

FUTURE CHALLENGES

To U.S. Space Systems

June 1998

Graphics and Layout by:
Christine Redding

**Comments or questions
should be directed to:**

David R. Tanks,
Principal Study Investigator

Washington, DC Office:

1725 DeSales Street, NW, Suite 402
Washington, DC 20036
Tel: 202•463•7942
Fax: 202•785•2785

Cambridge, MA Office:

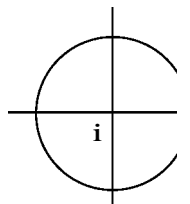
Central Plaza Building,
Tenth Floor
675 Massachusetts Avenue
Cambridge, MA 02139
Tel: 617•492•2116
Fax: 617•492•8242



The Institute for Foreign Policy Analysis, Inc.

TABLE OF CONTENTS

Introduction	1
Assumptions	2
Background	3
Techniques for Interfering with Space Systems	4
• Antisatellite Interceptors	4
• Co-orbital	5
• Direct Ascent	5
• Nuclear	7
• Kinetic Energy	7
• “Buckshot”	7
• Directed Energy (DE) Weapons	8
Adaptive Optics Insert	9
• Electronic and Information Warfare	11
• Attacks on Ground Stations	13
How Might Other States Seek to Limit the United States’ Use of Space Assets?	14
• First Scenario	14
• Second Scenario	15
• Third Scenario	16
Potential Courses of Action	18
Conclusions	19



FUTURE CHALLENGES

To U.S. Space Systems

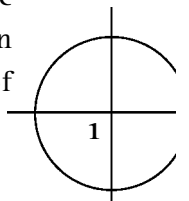
Introduction

During the past 40 years of space exploration and development, the free access and use of space has been the norm. However, as the threshold of the twenty-first century approaches, this situation shows signs of change as countries become increasingly aware of the tremendous military advantages that space-based assets provide. These advantages were publicly demonstrated during *Operation Desert Storm*, making a powerful impression on the thinking of national policymakers around the globe. Consequently, there is a growing interest in the question of space control. Although the two super powers of the cold war era have long supported research and development programs aimed at countering the others' key space assets during a crisis, it has not been until recent years that other states are believed to have become actively involved in this issue.

Space capabilities and technologies are proliferating. The end of the cold war freed up a tremendous amount of human talent and production infrastructure that formerly had been devoted to the research and development of military-related space capabilities. One of the "peace dividends" has been the reorientation of this highly skilled capability into commercial space development. Although the commercialization of space promises to improve people's lives and yield significant economic benefits to the United States, the commercialization trend also increases the importance of such issues as free access to space and the control of space assets during conflict.

The implication of this pool of excess human space talent is that countries desiring to develop space warfare capabilities have a pool of already trained manpower to draw upon. With the free movement of people and knowledge internationally a key factor of the information era, it should be expected that space capabilities will also be affected, spreading around the globe as the twenty-first century unfolds. What is less certain is the speed with which this proliferation will occur.

In an attempt to shed some light on this issue, this mini-study will examine potential future threats to space assets, as they relate to U.S. interests, to determine the potential courses of action that should be explored to ameliorate potential future threats. This report represents the first of a series of efforts which will examine each of the varied aspects of space issues and policies.



FUTURE CHALLENGES

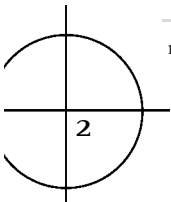
To U.S. Space Systems

Assumptions

It has been assumed that:

- **The economic factors used to project the development of space are generally correct.** This means that the ongoing plans to commercialize space continue and that the current economic slow-down in Asia reverses itself during the next couple of years and does not trigger some unforeseen catastrophe, such as a global economic depression. Obviously, the commercialization of space will require a substantial investment of capital. Much of this capital will be contributed from Asia. In addition, many of the states that are attempting to get into space are countries that are now experiencing economic difficulties. The future rate of space development will hinge on their ability to invest in the aerospace sector.
- **The United States continues its movement toward the military exploitation of space and its resulting increased dependency on space products for terrestrial combat operations.** Space provides tremendous signal intelligence; and imagery. These advantages are of such significance that space development will continue despite the vulnerabilities that such dependency will create.
- **International transfers of sensitive technologies will continue and skilled foreign space experts will continue to be available for hire.** The end of the Cold War resulted in the termination of many military space programs. While the number involved is unknown, reports indicate that some space experts have taken positions overseas. Considering the large cutbacks in space programs in Russia and the poor economic conditions in that country, the continued availability of space expertise to any state willing to pay the required salaries is assumed.
- **Other parties will increase their efforts to deny the United States and other space powers the advantages derived from space assets.** In terms of asymmetrical warfare considerations, adversarial countries in conflict with the United States and other space powers will try to disrupt the use of space assets. Thus, the indicators that other states are exploring potential capabilities for space warfare will increase during the first decade of the twenty-first century.¹
- **In the future, new actors will attempt to create their own space-based networks or exploit the commercial assets which will become available.** There are reports of space programs in other states that are working to create their own versions of space

¹ For example, Iraq is clearly interested in an ASAT capability as a counter to Israel's space reconnaissance satellites. See "Iraqi Memo to Arab League Warns of Israeli Space Activity," Cairo *MENA*, translated in *FBIS-NES-98-066*, March 7, 1998.



navigation and intelligence collection constellations. They will also undoubtedly attempt to gain the advantages available to the major powers by exploiting commercial space applications as they become available.

Background

In opening new high-risk frontier areas, a general pattern of military and government-led exploration efforts is inevitably followed by commercial exploitation activities. The same pattern seems to be holding for space. Governments opened the way; commercial operations are following. Although telecommunication has been the predominant commercial space activity, the areas of remote sensing and other products that are expected to be unveiled are now emerging as new areas of commercial space endeavor. Many of the planned commercial ventures are multi-national in composition; a number of ventures are also headquartered in countries other than the United States. The increase in multi-national space activity undoubtedly will trigger a plethora of international disputes similar to those of past centuries that accompanied the development of international norms for controlling the use of the high seas.

