Threats to United States Space Capabilities

Tom Wilson
Space Commission Staff Member

Prepared for the Commission to Assess United States National Security Space Management and Organization

The information presented in this paper is based on research done by the author. Although it was prepared for the Commission in conjunction with its deliberations, the opinions expressed in this paper are those of the author alone and do not represent those of the Commission or any of the Commissioners.

Table of Contents

I. Introduction

The employment of space systems increases the effectiveness of terrestrial warfighters by performing as a force multiplier. In peace, space systems are a key element of deterrence. In crisis, they provide a wide spectrum of options to the National Command Authorities and Commanders in Chief while providing confidence to our allies. In war, space systems enhance combat effectiveness, reduce casualties and minimize equipment loss.

At the same time, the United States' (U.S.) increasing economic and military dependence on space creates a vulnerability that is an attractive target for our foreign adversaries. If adversaries are able to employ offensive counterspace operations—operations which are intended to deceive, disrupt, deny, degrade, or destroy U.S. space systems—the force multiplication effect they provide would be reduced or eliminated. This could lead to more expensive victories or even to defeat.[1]

Current trends such as technology proliferation, accessibility to space, globalization of space programs and industries, commercialization of space systems and services, and foreign knowledge about U.S. space systems increases the likelihood that the U.S. will experience a "Space Pearl Harbor." For example, in July 2000, the Xinhua news agency reported that China's military is developing methods and strategies for defeating the U.S. military in a high-tech and space-based future war. It noted, "For countries that could never win a war by using the method of tanks and planes, attacking the U.S. space system may be an irresistible and most tempting choice …"[2] These reports illustrate an unpleasant but little noticed view of the future.

The ability to restrict or deny freedom of access to and operations in space is no longer limited to global military powers. The reality is that there are many extant capabilities to deny, disrupt or physically destroy space systems and the ground facilities that command and control them. Knowledge of U.S. space systems functions, locations and physical characteristics, as well as the means to conduct counterspace operations, is increasingly available on the international market. Nations or groups hostile to the U.S. possess or can acquire the means to disrupt or destroy

[1] Department of Defense Studies, 2000, p. 4.
[2] Al Santoli, "Beijing Describes How to Defeat U.S. in High-Tech War," *China Reform Monitor*, 10 October 2000.

U.S. space systems by attacking the satellites in space, their communications nodes on the ground and in space, or ground nodes that command the satellites.

Offensive counterspace operation technology is spreading throughout the world. Even so, some types of antisatellite (ASAT) weapons are obviously more complex to design, build and test than others. Kinetic and chemical interceptors, conventional guns, and low power lasers are the least sophisticated. Nuclear weapons and radio frequency weapons are more complex. High-energy lasers and particle beam weapons are the most sophisticated. Note that this rating should not be considered by itself, as the use of a complex weapon could make other aspects of the overall system simpler. For example, using a nuclear weapon on an interceptor makes virtually every other aspect of system development less complicated since its lethal radius is large.[3]

The U.S. reliance on space, coupled with the growing amount of information available about our space systems, increases the likelihood that our adversaries will employ counterspace weapons technologies. Of concern is the likelihood that today, the U.S. has neither the doctrine nor the means to respond to potential counterspace threat situations.

II. Scope

Space threats can be viewed from two different perspectives: direct threats to U.S. space systems and threats to U.S. military forces from foreign use of space systems. Although this paper will focus on the former, it is important to recognize that there is a growing threat from the adversarial use of widespread space capabilities and technologies. Today, small nations, groups or even individuals can acquire, from commercial sources, imagery of targets on earth and in space. They can acquire accurate timing and navigational data and critical weather information generated by government-owned satellites. Improved command and control capabilities are available through the use of commercial communications satellites. Even launch capabilities can be contracted for with legitimate companies. At the same time, a number of smaller nations are developing their own space launch vehicles.

[3] Department of Defense Studies, 2000, p. 1011-1012.

This paper examines direct threats to U.S. space systems, the potential impact of execution of these threats, and potential countermeasures to these threats. It begins with the fundamental knowledge base for conducting counterspace operations—space object tracking and identification capabilities.

III. Space Object Tracking and Identification Capabilities

Foreign knowledge of U.S. space operations is a necessary precursor to the successful conduct of counterspace operations or camouflage, concealment, and deception (CC&D) activities. Potential adversaries and competitors can learn about U.S. space systems and operations using standard HUMINT, SIGINT or IMINT[4] intelligence collection techniques, as well as through dedicated space object surveillance and identification (SOSI) systems.[5] More recently, with the advent of amateur satellite observers posting data on the Internet, the availability of intelligence regarding U.S. space system capabilities and orbital locations is increasing available to U.S. adversaries. Satellite situational awareness databases are maintained by organized clubs and organizations, which readily publish their information on Internet web pages such as those of the Federation of American Scientists and several Universities.

In addition, knowledge of a satellite's position and velocity can now be obtained with relatively unsophisticated optical, radar, and signal tracking systems. Advances in focal plane and other technologies have enabled ground based optical space object tracking systems smaller than a meter in aperture to acquire, track, and, in some cases, image objects out to geosynchronous orbits (GEO) and beyond. As an example, using a 35mm camera, an amateur satellite observer can capture an image of a satellites track in low Earth orbit (LEO).

The proliferation of air and theater missile defense radars, such as those associated with the SA-10, have enabled many countries, such as China (who purchase these radars from Russia), to field space-based tracking systems capable of accurately locating objects in LEO. These mobile radars were originally designed to track reentry vehicles but, due to their low-cost and mobility, are attractive as space-based object trackers as well.

[4] HUMINT, SIGINT and IMINT are intelligence derived from human, signal and imagery sources and methods.
[5] Department of Defense Studies, 2000, p. 1.

The increasing dispersion of satellite communications terminals has increased our adversaries' capability to target our space systems by locking onto the satellite's transmit and receive signals. Geosynchronous satellites, by virtue of their typically 'fixed' position, are particularly vulnerable to this type of acquisition and tracking.

Many countries also have the capability to deploy sophisticated networks of space object surveillance and identification (SOSI) sensors to observe the satellites of concern. Countries that have been unable to develop such sensors indigenously can acquire them commercially. Suitable sensors include radars, optical telescopes, passive radio frequency (RF) and in some cases satellite signals intelligence (SIGINT) receivers.

A. Non-Government Satellite Observers

Non-government satellite observers (NGSOs) are amateur observers in countries such as the United States, the United Kingdom, Canada, Australia, South Africa, Belgium, France, Germany, Finland, Sweden, and the Ukraine. These NGSOs are organized and networked to provide common databases from which satellite element sets—data sets that can be used for accurately locating a satellite at a specific point in time—are developed. The data is shared through voice, facsimile, electronic mail, and Internet discussion groups, such as electronic bulletin boards and on-line service forums. The NGSOs obtain their data from visual tracking, radio signals and official government sources such as United States Space Command and NASA's Goddard Space Flight Center, which routinely release and publish element sets for unrestricted satellites.

Traditionally, NGSOs have gained orbital information through measurements based on optical observations. The NGSO's ability to optically track the satellite is largely determined by the amount of sunlight that is reflected by the satellite to the observer. This reflectance or satellite brightness is affected by the satellite's: orbit and inclination, reflectivity of its surface and components, size and attitude. Optical observation measurements are typically made with the aide of binoculars, such as 7 x 50, or astronomical telescopes, a star atlas and a stopwatch accurate to 0.1 second. NGSOs claim that geosynchronous orbit satellites can be tracked using an eight-inch telescope.

