STRATEGIES FOR DEFEATING COMMERCIAL IMAGERY SYSTEMS

by

Stephen Latchford, Lieutenant Colonel, USAF

December 2005

Occasional Paper No. 39
Center for Strategy and Technology

Air University
Maxwell Air Force Base, Alabama 36112

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Strategies for Defeating Commercial Imagery Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Air War College,Center for Strategy and Technology,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**53**	

STRATEGIES FOR DEFEATING COMMERCIAL IMAGERY SYSTEMS

Stephen Latchford, Lieutenant Colonel, USAF

December 2005

The Occasional papers series was established by the Center for Strategy and Technology as a forum for research on topics that reflect long-term strategic thinking about technology and its implications for U.S. national security. Copies of No. 39 in this series are available from the Center for Strategy and Technology, Air War College, 325 Chennault Circle, Maxwell AFB, AL 36112, or on the CSAT web site at http://www.au.af.mil/au/awc/awcgate/awccsat.htm. The fax number is (334) 953-6158; phone (334) 953-6460.

Occasional Paper No. 39
Center for Strategy and Technology

Air University
Maxwell Air Force Base, Alabama 36112

Contents

Page

Disclaimer

The views expressed in this academic research paper are those of the author 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.

Illustrations

Tables

Author

Lieutenant Colonel Stephen Latchford is currently the Command Electronic Warfare Officer and Chief of Special Technical Operations for Air Force Space Command, Peterson AFB CO. He is responsible for all aspects of Integrated Joint Special Technical Operations special-access capabilities related to Air Force Space Command. Colonel Latchford began his Air Force career as a navigator and electronic warfare officer on the KC-135 Rivet Joint. His previous assignments include Offutt AFB NE, the National Security Agency, and United States Central Command. He is a graduate of the Air Force's Air War College and holds a M.S. in aeronautical science management from Embry-Riddle Aeronautical University and a B.S. in political science from the U.S. Air Force Academy. In 2004 Colonel Latchford received the Air War College Commandant's Award for his paper entitled "Strategies for Defeating Commercial Imagery Systems."

Abstract

High-quality space-based imagery, once among America' s most closely held secrets for force enhancement, is now openly available through commercial providers. The United States faces questions of how to keep this source of valuable intelligence information from its adversaries, and whether it is even possible or desirable to do so. This paper addresses strategies for countering the threat to military operations posed by commercial earth-sensing satellites. The paper emphasizes technical countermeasures, using a combination of nodal and value analysis to arrive at possible solutions. It also considers strategies necessary to make those countermeasures militarily useful and politically acceptable. The result of the research is a recommendation for long-term pursuit of co-orbital weapons with reversible effects, while in the short term, integrating current technology into ground-based and airborne radio-frequency jammers and low-power lasers for point defense. In the process it highlights the need for surge capacity in space lift, so the United States can have a defensive space-control capability without accelerating the arms race in space.

I. Introduction

> *The unique spaceborne advantage that the US has enjoyed over the past few decades is eroding as more countries—including China and India—field increasingly sophisticated reconnaissance satellites. Today there are three commercial satellites collecting high-resolution imagery, much of it openly marketed. Foreign military, intelligence, and terrorist organizations are exploiting this—along with commercially available navigation and communications services—to enhance the planning and conduct of their operations.*
>
> -- CIA Director George Tenet to the U.S. Senate Armed Services Committee, 19 March 2002[1]

The 1991 Persian Gulf War provided the first evidence of the growing danger commercial earth-imaging satellite systems posed to United States military operations. For the first time in history, military commanders recognized commercially available satellite images could deny their forces the element of surprise because images had become sharp enough to detect force deployments and movements. Since 1995 more than sixteen countries and multi-national consortia have put commercial satellite-imagery systems into service, half with image-quality better than eight meters, further raising the threat posed to American and allied forces.[2]

In the United States, military strategy has not consistently served as the medium for encouraging technological innovation. Typically, strategy evolves slowly, taking advantage of new technologies developed by defense laboratories and industry. Practitioners adapt the capabilities to new uses, which subsequently results in improved tactics. The Wright brothers, for example, did not develop the airplane to meet stated needs of the United States. In fact, the Wrights could not generate government interest in their technology until after it found success in Europe.

Likewise, it is reasonable to expect space capabilities and space strategy will evolve in a similar manner. New strategies for space warfighting sometimes run counter to currently held international norms, and because it can be difficult to create new strategies if the enabling capabilities to achieve them are not yet envisioned, existing strategies may be unnecessarily narrow, resulting in little popular support. Typically, when research scientists develop new technologies, users often request improvements to make it more suitable to their applications. While technology breakthroughs occasionally result in a new capability, the iterative approach is just as valid, but it takes resources to keep that process going.

The problem with the iterative process is that in the time it takes for strategy and technology to evolve, a surprise may occur, one for which the country is not prepared to respond. As the nation's dependency on space increases, civilian and military leadership will levy requirements for protection against hostile attacks upon space-based systems. Finally, as adversaries challenge U.S. space power through capabilities of their own, or worse if they can deny U.S. access to space, requirements will likely appear for offensive weapons to fight for, in, and from space. A proactive policy will lessen the likelihood of a strategic surprise.

To prevent strategic surprise and to push technological capabilities and operational concepts forward more quickly, today's leaders should analyze current and future space threats and generate a clear, unambiguous strategy for hedging against them. Such a strategy would generate validated requirements, which are the primary source for procurement actions taken within the military and supporting government agencies.

Commercial imagery poses a real, if indirect threat to U.S. interests, yet the U.S. is slow to move ahead without a clear policy and strategy to do so. In March 2002 the Director of Central Intelligence told the Senate Armed Services Committee that U.S. enemies are exploiting commercially available imagery to plan attacks.[3] The threat is compounded by a complex set of problems that must be addressed. Prioritization of funding within the Defense Department is difficult when there is a lack of documented requirements. Formal requirements are difficult to produce because the legal considerations and financial obligations are significant. If the threat is as the director describes, however, the military needs to have a strategy for countering it. And that strategy should be built on a coherent policy from which all the branches of government and industry can act. Such a policy will ensure diplomatic and economic instruments of power are working to shape the environment to permit military employment, should it become necessary.

The purpose of this paper is to advocate for an overarching policy on countering a single space-based threat, specifically commercial earth-imaging satellite systems delivering militarily useful imagery products to an enemy. Additionally, it will advocate a strategy, along with corresponding weapons technology for development. The paper focuses on countering dissemination of updated or new imagery, since imagery that has been sold and disseminated to the public is irretrievable. While old imagery can provide extremely valuable targeting information on fixed targets, such as buildings, updated imagery is arguably the main threat since it provides up-to-date information for attacks against military deployments and post-strike battle damage assessments against all types of targets. Though some ideas presented in this paper may be applicable to other threats, this analysis is limited to the problem of commercial imagery systems.

Information about commercial imaging systems is plentiful. Many technical operating parameters are a matter of record, reported to the Radio Regulations Board of the International Telecommunications Union.[4] The Joint Spectrum Center in Annapolis, Maryland, maintains updated files on every internationally registered communication system. Trade publications, company brochures, and various Internet sites provide imaging-system resolution, capabilities, system architectures, and sample images.[5] Conversely, detailed technical information on counter-surveillance technology is sparse. During the literature search, a number of documents by service scientific and technical intelligence centers had titles that appeared to be on topic. However, in order to avoid compromise of classified information, they were not used in this study.

After reviewing the threat and advocating a need for a policy that will generate strategy-based requirements, this paper will review some countermeasure techniques worthy of further development and fielding. The first step is a nodal analysis on several representative satellite systems in an effort to identify typical sub-systems for targeting. Next, a set of desired effects will be developed to provide a standard for comparing countermeasure techniques and for ranking their suitability. The resulting scores will then be used to identify the most promising countermeasure techniques and discusses weapon-specific advantages and limitations of each countermeasure. The top-scored countermeasure techniques will be assessed to determine if they meet the strategy requirements and whether they should be considered for research, development, and fielding.

II. Commercial Imaging Systems and the Threat to National Security

Commercial imagery systems provide legitimate products essential to scientific and economic growth, yet they have the potential to be used as a military force-multiplier. Today, corporations and quasi-governmental consortia operate sophisticated imaging satellites and sell their images to the public for purposes such as earth mapping and cartography, agricultural monitoring, environmental studies, oil and gas exploration, weather prediction, treaty monitoring, news gathering, and disaster response. Imagery systems designed for non-military purposes can still have significant military value. In fact, the Director of Central Intelligence last year ordered use of commercial satellite imagery to augment military reconnaissance-satellite products. Under the new "Clearview" agreements, the government will pay up to one billion dollars to two companies over a five-year period.[6] If the U.S. government, which has its own high-quality imagery systems, is buying imagery on the open market, there is every reason to suspect countries without such indigenous capability will find an advantage in doing so.

The threat comes from the particular way imagery products might be used by an enemy to find, fix, track, target, engage, and assess U.S. interests.[7] Archived imagery is readily available through a number of open sources, including the Internet; so military commanders should assume the adversary has precise knowledge of strategic targets such as ports, airports, military installations, power plants, government buildings, commercial centers, and sports venues. As this paper will show, however, once friendly forces begin to mobilize for combat, access to new imagery depicting updated force concentrations and movements, supply stations, deployment progress, and battle-damage imagery intelligence can be especially helpful to enemy planning.

Imaging Systems

The first step in being able to understand the potential harm to the nation's forces is to understand the capabilities of commercial imaging systems. For the purpose of this paper, "commercial imaging systems" includes all the components of systems that use earth-orbiting satellites to make and distribute images of the earth. Such systems use electro-optical, infrared, multi- or hyper-spectral, or radar sensors. Government-operated and government-subsidized systems are included here, but only those that distribute images to the public for a fee, not those operated strictly by governments for their own use, such as military reconnaissance satellites.

One of the key quality-measurements of imagery systems is the resolution of the image. "Resolution is dramatically increasing—10m in 1999, 1m in 2000, 62cm in 2002, and licenses for 50cm have been granted by the U.S. government."[8] Depending on the specific sensor, different image resolutions are achievable. Gray-scale panchromatic images are available with resolutions down to 0.5 meters. SpaceImaging Corporation advertises *IKONOS* satellites can provide color images down to 1-meter resolution. Infoterra's *QuickBird* multi-spectral resolution can achieve resolutions accurate to 2.4 meters, and Radarsat's radar images are accurate to 8 meters.[9]

Another measure of a satellite's capability is how often it can revisit a target. Some orbiting systems can revisit a site every two or three days, but with mirror steering, they can look at the site for several consecutive orbits before losing sight of it. Systems with multi-satellite constellations can claim even more frequent looks. The value of frequent revisits is militarily significant for indications and warning and battle damage assessments.

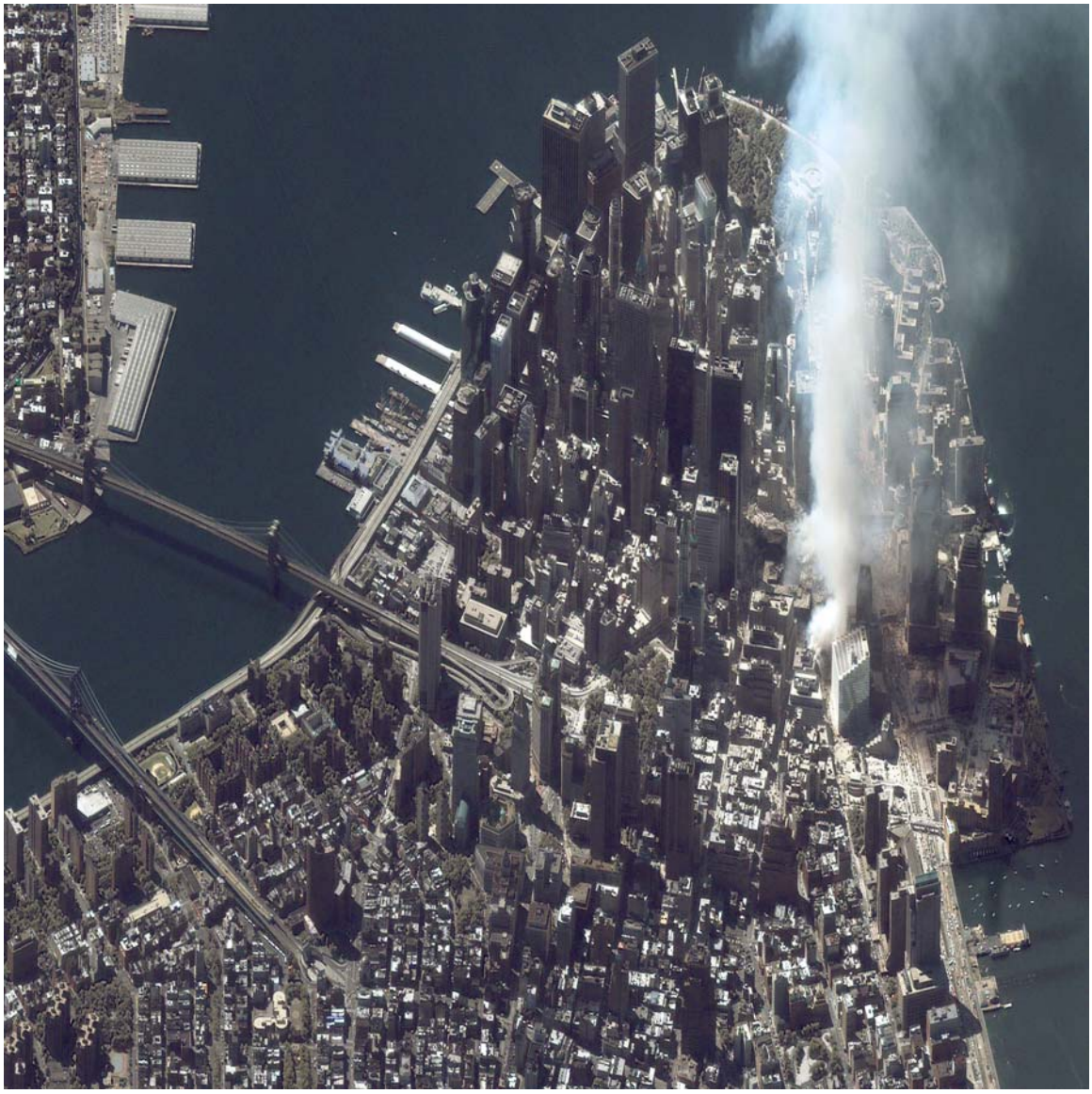

Figure 1. Example of color image at 1-meter resolution--Manhattan 12 Sep 01 taken by commercial *Ikonos* satellite. Used with permission, SpaceImaging.com

The French consortium Centre National d'Etudes Spatiales, which runs the SPOT Image Corporation system, is an excellent example of the improvements in earth-imaging capabilities over the last twelve years. *SPOT* provided frequent high-fidelity commercial images to coalition forces in the Persian Gulf War, while denying them to Iraq.[10] Its formidable capabilities at that time included four spectral bands—a stereo-vision panchromatic band with 10-meter resolution and three multi-spectral bands in the green, red, and near-infrared bands with 20-meter resolution. An image area of 60 kilometers x 950 kilometers could be revisited every three days using steerable mirrors.[11] This level of fidelity was sufficient to detect large armor concentrations and movements and could have given Iraq advance notice of U.S. attack plans.[12] Today, SPOT advertises 2.5-meter panchromatic resolution, 10 to 20-meter multi-spectral resolution, and the ability to provide daily coverage of desired targets.[13]