During the evolution of space utilization, the United States did not organize itself to deal with space in any unified sense. Various government agencies, such as NASA, the intelligence agencies, and the military all treated space as if it were a vacant field in which to park their assets. Very little coordination existed between these entities on the development of space assets or the use of space.

It now seems clear that the United States eventually will lose its hegemonic dominance of space.² Consequently, the various agencies using space, by necessity, are being forced to coordinate space activities much more closely than they have in the past and to develop unified national positions in their handling of international space issues.

One of the key challenges that increasingly will confront future U.S. policymakers is the issue of security of critical space capabilities. In a series of war games and assessments designed to examine the vulnerability of U.S. space assets, a number of issues came to light:³

- First, the U.S. global positioning system (GPS) was a priority target for opposing forces.

² "DIA Says Days of U.S. Hegemony In Space Are Numbered," *Armed Forces Newswire Service*, January 2, 1998.

³ William B. Scott, "Wargame Raises New Space Policy Dilemmas," *Aviation Week & Space Technology*, February 23, 1998, pp. 98-99; and Bill Gregory, "Down to Earth," *Armed Forces Journal*, December 1997, p. 12.

- Second, determining if opposing forces had conducted an attack against U.S. space assets was often difficult because there are no means now in place with which to determine why satellites suddenly stop functioning.
- Third, there are numerous possible methods for disrupting space assets, not all of which are intuitively obvious.

Techniques for Interfering with Space Systems

A number of states are known to have conducted research and development into methods of interfering with space systems. Although much of the information dealing with this issue is classified, enough has become known to paint a fairly clear picture of the current and anticipated methods that could be used to disrupt satellite operations.

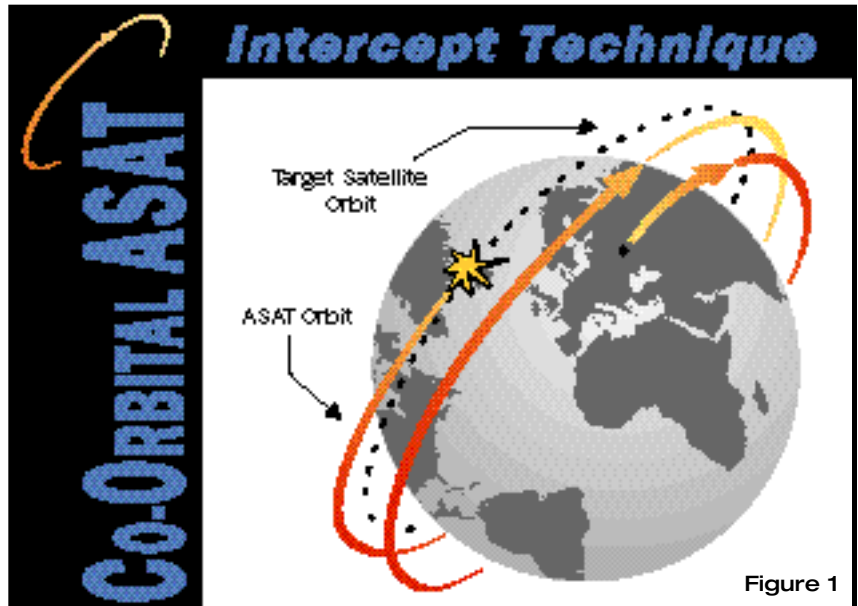
Obviously, the most straightforward method is to launch antisatellite (ASAT) weapons into space to attack designated targets, killing the desired system(s). The ASAT might be armed with conventional high explosive or nuclear warheads or use some type of kinetic kill mechanism based on hit-to-kill principles. Other methods can disrupt satellite operations without being launched into space or

necessarily doing permanent damage to the satellite. For example, jamming, ground-based laser employment, and information warfare (IW) can be conducted using terrestrial-based assets. Even easier is the use of newer IW approaches such as induction of computer viruses, covert penetration and corruption of software, or use of remote command systems to take control of specified satellite constellations. Finally, sabotage operations against the satellite ground-link stations are a further possibility for certain satellite networks.

Antisatellite Interceptors. Many countries possess the technology and capabilities to develop a system that could pose a risk to some U.S. satellites. While certain methods clearly require advanced aerospace capabilities, rudimentary but effective ASAT capabilities employing off-the-shelf launch vehicles could enable selected nations to assemble and deploy crude ASATs. Few nations are currently acknowledged to possess dedicated ASAT weapon programs, although enabling technologies are becoming widely available.

Ground-launched ASAT weapons can intercept their target in one of two modes: co-orbital or direct ascent. Each has distinct characteristics that have implications for post-Cold War space operations.

- *Co-orbital.* Most information regarding co-orbital ASAT weapons is a result of some twenty Soviet tests conducted between 1968 and 1983. While some conjecture exists regarding the altitudes at which this technique is effective, it is generally agreed that the co-orbital method is more likely to be used against satellites in low-earth orbit (LEO: 60-300 miles) and mid-earth orbit (MEO: 300-22,300 miles). It is also the system that could allow countries with advanced ASAT capabilities to attack satellites in geostationary orbits. However, the co-orbital approach has a number of drawbacks:



- First, it requires a dedicated SLV as a launch vehicle, which is larger, more expensive, and more difficult to obtain than a launch vehicle required for the alternative direct ascent engagement method.

- Second, co-orbital vehicles must be launched from fixed sites, increasing their vulnerability to surveillance and attack.

- Third, co-orbital antisatellite weapons require the kill vehicle to complete as many as two revolutions around the earth to rendezvous with its target, it can take up to 3½ hours to achieve an intercept (See Figure 1). This provides ample time for a targeted satellite, if alerted, to conduct evasive maneuvers.⁶

- *Direct Ascent.* Direct ascent ASAT weapons are the more likely systems to be adopted by Third World states seeking an ASAT capability.⁷ These systems have some important advantages over the co-orbital method of satellite attack:

⁴ On its co-orbital ASAT, the USSR used both radar and optical tracking of targets. Reportedly, the Soviets found that the radar-guided ASATs were far more effective. Andrew Wilson, ed., *Jane's Space Directory*, Twelfth Edition, (Jane's Information Group: Surrey, UK) 1996-1997, p. 145.