Using commercially available satellite orbit prediction software, satellite element sets available on the Internet, and a star chart, the NGSOs are able to determine the target area to be searched. The satellite's position is determined by: recording the time when the target satellite passes between two close stars or past a single star, comparing the "eyeballed" position to a star atlas, then interpolating the position at the recorded time. Experienced observers can find a satellite in as little as one minute of searching or as much as one-half hour for lower orbiting and maneuverable satellites. The accuracy of the orbital element products depend on the observer's ability to "eyeball" the satellite between the reference stars, the speed at which the satellite is moving, the quickness of the time measurement and the availability of existing element sets on the satellite.

Since the launch of Sputnik in 1957, NGSOs have also used satellite radio signal reception to track satellites and provide information on mission type. The tracking is enabled because of the Doppler shift that is experienced as a satellite passes overhead. As a satellite approaches, its frequency strength increases to its strongest point directly overhead, then decreases again as passes over the observer. The NGSOs use a short-wave receiver, an antenna, a tape recorder and an accurate timepiece for this type of observation. The NGSOs can also get orbit and frequency information from the International Telecommunications Union (ITU).

The NGSOs are able to track satellites in low earth (LEO), geosynchronous (GEO), and highly elliptical (HEO) orbits. These amateur observers have also observed boosters conducting burns while in the process of delivering payloads to orbit. NGSOs claim good accuracy results from these types of observations. NGSO capability is considerably improved by the sharing of observational data and element sets on amateur satellite tracking bulletin boards found on the Internet. Examples of specific details on these NGSO Internet sites are as follows:

- The German Space Operations Center hosts a web site that is frequently used by NGSOs. The web site is at http:// www2.gsoc.dlr.de/scripts/satvis/satinfo.asp?SatID=satellite#. This site provides anyone with Internet access the most current element set for a given satellite along with other orbital data, visual brightness data, and a map with its current position over the earth.

- One of the most renowned amateur groups is the Kettering Space Observer Group of England. The group originated with the Kettering Boys School; its primary interest was observations of

Soviet satellites. The group's collection capabilities include reception of radio signals and “electronic intelligence (ELINT) type transmissions.” The group has reportedly even received data from the then Soviet Cosmos satellite, which it subsequently translated into imagery. The advanced techniques used by the group enable it to be considered experts in analyzing orbits and missions.

- The Royal Astronomical Establishment (RAE), formerly part of Britain's Ministry of Defense but now privatized, has a close working relationship with the Kettering Group. The RAE takes observations made by the Kettering Group to estimate satellite populations and status. The resulting lists are then published and sold to the public.

- The Belgium Working Group Satellites (BWGS) is a network of amateur observers actively involved in monitoring satellites, particularly “spy” satellites. Members of this group, approximately 40 people worldwide, post their observations electronically where they are reviewed and commented on by observers from around the world. The BWGS group has been making observations since 1987. The group is part of the Belgian Astronomical Society (VVS, Vereeniging voor Sterrenkunde).

- The Canadian Space Society (CSS) of Toronto is the apparent focal point for an international group of amateur satellite observers. Members of the group relay observational data via voice and electronic mail to a coordinator who uses a personal computer to generate element sets. The group reportedly has observers in Australia, Canada, Europe, Scotland, South Africa, and the United States.

- The Federation of American Scientists (FAS) was formed in 1946 “to act on public issues where the opinions of scientists are relevant, those which affect science or in which the experience or perspective of scientists is a needed guide.” FAS collects observational information from amateurs around the world and uses the information to track satellites.

- The University of Surrey's Electronics and Amateur Radio Society (EARS) has demonstrated an impressive capability to track and command amateur satellites. The EARS facility is entirely student developed and operates UHF and VHF receivers and transmitters.

> The university's computer system is used for orbital analysis. Students have been able to achieve a tracking accuracy of 0.5 degrees.

These satellite tracking web sites provide amazingly accurate satellite overflight times, pass durations, and revisit times for several hundred satellites, rocket bodies, and debris that are observed by amateurs. With this level of information it is possible to employ some of the less sophisticated counterspace threats, such as denial and deception and high-power radio frequency weapons. However, some of the more sophisticated counterspace threats, such as high-powered lasers and direct-ascent hit-to-kill vehicles, require more precise tracking information. Many countries have the capability to precisely track and identify space objects using advanced optical, radar, passive RF and SIGINT tracking systems.

B. Optical Tracking and Imaging Systems

The goal of any method of satellite tracking is to determine where a satellite is and where it is going. One of the most common techniques for making these determinations is to use either film-based or electro-optical cameras to measure the distance between the satellite and reference stars at various points along the satellite's track. Reference star’s positions are well known and documented in catalogs such as the Smithsonian Astrophysical Observatory (SAO) star catalog. With these pieces of information the position of the satellite and its orbit can be accurately calculated. These systems are in general low cost and easy to use, which makes them attractive to amateur astronomers and third world countries. Many countries including the U.S., Russia, China, Japan, France, Germany and Australia have active space object optical tracking and imaging systems.[6]

Film-based systems use the telescope to track the apparent motion of the stars, causing them to appear as single points. Simultaneously, time is recorded on the film as a shutter periodically moves across the film plate which causes the satellite's path to appear as streaks across the film. The position of the satellite is then determined by comparing known stars with the time and position of the blank portions on the streaks of the satellite's path. Although time-consuming (processing the film and taking measurements from it can take from one to several hours) this process can

[6] Grant Stokes, “Asteroid Search Systems, Present and Future,” Massachusetts Institute of Technology Lincoln Laboratory, 28 September 00.

provide a high degree of accuracy. Under ideal conditions, satellites can be accurately located to within three arc-seconds (arcsec), or about 530 m at geosynchronous range.[7]

Electro-optical based systems, such as vidicon tubes or charge-coupled device (CCD) detectors, eliminate film development time by using the digitized information from the detectors for parameter calculation. By using fast electro-mechanical devices and computers, the time to calculate accurate orbital elements can be significantly reduced. If one is willing to use sophisticated models and considerable data processing resources to eliminate errors, this technique can provide accuracies approaching one arcsec. Very dim objects can also be tracked by moving the telescope with the tracked object to increase the exposure time. However, since the operator or sensors cannot verify acquisition of such dim objects until after integration, the trajectory of the object must be known before the tracking sequence.[8]

The advantages of tracking satellites with optical systems include:[9]

- Satellites at geosynchronous altitudes can be tracked with telescope apertures on the order of one meter, making them less per unit basis when compared to radar tracking capabilities with the same range. (Telescopes with apertures of less than 0.5 m can track also geosynchronous satellites provided sensitive detector arrays or long exposure times are used.)

- Higher precision measurements than radio frequency systems because light wavelengths are shorter than radio frequency wavelengths.

- [2] A satellite cannot detect that it is being tracked by a passive optical system since the Sun is being used as a transmitter; the optical site does not give away its location in performing the optical observation.

- Satellites in lower orbits can be imaged with telescopes a few meters in diameter and larger.