Orbits

Geosynchronous earth orbiting satellites typically trade resolution for the ability to maintain constant coverage of a specific area. This is done by putting the satellite in an equatorial orbit at approximately 22,500 miles in altitude—the latitude and altitude necessary for the satellite to circle the planet once daily, thereby keeping its relative position with the ground. Weather satellites are an example. With resolutions of one kilometer or more, weather satellites are not normally considered to be sufficient for observing militarily significant targets on the ground. They can, however, be used to look for large, environment-influencing indicators such as aircraft contrails, smoke, and clouds of dust. The usefulness of *Meteosat* for indications and warning during Operation DESERT STORM was limited by its 8-kilometer resolution and its downlink rate of one full picture every thirty minutes, yet it demonstrated an important military contribution:

> Meteosat satellites provided visible and infrared images of Iraq and Kuwait during the Persian Gulf War, including the first images of the smoke plume from the oil terminal off the Kuwaiti coast of Mina Al-Ahmadi. Every half hour, 24-hours a day, the Meteosat system provided visible evidence from space of Iraq's systematic destruction of Kuwaiti oil wells. The satellites also sent back information on wind direction during the early phases of the allied ground assault, considered critical if Iraq had resorted to using chemical weapons. Although the satellites provided images with resolutions of only about eight kilometers, they did so in minutes rather than hours or days, and were considered an important asset during the conflict. [14]

Today, *Meteosat* advertises 1-kilometer resolutions and the ability to download a picture every fifteen minutes.[15]

Most imaging satellites use lower orbits designed to maximize the effectiveness of their payloads and to access specific geography for imaging and for communication with the ground site. For example, polar orbits are better than equatorial orbits for imaging polar icecaps. Because low-orbit satellites operate at lower altitudes than geosynchronous satellites, typically about 400-1000 kilometers, they are in constant motion in relation to fixed points on the earth. The addition of infrared or radar sensors improves the utility of low orbits because they make the nighttime portions of the orbit useable. The additional benefit of radar sensors is that they can see through clouds and some camouflage coverings. Higher image-resolution and better target access are achievable in low orbits, but since communication with the satellite requires line-of-sight to a ground station, geography may limit the orbit or require additional ground stations. For example, *Landsat*, the United States government's low-orbiting system, sells 15-meter earth imagery to users worldwide and has ground stations in eighteen foreign countries, including China.[16]

Sensor Technology

Earth imaging satellites may carry more than one type of sensor, each designed for a specific purpose, and each using different sensing materials and covering different frequency ranges, expanding their utility. For example, *Landsat-7*, launched in 1999, features an enhanced thematic mapper in addition to its multi-spectral scanner. The enhanced thematic mapper uses eight spectral bands. The first four cover portions of visible light spectrum from 0.45 to 0.9 micrometers using silicon photodiodes. Sixteen indium antimonide detectors serve the bands from 1.55 to 1.75 micrometers and 2.08 to 2.35 micrometers, and four mercury-cadmium-telluride detectors are added for the 10.4 to 12.5 micrometer band.[17] Not

all bands in a system have a need for high resolution, however. Multiple discrete bands are used together to produce multi-spectral images. Though multi-spectral images are lower resolution than panchromatic images, they can provide information such as foliage types, operating status of heat-generating infrastructure and equipment, and aircraft contrails. As the previous *METEOSAT* example showed, depending on the intended target and the spectral bands available to image it, low-resolution multi-spectral systems can have useful military applications. The number, type, and frequencies of the sensor bands vary from system to system, frustrating the concept of a simple, universally applicable countermeasure.

Processing and Distribution

Future enemies may already have an archive full of useful imagery, but they must rely on the satellite operator's processing and distribution system to get up-to-date imagery. It can take from minutes to weeks for desired images to be received depending on the tasking—the desired angle, resolution, sensor type, the number of satellites in the constellation, their orbits, and the number and locations of suitable ground sites. SPOT's system is typical.[18] The satellite operator passes instructions to the sensor, such as where, when, and how to look at a target, which sensors or bands to use when looking, which ground sites should receive the downlink and which customers should receive the product.[19] Depending on the system, the image downlink may be processed where it is received, or it may have to be retransmitted to a processing facility somewhere else in the world. The processing center then creates the products from the image data and licensed distributors can provide them to customers. Potential enemies may get imagery from a licensed distributor, another customer, or through surreptitious acquisition such as unlicensed reception.

Nodal Description

A quick survey of space systems leads to the conclusion that all imaging systems are comprised of both space and ground components. The space component consists generally of the spacecraft platform, also called the bus, the sensor payload, and the communication and control system. A complex ground component can be distributed across several countries and consist of multiple ground receive-stations, an imagery-processing station, terrestrial communications between nodes, and a product distribution system. As described earlier with *Landsat*, some systems use direct-receiving stations, which support licensees in different countries or collect data for specific geographic areas. In those cases the reception and processing nodes may be co-located and have reduced need for specialized communication nodes beyond what is needed for product distribution.

The capabilities described in this section form a threat to the homeland and to U.S. military operations worldwide, a threat that requires attention today if timely responses are expected in a crisis. If an enemy today were using updated imagery to plan attacks capable of significant damage to U.S. interests, the short list of available responses would be unappealing. For example, turning off or disrupting the space-based nodes, i.e. the satellites themselves, would effectively deny new information to legitimate users and friendly forces that are dependent upon it. Voluntary interruption of *METEOSAT* or *Landsat* data might be unacceptable in a time of crisis management, such as following a chemical attack where such data is used in managing the response. Disruption of selected terrestrial nodes, such as a direct-receiving station or the portion of the product distribution channel within the adversary's borders, might limit the effects of the service denial to a subset of users and customers, but again, the impact on non-belligerent users might be substantial.

III. Implications of a Space Control Strategy

> *It is almost certain that sometime early in the 21st Century, the fielding of space-based weapons will occur under the auspices of defense, in much the same manner as the nuclear weapon buildup that occurred within the latter half of the 20th. And, like nuclear weapons, once fielded, there will be no reversing course. This too is an historical lesson of warfare.*
>
> --James Oberg, *Space Power Theory*[20]

The current U.S. strategy for operations against space threats is unclear. Part of the problem is that discussions on space threats are often focused on land-based threats to U.S. space-based infrastructure. Public strategy documents pay little attention to threats posed by enemy capabilities from space, or the threat from commercial imagery specifically. The President's 2002 *National Security Strategy* focuses on protection of U.S. infrastructure and assets in outer space but is silent on threats from other countries' space resources.[21] The subordinate 1997 *National Military Strategy*, now superseded by the 2004 version, guardedly advocated controlling an adversary's use of space:

> We will also endeavor to maintain our current technological lead in space as more users develop their commercial and military capabilities. It is becoming increasingly important to guarantee access to and use of space as part of joint operations and to protect US interests. Space control capabilities will ensure freedom of action in space and, if directed, deny such freedom of action to adversaries.[22]

The important caveat to denying freedom of action to the enemy is, "if directed." Defense officials are essentially stating there is no policy permitting the military to deny freedom of action to adversaries. If the Defense Department wanted to encourage development of capabilities in that area, the document should have been more directive, saying "we will develop and maintain space control capabilities to ensure freedom of action in space, and to deny such freedom to adversaries."

From a review of public policy documents, U.S. space control strategy appears to be limited, and that is likely to have direct impact on funding for research and development. Looking at the Defense Department's definition of "space control," it is easy to see why the administration needs to have a carefully considered concept before declaring a strategy that will no-doubt have international repercussions. According to joint doctrine:

> Space control operations provide freedom of action in space for friendly forces…and negation of enemy adversary space systems. Space control operations encompass all elements of the space defense mission and include offensive and defensive operations by friendly forces to gain and maintain space superiority and situational awareness if events impact space operations.[23]

The United States Strategic Command inherited the former United States Space Command's mission to be prepared to apply force from space. It is currently limited to theorizing since a policy change is necessary to permit an attack. Strategic Command states, "In the future, being able to attack terrestrial targets from space may be critical to national defense….USSTRATCOM currently does not have an operational anti-satellite

weapon….Research and development into anti-satellite technology is continuing."[24] The lack of a declarative U.S. policy on conducting space control operations leaves little room for the military to declare a space-control strategy. Without a policy or a strategy, support for building capabilities is likely to get vague, inconsistent, and cautious support from Congress and the public.

Suggesting a strategy in response to the commercial imagery threat will likely generate resistance at home and abroad if it implies any form of space weaponization. It is still a goal of the world, including the United States, to preserve the use of space for peaceful purposes. The United Nations Conference on Disarmament has been working on the details of an agreement entitled, "Prevention of an Arms Race in Outer Space," since 1981. It has not progressed since 1995 for a number of political reasons, including a U.S. assertion that it is unnecessary because there is no arms race in space.[25] Despite slow progress, support for such a measure in the 2002 General Assembly remained nearly unanimous, with only the U.S. and Israel abstaining.[26] Even if the U.S. generally supported the premise of space used for peaceful purposes, precipitous agreement on binding treaty language could severely limit options for countering or preventing hostile space activities by others in the future.

International law, destabilization, deterrence, and business impacts of commercial satellite countermeasures are current concerns in the development of ground and space-based weapons for space control. They are considered here, in the context of the current threat from commercial imagery, to avoid assumptions related to other applications of space control.

International Law

International law is among the first considerations when establishing a policy permitting a space control strategy against commercial imagery systems. The first question is whether international law allows the U.S. to interfere with a commercial imagery system, what components of the system may be attacked, and under what conditions and restrictions, and the level of force that is permissible. Another deals with the permissible methods for doing so, in particular whether defensive countermeasures may be space-based.

International law comes not from a single international code but from conclusions that may be drawn from the totality of international norms. "International law is a body of principles, rules, and norms, generally observed by the members of the international society in their international relations or when they are dealing with international organizations or citizens of other states."[27]

Legality of Attacking a Commercial Imagery Operator

The question of whether to interfere with, obstruct, or otherwise attack a commercial imagery-satellite operator must first address whether the system is a legitimate target. International law is so complex that decisions on the legality and methods of attacking commercial operators should not be left until a crisis is at hand. To begin, maritime and land warfare law have addressed the problem of dealing with non-combatants providing tangible war materiel to parties of a conflict, but the guidance is not clear. With certain exceptions, such as humanitarian assistance, maritime law recognizes the right of combatants to halt trade by persons who abrogate their neutral status by supporting a belligerent with military aid. Since space law attempts to take advantage of existing maritime and air law, it was maritime law that established "a nation's jurisdiction extends to any spacecraft under its flag."[28] Therefore, familiar mechanisms for dealing with suppliers of our enemies may have direct application in thinking about space control.

Using the parallel between maritime and space law, trade in imagery products is permissible during peacetime. If, in a crisis, the United Nations subsequently imposes sanctions, the licensing state may, under its sovereign authority, demand its commercial enterprises abide by the resolutions. It is important to note that until hostilities begin, the U.S. may not be able to unilaterally enforce the sanctions. For example, during Operation Desert Storm, if Iraq owned a space-based imagery system, the United States could have attacked the ground components as part of Iraq's intelligence infrastructure, in accordance with the laws of armed conflict. If instead Iraq had purchased its imagery, the question remains: Could the U.S. legally attack a commercial entity's ground components as part of that same intelligence infrastructure?

If a neutral country permits its citizens to export imagery data, U.S. commanders may be unable to forcibly interrupt the data unless the President or Secretary of Defense declares the country to be hostile, or the commander determines a need to act in self-defense. The *Hague Convention V* of 1907 says neutral states have no responsibility to prevent the export of anything that might be useful to a belligerent.[29] Despite that, commanders in the field have a great deal of latitude to act in self-defense, and they may use any legal weapon available to attack a commercial imagery system, in space or on the ground. Self-defense against a camera may be difficult to justify if the operator is powerless to stop the imagery from going to the enemy. In that case, only the enemy's forces, not the civilian imagery system, would be the legal targets.

The complexity of the problem is made worse by an exception for communications systems. The Air Force advises its commanders:

> If a neutral nation permits its information systems to be used by the military forces of one belligerent, the other belligerent generally has a right to demand that it stop doing so. If the neutral refuses, or if for some reason it is unable to prevent such use by a belligerent, the other belligerent may have a limited right of self-defense to prevent such use by its enemy. There appears to be a limited exception to this principle for communications relay systems. This exception only applies to systems that merely relay communications, not to systems that generate information.[30]

This exception for relay systems may have been derived from Article 8 of the *Hague Convention V* (1907), which says, "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[31]

Adding still more complexity are the agreements under The Helsinki Principles on the Law of Maritime Neutrality, part of the United Nations Convention on the Law of the Sea of 1982. These principles state, "Merchant ships flying the flag of a neutral State may be attacked if they (a) engage in belligerent acts on behalf of the enemy; (b) act as auxiliaries to the enemy's armed forces; or (c) are incorporated into or assist the enemy's intelligence system …"[32] Recalling that imagery satellites are flagged by the states that license them, these elements seem to imply commercial systems would be legitimate targets in some cases. While the Air Force Judge Advocate has provided guidance to commanders on the subject of neutral information systems, it would be helpful for the Defense Department to make a declaration on the legality of attacking commercial imagery systems. A full analysis of a question of this complexity should not be postponed until a time-critical crisis is at hand.

Considering Methods of Attack

If the rules of engagement permit self-defense against neutral systems, or if commercial system operators are declared hostile, leaders will still have to consider which weapons are appropriate to attack the systems. With weapons for use against space-based nodes, commanders will have more options for conducting attacks while avoiding heat, blast, and fragmentation that put lives at risk unnecessarily. Space-based targets might also be more accessible than terrestrial targets, but the determining factor for alternatives is the weapons that are available.

When weapons capable of attacking space systems are available, they will probably be controlled at very high echelons of command, at least initially, because of their political sensitivity. Any decision to target an imagery system of an otherwise neutral party will require direct evidence the imagery is giving a military intelligence to the adversary. Proof acceptable to U.S. military commanders may not be sufficient to sway public and international opinion, and may keep civilian leaders looking for options less controversial than an overt attack against the system. The question of whether an attack on a commercial system can be politically justified gives a commercial satellite operator a measure of protection. Accordingly, by buying third-party commercial imagery, the adversary gets a source of high-quality imagery without the expense of building it himself, plus a degree of built-in survivability, owed to the potential political dilemma. The adversary does run the risk, however, that the provider can decide to suspend service.

Once the legitimacy of the target is established, the question becomes one of necessity, proportionality, and political acceptability. Currently, operators of commercial satellites may expect a level of protection as neutral parties participating in legal commerce. A statement in a USAF School of Advanced Airpower Studies paper by Major James G. Lee reinforces that attitude, making a key assumption that the United States will not attack a third party's commercial satellite, even if that party is providing intelligence to the enemy. "In no case is attacking [a satellite owned by another nation but supporting a belligerent] with hard- and soft-kill mechanisms viewed as being politically acceptable."[33] The real question is whether the assistance provided by the imagery system operator is so damaging that it warrants a military response, in spite of the international acrimony that is likely to follow. A counter to Lee's argument would take the position that when American lives are lost as a result of material aid given to the enemy, the commercial enterprise may be declared a legal target out of necessity. It may then be put out of business in a proportional manner. The means of stopping commercial imagery will be evaluated in the context of international law and diplomacy, but the range of options is constrained by the weapons and tactics available.