⁵ In 1987, General John Piotrowski, then-Commander of the USAF Space Command, credited the Soviet co-orbital ASAT system with a 70-75 percent effectiveness rate, to an altitude of 5000 km. Wilson, *op cit.* Other analysts, however, cite a lower effectiveness rate, roughly fifty percent at altitudes of 2500 km or less. David Hobbs, "Space Warfare," *Advanced Technology Warfare*, (Crescent Books: New York, NY) 1985, p. 82.

⁶ Modified co-orbital techniques have been developed to prevent the target satellite from maneuvering out of harm's way. The ASAT enters a "parking orbit" at a lower altitude than the target. Once below the targeted satellite, thrusters fire, raising the kill vehicle into an attack position.

⁷ Allen Thompson, "Satellite Vulnerability: A Post-Cold War Issue?" *Space Policy*, February 11, 1995, pp. 19-30.

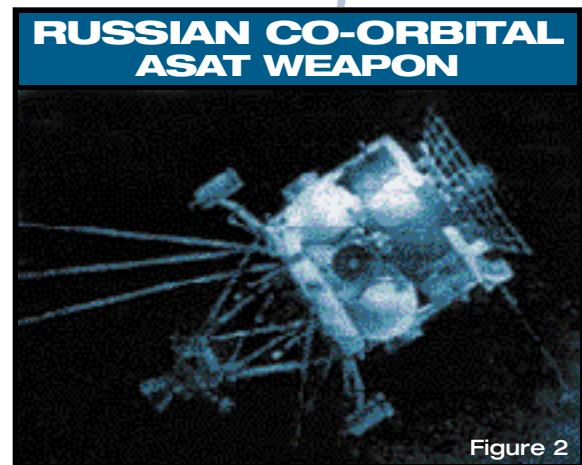
FUTURE CHALLENGES

To U.S. Space Systems

- Ý First, this technical approach can use ground-mobile or airborne launchers to conduct the attack, making them difficult, if not impossible, to identify and counter prior to missile launch.
- Ý Second, it is possible to launch a direct ascent ASAT using modified off-the-shelf systems, including sounding rockets or interceptor systems, such as THAAD or the Russian exoatmospheric anti-ballistic missile systems. It is even possible to attack a satellite in low-earth orbit with a Scud missile or perhaps a supergun. According to Iraqi defector Hussein Kamel, the supergun "was meant for long-range attack and also to blind satellites. Our scientists were seriously working on that. It was designed to explode a shell in space that would have sprayed a sticky material on the satellite and blinded it."⁸
- Ý Third, direct ascent ASATs travel to their target without first having to orbit the earth. Hence, they can often achieve an intercept in a matter of minutes, rather than hours.

The Soviet Union is the only nation known to have fielded an operational antisatellite (ASAT) weapon. Operational since 1972, the

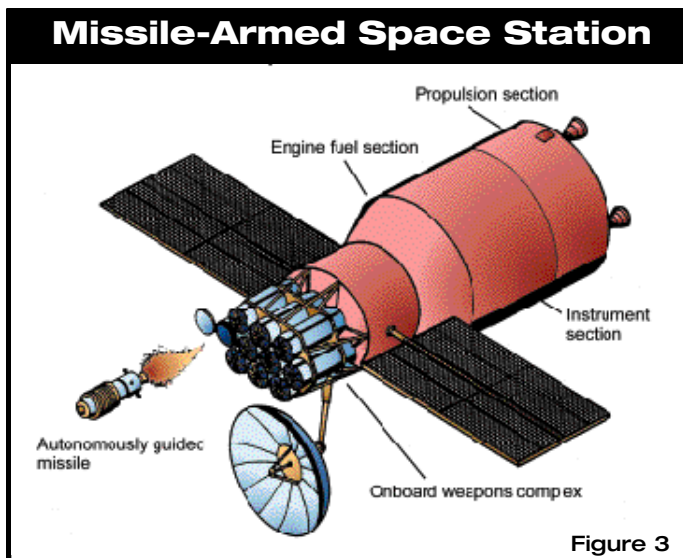
Russian system was part of a comprehensive military space program not only involving the ASAT interceptor, but also a number of ground-based high-powered laser facilities and planned space-based weapons. Despite a 1983 self-proclaimed moratorium on space weapons by President Yuri Andropov, to date Russia reportedly still conducts tests of components applicable to antisatellite operations. Reports emerged as late as 1994, for instance, that Russia had modified two MiG-31 *Foxhound* interceptors to fire air-launched ASATs. A recent report indicates that these aircraft may soon be offered for export.⁹



Despite imposing costs and technical challenges, ASATs can also be launched from satellites. As early as the 1970s, for instance, Russia had planned to develop and deploy a

⁸ "Iraqi Tells of Mass Graves, Space Weapon," *UPI*, September 22, 1995.

⁹ Ivan Safronov, "MiG-31 To Be Turned Into Space Launch Platform," *Kommersant*, translated in *FBIS-UMA-98-082*, March 23, 1998.



space-based antisatellite launch vehicle as part of a comprehensive antiballistic missile and ASAT program. According to plans developed by the Energia design bureau, a missile-armed space station could be placed into orbit and operate autonomously (See Figure 3). During periods of intensive operations, a two-man crew could be deployed to operate the station for a period of fourteen days.¹⁰

Once in proximity to its target, an ASAT interceptor may employ several methods to achieve a kill:

- **Nuclear.** The most immediate and obvious implication of a nuclear-armed ASAT

would be an increased destructive multiple kills per shot. As warheads on antisatellite weapons, however, their effects go far beyond the thermal energy and prompt radiation effects of the nuclear blast, which would affect most LEO satellites within line of sight. The detonation of a nuclear weapon in space would significantly raise space-resident radiation levels, particularly in the Van Allen belts surrounding the earth.¹¹ The resulting radiation increase could last for a year, causing satellites, particularly those in low-earth

orbit, to cease functioning within a matter of one-two months. Compounding this problem is the fact that newer satellites, both commercial and military, rely increasingly on miniaturized circuits; such microelectronics are more vulnerable to the effects of supplemental radiation.¹²

- **Kinetic Energy.** Kinetic energy antisatellite weapons (KE-ASATs) kill by colliding with a targeted satellite.¹³ This method demands terminal guidance systems, such as radar, infrared, or optical sensors, to bring the kill vehicle into contact with its target.
- **"Buckshot."** This method involves detonating a conventional warhead to disperse

¹⁰ For an excellent overview of Soviet space warfare efforts see, Steven J. Zaloga, "Red Star Wars," *Jane's Intelligence Review*, May 1997, pp. 205-208.