The disadvantages of tracing with optical systems include:[10]

[7] Department of Defense Studies, 2000, p. 332.
[8] Ibid., p. 333.
[9] Ibid., p. 329.

- To see the reflection of the satellite, the tracking site must be in darkness while the Sun illuminates the target.

- Inability to track during adverse weather. Clouds, fog, and dust may severely reduce an optical system's ability to function.

- Optical systems have no starting time reference since they use the Sun as a transmitter. Therefore, these systems cannot directly measure range information. One exception would be to use several optical tracking sites to simultaneously track an object. Triangulation calculations on the resulting track data would yield the range of the target.

- Limited search capabilities.

- Relative low object tracking rate capability.

There are many research and development efforts under way to improve the capabilities of optical tracking and identification systems. These improvements include:[11]

- Passive daytime optical tracking. By using visible light filters and narrow field of view optics, or the infrared (IR) signature of a satellite viewed against the cold background of space, low earth orbit (LEO) satellites can be tracked during daylight hours. However, certain constraints on the relative location of the Sun, the satellite, and the viewing instrument still apply. No operational systems are known to be deployed in foreign countries.

- Laser rangefinder (LRF). An LRF uses light in the same way radars use radio waves to measure the round trip transmission time to an object to directly determine its range. However, using an LRF for satellite ranging requires the satellite to carry retroreflectors to reflect the laser light pulse back to its source. Foreign countries are known to have deployed these systems for operational use.

- Technological advances in mirror manufacturing have made it possible to build monolithic (one piece) honeycomb mirrors of approximately eight meters in diameter. In addition, several

[10] Ibid.
[11] Ibid., p. 330, 337.

> telescope projects are planning on using such mirrors cooperatively to form a larger effective aperture, such as the Very Large Telescope (VLT) being built by the European Southern Observatory in Chile. It will use four 8.2 m telescopes to form an equivalent aperture of 16 m. These large optical systems will enable observers to see very dim objects at great distances and can be used to image objects in lower orbits.

C. Radar Tracking and Imaging Systems

Radar tracking and imaging systems use dedicated transmitters to generate electromagnetic radiation to form non-literal images of satellites. Since the system is an active sensor and thus provides its own source of illumination, it is useful at any time of the day and under almost all weather conditions to provide high-volume means of tracking space objects. Because of these facts, radar systems are, in general, more frequently available than visible systems.[12] However, they are most commonly used to provide highly accurate tracking information on spacecraft in low Earth orbit (LEO), typically at an altitude less than 3,000 km, and, due to high cost for the necessary power, are not used to track geosynchronous satellites.[13]

In general, radar systems are of two types: synthetic aperture radar (SAR) and inverse synthetic aperture radar (ISAR). The differences of these two types of systems are thoroughly discussed in recent Department of Defense (DoD) studies as follows:[14]

> In a SAR system, the motion of the target platform relative to a fixed target (such as the surface of the earth as seen from an airplane or a satellite) induces a different Doppler shift to the energy returning from different parts of the scene. This, coupled with the normal time difference of arrival from different parts of the scene that vary in range (additional pulse compression techniques are used to achieve very high range resolution), allows the energy returning to the sensor from the scene to be sorted into range and azimuth bins. By combining data coherently (i.e., phase data must be preserved), it is

[12] Ibid., p. 274-275.
[13] Department of Defense Studies, 1997.
[14] Department of Defense Studies, 2000, p. 274.

possible to integrate data from different pulses and form a non-literal image. As the number of integrated pulse returns increases, the azimuth resolution of the image improves, a result of using a larger “synthetic” aperture (the synthetic aperture results from sensor motion during the imaging event-the more pulses integrated the larger the synthetic aperture and the finer the azimuth resolution), and targets, which are less radar reflective, become more identifiable.

A similar technique, ISAR, can be used to image satellites from fixed ground-based radars. In this case, the relative motion needed to produce the appropriate Doppler shifts is provided by the target (both in terms of the satellites motion about the earth and its angular motion about its center of mass), rather than the imaging sensor.

Radar systems are also capable of providing space object identification (SOI) information. Data obtained by the radar while tracking the satellite results from both its relative motion and its configuration. The data can be used to determine whether the satellite is pointing an instrument at a particular location on the ground and whether changes occur in the orientation and stabilization. Detailed configuration information can determine such things as size and orientation of solar collection panels, size and orientation of antennas, etc.[15]

One example of a highly capable space object tracking radar is Germany's TIRA imaging radar. The tracking radar's detection limit operating as a monostatic system is a 1.8 cm sphere at a range of 1,000 km. Germany's L-band radar was reportedly used to test bistatic operations due to the belief that further improvements in space debris detection and characterization capabilities could only be realized using a more powerful receiver. The plan proposed using the German L-band radar as the transmitter in conjunction with a receiver 21 km away. The 100 m radio telescope at Bad Munstereifel Effelsberg, Max Planck Institute for Radio Astronomy (MPIfR), Bonn, Germany, was used as the receiver. The MPIfR is the world's largest steerable radio telescope. The experiment took place in November 1996 and resulted in 0.9 cm objects being detected at a 1,000 km range.

[15] Department of Defense Studies, 1997.

Another example, found in advertising literature from the Russian Research Institute of Long-Range Radiocommunications (NIIDAR), lists the following parameters for a space object tracking and identification radar called BAKSAN:[16]

- Space Object (SO) detection at ranges up to 3,000 km
- 20 x 20 degree electronic scan
- Efficient Identification and Tracking up to 1,500 km
- Operates in UHF and VHF
- Up to 250 m range error
- 5 arcminute angular error
- Tracks up to 300 satellites in 24 hours
- Five dish interferometer either independent or slaved to phased array
- 20 people to operate
- Set-up and testing up to 6 years
- Cost of 30 million dollars

D. SIGINT and Passive RF Tracking and Characterization Systems

Signals Intelligence (SIGINT) tracking and identification involves the collection and analysis of electronic signals for intelligence purposes. Typical targets for SIGINT collection include space system components that emit electromagnetic waves; either uplink, downlink, or crosslink transmitters. The basic capability to collect communications signals from satellites requires little more equipment than what is used by many home satellite television subscribers.

[16] Department of Defense Studies, 2000, p. 622.

Passive RF tracking involves the use of antennas on the ground to gather tracking information to precisely locate the source of a satellite's signal. Because electromagnetic waves from a satellite's transmitter travel in a straight line, the direction of arrival of the signal is the direction of the transmitter. Directional bearing information on a particular radiator can determine the location of that radiator. Data, from one of the sources discussed in the previous sections, on the location of a satellite can be used as a source for the initial satellite tracking information.

IV. Offensive Counterspace Operations

Offensive counterspace operations involve the use of lethal or non-lethal means to neutralize an adversary's space systems or the information they provide. According to recent DoD studies, offensive counterspace operations are designed to achieve five major purposes:[17]

- Deception—manipulate, distort or falsify information
- Disruption—temporary impairment of utility
- Denial—temporary elimination of utility
- Degradation—permanent impairment of utility
- Destruction—permanent elimination of utility

To accomplish these objectives, four types of offensive counterspace operations are used: denial and deception; attack or sabotage of ground segments; direct antisatellite (ASAT) attacks on space assets; and electronic attack on the communications, data, and command links of the satellites and ground stations. With the proliferation of satellite warning data, denial and deception has become a highly effective means of limiting the information obtained by an intelligence collection satellite. Attacking or sabotaging the supporting ground facilities has long been considered one of the easiest methods for a U.S. adversary to conduct offensive counterspace operations. Most of these facilities are relatively easy to get in close physical proximity to or access by way of a computer network, making them a prime target.