Space-based Weapons for Defensive Countermeasures

Three important treaties to consider when discussing weaponization of space are the Limited Test Ban Treaty, the Outer Space Treaty, and the now-obsolete Anti-Ballistic Missile Treaty. The Limited Test Ban Treaty (1963) banned nuclear weapons test explosions, and any other nuclear explosion, in and beyond the atmosphere, specifically outer space. Its main purpose was to prevent environmental and physical damage from radiation and electromagnetic pulse.[34] The Outer Space Treaty (1967) developed at the height of the Cold War, proscribes, among other things, putting nuclear weapons or other weapons of mass destruction in orbit around the earth. It prohibits certain activities on the moon, specifically testing weapons of any kind, conducting military maneuvers, and establishing military installations. The Outer Space Treaty also established the universal right to orbit over sovereign countries by denying territorial rights in space, a clear departure from maritime and

aeronautical law with respect to national sovereignty.[35] The obsolete Anti-Ballistic Missile Treaty (1972), which grew out of the 1969 Strategic Arms Limitation Talks I, prohibited developing an anti-ballistic missile and specifically prohibited space-based missile defense systems. Its purpose was to ensure that no country felt impervious to an intercontinental ballistic missile attack—a sense that could lead to undeterred bellicosity.[36]

Though the Anti-Ballistic Missile Treaty is no longer in force, its stabilizing philosophy will no doubt continue to be a goal of most members of the United Nations, as the Disarmament Committee continues its work to secure the use of space for peaceful purposes. Although literalists argue weaponization is permissible as long as the weapons are non-nuclear, such weapons may still violate the tenet of "customary use" of space. Cicero described customary use. "Justice has emanated from nature. Therefore, certain matters have passed into custom by reason of their utility. Finally the fear of law, even religion, gives sanction to those rules which have both emanated from nature and have been approved by custom."[37] Still, customary use is evolutionary and open to argument. In 1959, United Nations Resolution 1721 established that other international laws, such as those for air and the sea may have applicability in space.[38] This is important, because it supports the view that when a treaty is silent on a matter, there may be relevant rules that apply from other treaties or custom. Because of that, the language on the purpose of the Anti-Ballistic Missile Treaty might remain a sticking point during weaponization discussions, even though the U.S. has withdrawn from this treaty. If U.S. legal advisors agree certain types of space weapons are consistent with international law and customary use, the first to put weapons in orbit is likely to draw international condemnation for their destabilizing effects. For the U.S., a decision to deploy defensive weapons is likely to be criticized as a momentous stride down the slippery slope toward martial space.

Weaponization Without Destabilization

Beyond the din generated by the international community, the United States will need to consider the actual destabilizing effects of deploying a space weapon, even if nominally defensive. As the world's superpower, a rush to weaponize in absence of an impending threat to its military superiority will be regarded with suspicion. American politicians must be prepared to respond to the question, "What threat is so grave that it cannot be handled by America's prodigious terrestrial capability?" Although competitors may not respond militarily to U.S. weaponization, some will see it as a dangerous move by a hegemon and will shift to create a counterbalance. Coalitions are likely to form, particularly in diplomatic circles, in resistance to any effort to capitalize on weaponization, and adversaries will look to field asymmetric countermeasures against those weapons. Even a U.S. policy to build space weapons to be held in reserve until needed is certain to draw fire from those who perceive little difference between a quick-reaction defensive capability and an offensive capability.

If a decision were made to put a defensive counter-imagery capability in space, the details of its deployment are as important as its technical abilities as a weapon. A number of reasons have been raised supporting the general idea of weapons in orbit.[39] The most compelling among them would give the United States the ability to

- Deter others from attacking critical information infrastructure
- Disrupt enemy use of its indigenous or commercial information sources
- Project power around the globe quickly and precisely
- Defend the United States and its allies from ballistic missile attacks

The wording alone in the first three bullets implies an offensive capability, while the last bullet looks to be more defensive. However, it is a type of defense that generated the

concerns resulting in the Anti-Ballistic Missile Treaty. The point being that even defensive measures can be seen as destabilizing.

It stands to reason that orbiting weapons could have a stabilizing effect if they only counter the existing threat, are not able to punish, and do not comprise an impenetrable national defense. Defensive countermeasures against imaging satellites can meet that standard. It is a well-established rule of international law, established in the United Nations Charter, that "peaceful purposes," key wording in the Outer Space Treaty, include the right of self-defense.[40] It may be argued weapons targeted against a specific satellite before they are launched, in response to an ongoing attack, are contributing to the peaceful use of space. In anticipation of a threat, weapons could be deployed or launched against a general type of target, such as imaging satellites, and then receive specific target information later if the U.S. declared such a satellite "hostile." The use of space stations, shuttles, or other satellites that wait in orbit for contingency tasking meets these criteria. However, their ability to go after non-belligerent satellites, if so ordered, may appear offensive and inconsistent with the peaceful use of space.

Deterrence

The U.S. currently has no credible, proportional military option that would deter commercial imagery operators from providing products to enemies. Military commanders will not use disproportionate force against an imagery provider or the country that licenses its operations. The challenge for the U.S. is to create a weapon that can be used in a counter-imagery role while meeting proportionality standards by reducing the chance of unnecessary human casualties.

Weapons that can be employed quickly have higher deterrent value than those with long deployment timelines. A satellite capable of interfering with a commercial imagery satellite does not have to be in orbit to be credible, but it loses credibility if it cannot be employed quickly, because the provider may use the deployment timeline to his benefit. The deterrent effect of a space-based system can be achieved by having systems on the ground that can be put into service rapidly. It requires an assumption of risk directly related to the time it takes to get the weapons deployed, which includes the commitment to ensure the response capabilities exist when they are needed.

Dissuading Vendors of Commercial Imagery

Foreign states are responsible for the activities of their citizens in space, and U.S. attempts to control foreign imagery will likely begin with the foreign government. Of all the options for persuading a company not to sell imagery, the use of force is a last resort. If the vendor is a United States corporation, the government can instruct it not to provide imagery.[41] For foreign companies subject to the laws of a friendly government, a diplomatic request should be sufficient, since states maintain responsibility for all objects in space. The Convention on the Registration of Objects Launched into Outer Space (1976) requires states to register their spacecraft with the United Nations. In the case where more than one country is party to the mission, it requires those countries to decide which shall register it. According to Reynolds and Merges, "the state on whose registry the object is carried retains full jurisdiction and control over the object under Article 8 of the Outer Space Treaty of 1967."[42] With such agreements in place, the use of force can then be reserved for non-cooperative states, companies, or individuals, regardless of whether the satellite system is operated by a person, government, or international consortium.

It is important to point out that an entity cannot generally be declared hostile unless it is cooperating with the belligerent. The U.S. would not be able to attack an imagery system being exploited by an enemy without the system operator's knowledge or permission.[43]
In the past the United States has used exclusive marketing agreements in and attempt prevent the enemy from getting any support.[44] This can come in especially handy when dealing with companies subject to the laws of a licensing state that is neutral or sympathetic to the enemy, and therefore unwilling to intervene on behalf of the United States. Should a more aggressive response be required, the United States will first warn the offender to desist, and if the warning failed to achieve the desired result, the next step could be a direct attack against the system. For the warning to be effective the decision maker, whether at the state or company level, must perceive an ability and willingness of the United States to follow through.

Foreign companies may be unwilling to support the decisions made by their political leaders. During Operation Desert Storm, France was a coalition member, and SPOT Image Corporation allowed imagery access to the coalition while denying it to Iraq. By contrast, in Operation Iraqi Freedom there is evidence in news reports that Russian companies were providing Iraq with jammers to counter the Global Positioning Service, even though Russia supported the United Nations sanctions against Iraq.[45] The Russians contended the vendors were not operating with government consent. The U.S. used the political instrument of power to persuade the Russians to stop the activity. Diplomacy can be most effective in denying imagery access to an adversary while maintaining it for friendly use. In those situations where diplomacy is ineffective, the field commander will need other countermeasures to deal with the enemy's imagery providers.

Many commercial systems are owned and operated by a consortium of private companies or governments, but spacecraft and ground sites are under the jurisdiction of states. The multi-national nature of some companies makes it difficult to assign responsibility for policing a company's activities. Such is not the case with spacecraft and ground stations, which are under the jurisdiction of sovereign states. It is important that multinational corporations be made aware of United States policy so they have the ability to react appropriately when approached with a demand to desist. Even if the U.S. cannot directly influence decisions by a multinational company, it can take the matter up with the state of registration bilaterally. A corporate decision maker, regardless of nationality, will be at a disadvantage for negotiating a favorable outcome if the state of registry cooperates in response to political pressure.

Business Impact and Policy

The business impacts associated with a space-control policy could have unintended consequences. Supporting the policy is the deterrent effect of fear that a company could lose its satellite for failing to cooperate, or that it could lose business from some countries that prefer not to risk service interruptions. An announcement by the U.S. of a policy to attack satellites in orbit will likely generate a response from insurance companies trying to rate the risk of attacks on satellites. This could affect not only imagery companies, but also the entire space industry if the announcement generates an overall perception of an arms race in space increasing risk to every space-system operator. It would be ironic if a policy to control the dissemination of militarily significant imagery indirectly caused unrelated businesses to go out of business because of increased costs to operate. Once again, the types of weapons and tactics can have a major impact. For example, a kinetic anti-satellite weapon that impacts the target, destroys it, and leaves space debris in its wake is more problematic than a co-orbital screen that temporarily blocks the sensors' view of earth and de-orbits after the mission ends.

The value of a clearly stated policy to permit the development of a space control strategy is that it focuses everyone's attention. Such a policy may also influence the actions of enemies against whom the strategy is to be directed. The United States, by openly stating its intent to protect its forces if they are threatened by commercial satellite systems, will keep planners and visionaries from assuming away potential military responses as Lee did in his paper. In addition, commercial satellite operators and the governments that regulate their activities will be more likely to put safeguards in place so they may choose to cooperate during hostilities rather than contemplate the loss of their system. An ambiguous policy invites the proliferation of imaging systems technically unable to respond appropriately in a crisis, and the most effective and inexpensive option for protecting U.S. interests is lost.

IV. Strategy Recommendation

> *Unless you plan your strategy and tactics far ahead, unless you implement them in terms of the weapons of tomorrow, you find yourself in the field of battle with weapons of yesterday.*
>
> --Alexander De Seversky, Air University, 28 May 1948[46]

The United States strategy for weaponizing space is best served by endeavoring to be the second to engage in warfare from space. Since the high-altitude nuclear testing of the 1960s, the world has resisted the weaponization of space in order to preserve it for peaceful uses by all mankind. Changes in the post Cold War geopolitical environment, combined with advances in technology, suggest the world's few space powers should consider anew the benefits and implications of weaponizing space to find agreement on defensive space weapons. For instance, space-based capabilities against commercial imaging threats need not be placed in orbit ahead of a demonstrated peril. The desired deterrent effects can be achieved with capable systems stored on the ground until needed. A response-based weaponization strategy requires space lift to be available in sufficient quantities and timeliness to launch the weapons necessary to counter the threat and to launch replacements for any satellites that might have been damaged by an attack. Such a strategy will require the technology and the budget priorities be made available to make it possible.[47]

Policy Statement

The United States needs a clearly stated policy so that a solid supporting strategy, and commercial coping strategies, may be developed. The current policy, described previously, is vague. It does not go into enough detail on how space superiority will be achieved when U.S. interests are threatened. American strategies and policies need not be overly specific, they simply need to support the coherent message that U.S. will take the actions necessary to protect its interests from attacks enabled by space-based commercial imagery systems. Such a policy, combined with overt research, development, test, evaluation, and deployment of space-control weapons, will provide adequate notice of national intent and will serve to motivate commercial imagery operators to consider ways to avoid confrontation.

Threats can be neutralized in a way that mitigates legal and political fall-out, if the proper weapons are available. Today's atmosphere of international scrutiny and political sensitivities is best handled in advance with a clear, systematic approach to dealing with commercial imagery operators aiding the enemy during hostilities. If the attack is conducted in response to aggression, while minimizing the chances of physical harm to equipment or

personnel and aiming to make the results reversible, the legal requirement of proportionality can be met and the political price for protecting friendly operations minimized.

Elements of a Decision to Use Force Against a Commercial Imagery Satellite

A strategy for space-control should be more detailed than the public policy and should first define the criteria under which the United States would take action against a commercial system, describing the desired post conflict end state in terms of whether the commercial imaging satellites are expected to resume operating. The decision to use force would be based on a set of criteria to ensure the attack is necessary and proportional, given the existing mix of weapons and tactics. Therefore, the strategy must address the response criteria and timeliness necessary for employing ground based countermeasures and launching space-based countermeasure. A threat-based analysis suggesting parameters for system requirements will normally generate short-term and long-term goals for capabilities. Because a situation requiring a counter-space response is a present threat that can occur at any time, defense officials should waste no time in pursuing long and short-term systems and the capacity to quickly employ them. These systems will be reliant on solid technical intelligence for their development and properly trained personnel for their employment.

A space control strategy would most likely make use of non-military instruments of power first, to lay the groundwork for cooperative denial of products to the enemy. It would use demarches to encourage non-combatant/neutral imagery providers not to aid the adversaries of the U.S. and its allies. It would also use military tactics such as operational security and deception to mitigate the usefulness of commercial images, which could reduce the need to resort to an attack. All of these steps could be taken prior to actual hostilities.

If the threatening activity could not be stopped through peaceful means, national decision makers would consider declaring the imagery provider, or its host nation, "hostile." Commanders could then consider any currently available non-destructive or reversible-effect weapon such as jammers, lasers, obscurants, or cyber weapons. If those were unavailable or ineffective, they could consider using more lethal means such as conventional munitions against terrestrial nodes, or destructive high-power directed energy against ground or space-based nodes. These weapons would only be used if the U.S. were engaged in hostilities, because the imagery provider is conducting legal trade as a non-combatant up until the time it provides products to an enemy engaged in hostilities with the United States.

If at any time friendly intelligence sources conclude U.S. forces are being targeted using such systems, commanders could use any available weapons in self-defense. It is possible that national decision makers will not make all space-control weapons available to field commanders, just as field commanders do not have access to nuclear weapons for unit self defense. These steps demonstrate the scope of options available when a clear policy has been articulated and the military-industrial complex has been permitted to establish capable weapons systems, ready to respond when national security is threatened. This paper will later discuss the types of techniques that might be most desirable for weaponization in order to achieve the goals of a stated policy.

Deployment Strategy

For a nation as great as the United States, a more realpolitik approach might be to prepare for combat in space, but to leave the capabilities earth-bound until they are needed. The effects of space weapons can be achieved by having the necessary space lift and weapons available for rapid response to a developing threat. By waiting for another country to be the

first to weaponize space, the United States could avoid the political fallout of being the first to do so while garnering international support for defenses against the interloper.

The long-term value of a second-to-weaponize approach is that it enhances America's "soft power." Harvard Dean Joseph Nye says soft power "arises from the attractiveness of the country's culture, political ideals, and policies. When U.S. policies appear legitimate in the eyes of others, American soft power is enhanced. Hard power will always remain crucial in a world of nation-states guarding their independence, but soft power will become increasingly important in dealing with the transnational issues that require multilateral cooperation for the resolution."[48] Soft power is helpful in getting cooperation from the international community in the fight against terrorism and other trans-national threats. American interests are better served when the U.S. protects its interests in space, without being regarded internationally as a menace whose power must be counterbalanced.