¹¹ Van Allen radiation belts are two belts of radiation outside the earth's atmosphere, extending from c.400 to 40,000 miles (c.650 to 65,000 km). The region of the belts is called the magnetosphere. The high-energy protons and electrons that compose the belts circulate along the earth's magnetic lines of force. These particles are probably emitted by the sun in its periodic solar flares and, after traveling across space are captured by the earth's magnetic field. The belts were discovered by detectors aboard *Explorer I*, the first U.S. artificial satellite. Information from www.encyclopedia.com.

¹² "Doomsday Scenario," *Aviation Week & Space Technology*, May 1, 1995, p. 21.

¹³ Among the techniques developed to improve the chances a KE-ASAT achieves an intercept is for the kill vehicle to deploy one or more umbrella-like devices, in some cases increasing the size of the KV by a magnitude.

FUTURE CHALLENGES

To U.S. Space Systems

pellets or other objects, such as coarse sand, into the path of an oncoming satellite or, alternatively, to blast the satellite, shotgun style. When employed by the Soviet Union on its co-orbital ASAT, a rudimentary "shotgun" technique was able to achieve functional kills from distances exceeding one kilometer. For regional adversaries seeking to obtain a crude ASAT capability, one of the buckshot approaches could be used for a direct-ascent attack. If salvo-fired into the paths of LEO satellites, using launch vehicles no more sophisticated than *Scud* missiles, the buckshot technique could prove to be an effective counter to selected U.S. satellite systems.¹⁴

Directed Energy (DE) Weapons. When considering the velocities and distances that must be dealt with when engaging satellites in various orbits, the operational advantages of speed-of-light weapons are clear. Several nations already have either built or are developing the technology to construct ground- and air-based directed energy antisatellite (DE-ASAT) weapons. In the future, despite cost and technical obstacles, this threat may be further augmented by space-based systems. While such exotic DE technologies as neutral particle beam accelerators and radio frequency weapons may emerge as threats later in the next century, it

is lasers and high-energy microwaves that appear to be the more likely candidates for entry into the directed-energy weapon inventories of states developing DE capabilities.

Ground-based lasers offer perhaps the least technologically challenging method to obtain an antisatellite DE capability and, hence, the most likely to be developed by regional powers fairly early in the next century. According to Robert Bell of the National Security Council, as many as twenty to thirty nations already possess the ability to fire lasers at space-based targets.¹⁵ While adaptive optics and spacecraft tracking software are among the supporting disciplines that need to be mastered to obtain a true DE-ASAT capability, these technologies are becoming more available to regional powers (See text box). If mated with low-power lasers, it is possible to irradiate low-earth orbit satellites, resulting in malfunctions or, in the case of imagery systems with focal plane arrays, optical sensory overload.

The utility of low-power lasers against such satellites was demonstrated recently in an Army experiment in which a 30-watt commercial laser, when reflected from a 1.5 meter mirror, saturated the sensors of an earth-observing satellite in LEO, effectively

¹⁴ Remarks by Henry Spencer, "Chinese ASAT and Rates of Change," December 31, 1995.

¹⁵ Bill Gertz, "Shared Satellite Laser Test. Weighed; U.S. Plan Could Breach Security," *Washington Times*, January 2, 1998, p. A1.

Adaptive Optics

Acquiring and engaging objects in space using ground-based lasers is made more difficult by atmospheric distortions. Compensating for such distortions to obtain a clear image—or, in the case of DE-ASATs, a focused laser beam—can be accomplished through a process known as adaptive optics. Adaptive optics allow objects to be tracked through atmospheric distortions by measuring the incoming waveform distortions in real time, computing the appropriate correction, and shaping a deformable mirror or equivalent element to cancel the distortions.¹⁶ Essentially, atmospheric distortions act like a prism on light waves, they bend and scatter the waveforms. Adaptive optics distort the light or laser beams at origin so that the atmospheric distortions reconcentrate the beams into a focused waveform rather than diffusing it throughout the atmosphere.

Once limited to a very few countries, adaptive optics technology is now available on the commercial market and through a number of recently declassified DoD studies on AO.¹⁷ If ground-based lasers are pointed by available commercial space-tracking software, nearly any satellite in low-earth orbit potentially could be engaged by hostile entities.¹⁸

blinding it.¹⁹ The results of this test are especially relevant in light of the fact that most U.S. photo reconnaissance satellites maintain elliptical orbits, orbits with an apogee of around 500 miles or higher and a perigee at roughly 100 miles (plus or minus).

Higher-powered lasers, while more difficult and expensive to construct, may nevertheless be within the reach of regional powers fairly early in the next century and could cause significant damage to U.S. space assets. In the past, Russian lasers of this type have been

employed against American space platforms, sometimes with serious results. In October of 1984, for example, the Soviet Union employed a high-energy laser (in low-power mode) based at Sary Shagan to illuminate and track the Space Shuttle *Challenger*, resulting in malfunctions on the orbiter and discomfort to the crew.²⁰

Compounding concerns that regional powers may develop similar systems indigenously is the fact that Russia may have recently decided to export a number of its laser

¹⁶ Adaptive Optics Association homepage, www.aoainc.com, February 3, 1998.

¹⁷ G.P. Collins, "Making stars see stars: DOD adaptive optics work is declassified," *Physics Today*, February 1992, pp. 17-21.

¹⁸ See Leonard David, "New Software Enables Amateurs to Track Satellites," *Space News*, August 12-18, 1996, p. 8.