[17] Ibid., p. 3.

The U.S. space assets themselves are also very vulnerable. While some national security space systems have built-in security and countermeasures, most of our government and all of our commercial space assets are vulnerable to a variety of ASAT attacks. The reason for this vulnerability is that the additional cost and weight of the security and countermeasures is regarded as unnecessary when compared to what is incorrectly characterized as a lack of threats to our space assets.

The proliferation of ballistic missile and space technology has made it easier to develop direct ascent antisatellite weapons and to obtain the capability to deliver nuclear warheads into space. Studies have shown that the detonation of a low-yield nuclear weapon in LEO will not only fatally damage nearby satellites but will also increase the naturally occurring radiation around the earth, reducing most LEO satellites lifetimes from years to months. Many countries such as China, India, Iran, Pakistan, and Russia have this capability.

Advancements in miniaturized space systems technology have led to a global proliferation in the use of micro/nanosatellites. Microsatellites (<100kg) and nanosatellites (<10kg) are space systems that are made of the latest composite structures technology, with computing power better than most desktop computers. These micro/nanosatellites, when employed as unacknowledged secondary payloads, can covertly rendezvous with other space assets to perform satellite inspection and other missions to disrupt, degrade, or destroy space assets. Small, low-powered, ground-based lasers can be used to ìblindî optical satellites in orbits out to GEO. With advances and proliferation in stand off weapons technologies, laser, radio frequency and particle beam weapons will likely be available to adversaries in the coming decades.

Electronic attack on the communications, data, and command links, that couple the satellites to their ground facilities and users, is a low-cost method of denying and disrupting the use of space assets. Any country that has commercial satellite communications equipment has inherent electronic signal jamming capabilities against communications satellites. There are also countries that are globally marketing military jamming capabilities such as the Russian handheld Global Positioning System (GPS) jamming system.

A. Counterspace Denial and Deception

Countries can attempt to defeat the reconnaissance function of satellites by obtaining sufficient information about the satellites' orbital and sensor characteristics. This information can be used to either deny access to the reconnaissance targets at critical times or to carry out deception efforts to confuse and complicate their signatures. When more information is made available concerning reconnaissance satellite characteristics, denial and deception are made easier for our adversaries and information collection more difficult for the U.S.

Counterspace denial and deception generally falls into two categories: activities that are designed to react or respond to a specific platform overflight (directed) and routine activities that may not be driven by a specific platform (non-directed). Both directed and non-directed types of denial and deception can employ camouflage, concealment, and deception (CC&D) techniques to deny or corrupt intelligence collection by satellites. Potentially suitable CC&D techniques include:

Passive	
Camouflage	Use of special coverings or coatings to blend the appearance (visual, thermal, radar) of objects into the background
Concealment	Use of coverings or terrain to hide objects from threat sensors
Obscurants	Use of smoke or aerosol clouds to provide a sensory barrier between the threat sensor and the object
Decoys	Use of false objects to overwhelm, confuse, or redirect threat sensors
Corner reflectors	Corner reflectors and similar devices are used to confuse radar sensors and obscure real targets
Communications security	Avoid talking about sensitive subjects over communication links subject to monitoring
Emission control	Turning off emitters when they might be detected by threat sensors
Deception	Allowing threat sensors to "see" certain possibly scripted activities for the purpose of perception management

Active	
Spoofing/masking	Emitting false signals that are similar to real signals to cover the real signals; a type of electronic decoy
Jamming	Emitting noise or some other signal for the purpose of preventing the threat sensor from being able to collect the real signals

B. Ground Segments Attack or Sabotage

One of the easiest ways to disrupt, deny, degrade, or destroy the utility of space systems is to attack or sabotage the associated ground segments. Space system ground segments consist of facilities associated with satellite communications, data reception, command and control, launch, and assembly facilities, and their supporting infrastructure.[18] These specialized facilities are critical to the continued operation and effective use of a satellite. At the same time, these facilities often represent the most vulnerable segment of most space systems because they are subject to attack by a variety of means, ranging from physical attack to computer network intrusion.

While most mission control facilities for U.S. space systems are located within the continental U.S., there are still many of these facilities located outside the U.S., in remote areas, which can make physical security of the site difficult. For example, the Global Positioning System (GPS) has five fixed monitoring stations, and four fixed ground antennas located around the world. The accuracy of the GPS system is highly dependent on contact between the GPS satellites, the five fixed monitoring stations and the GPS Master Control Station in Colorado.[19] Loss of some of the monitoring stations or ground antennas could result in a significant decrease in GPS performance worldwide. If the GPS system were to experience widespread failure or disruption, the impact could be serious. Loss or degradation of GPS timing could disable the majority of pager and cellular telephone networks around the world; disrupt the global banking and financial system, which depends on GPS timing to keep worldwide financial centers connected; and interrupt the operation of electric power distribution systems. Loss of the precision navigation data from GPS could affect search and rescue, as well as air and sea navigation worldwide.

[18] Ibid., p. 8.
[19] United States Army, "Chapter 8: Threats and Countermeasures," in *Army Space Reference Text*, July 1993, p. 2.

There is also evidence that computer network intrusion is increasing. Hackers are routinely probing DoD networks and computers. The U.S. Space Command's Joint Task Force for Computer Network Defense reported that detected probes and scans are increasing, access to hacking tools is becoming easier, and hacking techniques more sophisticated. In 1999 the number of detected probes and scans against DoD systems was just over 22,000; in the first eleven months of 2000, the number had grown to 26,500.[20]

The impact of an attack on space launch facilities would affect the U.S. ability to place new or replenishment satellite systems on-orbit. Due to the fact that satellites are typically designed and built to launch on specific launch vehicles, it is possible to affect one or more specific space systems' capabilities by attacking a specific space launch pad. The impact of an attack would be felt for years. Compounding the problem is the fact that all U.S. space launches, even those conducted by the NRO, are announced in advance.[21]

During the lifecycle of a space system, it goes through integration and test at facilities that are well known and are also susceptible to physical attack. This includes U.S. military satellites as well as commercial satellites. For example, on 10 May 1992, two individuals scaled the fence surrounding the Rockwell facility in Seal Beach, CA. Using false identifications, the individuals penetrated a clean room where the GPS-33 satellite was being assembled and attacked it with axes. Several million dollars worth of damage was done before the two were subdued.[22]

C. Non-Directed Nuclear ASATs

Many people believe that a nuclear detonation in space is the ultimate antisatellite weapon. This is largely because of the relative technical ease of deployment and the fact that every satellite in LEO simultaneously feels the effects of the detonation. All that is needed to conduct a nuclear attack is: a launch vehicle; an unsophisticated nuclear device, possibly bought on the international black market; and a timer or command receiver to assure appropriate detonation altitude. Since the effects of nuclear detonation move out rapidly and permeate all space, no satellites have to be directly

[20] Colonel John G. Boynton, Director of Operations, J3, Joint Task Force-Computer Network Defense, electronic mail, December 20, 2000.
[21] Department of Defense Studies, 2000, p. 10.
[22] Ibid.

