The Heritage Foundation Backgrounder (August 25, 1999) <http://www..heritage.org>

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

"Joint Task Force on Computer Network Defense Now Operational, 2002. <http://defenselink/news/Dec1998/b1230/1998_bt658-98.html>

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

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

Morning, Frank, Jr., "Space Battle Looms for U.S. Giants." Aviation Week & Space Technology, 10 December 2001, 62.

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

National Infrastructure Protection Center Homepage <http://www.nipc.gov>

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.

Newberry, Major Robert D., Space Doctrine for the Twenty-first Century. (Air University Press), 1998.

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

"Hackers Reported Seize British Military Satellite." Reuters, 28 February 1999.

Space Publications, *State of the Space Industry*, 1998.

Streeter, Staff Sgt. Melanie, "U.S. Space Commander Charts Future Course." Space Daily (* February 2001). <http://www.spacedaily.com/news/milspace-02d.html>

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 States Space Command, *Long Range Plan*, 1997. (Air University Press), 1998.

USSPACECOM/J3, *Commercial Space Asset Protection, National Defense Industrial Association (NDIA) Summer Study*, October 1998.

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

Wilson, J.R., "Rising Prospects for Military Space." Aerospace America, January 2002, 41.

Ziegler, Maj David W., *Safe Heavens: Military Strategy and Space Sanctuary Thought.* (Air University Press), 1998.