¹⁹ John Donnelly, "Laser of 30 Watts Blinded Satellite 300 Miles High," *Defense Week*, December 8, 1997, p.1/13.

²⁰ Zaloga, *op cit*.

FUTURE CHALLENGES

To U.S. Space Systems

technologies. Reportedly, India has already expressed interest in purchasing lasers from Russia, whose press sources claim that Moscow now "feels that laser technologies it has developed would be widely accepted the world over."²¹

While ground-based systems appear to offer the most immediate near-term laser threat, such systems may be supplemented by air-based laser weapons. Platforms similar to the U.S. Air Force's YAL-1 Airborne Laser (ABL), which has clear potential against satellites, may emerge in the inventories of future adversaries in the next century. Even though there have been some difficulties associated with developing the YAL-1, most of the difficulties have been associated with the requirement to propagate a multi-megawatt laser beam through several hundred kilometers of atmosphere and intercept an ascending ballistic missile, a requirement not inherent in airborne ASAT operations which only have to penetrate less than 80 kilometers of thinning atmosphere to destroy a target that is considerably softer than a missile. According to one DoD official involved with the YAL-1, "we found in all our



Figure 4

studies that the higher [the ABL] went, the better it could do because of the reduction in atmospheric turbulence and distortion...If you look up [at spacecraft], you're not looking through the atmosphere.... It's much easier."²² Outside of the United States, Russia has already developed an airborne laser testbed, on a modified Il-76 *Candid* transport plane (See Figure 4), although this aircraft is not believed to be currently operational.

Space-based antisatellite lasers could emerge by the mid-twenty-first century in the arsenals of peer or near-peer competitors. Although development has slowed since the

²¹ "India: Russia Shows Willingness To Offer Laser Technology," *Delhi Financial Express* (Internet version) December 18, 1997, FBIS Transcribed Text Document: Near East/South Asia, FBIS-NES-97-352, December 22, 1997.

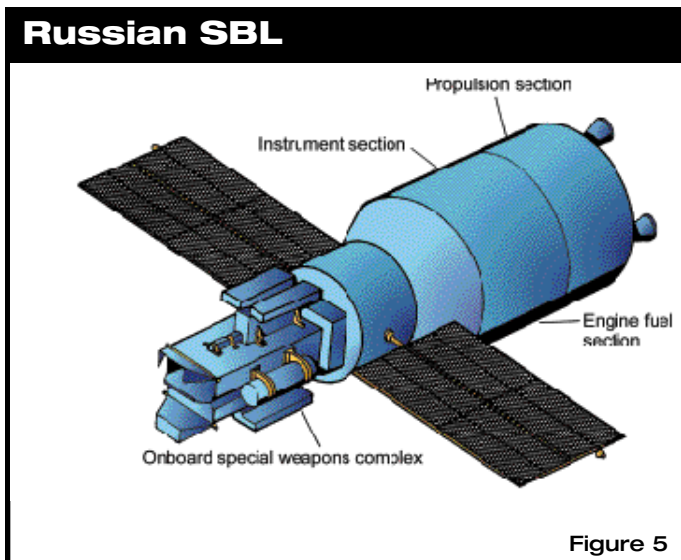
²² David A. Fulghum, "Laser Offers Defense Against Satellites," *Aviation Week & Space Technology*, October 7, 1996, p. 27.

end of the Cold War, both the United States and Russia continue research programs for space-based lasers, primarily as part of strategic antiballistic missile systems, but with implicit ASAT capabilities. Cost is clearly a major concern in addition to imposing technical hurdles. Perhaps the most significant technical challenge relates to the enormous power quantities these systems use. Consequently, SBLs must devote much of the volume within the satellite to laser power generation, leaving little space for fuel to maneuver the system. For their part, Russia had planned to overcome this limitation by fielding a mix of laser- and missile-armed space stations. Like the aforementioned ASAT space station, the Russian space-based laser would normally be operated autonomously, but could be manned

in times of intense operations.²³ Before the Cold War ended, the Soviet Union planned to have six of these space-based lasers (See Figure 5) operational by the early 1990s.²⁴

Electronic and Information Warfare. Satellite operations depend upon reliable communication links with ground stations many thousands of kilometers away. Such an extended distance provides adversaries with a number of opportunities to disrupt, override, or alter unprotected transmissions because a number of satellite functions are theoretically vulnerable to electronic interference. The most mission-critical may be attacked in what is termed a "front door" manner, which targets communications and TT&C (telemetry, tracking, and command) operations. "Back door" threats, on the other hand, attack the more generic satellite functions, including power, altitude control, thermal control, and propulsion.²⁵ In addition to such electronic interference with satellite communications, the possibility remains that adversaries may employ information warfare methods, including computer viruses and malicious software.

Currently, both front and back door jamming of military satellites is difficult, but future technological



²³ Zaloga, *op cit.*

²⁴ Hobbs, *op cit.*

²⁵ Myron L. Cramer, Floyd A. McLaurin, and Stephen Pratt, "Space Systems Electronic Warfare," *Space Electronic Warfare Countermeasures Handbook*, Chapter 51, JCL/TPEW, available through Surviac, 1993. Obtained from <http://infowar.com/survey/space.html>.

FUTURE CHALLENGES

To U.S. Space Systems

advancements are expected to make it a less difficult task in the future. Electronic warfare is a fast growing discipline. Considering the degree to which a number of the world's militaries are investing significant levels of resources in EW capabilities, it is conceivable that regional powers may develop systems capable of interfering with U.S. military satellites. Of greater concern is the heightened vulnerability of commercial providers to such interference. Most private satellites are not hardened to operate in a nuclear environment, and such systems often do not employ frequency-agile transmitters or other counter-measures to protect against jamming. Moreover, such systems almost always operate on publicly known frequencies, rendering transmissions even more susceptible.