While space-based weapons are held in reserve, surface and airborne countermeasures can be deployed as the first-echelon defense. Once an imagery system is identified as a target, surface and airborne countermeasures such as jammers and lasers can be used to defend against it. If those systems are unable to counter the threat, commanders can decide whether to move to lethal force, such as conventional precision-guided munitions, or destructive directed energy against the ground-site with precision-guided high-power microwave munitions. If commanders need a temporary effect, they may then look to launching space-based defensive systems such as co-orbital jammers to go against terrestrial and space nodes, or on-orbit disabling techniques such as micro-satellite delivered mechanical devices or a screen that obscures the imagery satellite's view of the earth. This option requires readily available space lift to be a tenable option.

If the United State pursues a responsive second-to-weaponize strategy, it needs to dedicate the resources to launch capacity, weapon systems, and infrastructure replacements. It appears the Defense Department needs to determine a requirement for space-lift surge capacity, in terms of launch rate by class, if this strategy is to be credible. The Air Force Research Laboratory recently addressed the advantages of on-demand surge capacity saying:

> If we could quickly launch platforms that provide joint force commanders with whatever space assets are required, then we could strategically respond to situations in ways that eliminate the need for ultrahigh-resolution worldwide intelligence, surveillance, and reconnaissance assets in predictable orbits. We want to arm our joint force commanders with the ability to respond rapidly in any given situation by supplying space assets in near real time. We can accomplish this by launching or moving space platforms or weapons to wherever they are required within several hours.[49]

This statement clearly shows how responsive, on-demand launches will improve warfighting capability. It supports the 1994 *SPACECAST 2020* study recommending development of a standardized, reusable launch vehicle to reduce cost of launches. The requirement to develop surge capacity was more implied than stated in the study, which put the typical timeline for vehicle integration and checkout at sixteen weeks and quoted a cost to commercial users of $50 million per launch.[50] Sixteen weeks will not be an acceptable timeline to joint force commanders, and the number of launches required remains undefined.

A recent study funded by the National Aeronautics and Space Administration (NASA) addresses the future need for launches and indicates almost no growth in demand for launches over the next twenty years. Counting government and commercial launches worldwide, "aggregate global launch vehicle demand remains relatively flat at between about 70 and 80 launches a year….The forecast also indicates a gradual switch from medium to intermediate

class launches and a steady increase of commercial market share from a quarter to half of launches, and the continued erosion of U.S. market share of all launches from the 40 percent down to the 25 percent level."[51] A major flaw in this study is its failure to indicate a requirement for a surge capacity during war, even though the study claims to be comprehensive in its accounting for Defense Department launch requirements.

Surge capacity estimates for commercial and Defense Department launches should anticipate critical space-based infrastructure replacement, not just wartime weapon launches. The problem of replacing critical information infrastructure damaged by an attack could be lift-intensive, especially in heavy-class launches. Replacement systems, if available, would have to be mated to system-compatible lift. While new space-based systems may be designed to meet constrained lift specifications, many satellites currently in orbit used large, customized lift that could overwhelm the availability of the Evolved Expendable Launch Vehicle—heavy lift vehicles projected in the NASA study at twenty per year.[52] The challenge comes in making surge capacity a priority for available funding, especially when launches currently cost about $190 million each.[53]

A strategy of being second to weaponize space allows the United States to be one of the governments negotiating to keep other states' weapons out of space. National leadership must decide whether the terrestrial responses are sufficient against current and foreseen threats. A ballistic missile attack against the homeland may be so dangerous that space weaponization will occur to counter that threat, despite the political cost of breaking the weaponization threshold. President Bush's decision to withdraw from the Anti-Ballistic Missile Treaty does not necessarily mean the U.S. will deploy a space-based system. It could instead end up deploying surface or airborne systems, or nothing at all. If a space-based anti-ballistic missile system is deployed, that deployment will probably clear the path for defensive space weapons against imagery satellites as well.

The United States should prepare now for an uncertain future by adopting the second-to-weaponize strategy. By keeping weapons on the ground until needed, the nation can continue to reap the benefits of space used for peaceful purposes. It can simultaneously pursue technological innovations, modernize and maintain the space-weapons inventory, and build sufficient launch vehicles for use in space combat. This approach creates deterrent effects without weaponizing space. If the U.S. does not take the opportunity to prepare now, it will still be able to fight, but victory will come more slowly and at higher cost.[54]

V. Countermeasures

> *A key objective for transformation, therefore, is not only to capitalize on the manifold advantages that space offers the United States but also to close off U.S. space vulnerabilities that might otherwise provoke new forms of competition. U.S. forces must ensure space control and thereby guarantee U.S. freedom of action in space in time of conflict.*
>
> --Military Transformation: A Strategic Approach, 2003[55]

When the U.S. needs to stop the flow of commercial imagery to adversaries, it is more effective to ask the system operator to suspend service than to forcibly prevent the service from being delivered. Companies providing imagery services are logically in the best position to install effective controls on their own collection and dissemination systems to interrupt subscribers' ability to receive products. However, the United States must be prepared for situations where the company has either inadequate controls or does not desire to

control product availability. Since attacking a system in any effective way would likely restrict the flow of imagery to all customers, companies may be motivated to provide their own high-grade security to protect their technology investment and their customer base. For example, *SPOT* and *Landsat* imaging satellites cost roughly $350 million each to build and launch.[56] During Operation Desert Storm, *SPOT* demonstrated the ability to deny products to Iraq while permitting other customers to receive them. That is a much better solution financially, compared to having the system forcibly shut down. This is not to say the U.S. would attack a commercial imagery provider just because it was unable to stop unauthorized reception, but it might go after nodes owned or controlled by hostile entities, which might affect the operator's on-site equipment, or service to other customers. Companies in business to make money are likely to have controls to protect their property rights from unauthorized exploitation. If nothing else, they will adhere to state's licensing requirements, which may or may not require the company to deny imagery to enemies. In either case, the U.S. should be interested in the specific techniques the companies use to prevent unauthorized exploitation to ensure they are effective.

Cooperative Measures

Foreign governments and multinational corporations should be encouraged to voluntarily abide by a minimum data-denial standard. Companies should be warned that their data is militarily valuable, and a determined adversary may exploit it, resulting in loss of economic opportunity for the company, and a security risk to others. Once a satisfactory standard is developed, foreign companies will know whether their systems are technically capable of denying new imagery to unauthorized recipients. Foreign cooperation is a more efficient countermeasure for the U.S. and provides a measure of protection to companies that participate. In the event a company is unwilling or unable to take steps deny the data, the U.S. may have to use more forceful methods to prevent the enemy from obtaining imagery.

Government encryption is one obvious method for denying data to unauthorized recipients, but commercial providers are reluctant to use it. In 2001 the U.S. government made encryption mandatory for some U.S. operators. The *National Information Assurance Policy for U.S. Space Systems, National Security Telecommunications and Information Systems Security Policy Number 12* requires American companies to use National Security Agency-approved cryptography on commercial imaging satellites that might be used for national security requirements. Its goal is to ensure these capabilities are designed into future systems.[57] A U.S. Senate report the following year quoted industry officials who expressed deep concerns with establishing encryption requirements because of the complexity of managing cryptographic materials, particularly overseas. Additionally, they said encryption does not provide much greater security than other techniques that protect data links.[58] The specific techniques were not mentioned, but it is possible that they include commercial encryption or proprietary coding. Without a detailed technical review, defense officials are not likely to accept claims that techniques not involving government encryption are good enough to deny data access to an adversary—especially those who were once legitimate customers, or licensees, with direct-receive equipment and software.

Passive and Active Countermeasures

Passive countermeasures are actions taken to minimize the effectiveness of the system without taking the initiative against the targeted system.[59] Passive countermeasures are useful not only during hostilities but throughout the range of military operations, including pre- and post-conflict phases. Operations security, one of the elements of today's integrated

warfighting strategy, is an example. The goal is to "select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation."[60] The ability to deny an adversary information for his operations requires some knowledge about how he gets that information. Intelligence support is essential for determining the degree to which friendly forces are vulnerable to space surveillance. Similarly, when the operations can be disguised by denial or deception so that the enemy is unable to use the imagery intelligence in a timely manner, then the commander is not at risk, and he may be able to avoid active countermeasures like attacking or jamming the systems.

When commanders in the field foresee a need for active countermeasures, and few are available, a key task will be to determine what capabilities are needed and which techniques have the most promise for development. If voluntary cooperation and passive countermeasures are ineffective, commanders today have little ability to act directly against hostile commercial imaging systems, except to attack the ground sites. Value analysis is a technique by which a variety of other countermeasure techniques can be compared objectively, based on how they contribute to set criteria. Changing the criteria or the assumptions will change the overall ranking of compared countermeasure techniques. In the appendices of this paper, readers will find sufficient detail on how the criteria were selected, valuations defined, and overall scores calculated, so the results can be changed to meet new entering assumptions. When it comes to future requirements for countermeasures systems, the objective is not to determine what can be done, but what should be done. These analyses can push research and development in a direction to satisfy the most reasonable requirements.

The list of countermeasure techniques selected for evaluation (see Table 1) was derived from techniques discussed by Major William Spacy in his 1999 paper on space-based weapons.[61] It is important to differentiate between weapons and techniques. Techniques are ideal applications, unconstrained by the fact that the technology may not be available or efficient. Weapons, on the other hand, are systems capable of employing the techniques. Weapons are equipment that have actual mass, interfaces, and must be used within operating limits. The listed techniques are intended to be theoretical and are not concerned with the challenges of how they can be weaponized. A weakness of this evaluation is that techniques other than those listed were not considered. However, alternative techniques can be evaluated using the comparison tables in appendix C. Figure 2 shows nodes common to all commercial imaging systems.

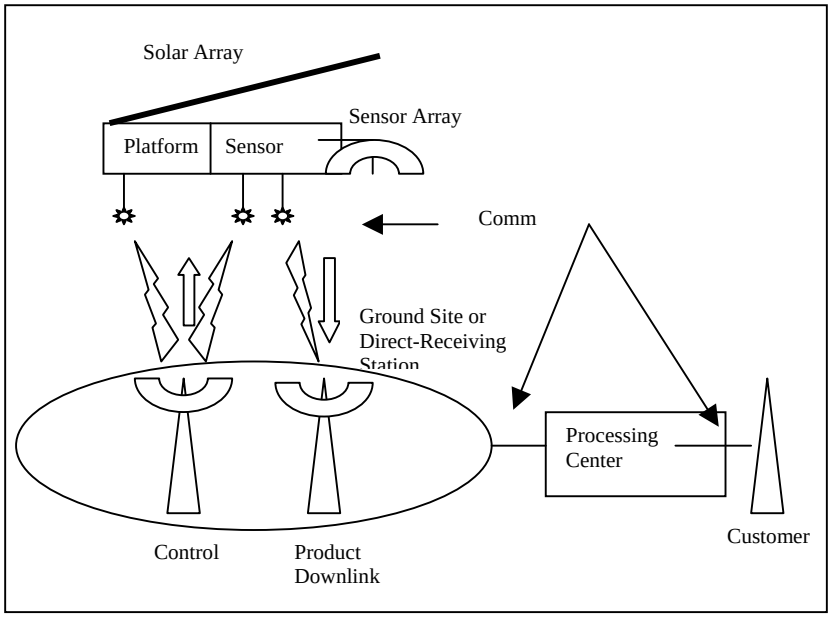

Figure 2. Simple Depiction Of Nodes Common To Commercial Imaging Systems

The countermeasure techniques were evaluated on their ability to impact the previously identified nodes with the following desired effects:

- End state—the potential to return the system to its pre-attack condition
- Sustainability—of effects over the duration of hostilities
- Vulnerability—of the weapon, or it effects, to negation by the enemy
- Covert—whether the weapon must be covert to be effective
- Target accessibility—likelihood the technique can access the targeted node
- Collateral damage
- Space debris—caused by effects of the technique
- Political will—to employ the technique as a weapon

The definitions and the weighting of each of the effects are listed in appendix B. Each evaluated technique received a standardized score for each node of a typical imagery system. Definitions of the techniques and the examples are in appendix B.

Technique	***Example***
Conventional Attack	Precision Guided Munitions
Kinetic Destruction	Anti-satellite missile Space Mines
Disabling electronic attack	Radio-frequency jamming Low-power laser dazzling
On-orbit disabling	Micro-mechanical robots Micro-satellite options
Cyber attack	Sensor commands Image Alterations
Destructive directed energy	High-power microwave High-power laser Particle beams

Table 1. Countermeasure Techniques

Technique-Node Scoring

Table 2 shows a summary of the standardized scores by node. It is useful in drawing general conclusions about the best technique-node pair for achieving most of the desired effects, but the expanded scoring table in appendix C is more detailed and can give greater depth to understanding a particular technique for weaponization. Blanks in the table indicate the technique-node pair is not applicable. A critical contextual assumption in this scoring is that the conflict is open, not covert. The scoring and the standards change considerably if the commander wants to deny not only the use of the imagery, but also the fact that an operation is occurring or that a countermeasure is being employed. Covert countermeasures may be used in overt operations, but overt countermeasures may expose a covert operation.

	Space Platform	*Sensor Optics*	*Command uplinks*	*Ground Receive stations*	*Ground processing stations*	*Terrestrial Communi-cations*
Conventional attack				27	17	23
Kinetic satellite destruction	12	10	12			
Destructive directed energy	22	20	23	28	18	27
Disabling electronic attack		28	32	34		24
On-orbit disabling	29	28	28			
Cyber attack			21	23	16	22

Table 2. Technique Score Summary

The summary table points to two techniques, disabling electronic attack and on-orbit disabling, as potentially the most lucrative areas for further analysis since they have consistently high scores across several nodes. The score in each cell of the table is the sum of the effect-scores for each node, detailed in appendix C. The highest scoring pair, disabling electronic attack against the adversary's ground receive station, received a sum of 34, but the specific weapon indicated in this case would be an orbiting jammer in close proximity to the imagery satellite. It has outstanding promise for meeting the eight effects considered, but the political-will score for a jammer on stand-by orbit is probably zero, which in the value analysis is a multiplier against the overall score. If the political will is zero, the technique will not likely be supported for weaponization. The political-will score could become a one, if the jammer is kept on the ground, and is only launched in response to a specific action by an enemy. The table shows a sum of 34, as at this point political will is not prejudged. The purpose of the analysis is to determine effectiveness; acceptability will be determined later.

Description of Selected Techniques

The techniques are described in appendix B in sufficient detail to permit the value analysis. The scores in Table 2 identified disabling electronic attack and on-orbit disabling for more detailed consideration. Destructive directed-energy scored well against ground sites but not against other nodes. The weaponization envisioned in that case was a conventional precision-guided munition containing a high-power microwave warhead. As the application was more limited than the other two techniques, it was not selected for further analysis here.

Disabling Electronic Attack

According to doctrine, electronic attack is "employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams)."[62] Electronic attacks powerful enough to cause physical damage to the target were categorized as *destructive* directed-energy weapons, while those intended to have a temporary or transient effect are *disabling*, but not necessarily destructive.