targeted. The aggressor can simply aim the weapon at an empty point in space, reducing the requirement for a highly accurate missile guidance system.[23] Many countries hostile to the U.S., such as Iran, North Korea, Iraq, and Pakistan, possess missiles and either have or are suspected of developing nuclear weapons. In addition, there is much evidence that many countries have or are developing the inherent capability to launch a high altitude non-directed nuclear ASAT. The following is a list of recent examples of the extent of missile proliferation events:[24]

- Iran test fired the Shahab-3 based on North Korean Nodong-1 design (1998).
- Pakistan constructed a factory to indigenously build M-11s and test fired the Ghauri (Hatf V) in 1998. A bigger missile, Ghazni, is under development.
- North Korea's Nodong-1 may have entered deployment in 1998 and the Taepo-Dong 2 is in development. North Korea has also sold Scud missiles to Iran, Egypt, Syria, and Libya.
- Libya is continuing its quest for missile components and technology worldwide.
- Syria has recently received an unknown number of M-9 missiles from China.
- Taiwan is developing the Tien Chi missile capable of hitting mainland China.
- China is continuing missile technology sales to Iran, Syria, and Pakistan. It is also acquiring missile technology from Russia and the Ukraine.
- U.S. placed export curbs on Indian firms for their role in India's missile program that developed the Prithvi, Prithvi II, Agni, AgniII. The Sagarika, a nuclear capable sub-launched missile, is also under development (1997).

[23] Mr. Lewis Cohn, Defense Threat Reduction Agency, and Mr. Glenn Kweder, Logicon Advanced Technology, “Third World Nuclear Threat to Low Earth Orbit Satellites,” 16 November 2000, p. 1-6.
[24] United States Air Force, “Directed Energy Master Plan,” June 2000, p. 10.

- U.S. and Israel protested Russian assistance in Iran's missile program (1997).

- U.S. accused Israel of violating MTCR by exporting missile components (1998).

- North Korea successfully launched a Taepo-Dong missile (1998).

The other factor, which makes this type of attack tempting from the perspective of a rogue third world country, is the deniability of hostile intent. The aggressor could claim they were only doing a test and could perform the test in the vicinity of their own country. Since no lives would be lost and no homes destroyed, only the eventual destruction of billions of dollars of satellites, the nature and amplitude of a U.S. military response would be a politically difficult decision.[25]

The detonation of a nuclear weapon at high altitude (above 20-50 km)[26] will produce two devastating effects. The first is High Altitude Electromagnetic Pulse (HEMP), principally of concern to the satellite's ground segment. Second would be a significant increase in the level of LEO ambient radiation, enough to severely damage nearby satellites and shorten the lifetimes of satellites in LEO from years to months or less.

The HEMP signal from a high altitude nuclear burst propagates through the line of sight of the burst. The propagation manifests itself in the form of fairly large magnetic fields over very large areas. For example, detonating a multi-megaton thermonuclear weapon at 100 km over Omaha, Nebraska would cover a circular region with a diameter stretching from Kentucky to Colorado. If the altitude were increased to 500km, the entire continental U.S. would be covered by the HEMP electric field. The effect of the HEMP signal is to cause significant upset, degradation and permanent damage to electrical systems. The extent of the damage depends on weapon yield and design, burst altitude and the characteristics of the exposed electronic equipment. [27]

From the perspective of the ground segment, HEMP is the principal concern from a high altitude nuclear detonation. However, satellites in line-of-sight of the detonation will also feel some effects. Direct radiation can upset or damage satellite electronics and other components. This

[25] Cohn and Kweder, "Third World Nuclear Threat to Low Earth Orbit Satellites," p. 1-6.
[26] Department of Defense Studies, 2000, p. 1292.
[27] Ibid.

situation occurs when electrons produced by the nuclear explosion penetrate the interior of the satellite and deposit their charge, building up large electric fields on dielectrics, including printed circuit boards, solar cell cover slips and thermal control materials (paints, thermal blankets or second surface mirrors). These fields eventually may exceed the breakdown strength of the material and cause a discharge to occur. Energy from the discharge can couple directly into electronic components and cause upset or burnout.[28]

Naturally occurring ambient radiation is present in the Earth's Van Allen belts in the form of highly energetic electrons and protons. Satellite designers consider radiation hardness of electronic components in the design of satellites that will pass through these radiation belts. The total ambient radiation dose a satellite will receive is dependent on its orbit. A byproduct of a high altitude nuclear burst above about 100 km is large quantities of highly radioactive debris, in the form of an expanding plasma, strongly interacting with the Earth's magnetic field.[29] This radioactive debris increases the electron flux levels of LEO orbits within a few hours. The effect is to significantly increase a LEO satellite's ambient radiation environment. The radiation effects can remain trapped in these orbits for months to years, drastically reducing the lifetime of satellites in LEO from years to months or less. As important is the fact that the lingering effects of increased ambient radiation could make satellite operations futile for many months.

In general, high altitude nuclear detonations above +/- 30 degrees latitude tend to affect satellites in orbits above 2,000 km altitude, while detonations between +/- 30 degrees latitude tend to affect satellites impact orbits below 2,000 km. The following is a list of the examples of the affects:

- In 1962, a 1.4 Megaton nuclear weapon was detonated at 400 km over Johnston Atoll in the South Pacific. This event, code name Starfish, produced an enhanced electron environment that was responsible for the early death of four satellites in less than ten days. The radiation belts remained enhanced for 1-2 years.[30]

[28] Ibid, p. 1292-1293.
[29] Ibid, p. 1305.
[30] Ibid.

- The Defense Threat Reduction Agency (DTRA) estimates that a low-yield, 10 kiloton nuclear burst over Japan, at an altitude of 150 km, would dramatically reduce the lifetime of LEO satellites. For example, the Hubble Space Telescope lifetime would be reduced from 15 years to less than a few months. The satellites in the Globalstar and Orbcomm communications constellations would have their lifetimes reduced from approximately 7 years to less than 5 months. Furthermore, if replacement satellites for these communications constellations were launched three months after the detonation, they would only last for less than eight months.[31]

- Recent DoD studies discuss open source reports, which claim that in the early 1960s the Soviets considered using 100 Megaton nuclear warheads for long range ASATs. The system was reportedly intended to give a sure kill, probably using hard x-rays, at a range of 1,000 km. According to these sources, a special ballistic missile was to be developed for just this purpose. The Soviets later abandoned the project, possibly after learning of the less desirable side effects of space nuclear detonations.[32]

D. Interceptor ASAT Weapons

Interceptor ASAT systems and system concepts can be divided into a number of distinct categories: low-altitude direct-ascent interceptors, low-altitude short-duration-orbital interceptors, high-altitude short-duration-orbital interceptors and long-duration-orbital interceptors. These weapons are typically ground or air launched into intercept trajectories or orbits that are nearly the same as the intended target satellite. Radar or optical systems onboard the ASAT guide it to close proximity of the target satellite. The complexity of the interceptor is a function of its damage mechanism (kinetic, chemical, nuclear, or radio frequency), its engagement relative velocity, how close it must get to the target to result in a kill, and whether the ASAT is ground-, air-, or space-based.[33] From the standpoint of the interceptor guidance and control systems complexity, kill mechanisms with large lethal radii are preferable to those with small lethal radii.[34]

[31] Cohn and Kweder, “Third World Nuclear Threat to Low Earth Orbit Satellites,” p. 10-11.
[32] Department of Defense Studies, 2000, p. 24.
[33] Ibid., p. 15.
[34] Ibid., p. 1012.