In early 1997, as a result of a dispute over utilization of an orbital slot, the Indonesian Pacifik Satellite Nusantara (PSN) Corporation allegedly jammed communications of a Hong Kong satellite. This Apstar-1A geostationary communications satellite was placed in an orbital slot by the tiny Pacific nation of Tonga and leased to Hong Kong. Indonesia accused the TongaSat Corporation of renegeing on a 1993 agreement. TongaSat claimed the agreement was temporary, but PSN claimed it was permanent and subsequently jammed satellite communications.²⁶

In addition, the next century may see the emergence of more insidious threats, including any number of information warfare techniques, such as transmitting computer viruses and spoofing. Just as with electronic warfare, military assets will certainly be affected by IW attack. However, commercial satellites will likely be far more vulnerable. Nations and non-state actors around the world have acknowledged the emerging importance of IW—on its own and as a component of a more comprehensive strategic campaign. Space systems are known to be an integral part of the U.S. information architecture; therefore, military and commercial systems are attractive targets for attack.

The manner in which offensive IW operations may affect satellites cannot be understated. Satellites require precisely written software to function as designed. Even a slight corruption of the coding can totally degrade the performance of a system (as the year 2000 "millennium bug" concerns have illustrated).²⁷ Navigation satellites, for example, rely on precise software-driven timing to coordinate the satellites with one another and to send messages to receivers on the ground. If the software is interfered with, information will be improperly calculated or distributed.²⁸

²⁶ "Tonga Accuses Indonesia of Jamming Satellite Signals," *Satellite News*, March 3, 1997.

²⁷ See, for example, Francis Hammit, "Geo-referenced Images, GPS, and the Year 2000 Problem," *Advanced Imaging*, July 1997, p. 24.

²⁸ GPS software has been stolen by international hackers from Pentagon computers, see Harry Summers, "Achilles Heel of the Military," *Washington Times*, April 30, 1998, p. A18.

In many cases, moreover, a successful IW attack against satellite operations may not be recognized for what it is. According to one GAO report:

Since...1992, DISA [the Defense Information Systems Agency] has conducted almost 38,000 attacks on Defense computer systems to test how well they were protected. DISA successfully gained access 65 percent of the time. Of these successful attacks, only 988 or about 4 percent were detected by the target organizations. Of those detected, only 267 attacks or roughly 27 percent were reported to DISA. Therefore, only about 1 in 150 successful attacks drew an active defensive response from the organizations being tested.²⁹

Another related and growing concern is the fact that adversaries may be able to override legitimate commands, in effect commandeering a satellite. If a signal sent to a satellite is stronger than the legitimate transmission, the original commands may be overridden. Satellites could therefore be instructed to shut down, move to a different orbit, or even conduct operations for unauthorized users.³⁰

Attacks on Ground Stations. Perhaps the easiest near-term way to counter U.S. satellite systems is to attack the ground stations necessary for satellite communications and operational control. As would be expected, commercial downlink facilities are the more vulnerable to terrorist or sabotage operations, since their locations are generally publicly available and they tend to be less well protected than their military counterparts.

Nevertheless, even some vital government-operated ground stations are vulnerable to attack. The Global Positioning System, for instance, is dependent upon just five ground-monitoring stations (located at Colorado Springs, Hawaii, Ascencion Island, Diego Garcia, and Kwajalein Atoll) and three ground-based uplink antennas (located at Ascencion Island, Diego Garcia and Kwajalein) which track and control the system. The monitoring stations and antennas use GPS receivers to track the navigation signals on all satellites, which is then processed at the Master Control Station, operated by the 50th Space Wing's 2nd Space Operations Squadron at Falcon Air Force Base, Colorado.³¹ If any of the ground monitoring stations or antennae were destroyed, a significant proportion of the twenty-four-satellite constellation could be rendered inoperable. Furthermore, the downlink stations and antennae are

²⁹ GAO Executive Report B-266140, obtained from http://www.infowar.com/CIVIL_DE/gaosum.html-ssi#APPX.

³⁰ Pat Cooper, "Pentagon Eyes Ways to Counter Commercially Available Threats," *Defense News*, August 12-18, 1996, p. 18; and "Army: U.S. Needs Next-Gen Self-Protected GPS," *Military Space*, July 21, 1997, p. 6.

³¹ GPS System Summary, http://doradus.einet.net/editors/john-beadles/sum_sys.htm#control_seg.

FUTURE CHALLENGES

To U.S. Space Systems

unmanned, which could render them attractive targets for potential adversaries.³²

Even though conventional military or WMD attacks on ground-link stations are a distinct possibility, such a threat soon may be supplanted by more innovative, if less physically destructive, methods. Radio frequency (RF) weapons, for example, may emerge as a preferred covert method to attack ground-based satellite control stations. Designed to disrupt any system or platform dependent upon electronic circuitry, radio frequency weapons emit a powerful pulse of electromagnetic energy which induces a high-voltage surge in electronic components, overloading their capacity, burning out their circuits, and causing system failure. If placed within line of sight of a ground monitoring station, such a weapon would leave little physical evidence of use, but could destroy much of the electronic circuitry within its range envelope.

In short, the means with which U.S. space operations can be disrupted range from the obvious to the covert. Some of the means for disrupting U.S. space operations are more easily employed than are others, some could pose near-term threats to U.S. space assets, others are clearly long-term possibilities. All, however, pose reason for concern.

How Might Other States Seek to Limit the United States' Use of Space Assets?

To illustrate how the various methods for interdicting space capabilities could be employed in some future crisis situation, it may be of value to discuss a few hypothetical scenarios. In some cases, specific country names are cited. However, this citation is not to imply that the author is predicting a conflict with any of the countries named.

First scenario. Conflict between North and South Korea within the next five to ten years. North Korea has developed an extensive unconventional warfare capability. It is also believed to have 1-5 nuclear weapons. It is uncertain, however, if North Korea has been successful in gaining access to any of the fissile material believed to be leaking out of Russia.³³ In the time frame cited, the United States is likely to be using primarily government owned satellites for imaging with some supplemental capability being purchased from commercial firms. Communications will be provided by a mix of government and commercial space assets. North Korea will understand the need to deprive the United States of at least some of its space assets.