Jamming may be conducted is several ways. As mentioned above, jamming a ground site from co-orbit with the satellite scored the highest of all countermeasure techniques, providing it can be made politically acceptable. Another method, low-power co-orbital jamming of the sensor's command-and-control receiver aboard the satellite, is assessed to be effective. While it would be space-based, it may be more politically acceptable when targeted against a specific satellite, since it is low power, defensive, does not attack a ground site from space, does not threaten the environment, does not generate a feeling of military invulnerability, and can be designed to prevent collateral damage to other orbiting systems.

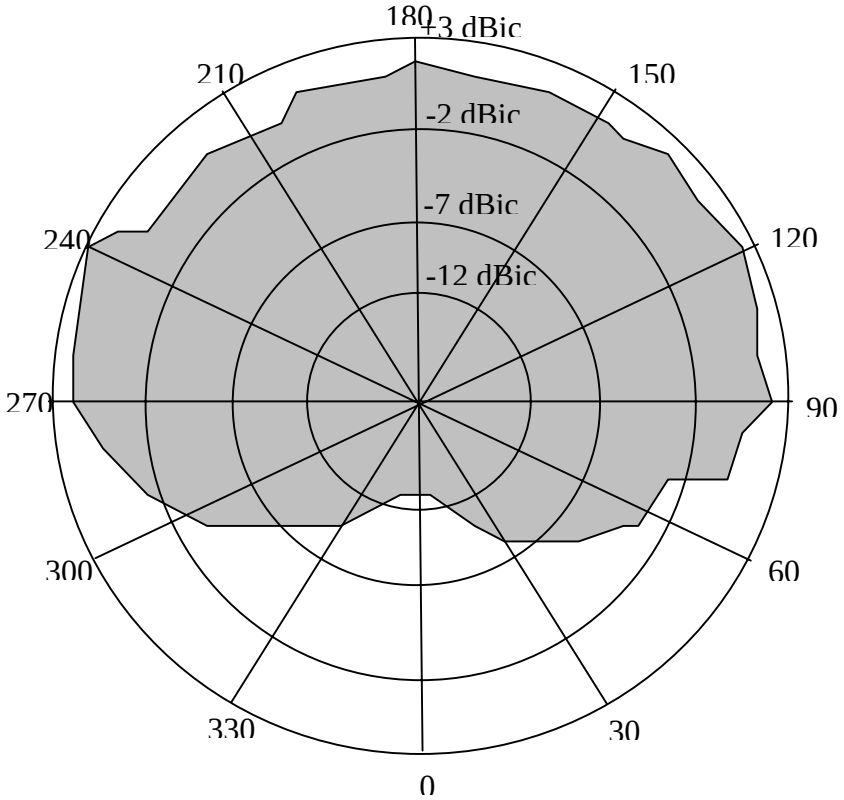

Figure 3. WorldView Satellite Receive Antenna Pattern (402MHz)[63]

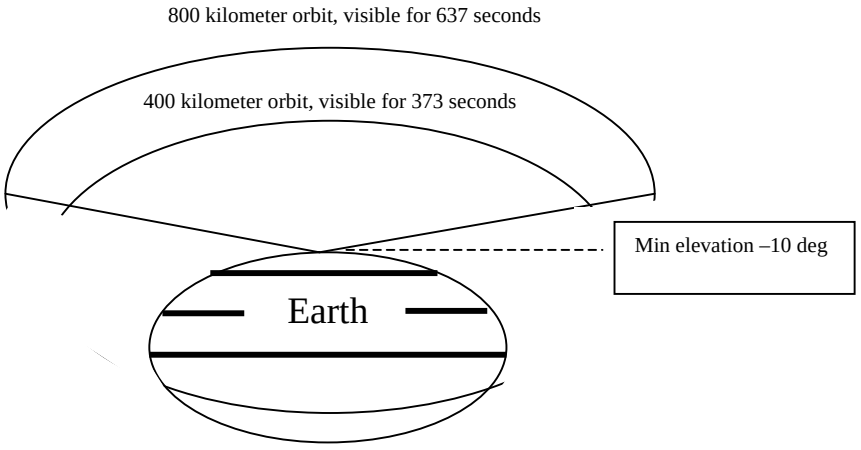

Figure 4. Ground Station Visibility [64]

A look at the design of a typical imagery system shows why co-orbital jammers are better than terrestrially-based jammers. Government information obtained from the Joint Spectrum Center indicates the large, six to twelve meter antennae used for downlink reception on the ground, have highly directional beam patterns for receiving signals. In order to jam the ground-station's receiver, a jammer on the surface of the earth would have to be very close to the receive-antenna boresight with enough power to exceed the gain of the satellite's signal. At any appreciable distance from the ground site, the task is nearly impossible. At ranges close enough to make this technique effective, a weapon such as an expendable jammer near a ground site risks detection and negation by the adversary.

The antennae features that make jamming ground sites so difficult are not duplicated aboard spacecraft. The receive antennae on satellites are isotropic, making them much easier to jam from the ground or from space (Figure 3). Co-orbital jammers need far less power than ground-based jammers, which means the jamming might be difficult for the commercial system operator to detect, recognize, and troubleshoot. The receive antenna on satellites are designed this way to allow ground sites to maintain contact with a satellite as it transitions from horizon to horizon. It is this design that makes the satellite receivers more vulnerable than ground sites to jamming. The shaded area in Figure 3 shows the direction of the receive-antenna sensitivity, in this case a high-gain sensitivity from 90 to 270 degrees, which more than covers the portion of the earth's surface in view from orbit. Land, sea, and air-based jammers can exploit that design. The area of the figure from 270 back to 90 degrees is the backside of the antennae, facing away from the earth. There is no need for it to be sensitive in that direction, so space-based jammers that are behind the satellite will need a stronger signal to get into the receiver from that direction, as indicated by the –12 decibel ring.

The disadvantage of sea- and land-based jammers is that while they can jam the satellite receivers within line-of-sight, they may not be able to get close enough to the ground site to prevent the satellite from having some effective line-of-sight time. Airborne jammers can substantially increase the area of coverage, but depending on geopolitical borders, the rules of engagement, the ability of an aircraft to be on-station for each pass of the satellite, and the enemy's defenses, this airborne weaponization may also be inadequate as a sole attack method. The best solution for keeping jamming on the targeted system, while permitting access by friendly ground stations and not hostile ones, is to have the jammer in co-orbit with the satellite. Low-power space-based radio frequency jammers can be built so they are difficult to detect and locate, yet produce effects that are verifiable by friendly intelligence systems. These characteristics complicate the enemy's ability to respond while providing a level of battle damage assessment. While space-based jammers earned the highest score for effectiveness, ground-based point defense using lasers against the sensor scored almost as high. Ground-, air-, or sea-based lasers can be used to prevent an area from being imaged during hostilities. A laser located in proximity to the friendly activity to be protected can saturate the receiver(s) so no clear image can be discerned. By knowing the orbit of the satellite, a laser can be aimed directly at it. The "blooming" of the image will last only as long as the sensor is looking in the direction of the properly tuned laser. The satellite operator might then choose to redirect the sensor to collect usable data of other areas, limiting the effects of this particular technique. Disadvantages of this weapon are that its use is highly detectable, it requires precise aiming throughout the visible window, and the laser power and frequency must be highly accurate. A laser that is too powerful may cause undesired permanent damage to the sensor, while one that is too weak or not properly tuned might not be effective.

Temporary disabling of satellites by lasers can be a technically challenging problem. Separate lasers may be necessary to handle multiple bands of multi-spectral sensors. Earth imaging satellites often carry more than one sensor, each designed for a specific purpose, and

each using different sensing materials and covering different frequency ranges. For example, *Landsat-D* has a thematic mapper in addition to its multi-spectral scanner. The thematic mapper uses seven spectral bands—the first four cover portions of the visible light range using silicon photodiodes. Sixteen indium-antimonide sensors serve bands from 1.55 to 1.75, and 2.08 to 2.35 micrometers, and four mercury-cadmium- telluride detectors are added for the 10.4 to 12.5 micrometer band.[65] *Landsat-7*, the most advanced of the Landsat series, launched in 1999, is even more diverse.[66] The difficulty in simultaneously jamming all the applicable sensors on the same satellite is difficult enough, but to ensure that the laser targeted against one sensor type does not permanently damage an adjacent sensor of different construction will require in-depth system analysis. According to Anderberg and Wolbarsht, "If the wavelength is one which the sensor system is designed to accept, the laser energy will be transmitted through the system itself, destroying or jamming vulnerable detectors. Sensors are normally designed to handle very small amounts of radiation and cannot accept the high intensities of radiation achieved by even very-low-energy lasers."[67] They go on to say dye lasers can be narrowly tuned within the visible to near-infrared part of the spectrum. Each dye is limited to about 50 to 100 nanometers. "For example, one dye may allow tuning of the laser within the orange part of the spectrum, but obtaining a wavelength in another part of the spectrum requires changing the dye."[68] They describe a technique called "Raman shifting" that marginally changes the wavelength of lasers by adding energy to the pump. The capabilities of targeted imagery systems are important when trying to design capabilities that are effective, while economizing on weight, space, and the number of lasers to make the techniques feasible as effective weapons. An imagery system carrying electro-optical, multi-spectral, and radar sensors would require an even more sophisticated ground based system for point defense. The Russian *Resurs-021* earth-imaging system uses an active radar sensor in addition multi-spectral bands.[69] An array of both low-power lasers and radar jammers might be necessary to adequately protect against this system.

On-orbit Disabling

New technologies promise to provide capabilities not even possible with manned spaceflight. For example, microsatellites are expected to permit close inspection of low-earth orbiting satellites, while making on-the-spot corrections for execution problems. Dr. Donald C. Daniel, Deputy Assistant Secretary of the Air Force, testified before Congress that current research and development programs will "provide the technology base for 10-100 kilogram microsatellites that will offer new options in many areas of space applications. Applications previously considered not cost-effective due to size and weight limitations, such as satellite servicing or launch on demand, become possible."[70] The transition from satellite servicing to satellite attack does not appear to be much of a stretch. Attacks might be carried out by remote robotics, including micro-mechanical robots. Radio controlled relays incorporated into an attack could be used to command re-connection of interrupted circuits, permitting a system to be returned to service without making a second rendezvous for the subsequent repair. A disadvantage with this approach is that any physical contact with the satellite could cause irrecoverable damage.

An associated technique would be to erect a screen designed to permit the satellite operator to keep the platform operating properly, while blocking the desired sensor(s), effectively putting a lens cap on it. This would avoid the hazards of actual contact with the satellite, the risks associated with blocking vital communication, and risks associated with unintended laser damage to the sensor. A disadvantage of this application is similar to sensor lasing, in that eclipsing the sensor denies the product to all subscribers for the duration of the

attack, not just to the adversary. A clear advantage is the potential for the effects to be completely reversible once the crisis subsides.

Required Development

The scores shown in the tables assumed 100 percent effectiveness, without compensation for physical or technical limitations imposed by actual weaponization of the techniques. Weapon development supported by detailed intelligence will be necessary for some of the techniques to achieve the results suggested in this analysis. For example, intelligence may suggest a command-and-control uplink can be successfully jammed, but the satellite will still image the territory and downlink image to the ground, based on previous instructions. This would be different from *SPOT*, where the downlink is commanded from the ground.[71] Detailed intelligence on the actual target is required to know the full effect of the techniques.

As the foregoing suggests, different techniques will require unequal levels of effort to be used as weapons. Jammers have been weaponized for self-protection on small fighter aircraft, and subsequently need only be adapted to weaponization against commercial imagery nodes. Others, such as laser weapons, need further development if they are to be deployed aboard aircraft for access and aspect-angle advantages in point defense. Finally, some concepts require new discoveries in the basic sciences. Micro-mechanical robots may have a role when employed using microsatellites, but will need sufficient power-supplies, sensors, processors, mobility, and task-adaptable actuators for autonomous operation on satellites in space. Other systems, such as neutral particle beam weapons, are currently large, weigh hundreds of tons, and suffer from considerable atmospheric attenuation.[72]

VI. Strategy to Task Ends, Ways, and Means

> *Where the strategist is empowered to seek a military decision, his responsibility is to seek it under the most advantageous circumstances in order to produce the most profitable result. Hence his true aim is not so much to seek battle as to seek a strategic situation so advantageous that if it does not of itself produce the decision, its continuation by battle is sure to achieve this.*
>
> --B.H. Liddell Hart [73]

While countermeasure policy, strategy, and techniques have been the focus of this paper, it is helpful to step back and examine how commercial imagery countermeasures can be a part of broader U.S. space power. This section considers the role of strategy, policy, and acquisition funding to enhance U.S. space power.

For the United States to be successful in its ability to counter its enemies in space, it must maintain its space power through international engagement. The interrelationship between the government, industry, and the military is inseparable in attaining, using, and keeping space power. American space objectives may be in conflict with other countries, or the international community as a whole, and while “space power” implies a focus on military advantage, it goes beyond the desire for military prowess. American military, diplomatic, information, and economic power are interdependent instruments for achieving the wide range of goals described in the *National Security Strategy*, including opportunities for economic growth. A good policy on space control would be more than a blueprint for future development, it would provide guidelines to practitioners, strategists, politicians, and the public as they debate the future of space power, and consider precedent-setting decisions in the international community that can either support or stifle freedom of action.

International Negotiation

The U.S. should never lose sight of the ability of the international community to collectively weaken American military options indirectly. Responding to the suggestion that the U.S. is the only world superpower, Joseph Nye writes, "On interstate economic issues, the distribution of power is already multipolar. United States cannot obtain outcomes it wants on trade, antitrust, or financial regulation issues without the agreement of European Union, Japan, and others."[74] Accepting his position, and the position that military power is a tool of last resort for achieving objectives, the obvious conclusion is non-military space power—that which comes from humanitarian, economic, scientific, and other nonmilitary prominence—must be maintained through leadership in the international community. While America moves ahead to use space for military operations, it must not jeopardize its broader interests abroad by trying to do so without a level of international acquiescence.

According to a paper by Hamilton DeSausser, the United States took the lead in civilianizing space for commerce by passing the Land Remote Sensing Commercialization Act of 1984, and in so doing set an international precedent for commercial imagery systems. Describing the years that followed the launch of the first American imaging satellite in 1960, DeSausser says the United Nations Conference on Peaceful Uses of Outer Space considered claims by Argentina, Brazil, and other Latin American countries that imaging systems violate national sovereignty and property rights. After years of debate, the General Assembly, in 1987, approved a weak resolution related to remote imaging from space. DeSausser described the result, "Since none of the multilateral space treaties cover remote sensing as a distinct regime, it is left to the practice of states to define the law in this area. The U.N. Resolution on Remote Sensing is simply too weak. Even if it were not, one state after another has declared that U.N. resolutions do not constitute binding obligations upon states."[75] According to Reynolds and Merges, the resulting resolution was decided by the existence of America's precedent-setting law on the subject. Since then, the French and others have capitalized on the permissive rules made possible by U.S. leadership. A history such as that demonstrates nicely the advantage of international engagement and negotiation in building and preserving U.S. leadership in space.