1. Low-Altitude Direct-Ascent ASAT Interceptors

Low-altitude direct-ascent interceptors are launched on a booster from the ground or from an aircraft into a sub-orbital trajectory that is designed to intersect that of a low Earth orbit satellite.[35] Because these interceptor systems are on a direct sub-orbital trajectory, the on-orbit lifespan of these systems is measured in minutes, making them the simplest type of interceptor weapons to design, build and test.[36]

2. Low- and High-Altitude Short-Duration Orbital ASAT Interceptors

A low-altitude short-duration-orbital ASAT is an interceptor that is launched from the ground into a temporary parking orbit from which it maneuvers to attack a specific low earth orbit satellite. A high-altitude short-duration ASAT is an interceptor that is launched from the ground into a temporary parking orbit from which it maneuvers to attack a high-altitude satellite.[37] Because these interceptor systems enter a temporary parking orbit, the on-orbit lifespan of these systems is measured in hours, which makes them slightly more complex than direct ascent weapons.[38]

3. Long-Duration Orbital Interceptors

The long-duration orbital ASAT is an orbital interceptor that is launched into a storage orbit for an extended period of time, possibly months to years, before it maneuvers to engage and inspect or attack the target satellite. The ASAT may be standalone or covertly placed on or in a "mothership" satellite. Feasible concepts, in order of increasing sophistication, include the farsat, nearsat, space mine, fragmentation or pellet ring, and space-to-space missile. Farsats are parked in a storage orbit away from their targets and maneuver to engage them on command. Nearsats are deployed and stay near their target to inspect and attack on command. Space mines are parked in orbits that intersect the target's orbit and are detonated during a periodic close encounter. Fragmentation or pellet rings are vast quantities of small, non-maneuvering objects that are dispersed from one or more satellites in such a way that an artificial earth-

[35] Ibid., p. 1007.
[36] Ibid., p. 1011.
[37] Ibid., p. 1007.
[38] Ibid., p. 1011.

orbiting ring is created. Satellites flying through the ring are damaged or destroyed. Space-to-space missiles are rocket propelled ASAT interceptors launched from an orbiting carrier platform into an orbit that intercepts the intended target.[39]

The major cost driver for long-duration orbital interceptors is that they must be designed, built and tested to be more reliable and sophisticated than the other shorter-duration interceptors. In general, these systems will be on-orbit for long periods of time, requiring more advanced systems such as attitude determination and control, thermal control and power generation. Also, since it is most likely that it will not be possible to service them once they are deployed, these systems must inherently be more reliable. In addition, the long on-orbit life spans typically require more costly radiation-hardened electronic components and other components that are hardened in accordance with prolonged exposure to the space environment (radiation, contamination, vacuum, etc.). For example, prolonged exposure to the space radiation environment may degrade nuclear warhead materials, decreasing the weapon's yield.[40]

Farsat

In the farsat concept, the interceptor, as either an independent satellite or part of a “mothership,” is maintained in a storage orbit different from that of its intended target. After receiving a command from the ground, the farsat would activate its ASAT package and maneuver to rendezvous with and inspect or attack its target. It is likely that farsats would be launched long before they were needed. A large number of them could be stockpiled on-orbit before the outset of an ASAT war, thereby avoiding the bottleneck caused by launch vehicle availability. It is also likely that, when deployed, the farsat would be made to look like some other kind of non-hostile satellite or piggybacked onto an existing satellite. Either way, an attempt could be made to hide the ASAT mission of the system by having it carry out some non-ASAT mission after it is launched and before it is used in the ASAT role. The ability of a farsat to engage other satellites and the time required to accomplish the mission depend on the orbit of the interceptor and the target, constraints on the engagement geometry, and the interceptor's maneuvering capability.[41]

[39] Ibid., p. 1007.
[40] Ibid., p. 1011.
[41] Ibid., p. 1157-1158.

Nearsat

In the nearsat concept, the interceptor, as either an independent satellite or part of a "mothership," is placed into orbit in close proximity to the target. The nearsat maneuvers to stay in close proximity to the target until it is commanded, from the ground, to inspect and/or attack the target satellite. How close to the target the nearsat must stay, and how frequently it must maneuver, depends on the lethal radius of the attack mechanism. In order for the nearsat to maintain its close proximity it must perform numerous station keeping maneuvers, thus requiring it to have a substantial maneuver capability. In addition, the nearsat would either have to possess autonomous station keeping capability or controllers that would track and command the nearsat.[42]

Space Mines

Space mines are non-maneuvering, relatively low-sophistication satellites that are put into orbits that intersect the target's orbit. The natural orbital mechanics provide periodic close encounters between the space mine and its target. During one of these periodic close encounters, the space mine is detonated, either by on-board fuse or ground command. Because the time between the decision to attack and the actual attack may be lengthy, a constellation of co-orbital mines may be deployed for a particular target.[43]

During the 1980s, Soviet authors frequently listed space mines as potential counters to space-based elements of a strategic defense system. For example, in the 1986 book "Weaponry in Space: The Dilemma of Security," the authors note:[44]

> Another good way of simultaneously putting out of action several stations would be to use the so-called 'space mines,' which are essentially satellites with high-yield explosives placed into orbits close to the opponents' battle stations, which explode on command from the ground. The mines could be supplied with all sorts of fuses, in particular mechanical- or thermal-actuated ones.

[42] Ibid., p. 1159-1160.
[43] Ibid., p. 1160-1161.
[44] Ibid.

Fragmentation or Pellet Rings

The fragmentation or pellet ring concept is an extension of the space mine concept wherein the number of interceptors is increased, but the individual size and complexity of the "mine" is reduced. Vast quantities of small, non-maneuvering objects, such as metal shot, sand, debris or ice particles, are dispersed from one or more satellites in such a way that an artificial earth-orbiting ring is created on demand. All satellites whose orbits carry them through the ring risk damage. The relative velocity between the target and the ring particles is sufficient such that even small objects can cause catastrophic satellite damage.[45] The same Soviet book, "Weaponry in Space: The Dilemma of Security," discusses the use of fragmentation or pellet rings:[46]

Still other active countermeasures are swarms of small pellets ('space shrapnel') traveling with a relative (to the satellite) velocity of 15 km/sec. In a head-on collision, a 30-g particle hitting the satellite at that velocity can pierce a 15-cm steel shield (or the satellite's skin). The most vulnerable components of a battle station are fuel compartments, power units, and mirrors. A small cloud of macroparticles produced in orbit may cause defects in the surface of the reflecting mirror that will make laser-beam focusing impossible.