Within this situation, North Korea would most likely use its unconventional warfare forces to

³² Hammit, *op cit.*

³³ For insight into Russia's fissile material security problem, see Institute for Foreign Policy Analysis, *A Study on Exploring U.S. Missile Defense Requirements in 2010*, April 1997, Chapter 2.

try to destroy the ground stations that link to and control U.S. space assets.³⁴ It may also use some of its missile capability to try to interdict a couple of the United States' imaging satellites during the critical first day or two of the conflict. As can be seen by the chart (Figure 6) showing U.S. satellite orbits over Tehran, Iran, the United States does not maintain continuous coverage over any point on the earth. By disrupting a few selected U.S. space assets at a critical juncture, a hostile country could hide critical troop movements at a time when battlefield information would be at a premium.

It is also possible that North Korea could detonate a nuclear device in space above the Korean peninsula in the weeks or months leading up to the crisis. They could do so hoping that the display of nuclear capability could deter the United States from entering the coming confrontation with South Korea. Unfortunately, the other effect of such a burst would likely be the fairly rapid elimination of all commercial satellite capability in LEO (See Figure 7).³⁵ Within less than two months of a 50-KT burst at 120 kms altitude, radiation effects would eliminate all low earth orbit commercial satellite constellations.

In short, under the conditions noted in this scenario, North Korea could destroy the commercial satellite assets in LEO without destroying human life, intimidate the United States in the face of a crisis situation on the Korean peninsula and, if conflict occurred, may well be able to deny the U.S. some access to critical space assets during the first 24-48 hours of the conflict.

Second Scenario. Five to ten years in the future, an Arab-Israeli crisis develops. In an effort to hide military preparations, both sides engage in activities designed to limit the other's access to space-based assets. Some of the Arab countries are assumed to have recently purchased a few Russian MiG-31s

ASSESSED NEAR-ZENITH FIRING OPPORTUNITIES Against 'KH 11-7', 'KH 11-8', 'Lacrosse 1' and 'Lacrosse 2' from Tehran, 15-20 March 1992 ¹				
Satellite	Date GMT	Trajectory	Maximum Elevation (degrees)	Minimum Range (kilometers)
KH 11-7	15 Mar92	N to S	84	905
Lacrosse 1	16 Mar92	SW to NE	81	675
Lacrosse 2	16 Mar92	S to NE	71	720
KH 11-8	17 Mar92	N to S	77	260
Lacrosse 1	18 Mar92	SW to NE	78	675
KH 11-8	18 Mar92	S to N	80	660
Lacrosse 1	20 Mar92	SW to NE	76	660

* Extracted from Thompson, op. cit. Figure 6

³⁴ According to a North Korean expert, North Korea's military planning calls for extensive use of sabotage teams and unconventional warfare forces to attack and destroy command, control, communications, missile defense sites, and the like. In essence, North Korea plans to use people as a replacement for long-range strike capabilities. Conversation with Joseph Bermudez, Jr., March 1997.

³⁵ Information derived from R.C. Webb, Lew Cohn, Joan Pierre, and Al Constantine. *The Cost Differential to Radiation Harden DoD Space Assets*, Defense Nuclear Agency presentation to American Defense Preparedness Association C'I symposium, U.S. Air Force Academy, March 27, 1996; and R.C. Webb, Briefing the U.S. Army Space and Missile Defense Command, May 13, 1998.

FUTURE CHALLENGES

To U.S. Space Systems

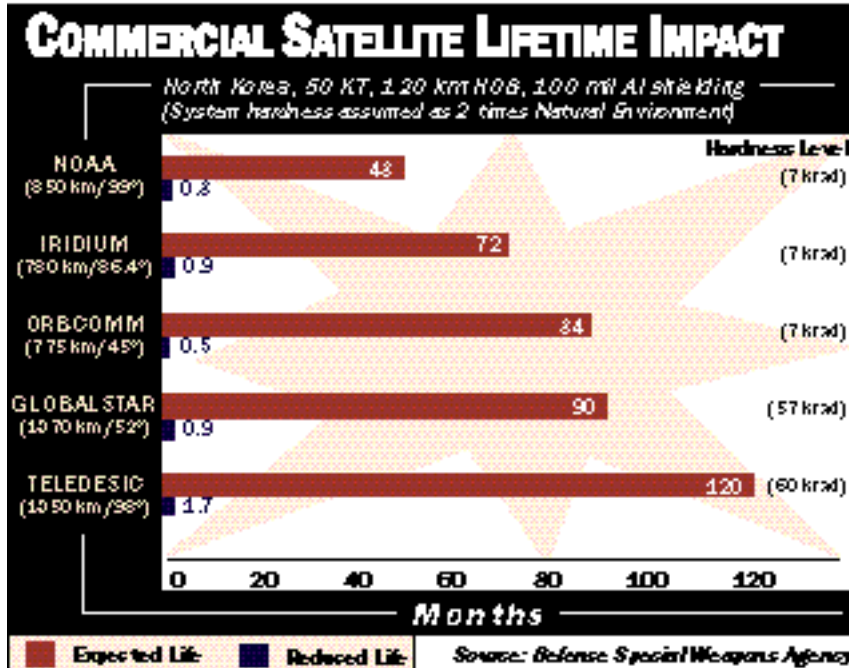


Figure 7

modified for launching small satellites into LEO.³⁶ In this scenario, the payloads on the rockets launched by these aircraft had been modified to provide direct ascent ASAT capabilities. In an attempt to deny Israel information on war preparations, the MiG-31s begin to launch attacks against Israeli reconnaissance satellites. Soon after, computer viruses begin to infect selected communication links and ground stations over which Arab countries were receiving some of their commercial imagery (due to Internet links and commercial cell phones, not all of the imagery will be stopped).

The Arab countries suspect that Israel is behind the disruptions and worry that Israel still has access to commercial systems. This worry is exacerbated when the United States is successful in getting the commercial satellite imaging companies to exercise shutter control when over Israel. Soon thereafter, a missile is launched from the Pakistani-Iranian border region carrying a 50-KT nuclear weapon which burst at 250 km altitude over the Indian Ocean.³⁷ Some satellites in LEO die immediately due to direct detonation effects. Within a week, other commercial satellites begin to go silent and in

less than two months, all commercial satellites in LEO are non-functional. There is some uncertainty if the nuclear weapon used originated in Iran or Pakistan.