Just as clear is the benefit of carefully crafted bilateral agreements. Every aspect of the international space business, including launch facilities, boosters, payloads, communications bandwidth, liability insurance, and more, contains examples of government support leading to international bickering over trade practices. In a 1990 case cited by Reynolds and Merges, Arianespace accused the Chinese of agreeing to an Arabsat launch for $25 million, half the price of American and European competitors. Because approximately sixty percent of the payload was built in the United States, Arianespace asked the U.S. to disallow the export license. In the end, Arabsat canceled its contract with the Chinese and signed with Arianespace for the launch.[76] Reynolds and Merges could not prove America's licensing power led to Arabsat's decision, but the Chinese defended their practices saying they had not violated the 1974 Trade Act signed with U.S., while asserting the agreement they signed was unfair. "China is a sovereign country. There should not be any limits imposed by outside governments like this. For a sovereign nation, this is not a good thing"[77]

The key lesson from these example cases is that the United States can and must continue to accrue space power through multinational organizations and bilateral agreements but must also exercise space power. Lost opportunities in international diplomacy lead to lost power in a real sense. Newcomers to space can find the environment hostile if the government has been ineffective in creating favorable conditions. Industry leadership in the development and use of space technology provides the opportunity for government to create policies that become the precedent for international law. Similarly, the careful crafting of bilateral

agreements, and the aggressive enforcement of their elements, can produce advantages for the space industry. Favorable international agreements will permit the U.S. more latitude in dealing with commercial imagery threats, while hedging against foreign companies resorting to political retaliation when the U.S. demands they limit imagery distribution. When government is successful in producing a favorable environment, it is important that industry be ready to exploit the resulting opportunities. This is the advantage of a national space control policy that paves the way for an effective control of space-based imagery systems.

Military Strategy in Space

In accordance with doctrine "the employment of American military power adheres to constitutional and other legal imperatives, the highest societal values, and the concepts of proportionality, decisiveness, and accountability to the American people." That doctrine is directive as well as descriptive. The Defense Department must develop technical weapons that minimize damage to existing infrastructure.[78] Shortfalls in that ability need to be identified, and considered by the combatant commanders for appropriate action within the Joint Strategic Planning System. According to joint doctrine, "Senior US military leaders are responsible for providing advice …. to the President and the Congress on military aspects of national security including the development of forces, implications of the use of force, and integration of military planning and actions with the other instruments of national power."[79]

The value of a clearly stated policy is that it focuses the efforts of planners on both sides of a potential conflict, but it can also have consequences. The United States, by openly stating its intent to protect its forces if threatened by hostile commercial satellite systems, will keep planners and visionaries from assuming away their military responsibilities. Commercial satellite operators, and the governments that regulate their activities, will be more likely to put safeguards in place so they may choose to cooperate during hostilities rather than contemplate sanctions that could include the destruction of the system. An ambiguous policy invites the proliferation of commercial systems technically unable to respond appropriately in a crisis. Potential adversaries are likely to react on two levels. First, they will look for sources of imagery that are less likely to be interrupted, i.e. commercial systems controlled by their allies, commercial systems that cannot control who receives their data, and developing indigenous capability. The second reaction may be to follow the U.S. lead and threaten to target any system providing imagery to the U.S.

While detractors might see either reaction as the genesis of a new arms race in space, the enemies of the United States are already preparing to negate U.S. space power. The Hong Kong newspaper, *Sing Tao Jih Pao*, indicates the arms race in space is already underway:

> According to the well-informed sources, to ensure winning in a future high-tech war, China's military has been quietly working hard to develop asymmetrical combat capability so that it will become capable of completely paralyzing the enemy's fighting system when necessary by 'attacking selected vital points' in the enemy's key areas. The development of the reliable anti-satellite 'parasitic satellite' is an important part of the efforts in this regard.[80]

Strategy must stay ahead of system development, or the weapon capability may be traded away during normal budget challenges to the programs. The political sensitivity of space warfare makes a public strategy debate difficult enough to undertake, but when the requisite technologies are not yet ready for weaponization, it becomes easy to trade controversial capabilities for cost savings unless there is a strategy in place that demands specific

capabilities. By establishing requirements early in the technology development phase, a coherent development effort can be achieved.

The two shortfalls most likely to make the proposed "second-to-weaponize" strategy untenable are failing to commit to weapon development and failing to provide surge capacity for space lift sufficient to handle competing launch priorities during a crisis. Air Force Space Command's *Strategic Master Plan for Fiscal Year 2004 and Beyond* explains how the organization will focus on transitioning from older Atlas, Delta, and Titan lift vehicles to the Evolved Expendable Launch Vehicle to provide routine, responsive launch capability.[81] However, it appears the strategy focuses on reduced cost for lift rather than developing surge capacity. While capitalization analysis is beyond the scope of this paper, the cost for surge capacity would likely be in the tens of billions of dollars and take ten years to complete, depending on anticipated requirements and program decisions.

Policy

The United States' overt policy on space superiority does not tell adversaries how superiority will be achieved when U.S. interests are threatened. Policy documents, such as the President's 2002 *National Security Strategy*, the President's *National Strategy for Homeland Defense*, and the Defense Department's *Transformation Strategy*, explicitly call for protection of American infrastructure and assets in outer space but are less clear on the requirement to defend American interests from foreign space-based threats. The policy needs to affirm the U.S. will protect itself from surveillance systems supporting hostile forces, whether hosted on government or private platforms. Such a policy combined with overt research, development, test, evaluation, and deployment of space-control weapons will provide adequate notice of intent, and serve to encourage system operators worldwide to consider their own control measures in current and future systems.

Counter-imagery weapons programs must be openly acknowledged. While the details are often cloaked in secrecy, there is no advantage hiding the programs if doing so widens the credibility gap and reduces the deterrent effect. Based on this research, the Defense Department should advocate unclassified intra-governmental guidance with this message:

> Given: Commercial imagery satellites pose a potential threat to national security. It is the goal of the United States to prevent our adversaries from getting unfettered access to commercial imagery when such access puts national security interests at risk. The United States Government will work to ensure U.S. and foreign commercial imagery providers have the ability to deny their data to unauthorized recipients. The Department of Defense will field systems to forcibly prevent the nation's enemies from receiving commercial imagery products.
>
> System Requirements: The United States will use ground-based and space-based systems to prevent the flow of unauthorized imagery products and data. The systems will be designed for effectiveness and efficiency so as to minimize the impact on the international community, the environment, and the commercial imagery provider.
>
> Current Recommendations: While the following systems are recommended for development, this list is not intended to curtail current efforts or impede innovation.
>
> 1. Space-lift capacity is needed to respond to a crisis whereby attacked systems can be rapidly replaced, and space-based weapons can be launched. The goal is to minimize negative impacts on economic and military activities while responding to hostile actions.

2. Countermeasure systems should be built for launched into orbit locations when necessary to interrupt the flow of imagery. Specifically, look at low-power co-orbital jammers and co-orbital systems capable of applying physical effects.
3. Mobile low-power lasers and jamming systems are needed to deny commercial imagery sensors a usable source of electro-optical, infrared, multi-spectral, and radar imagery.

Acquisition Funding

Some of the most effective technical countermeasures against commercial imaging satellites, such as co-orbital jammers, are not currently available. In the meantime, surface and air-based weapons can be developed. When political support for space-based weapons is achieved, those high-scoring systems should become a high-priority for consideration. According to a Rand study, decision makers are most likely to pursue funding for space-based weapons to:[82]

- respond to a threat posed by an adversary who is undeterred by other capabilities
- respond in kind to another nation's acquisition of space weapons
- forestall, control, or influence another nation's independent acquisition of space weapons
- demonstrate global leadership, protect U.S. and allied economic investments, and improve the efficiency and effectiveness of military capability unilaterally in the absence of a compelling threat

Interestingly, the fiscal year 2004 budget requested nearly $3 billion for classified and unclassified programs to conduct strategic war fighting from space, and more than $30 billion through 2009. The money is allocated for ground-based systems for disabling satellites, microsatellites able to rendezvous with other satellites, directed energy weapons, and keeping the cancelled space-based laser program on life support ($50 million).[83] Space-control advocates should be encouraged by this effort, but the budget is not detailed enough to glean whether any of those systems are capable of countering the commercial imagery threat.

Conclusion

The study conclusions, if accepted, provide foundational arguments for future decisions on developing systems to counter commercial imagery systems. Commercial imagery satellites pose a distinct threat to U.S. interests, but unfortunately this research did not uncover a single technical countermeasure capable of meeting all potential scenarios. It did identify three countermeasure techniques—co-orbital jamming, on-orbit disabling, and low-power lasers from surface and air—as the best candidates for research, development, and fielding. International law requires careful consideration, as it specifically prohibits only a few types of weapons in orbit around the earth. However, the international community is likely to resist almost any U.S. space weaponization. It is possible the U.S. can reduce military risk and international concerns by developing space weapons and keeping them on the ground until needed, provided space lift is plentiful and rapid. Most importantly, U.S. policy documents need to plainly state U.S. intent to defend against space-based threats, thereby encouraging commercial imagery providers to develop the means to deny new imagery to adversaries. Such a policy statement would guide strategists, research scientists, industry, diplomats, and negotiators responsible for maintaining U.S. interests and developing U.S. advantages in space power.

Appendix A

Sample of Earth Imaging Systems

The following table contains a subset of the earth-imaging satellite constellation. Analytical Graphics, Inc. web-based Spacecraft Digest contains 2303 records, 214 of which are classified as Earth-imaging entries. *Jane's Space Directory*, 18th ed., contained fewer systems, but previous editions are required to build a composite picture. DMS Market Intelligence's "Space Systems Forecasts" report on imagery systems at irregular intervals, and provide technical data on many systems. Issued reports are kept in a three-ring binder at the Air University Library reference desk. Analytic Graphic's website, http://www.stk.com, was particularly useful as a single source of up-to-date technical data on a wide range of systems. Facts were derived from multiple unclassified sources. When sources disagreed, the most capable assessment was used. It is presented for rough capability overview only.

Definitions[84]

Electro-optical: Sensors that input energy from visible-light portion of the electromagnetic spectrum into electronics. A digital sensor.

Hyperspectral: Measures many, possibly hundreds, of narrow, individual bands to detect very subtle differences among surface features such as vegetation, soil, and rocks.

Infrared: Images acquired by sensors measuring energy in one or more bands above 1000 nanometers.

Multispectral: Color images acquired by a digital sensors measuring energy in three to seven discrete bands at once. One set of detectors may measure visible red energy, while another set measures near infrared. The data are combined to create color images.

Panchromatic: Black and white images acquired by a digital sensor measuring energy over a single, wide portion of the electromagnetic spectrum simultaneously, typically 400 to 1000 nanometers. The image usually spans the visible to near-infrared part of the spectrum.

Worldwide Sampling of Earth Imaging Systems

Country	System	Launch	Type	Resolution
Australia	**ARIES-1 (Polar Orbit)**	2002	Panchromatic Hyperspectral	10-Meter 30-Meter
Canada	**Radarsat-1**	1995	Radar-C Band	8-Meter
China	**Feng Yun 2B (Weather)**	2000	Electro optical Multispectral	1.5 Kilometer 5.5 Kilometer
China, Brazil	**CBERS-2**	2003	Panchromatic IR	5-Meter 80-Meter
France	**CNES** **SPOT-5**	4 May 02	Panchromatic Multi-spectral IR	2.5-Meter 10-Meter 20-Meter
Europe (Italy and France)	**Cosmos Pliades**	2005 (planned)	Panchromatic Multi-spectral	.7 Meter 2 Meter
India	**IRS-P6**	2003	Panchromatic Multi-spectral	2.5-Meter 23-Meter
Israel	**ImageSat** **EROS 1A**	5 Dec 00	Panchromatic	.67-Meter
Malaysia	**TiungSat-1**	2000	Panchromatic Infrared	80-Meter
Russia	**METEOR-3M-NI (Polar Weather)**	2001	Multispectral	1-2 Mile
South Korea	**KOMPSAT-1 (Arirang-1)**	1999	Panchromatic Multi-spectral	6.6-Meter 1 Kilometer
United Kingdom Algeria, China, Nigeria, Turkey, Thailand, Vietnam	**Disaster Monitoring Constellation** **UK DMC SAT** **AlSat-1** **China Tba4** **Nigera Sat-1** **BILSAT-1** **Thai Paht 2** **Vietnam Tba 2**	 2003 2002 Planned 2003 2003 Planned Planned	 Panchromatic Panchromatic Panchromatic Panchromatic Panchromatic Multi-spectral Panchromatic Panchromatic	 12-Meter 32-Meter 4-Meter 30-Meter 12-Meter 18-Meter 30-Meter 30-Meter
United States	**LANDSAT 7**	1999	Panchromatic Multispectral	15 Meter 30 Meter
United States	**Digital Globe** **QuickBird 2**	18 Oct 01	Panchromatic Multi-spectral	.6-Meter 2.4- Meter
United States	**Space Imaging** **Ikonos-2**	24 Sep 99	Panchromatic Multi-spectral	.5-Meter 1-Meter

Appendix B

Definitions of Desired Effects, Weights, Countermeasure Techniques, and Nodes

Desired Effects and Weights

The definitions and the weights used in the technique-node analysis are listed below in the order in which they appear in the technique-node evaluation table in appendix C. Readers will find sufficient detail on how the criteria were selected, the valuation definitions, and how values were calculated, so the scores can be evaluated and changed, if desired, to meet new entering assumptions. The author invented the definitions and the weighting scale ranging from +5, meaning 100 percent effective in meeting the desired condition, to –5, meaning the technique would be ineffective or counter to the desired effect. A mid-point of zero indicates a questionable or doubtful impact, and therefore does not add or subtract from the value of the technique. All the criteria were scored on the same linear scale, except for political will, which was scored 1 or 0, and was weighted as a multiplier against the sum of all the scores. If the author judged the technique to be politically unacceptable, it the score would put it at the bottom for development consideration. Readers who find it necessary to weight other criteria should have no problem adapting their changes to this analysis. When evaluating criteria against specific nodes, scores across the entire +5 to –5 range were used, but all were simple estimates by the author, not backed by experimental data. The probability of each technique working as designed is assumed to be 100 percent.

end state. Relates to whether the attacked system can be returned to the operator in its pre-conflict condition. The risk of permanent damage or orbital decay from application of the technique reduces the score. Satellites and main processing ground sites have a high probability of unique, difficult-to-replace equipment. A score of –5 is appropriate if a satellite will be destroyed, where as 0 is appropriate when main processing ground sites are attacked since the downtime may or may not be significantly longer than the duration of the conflict. A score of +5 is appropriate if the system should operate as it did previously upon discontinuation of a temporary effect such as jamming or obstructing the sensors line of sight.

Condition	100 percent functional	Questionable	Destroyed/heavy damage
Score	+5	0	-5

sustainability. Relates to expectation that a technique's effects could be sustained continuously over several days, either with the reapplication of the technique over the period, or through continuous application. It assumes enemy forces cannot deny access to the target. A score of +5 is appropriate if the effect should be easily sustained. A score of 0 is appropriate if a single technique or a single weapon would be expected to lose coverage of the target from time to time during the attack. Sustainability of jamming against ground targets from other than space was scored 0. Since all techniques are expected to have some effect when applied, negative sustainability was undefined.

Condition	Very Sustainable	Unknown	N/A
Score	+5	0	

vulnerability. Relates to vulnerability of the weapon or its effects to countermeasures by the enemy over the duration of the mission. A score of +5 is appropriate if there is no reasonable enemy countermeasure to the applied technique. A score of –5 is appropriate if the enemy would normally be expected to counter the technique before a mission of undefined duration could be completed. A score of 0 is appropriate when there is insufficient information to make a decision.