Space-to-Space Missiles

Space-to-space missiles are rocket-propelled ASAT interceptors launched from an orbiting carrier platform into an orbit that intercepts the intended target. Space-to-space missile systems are comprised of carrier satellites, interceptor missiles and command and control assets. The carrier satellite could be designed to host multiple, independently targetable, rocket-propelled interceptors. [47]

Microsatellites—An Example of the Proliferation of Long-Duration-orbital Interceptor Technology

Advances in miniaturization and the proliferation of space technologies enable many countries to enter space with small, lightweight, inexpensive and highly capable systems that can perform a variety of missions. Included in this list of missions is counterspace operations, such as long-duration-orbital inspection and intercept. Microsatellites and

[45] Ibid.
[46] Ibid.
[47] Ibid., p. 1162.

nanosatellites, weighing from 100 kilograms to 10 kilograms respectively, are examples of the advances in miniaturized space system technologies that have enabled increasingly complex missions to be performed via smaller and smaller platforms. Microsatellites can perform satellite inspection, imaging and other functions and could be adapted as weapons. Placed on an interception course and programmed to hone-in on a satellite, a microsatellite could fly alongside a target until commanded to disrupt, and then disable or destroy the target. Detection of and defense against such an attack would be difficult.

Microsats are typically characterized by: rapid development timelines (typically from 6 to 36 months); low cost; incorporation of leading edge technology; and manageable portions. It is these characteristics that make microsats attractive to universities and emerging space nations, as well as to governments. Continued advances in microsat bus and electronics technologies (Microelectromechanical systems (MEMS), high-power solar, and high density/high-performance systems) will enable smaller, high-G enabled, and rad-hardened microsats and nanosats. Continued miniaturization of sensor technology will enable new mission scenarios such as the potential for on-orbit autonomous integration and deintegration and formation flying, which will in turn enable things such as robotic integration, array production, large space aperture production, satellite servicing, and commodity delivery in space.

Surrey Space Technologies, Ltd. (SSTL), in England, is considered to be the market leader in microsatellite technology. SSTL is a commercial, majority owned subsidiary of the University of Surrey. SSTL has conducted technology transfer and training programs with a goal of enabling emerging space nations to master microsatellite technology as a step in facilitating the development and deployment of an increasingly capable national space infrastructure. To date SSTL has conducted technology transfer and training programs with: China (Tsinghua-1), South Korea (KITSat-1/2), Portugal (PoSat-1), Pakistan (BADR-1), Chile (FASat-Alfa/Bravo), South Africa (UoSAT-3/4/5), Thailand (TMSAT-1), Singapore (Merlion payload), and Malaysia (TiungSAT-1). Recently, SSTL conducted a satellite inspection mission with the Russians and Chinese using the 6.5 kg SNAP-1 nanosat. In addition to SSTL, other countries involved in maturing microsat technology include: Russia, Israel, Canada, Sweden, and Australia.[48]

[48] Surrey Space Center Press Announcement, “Surrey Satellite Technology Ltd (SSTL) celebrates 15 years in business,” 12 June 2000, p. 2.

There are examples of plans to use microsatellite technology to develop and deploy long-duration orbital ASAT interceptors. The Sing Tao newspaper recently quoted Chinese sources as indicating that China is secretly developing a nanosatellite ASAT weapon called "parasitic satellite." The sources claim this ASAT recently completed ground testing and that planning was underway to conduct testing in space. The Chinese ASAT system is covertly deployed and attached to the enemy's satellite. During a conflict, commands are sent to the ASAT that will interfere or destroy the host satellite in less than one minute.[49]

The same sources discuss the three components of the "parasitic satellite" system as: a carrier ("mother") satellite, a launcher and a ground control system. Because the "parasitic satellites" reside with their hosts and are only activated during a conflict, their volumes must be very small to conceal their existence and avoid interfering with the normal operation of the host satellites. The sources also claim the cost of building the satellite to be between 0.1 and 1.0 percent of a typical satellite.[50]

The reason behind the development of the "parasitic satellite" system is strategic balance between China and the U.S. According to the sources:

> Beijing's decision to develop and deploy the ASAT system has both long-term and short-term strategic objectives. The long-term objectives are to establish a strategic balance among the larger nations, and to break up the monopoly on utilization of space that large space systems of the superpowers are holding; thus weakening their capabilities in information warfare. In the short-term China would strengthen its capabilities in controlling the usage of space globally, and change drastically the Chinese-American military balance so that the U.S. would not intervene easily in the event of a conflict in the Taiwan Strait and at the Chinese perimeter.[51]

[49] Cheng Ho, "China Eyes Anti-Satellite System," *Space Daily*, 08 January 2000.
[50] Ibid.
[51] Ibid.

E. Stand Off Weapons

Stand off ASAT weapons include lasers, radio frequency (RF) and particle beam weapons. They are termed "stand off" because they are predominantly either ground or air-based systems that never get very close to their target. Most of these concepts tend to be more technically sophisticated and may attack the target from longer ranges than the aforementioned interceptors. In addition, these technologies are capable of engaging multiple targets, whereas interceptors tend to be single shot systems. Furthermore, if the geometric conditions are right, directed-energy weapons can target and attack their targets in seconds; interceptor engagement times tend to be much longer.[52] Finally, stand off directed energy weapons offer the adversary a degree of deniability. This is largely due to the fact that the attack is relatively quick so there may be no intelligence indicators associated with the attack, and because the degradation of the target spacecraft may not be immediately apparent, making it difficult to figure out when and where the attack occurred.[53]

1. Laser ASAT Weapons

Laser weapons generate intense beams of light that can focus on a target a considerable distance away. There are two basic laser categories discussed here: low-power lasers and high-power lasers.[54] Low-power lasers are typically designed to spoof or jam satellite electro-optical sensors using laser radiation that is in the sensor pass band (in-band), thus temporarily blinding the satellite. High-power lasers can permanently damage or destroy a satellite by radiating enough energy to overheat its parts. The satellite systems which are susceptible to high-power lasers include satellite structures, thermal control surfaces and solar panels.[55] Laser weapons, as potential ground-, air- or space-based antisatellite (ASAT) weapons, are being developed today.[56]

Laser systems, including coherent radiation, aligned waveform, and other devices operating at or near the optical wavelengths, operate by delivering energy onto the surface of the target. The gradual or rapid

[52] Department of Defense Studies, 2000, p. 19.
[53] Ibid., p. 1014.
[54] Ibid., p. 1193.
[55] Ibid.
[56] Paul Nordin, "Other Hostile Environments," in *Space Mission Design and Analysis*, 2nd ed., ed. Wiley J.Larson and James R. Wertz, (Microcosm Inc. and Kluwer Academic Publishers, 1992), p. 220.

absorption of this energy leads to several forms of thermal damage for weapons application.[57] Generally, antisensor laser ASATs could be used against satellites at any altitude. This leads to the requirement for the laser beam to propagate over very long ranges (tens to hundreds or even thousands of kilometers) and still deliver a lethal fluence to the target. This results in demanding weapon system requirements: high laser power (megawatt class lasers are required for most long-range non-sensor blinding missions), high beam quality, large aperture beam director, extremely stable beam pointing system, etc. These factors make laser weapons extremely complex.[58]

The effectiveness of a given laser system is dependent upon the specific operational elements of the laser. Six basic elements are required for a laser ASAT system:[59]

1. A laser device with attendant power supply and thermal control

2. A stable optical system to point the beam at the target

3. An appropriate platform and/or booster, for air and space-based lasers

4. Space surveillance and tracking network

5. A means of determining the outcome of each engagement (kill assessment)

6. Algorithms and mechanisms for correction of beam distortion as it passes through the atmosphere

Due to the complexity of conditioning the beam in order to compensate for atmospheric effects, space-based laser ASAT weapons have been studied for years, as alternatives to ground- and air-based laser ASATs.