As tensions mount and diplomatic efforts fail to end the crisis, Arab armies prepare to invade Israel; however, Israel seems well informed of Arab troop movements. The Arabs suspect that the United States is providing satellite imaging from its National Technical Means to Israel. Just prior to launching the attack, several Arab countries begin to engage U.S. reconnaissance satellites, using modified MiG-31 space-launch aircraft and

³⁶ Safronov, *op cit.*

³⁷ According to research conducted by the U.S. Defense Special Weapons Agency, a 50-KT burst at 250-km altitude will destroy the commercial satellite constellations in LEO slightly faster than would the same size burst at 120 km. See *ibid.*

ballistic missile systems mounting crude ASAT warheads of moderate effectiveness. Concurrently, a couple of medium-powered lasers focus on the U.S. imaging satellites as they passed over in an attempt to disrupt their collection capability.

In short, a conflict of this type could spread in a ripple effect to negate selected space-based capabilities.

Third Scenario. China begins serious preparations for an invasion of Taiwan 10-12 years in the future. By that time, China will have perfected its technology for interdicting the global positioning system (GPS), will likely have a capable terrestrially-based ASAT system, and may have a rudimentary ASAT capability in space (although this time frame is probably 5-10 years too early for that development).³⁸

As tensions mount and Chinese preparations for an invasion of Taiwan become increasingly obvious, the United States begins the deployment of naval assets into the region. To pressure Taiwan, China begins to attack key military nodes in Taiwan using conventionally armed cruise and ballistic missile systems, many of which are equipped to navigate using GPS signals. In an attempt to limit damage to critical Taiwanese defenses, the United States blocks the

commercial GPS signal to that region (as the next generation GPS system will be equipped to facilitate). In retaliation, China begins ASAT attack against GPS satellites.

The United States moves its naval task forces close to Taiwan. The first three U.S. warships to enter the Taiwan Strait are sunk by shore-based supersonic cruise missiles. The U.S. retaliates by striking several missile installations near the Chinese coast. The United States' ability to assess the situation is disrupted by massive problems in its satellite control and downlink systems as computer viruses corrupt the software and satellites change orbits without being so ordered by U.S. ground control. Commercial imaging satellites passing over China stop responding and are believed to be inoperable. It is suspected that China is using lasers or high-energy directed microwaves to destroy these systems. As Chinese landing forces are reported by Taiwanese authorities to be embarking for the invasion, China informs the United States that the conflict is a national issue and that the United States is to stay out. China hints that it will conduct a limited nuclear strike against one or more U.S. targets if the United States involves itself in this domestic issue. In this case, the United States is uncertain of the status of China's ICBMs due to the disruption of space operations.

³⁸ China is working to obtain the capabilities cited. Chinese scientists claim that other medium powers also have ongoing ASAT research efforts. See John A. Tirpak, "The Rise of Space," *Air Force Magazine*, August 1997, p. 54; and Alastair I. Johnston, "China's New Old Thinking," *International Security*, Winter 1995/96, pp. 23-26, to include footnote 60.

FUTURE CHALLENGES

To U.S. Space Systems

In short, the ability to cripple U.S. space assets would raise strategic uncertainty. In many cases, the U.S. would be unable to prove that China was attacking its satellite systems since the satellites have no sensors that can detect and report the attack.

In the three hypothetical scenarios described above, the United States lost critical space assets, yet, in most of the illustrative cases cited, no human lives were lost as a result of counter-space activities. In a world with increased capabilities to retaliate with weapons of mass destruction, the issue of how to deal with attacks against space assets promises to be one of the more vexing political issues which will confront policymakers in the twenty-first century.

Potential Courses of Action

The United States has a space policy that advocates free access to space and a U.S. commitment of the development of space control capabilities. Unfortunately, it has not yet been determined how this policy can or will be implemented. Most officials involved with space issues doubt the United States will be willing to go to war if a potential adversary should attack U.S. space assets or conduct a nuclear test in space that results in the

destruction of the commercial space assets in LEO.

The issue of commercial space assets will be critical for future military operations. The number of U.S. government-owned space assets will be inadequate to provide sufficient resources to establish the degree of information dominance which futuristic military plans envision. Consequently, U.S. government assets will have to be supplemented by commercial assets. Yet, as shown in the foregoing, commercial assets are not hardened against unnaturally high radiation levels. As a result, a 50-KT exoatmospheric nuclear burst will destroy all unhardened satellites in LEO. Without the commercial assets, military operations will be hampered as critical functions will be curtailed by communication interruptions, and intelligence officers will have difficulty determining enemy order of battle and force dispositions, especially if enemy troops are on the move.³⁹

Clearly, the United States needs to act to lessen the future vulnerability of its space assets. The actions that will be needed include:

- Induce commercial satellite firms to increase the level of radiation hardening of selected key assets required to support U.S. military contingency operations.

³⁹ An intelligence officer who served in *Desert Storm* related that the satellite imagery he received only showed half of the battle area every 12 hours. Twelve hours later, he would receive the other half. He was thankful that Saddam Hussein left his forces in place because the U.S. would have had great difficulty determining which of the forces in the new satellite update had been simply moved from other portions of the battlefield during the last 12 hours. He noted that if the Iraqi forces had been mobile, it would have been much more difficult to track Iraqi operations with satellite assets. Personal conversations with author, 1992.

- Develop the technology needed to equip selected satellites with attack warning devices, so that U.S. ground command is aware that its assets are under hostile attack.
- Insure that encryption technologies used in the control of both commercial and military satellites are as strong as possible.
- Review ground station security with a view of either strengthening security procedures or providing sufficient redundancy so as to assure access to space products.

Conclusions

It is clear that space assets will become increasingly vulnerable in the future as more and more countries develop the wherewithal to disrupt the systems. If the United States continues to downsize its military under the premise that information dominance will permit smaller forces to dominate larger industrial-era armies, then the issue of space control will have to be addressed as a matter of national priority. More research is required on this subject, both in terms of technical needs and policy implementation requirements.