Condition	Not Vulnerable	Questionable	Very Vulnerable
Score	+5	0	-5

covert. Relates to limitations of employing the weapon. Use of a covert weapon implies risks that detract from its usefulness in a deterrent role. Covert weapons may have limited usefulness once the technique is used if use compromises its existence. The score for covert techniques assumes first-time application, and therefore does not reduce the sustainability or vulnerability scores. Also, since the negative affect during first use is only if the technique is compromised, the permissible scoring range is limited compared to the others.

Condition	Overt		Covert
Score	+5		+3

target access. Relates to whether a technique can be weaponized so as to access the targeted node. The geometry of electronic warfare weapons and their targets is important. The use of co-orbital jammers would improve target access scores against nearby systems in the same orbit, but reduce access to ground sites, unless deployed in sufficient numbers of orbits to ensure global access. Likewise, ground-based jammers may never achieve line-of-sight with orbiting satellites. Depending on system design, mission, orbits and geometry, target access may or may not be achievable when necessary. No pair was scored less than zero in this evaluation.

Condition	Accessible	Tenuous/Unknown	No Access
Score	+5	0	-5

collateral damage. Relates to the possible weapon effects on property and personnel, as well as the expectation of maintaining friendly use of the imagery product. Creation of space debris and creation of long-term problems for spacecraft operation are considered in other categories. Collateral damage scores may directly affect political-will score.

Scores were determined by subtracting the following from 5:

	Subtract
Is the technique likely to deny imagery to the US and others?	3
If not, is image quality or timeliness likely to be degraded?	2
Weapon effects on or near the ground capable of causing indiscriminate damage or injury near target:	2
Weapon effects in space capable of damaging other satellites: considerable or unknown some minor	 6 4 2
Reduced data quality to other users:	1
Create space debris—considered separately under "space debris"	0
Induce irrecoverable problems to spacecraft health and safety (uncontrolled flight)—considered separately under "endstate"	0

Condition	No Collateral Damage	See Above Table	High Risk to Neutral Personnel and Equipment
Score	+5	0	-5

space debris. Relates to the possibility that employment of the weapon will result in creation of orbiting debris. The problem of fratricide against friendly or neutral systems demands consideration of debris problems. This area was weighted equal to the others not only for military purposes, but also for political ones. If two options exist, and one does not create debris, it is assumed to be a better choice. On orbit disabling weapons and direct-attack munitions are not themselves space debris. It is assumed they would be designed to deorbit after mission completion. Likewise, a weapon that causes the target satellite to move intact to a useless orbit, or causes it to deorbit, would not be considered to have created space debris. Space debris may directly effect the political will score.

Condition	No Debris	N/A	Debris
Score	+5		-5

political will. Relates to likelihood the President or Secretary of Defense would agree to weaponize and use a technique-node pair. This is the most heavily weighted condition. It is a multiplier of l or 0, applied to the total score. If a technique is politically untenable, the total score is irrelevant. The fact that the political will score was also added to the total was mostly for formatting purposes, and only marginally contributes to the overall score.

Condition	Acceptable	N/A	Unacceptable
Score	+1		0

Countermeasure Techniques

conventional attack. Those attacks using conventional fire weapons, against a terrestrial target. Only conventional attacks comprised of precision-guided munitions (PGM) were evaluated since they are the state of the art for stand-off engagement. The specific weapon was not assumed. Special operations attacks involving troops taking physical control of a facility were not evaluated under conventional attack. Conventional attacks against satellites were considered impossible.

cyber attack. Those attacks of electronic systems intended to affect acquisition, processing, or display of information through commands recognized by the system. Cyber attacks differ from electronic attack (EA) in that they use available channels to get to their intended target, rather than using over-the-air transmissions to deny system access to the adversary. Examples include commands to the satellite sensor, through the TT &C link, directing observation of areas other than where friendly operations are taking place; or injecting an image into the system in place of the one created by the satellite processor. The types and scope of cyber attacks are limited by access to, and security of, the channels and the system itself. These types of attack can be quickly denied once the methods are compromised, so they are assumed to be covert.

destructive directed-energy weapons. Those attacks that use various forms of energy to destroy electronic/optical components. For many years, nuclear explosions have been known to emit electromagnetic pulses capable of destroying circuits. New weapons such as high-power microwaves (HPM), also known as high-energy radio frequencies (HERF) are attempting to do the same thing without the associated blast, heat, overpressure, and nuclear fallout. High-power lasers (HPL) are being developed to turn matter into plasma. They can destroy components of systems, or become a source of heat that will deform optics or throw satellite environmental systems out of systemic equilibrium. Particle beam (PB) weapons are similar, except instead of light, they bombard the target with atomic particles. These examples share the goal of destroying the target with directed energy, but they differ in their means.

disabling electronic attack. Those attacks intended to temporarily disable electronic/optical components through application of electromagnetic energy to the receive channel of a system. Examples include brute force radio frequency jamming that denies or degrades the system's receiver by saturating it with a stronger signal; smart jamming that subtly interrupts essential portions of a signal; and low-power lasers (LPL) designed to dazzle optics without permanently damaging them. The effects of disabling electronic attacks dissipate as soon as the weapon disengages the target.

kinetic destruction. Those attacks designed to destroy a satellite by hitting it with a projectile. The anti-satellite (ASAT) missile program was one example. Another example would be space mines designed to orbit the earth while closing in on their target. The force of the projectiles' impact will destroy the target satellite.

on-orbit disabling. Those attacks designed to temporarily disable a satellite by physically closing in on it to perform a procedure. Examples include manned rendezvous to install a lens cap and the unmanned placement of micro-mechanical robots on the satellite to install or disconnect a designated circuit. The technique is intended to be reversible, so that full functionality can be restored after a conflict.

Nodes Selected for Analysis

ground data communications (located in a country aiding the adversary). This node represents the ability to distribute data, processed or unprocessed, to customers or processing centers. Specifically it is the receiver equipment within that country, and may include intermediate communication steps through satellites, fiber optic cable, or the public telephone network.

main ground processing center (located in a country aiding the adversary). This node represents the full ability to process images from data, and distribute the images. If the main ground processing center were located in the adversary's country , it would be treated similar to any other military support target. If it were in a country not supporting the adversary, there would be no need to attack it. Therefore this node represents the case of the remaining case and its political constraints.

main ground receive station (located in a country aiding the adversary). The main ground receive station for data going to the satellite operator. This is typically the station that receives the data that is sent to customers and it may be the only receive station in the system. In contrast, remote direct receive stations are common among imagery providers. They often give their hosts direct access to some data and processing capability.

sensor command uplink. Includes all radio receive equipment on the satellite connected to those processors specifically controlling the sensor.

sensor optics. The actual optical arrays aboard the spacecraft sensor, including mirrors, lenses, microchip sensors, and transparent covers. Definition does not include sensor support items such as servo motors, and environmental controls.

spacecraft command uplink. Includes all radio receive equipment on the satellite that controls satellite functions. It may or may not control the sensor depending on whether the particular design has separate radio command channels for the sensor and the platform.

space platform. The actual spacecraft itself, including communications and payload.

remote ground receive station (located in the adversary's territory). A direct-receive station licensed by the satellite operator to directly receive data from the satellite. Depending on the contract, data may be forwarded to the company via terrestrial communications, and/or used by the host. The existence of a remote ground receive station does not necessarily imply the ability to process the data into usable images.

remote ground receive station (non-combatant party passing data to collaborating company, not directly to adversary). This node illustrates the scenario where a direct-receive station in a neutral country is conducting normal, legal commerce. The fact that the parent company receiving the data from that site is assisting the adversary, puts the non-combatant party at risk of being declared a de facto collaborator.

Appendix C

Techniques versus Node Scoring Table

This table shows the value analysis done on the technique-node pairs. The nodes are generally taken from the nodal analysis described in the paper, however they were expanded to account for how function and physical location might affect political will. A weakness of the evaluation is that it is easier to assume a political-will score of zero when there are other options without similarly negative political consequences. It is possible the chart indicates incorrect political-will scores, biased by surrounding options that are more appealing, and by the fact that political will is dependent on the actual situation at hand, and is therefore difficult to pre-judge. The definitions and the scoring criteria are detailed in Appendix B. The results are tabulated in section V, Table 2.

	Conventional (PGM)	Kinetic Satellite Destruction	Destructive Directed Energy (High-power Microwave)	Destructive Directed Energy (High-power Laser or Particle Beams)	Disabling Electronic Attack (Jamming) Air/Surface	Disabling Electronic Attack (Co-orbital Jammer)	Disabling Electronic Attack (Low-power Laser)	On-orbit Disabling/ Screening	Cyber Attack
Spacecraft Sensor Optics	N/A		Not Scored. There may be an effect but HPMs are more likely to be used against the Platform than the optics		N/A	N/A			N/A
Desirable characteristics									
End-state effects:		-5		-5			5	5	
Sustainability:		5		4			3	5	
Vulnerability to detection & negation:		4		5			3	4	
Technique requires covert operation:		5		5			5	5	
Target Access:		3		3			4	5	
Collateral Damage Score: notional		2		2			2	-1	
Space Debris:		-5		5			5	4	
Political Will:		1		1			1	1	
Total:		10 (1)=10		20 (1) =20			28 (1)=28	28 (1)=28	
Sensor Command Up-link	N/A						N/A		
Desirable characteristics									
End-state effects:		-5	-5	-5	5	5		2	5
Sustainability:		5	5	5	0	5		5	5
Vulnerability to detection & negation:		4	5	5	3	4		4	0
Technique requires covert operation:		5	5	5	5	5		5	3
Target Access:		5	5	5	0	5		5	0
Collateral Damage Score: notional		2	-2	2	2	2		2	2
Space Debris:		-5	5	5	5	5		4	5
Political Will:		1	1	1	1	1		1	1
Total:		12 (1)=12	19 (1)=19	23 (1)=23	21 (1)=21	32 (1)=32		28 (1)=28	21 (1)=21

	Conventional (PGM)	Kinetic Satellite Destruction	Destructive Directed Energy (High-power Microwave)	Destructive Directed Energy (High-power Laser or Particle Beams)	Disabling Electronic Attack (Jamming) Air/Surface	Disabling Electronic Attack (Co-orbital Jammer)	Disabling Electronic Attack (Low-power Laser)	On-orbit Disabling/ Screening	Cyber Attack
Space Platform Command Up-link	N/A						N/A		
Desirable characteristics									
End-state effects:		-5	-5	-5	2	5		2	5
Sustainability:		5	5	5	0	5		5	5
Vulnerability to detection & negation:		4	5	5	3	4		4	0
Technique requires covert operation:		5	5	5	5	5		5	3
Target Access:		3	5	5	0	5		5	0
Collateral Damage Score: notional		2	-2	5	5	3		2	2
Space Debris:		-5	5	2	5	5		4	5
Political Will:		1	1	1	1	1		1	1
Total:		10 (1)=10	19 (1)=19	23 (1)=23	21 (1)=21	32 (1)=32		28 (1)=28	21 (1)=21
Space Platform	N/A				N/A	N/\A	N/A		N/A
Desirable characteristics									
End-state effects:		-5	-5	-5				3	
Sustainability:		5	5	5				5	
Vulnerability to detection & negation:		4	5	4				4	
Technique requires covert operation:		5	5	5				5	
Target Access:		5	5	5				5	
Collateral Damage Score: notional		2	-2	2				2	
Space Debris:		-5	5	5				4	
Political Will:		1	1	1				1	
Total:		12 (1)=12	19 (1)=19	22 (1) =22				29 (1)=29	

	Conventional (PGM)	Kinetic Satellite Destruction	Destructive Directed Energy (High-power Microwave)	Destructive Directed Energy (High-power Laser or Particle Beams)	Disabling Electronic Attack (Jamming) Air/Surface	Disabling Electronic Attack (Co-orbital Jammer)	Disabling Electronic Attack (Low-power Laser)	On-orbit Disabling/ Screening	Cyber Attack
Main Ground Receive Station (located in a country aiding the adversary)		N/A		N/A			N/A	N/A	
Desirable characteristics									
End-state effects:	5		5		5	5			5
Sustainability:	3		3		0	5			5
Vulnerability to detection & negation:	0		0		2	4			0
Technique requires covert operation:	5		5		5	5			3
Target Access:	5		5		5	5			0
Collateral Damage Score: notional	0		0		2	2			2
Space Debris:	5		5		5	5			5
Political Will:	1		1		1	0			1
Total:	24 (1)=24		24 (1)=24		25 (1)=25	31 (0)=0			21 (1)=21
Remote Ground Receive Station (located in adversary's country)		N/A		N/A			N/A	N/A	
Desirable characteristics									
End-state effects:	5		5		5	5			5
Sustainability:	2		3		0	5			5
Vulnerability to detection & negation:	0		0		2	4			0
Technique requires covert operation:	5		5		3	5			3
Target Access:	5		5		5	5			0
Collateral Damage Score: notional	3		4		3	5			4
Space Debris:	5		5		5	5			5
Political Will:	1		1		1	0			1
Total:	27 (1)=27		28 (1)=28		24 (1)=24	34 (0)=0			23 (1)=23

	Conventional (PGM)	Kinetic Satellite Destruction	Destructive Directed Energy (High-power Microwave)	Destructive Directed Energy (High-power Laser or Particle Beams)	Disabling Electronic Attack (Jamming) Air/Surface	Disabling Electronic Attack (Co-orbital Jammer)	Disabling Electronic Attack (Low-power Laser)	On-orbit Disabling/ Screening	Cyber Attack
Remote Ground Receive Station (located in a non-hostile country)		N/A		N/A			N/A	N/A	
Desirable characteristics									
End-state effects:	0		3		5	5			5
Sustainability:	3		3		0	5			5
Vulnerability to detection & negation:	0		0		0	4			0
Technique requires covert operation:	5		5		5	5			3
Target Access:	4		4		4	5			0
Collateral Damage Score: notional	0		-3		2	2			2
Space Debris:	5		5		5	5			5
Political Will:	0		1		1	0			1
Total:	17 (0)=0		18 (0)=0		22 (0)=0	31 (0)=0			21 (1)=21
Main Ground Processing Station (located in a country aiding adversary)		N/A		N/A	N/A See **Ground data communi-cations** below	N/A	N/A	N/A	
Desirable characteristics									
End-state effects:	0		0						0
Sustainability:	3		3						5
Vulnerability to detection & negation:	0		0						0
Technique requires covert operation:	5		5						3
Target Access:	4		4						0
Collateral Damage Score: notional	0		0						2
Space Debris:	5		5						5
Political Will:	0		1						1
Total:	17 (0)=0		18 (1)=18						16 (1)=16

	Conventional (PGM)	Kinetic Satellite Destruction	Destructive Directed Energy (High-power Microwave)	Destructive Directed Energy (High-power Laser or Particle Beams)	Disabling Electronic Attack (Jamming) Air/Surface	Disabling Electronic Attack (Co-orbital Jammer)	Disabling Electronic Attack (Low-power Laser)	On-orbit Disabling/ Screening	Cyber Attack
Ground data communications (located in a country aiding adversary)		N/A		N/A		N/A	N/A	N/A	
Desirable characteristics									
End-state effects:	5		5		5				5
Sustainability:	3		3		0				5
Vulnerability to detection & negation:	0		0		0				0
Technique requires covert operation:	5		5		5				3
Target Access:	4		5		4				0
Collateral Damage Score: notional	0		3		4				3
Space Debris:	5		5		5				5
Political Will:	1		1		1				1
Total:	23 (1)=23		27 (1)=27		24 (1)=24				22 (1)=22

Notes

[1] George J. Tenet, Statement before the United States Senate Armed Services Committee, 19 March 2002, 15, on-line, Internet, 14 Feb 2004, available from Hhttp://www.senate.gov/~armed_services/testimony.cfm?wit_id=193&id=192H.

[2] See appendix A.

[3] Tenet, 15.

[4] International Telecommunications Union, n.p., on-line, Internet, 14 February 2004, available from Hhttp://www.itu.int/members/index.htmlH.

[5] Analytic Graphics, *AGI Space Digest*, n.p., on-line, Internet, available from Hhttp://www.stk.comH, This site was particularly useful as a single source of technical data on a wide range of systems.

6 Frank Morring, Jr., "Industry Could Gain $1 Billion From NIMA," *Aviation Week & Space Technology* 158, no. 4 (27 January 2003), 32.

[7] "Find, fix, assess, track, target and engage" are the elements of the Air Force Vision, describing the capabilities American Forces would like to preserve for itself and deny to an adversary. "Global Vigilance Reach & Power, America's Air Force Vision 2020," undated (but released in June 2000), 6, on-line, Internet, available at Hwww.af.mil/visionH.

8 John Douglas, "A New Paradigm for Remote Sensing," a paper presented at the 11th Australasian Remote Sensing and Photogrammetric Conference, Brisbane, 6 Sep 2002, 3, on-line, Internet, 9 December 2003, available from Hhttp://www.apogee.com.au/pdf/11arspc_paper.pdfH.

[9] Multiple websites, on-line, Internet, 9 Dec 03. Ikonos accuracy is published on the SpaceImaging website, Hwww.spaceimaging.comH. QuickBird accuracy was found on Infoterra.com found at Hwww.infoterra-global.com/quickbird.htmH, and Radarsat resolution was found on the Radarsat website at Hwww.radarsat.comH,.

10 Major James G. Lee, *Counterspace Operations for Information Dominance*, Thesis Paper (Maxwell AFB AL: School of Advance Airpower Studies, October 1994), 10.

11 Major Edwin C. Swedberg, *The Effect on Operational and Tactical Surprise by US. Military Forces Due to the Proliferation of Unclassified Satellite Imaging Systems*, (Ft. Leavenworth KS: Command and General Staff College, 1995), 6.

12 United States Congress, Office of Technology Assessment, *The Future of Remote Sensing From Space: Civilian Satellite Systems and Applications*, OTA-ISC-558, (Washington D.C.: Government Printing Office, July 1993), 160.

[13] SPOT Image Corporation, n.p., on-line, Internet, 9 Dec 03, available from Hhttp://www.spotimage.fr/html/_167_171_172_.phpH

14 "Space Systems Forecast-Meteosat," International Forecast/DMS Market Intelligence Report, February 1995, 3.

[15] *AGI Space Digest*, n.p.

16 National Aeronautical and Space Administration, "Landsat-7," n.p., on-line, Internet, 9 Dec 2003, available from Hhttp://landsat.gsfc.nasa.gov/groundstations/Igslist.htmlH.

17 "Landsat-D" (an undated brochure produced by General Electric), 4-5.

[18] "Toulouse Facilities, SPOT Technical Information," SPOT Image Corporation, 1-6, on-line, Internet, 21 February 2004, available on line from Hhttp://www.spotimage.fr/html/_167_224_230.phpH.

[19] "SPOT Satellite Programming, a Custom Service," SPOT Image Corporation, 1, on-line, Internet, 21 February 2004, available on line from Hhttp://www.spotimage.fr/html/_167_224_230.phpH.

[20] James Oberg, *Space Power Theory*, (Washington D.C: Government Printing Office, 1999), 149.

[21] White House, *The National Security Strategy of the United States*, September 2002, 15, on-line, Internet, 9 December 2003, available on line from Hhttp://www.whitehouse.gov/nsc/nss.htmlH.

[22] Chairman, Joint Chiefs of Staff, *The National Military Strategy of the United States*, 1997, on-line, Internet, 9 December 2003, available on line from: Hhttp://www.apc.maxwell.af.mil/pubs/nms/joint.htm#CharacteristicsH

[23] *Joint Doctrine for Space Operations*, Joint Publication 3-14, 9 Aug 2002, x, CD-ROM, Joint Staff J7, June 2003.

[24] Fact File, United States Strategic Command, undated, n.p., on-line, Internet 9 December 2003, available from Hhttp://www.stratcom.af.mil/factsheetshtml/spacemissions.htmH.

[25] Sarah Estabrooks, "Positive Steps At The Conference On Disarmament**,"** Ploughshares Briefing, Autumn 2003, on-line, Internet 10 Jan 2004, available from Hhttp://www.ploughshares.ca/content/MONITOR/mons03b.htmlH.

[26] Sarah Estabrooks, "Preventing the Weaponization of Space," Ploughshares Breifing, 03/3, n.p., on-line, Internet, available from Hhttp://www.ploughshares.ca/content/MONITORH.

[27] Quoted in Gerhard von Glahn, *Law Among Nations, An Introduction to Public International Law*, 6th ed. (New York: MacMillan Publishing Company) 4.

[28] Glenn H. Reynolds and Robert P. Merges, *Outer Space, Problems of Law and Policy*, 2d ed. (Boulder: Westview Press, 1997), 27.

[29] "Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land," Hague Convention V, 18 October 1907, articles 7 and 8, on-line, Internet, 28 January 2004, available from: Hhttp://library.byu.edu/~rdh/wwi/hague/hague6.htmlH. Article. 7. "A neutral Power is not called upon to prevent the export or transport, on behalf of one or other of the belligerents, of arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet." Article. 8. "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."

[30] Walter S. Kind, ed., *Military Commander and the Law*, 6th ed. (Maxwell AFB AL: Air Force Judge Advocate General School Press, 2002), Chapter 15, on-line, Internet, 12 December 2003, available from Hhttp://milcom.jag.af.mil/ch15/info.htmH.

[31] "Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land," Article 8.

[32] *United Nations Convention on the Law of the Sea of 1982*, Articles 9 and 50, on-line Internet, 9 January 2004, available from Hhttp://www.vilp.de/Enpdf/e025.pdfH. "The Helsinki Principles on the Law of Maritime Neutrality provide that Merchant ships flying the flag of a neutral State may be attacked if they (a) engage in belligerent acts on behalf of the enemy; (b) act as auxiliaries to the enemy's armed forces; (c) are incorporated into or assist the enemy's intelligence system; (d) sail under convoy of enemy warships or military aircraft; or (e) otherwise make an effective contribution to the enemy's military action, e.g., by carrying military materials, and it is not feasible for the attacking forces to first place passengers and crew in a place of safety. Unless circumstances do not permit, they are to be given a warning, so that they can re-route, off-load, or take other precautions." The United States is not a signatory of the Law of the Sea Treaty, but may abide by principles such as the Helsinki Principles.

[33] Lee, 1.

[34] Reynolds, 51-54. The formal name of the treaty is, "Multilateral Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water."

[35] Reynolds, 62. The formal name of the treaty is, "Multilateral Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies."

[36] Reynolds, 96. The formal name of the treaty is, "Treaty on the Limitation of Anti-Ballistic Missile Systems, May 26, 1972."

[37] Captain Michael G. Gallagher, "Legal Aspects Of The Strategic Defense Initiative," *Military Law Review*, Department of The Army Pamphlet 27-100-111, volume 111 (Winter 1986), 36.

[38] Ibid.

[39] William L. Spacy II, "Does the United States Need Space Weapons?" Cadre Paper (Maxwell AFB AL: Air University Press, September 1999), 10.

[40] Ibid., 96.

[41] *Land Remote Sensing Policy*, Section 5621, United States Code Title 15, Chapter 82 - 1992. "No license shall be granted by the Secretary unless the Secretary determines in writing that the applicant will comply with the requirements of this chapter, any regulations issued pursuant to this chapter, and any applicable international obligations and national security concerns of the United States."

[42] Reynolds, 204-205.

[43] Major Thomas Rogers, Professor of Space Law, United States Air Force Judge Advocate General School, Maxwell AFB AL, interviewed by author, 15 Jan 2003.

[44] Morring, 32.

[45] Mike Wendling, "Russian GPS Jammers Pose Little Threat In Iraq," CNS News.com, March 31, 2003, n.p., on-line, Internet, 26 October 2003, available from Hhttp://www.cdi.org/russia/johnson/7125-16.cfmH.

[46] Quoted in Col (Sel) Bruce W. Carmichael, et. al, "Strikestar 2025," Research Paper Presented To Air Force 2025, August 1996, 2.

[47] Jeffery Lewis, "Lift-off for Space Weapons: Spending on War Fighting from Space in the FY2004 Budget Request," Center for International and Security Studies at Maryland (CISSM), School of Public Affairs, University of Maryland, n.p., on-line Internet, available from Hwww.puaf.umd.edu/CISSM/Publications/AMCS/H. Estimates of the unclassified budget request for the FYDP 04-09 are in the range of $30 billion. Half is for Command Control and Intelligence, $13 billion is for

space-based missile defense, leaving $2.8 billion for various programs under space control and power projection.

[48] Joseph S. Nye, Jr., "U.S. Power and Strategy After Iraq," *Foreign Affairs* 82, no. 4 (July/August 2003), 66.

[49] Alan Garscadden and Michael Kelly, "Rapid Aerospace Response—Technological Capabilities Can Provide a Roadmap for Warfighter Operations," *Horizons*, June 2003, n.p., on-line, Internet, 30 January 2004, available from Hwww.afrlhorizons.com/Briefs/Dec03/PR0305.htmlH.

[50] *SPACECAST 2020*, (Maxwell AFB AL: Air University Press, 22 June 1994), 64.

[51] "Analysis of Space Concepts Enabled by New Technology," NASA funded study by Futron Corporation, 2003, 2-3. The four classes of launch, according to NASA are "small, medium, intermediate, and heavy," with intermediate class launches projected to make up roughly half of all launches through the end of the projection in 2021.

[52] Ibid, 3.

[53] "CDI Space Security Update #10," Center for Defense Information, 19 December 2003, n.p., on-line, Internet, 30 January 2004, available from Hhttp://www.cdi.org/friendlyversion/printversion.cfm?documentID=1962H.

[54] The Institute for National Strategic Studies created a consensus view of future wars out to 2025 based on a review of thirty-six existing studies of the strategic environment. It concluded that the United States enjoys overwhelming advantages in conventional air and sea-based capabilities. Sam J. Tangredi, "Consensus Views," *The Emerging Strategic Environment*, Unit 1, INSS, January 2004, 15-16.

[55] Department of Defense, *Military Transformation Strategy: A Strategic Approach* (Washington D.C.: Government Printing Office, Fall 2003), 19.

[56] Marco Caceras, "Industry Insights," American Institute of Aeronautics and Astronautics, Inc., September 2000, n.p., on-line, Internet, available from Hhttp://www.aiaa.org/market/index.hfm?mar=61&issuetocid=8H.

[57] Senate, "Critical Infrastructure Protection, Commercial Satellite Security Should Be More Fully Addressed," United States General Accounting Office Report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate GAO-02-781, Aug 2002, 18, on-line, Internet, 30 January 2004, available from Hhttp://www.fas.org/spp/military/gao/gao02781.pdfH.

[58] Ibid., 32.

[59] *Dictionary of Military and Associated Terms*, Joint Publication 1-02, 5 June 2003, 399, CD-ROM, Joint Staff J7, June 2003. Definition derived from Department of Defense definition for "Passive Defense."

[60] Ibid., 389.

[61] Major William L. Spacy II, *Does the United States Need Space-Based Weapons?* CADRE Paper (Maxwell AFB AL: Air University Press, September 1999), 66, Tables 1 and 2. This source contained a useful, unclassified list of counterspace weapons.

[62] *Joint Doctrine for Electronic Warfare*, Joint Publication 3-51, 7 April 2000, I-2, CD-ROM, Joint Staff J7, June 2003. "Electronic Attack is the subdivision of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (see Joint Publication [JP] 3-09, *Doctrine for Joint Fire Support*). Electronic attack includes actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception; and employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, or particle beams)."

[63] "Weekly Circular 2207/12/12/1995," Special Section no. AR11/A/1386, International Telecommunication Union, 12 December 1995.

[64] Worldview Imaging Corporation to the Federal Communications Commission," Application of Worldview Imaging Corporation for a Remote Sensing Satellite System Before the Federal Communications Commission," Figure A-6, December 1992.

[65] *Landsat-D*, General Electric brochure, undated, 4-5.

[66] David Baker, ed., *Jane's Space Directory*, 18th ed. (London: Jane's Information Group, 2002).

[67] Major General Bengt Anderberg and Dr. Myron L. Wolbarsht, *Laser Weapons: The Dawn of a New Military Age* (New York: Plenum Press, 1992), 148.

[68] Anderberg, 23.

[69] Baker.

[70] Jeffrey Lewis, "Lift-Off For Space Weapons? Implications of the Department of Defense's 2004 Budget Request for Space Weaponization," by Center for International And Security Studies at Maryland (CISSM), 21 July 2003, 15.

[71] "The SPOT Satellites Image Acquisition," n.p., on-line, Internet, 16 February 1997, available from http://www.spotimage.fr/anglaise/system/satel/ss-acquis.htm.

[72] Major Thomas A. Summers, "How Is U.S. Space Power Jeopardized by an Adversary's Exploitation, Technological Developments, Employment and Engagement of Laser Antisatellite Weapons?" (Maxwell AFB AL: Air Command and Staff College, April 2000), 40-41.

[73] Lt Colonel Charles M. Westenhoff, ed., *Military Air Power—The CADRE Digest of Air Power Opinions and Thoughts* (Maxwell AFB AL: Air University Press, October 1990).

[74] Nye, 60-73.

[75] Quoted in Reynolds, 199-200. Hamilton DeSaussure, "The Interaction of Domestic and International Law," a paper presented at the 38th Congress of the International Astronautical Federation, Brighton, United Kingdom, 10-17 October 1987.

[76] Ibid, 259-260.

[77] Ibid., 260.

[78] *Joint Warfare of the Armed Forces of the United States*, Joint Publication 1, 14 November 2000, v, CD-ROM, Joint Staff J7, June 2003.

[79] Ibid., vi.

[80] Quoted in Frank J. Gaffney, Jr., "Wake-up Call on Space," CNSNews.com, 9 January 2001, n.p., on-line, Internet, 27 August 2003, available from Hhttp://www.cnsnews.comH. Quote originally appeared in newspaper *Sing Tao Jih Pao*, Hong Kong, 5 January 2001.

[81] Air Force Space Command, "Strategic Master Plan FY04 and Beyond," 5 November 2002, 16, on-line, Internet, available from Hhttp://www.nukewatch.org/importantdocs/resources/Final004SMP.pdfH

[82] Bob Preston et al., *Space Weapons, Earth Wars*, (Santa Monica CA: Rand, 2002). Rand Corporation study sponsored by Lt Gen Roger DeKok, the Deputy Chief of Staff, Plans and Programs (AF/XP), xxii.

[83] Lewis, "Lift-off for Space Weapons: Spending on War Fighting from Space in the FY2004 Budget Request," 1-3.