[57] United States Air Force, p. 4.
[58] Department of Defense Studies, 2000, p. 1193.
[59] Ibid.

2. Radio Frequency (RF) ASAT Weapons

RF ASAT weapons concepts include ground- and space-based RF emitters that fire an intense burst of radio energy at a satellite, disabling electronic components. RF weapons are usually divided into two categories: high power microwave (HPM) weapons and ultrawideband (UWB) (or video pulse) weapons.[60] Although there are no known RF ASAT weapons deployed today,[61] multiple-shot, long-range, ground-based systems and multiple- or single-shot, short-range, space-based stand off systems and interceptor warheads are feasible in the near future.[62]

UWB weapons would generate RF radiation covering a wide frequency spectrum—nominally from about 100 MHz to more than 1 GHz—with limited directivity. Because of the UWB weapon's low-energy spectral density and directivity, permanent damage to electronic components would be very difficult to achieve, except at very short ranges.[63] The UWB couples through the satellite's antenna at its receive frequency, as well as through openings in the systems shielding. If enough power is applied, the received radiation may cause major damage to the satellite's internal communications hardware such as RF amplifiers, downconverters, or other devices on the front-end of the receiver.[64] However, in many cases, UWB weapons may cause system upset, which may persist only while the target is being irradiated, or may require operator intervention to return the satellite to its nominal functioning state.[65]

HPM weapons would generate an RF beam at a very narrow frequency band, in the 100 MHz to 100 GHz range, with higher directivity. The HPM devices operate by penetrating through antennas or into the interior of the target through cracks, apertures, or seams with longer wavelength radiation. The penetrating radiation causes damage or disruption as it is absorbed by internal electronic components.[66] Unlike traditional electronic warfare, the induced electrical energy does not need to be collected by a receiver in-band and made to look precisely like a train of specific input signals. Rather, UWB and HPM can produce so-called backdoor effects that arise from overwhelming circuits with induced

[60] Ibid., p. 1008.
[61] United States Army, p. 7.
[62] Department of Defense Studies, 2000, p. 21.
[63] Ibid., p. 1261.
[64] Nordin, p. 221.
[65] Department of Defense Studies, 2000, p. 1261.
[66] United States Air Force, p. 4.

signals and high power transients that penetrate system's openings or cracks. It is difficult to close off these paths in a real system, since features such as openings and electrical wiring are essential to system operation. Since disruption and upset require induction of only a few volts at the extremely low current levels of modern electronics, the power levels needed to achieve these effects can be fairly moderate, and the matching of signal waveforms can be quite imprecise.[67]

An RF ASAT weapon may be composed of four basic elements:[68]

- An RF generator with a prime power supply and pulse forming network, and an antenna to point the radiation at the target
- For airborne, missileborne and space-based RF weapons, an appropriate platform and/or booster
- Space surveillance and tracking network to determine the target's orbit and to maintain a target catalog for ASAT mission planning, guidance parameter definition (targeting), battle management, and support of kill assessment
- A means of determining the outcome of each engagement (kill assessment)

High Power Microwave technology research and development is approaching maturity after decades of research.[69]

[67] Ibid., p. 7.
[68] Ibid., p. 1262-1263.
[69] Ibid., p. 7.

3. Comparison of High-Power Laser and High-Power Microwave Weapons

The following table from the Air Forces "Directed Energy Master Plan" delineates the differences between high-power laser and high-power microwave weapons.[70]

High-Power Laser Weapons	**High-Power Microwave Weapons**
Irradiates a selected spot on a single target with high precision	Attacks area targets that may include groups of targets
Must be precisely aimed and pointed at susceptible area of target	Needs only be directed generally toward the intended target
Inflicts heavy damage on selected spot	Inflicts more subtle damage on electronic components.
Will not operate through clouds	Largely unaffected by clouds
Heats, melts or vaporizes a selected spot which in turn destroys or disables the target	Generates high electric fields over the whole target which in turn disrupt or destroy vulnerable electronic components

4. Particle-Beam ASAT Weapons

Particle beam ASAT weapon concepts are space-based systems that fire an intense beam of elementary particles at a satellite, disabling electronic components. These weapons accelerate atomic particles, such as negative hydrogen or deuterium ions,[71] to relativistic velocities (significant fractions of the speed of light) toward their target. They can cause permanent damage by radiating enough energy to overload the satellite's internal electronics.[72] Since these accelerated particles cannot penetrate the atmosphere, weapons using this technology against satellites must be based in space.[73] Particle beam weapons include both charged particle beam (CPB) weapons and neutral particle beam (NPB) weapons. Charged particle beams do not propagate in straight lines in outer space because of the Earth's magnetic field. Because of this, their utility in the ASAT role appears limited. However, neutral particles can propagate long, linear distances in outer space.[74]

[70] United States Air Force, p. 5.
[71] Nordin, p. 221.
[72] United States Army, p. 7.
[73] Nordin, p. 221.
[74] Department of Defense Studies, 2000, p. 1273.

To be an effective weapon, the spacecraft carrying the NPB would need several additional components:

- Sensors to acquire and track the target
- A propulsion system for orbit transfer maneuvers in order to engage multiple targets
- An attitude control system and highly rigid structure capable of controlling the vibration and thermal distortion induced by the solar heating, thrusters, machinery vibration, and beam operation
- A prime power supply and power conditioning system capable of providing power to both the weapon and spacecraft
- A thermal control system that can handle the heat surge generated by the weapon and its power supply [75]

Ground-based particle accelerators have been used since the early 1930ís for high-energy nuclear physics research and a few ground-based weapon prototypes have been demonstrated but no operational particle beam weapons are currently deployed by any nation.[76] The most likely particle-beam threat in the next 15 years is from space-based neutral particle beam weapons.[77]

F. Electronic Attack on Communications, Data, and Command Links

Electronic attack is defined as any action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack an adversary. The most likely targets for offensive counterspace attacks are communications satellites and other satellite's communications, data and command links. All military and commercial satellite communications systems are susceptible to uplink and downlink jamming or spoofing. In either case, the jammer must operate in the same radio band as the system being jammed. Uplink jammers on the ground

[75] Ibid., p. 1275.
[76] United States Army, p. 7.
[77] Department of Defense Studies, 2000, p. 1008.

must be roughly as powerful as the ground-based emitter associated with the link being jammed. However, ground-based downlink jammers can often be much less powerful and still be effective.[78]

Commercial satellite ground communications equipment has electronic jamming capabilities that can easily be used to disrupt the functions of some satellites. Many countries, including Russia and China as well as Iran, Cuba, Iraq and North Korea, also have military jamming capabilities. Most U.S. commercial and civil satellites lack built-in protection measures and are vulnerable to such attacks. Some recent examples of satellite jamming or interference include: [79]

- In April 1986, “Captain Midnight” used commercially available SATCOM equipment to overpower the uplink transmissions from HBO Corporation. The act was a response to HBO's encrypting their signal and demanding that satellite dish operators pay a decoder fee. Captain Midnight's protest message was received by all HBO customers.

- In 1994, the Hong Kong-based Chinese firm Asia Pacific Telecommunications (APT) placed its Apstar-1 satellite at the 131 degree east geosynchronous orbit slot without approval of the International Telecommunications Union (ITU). There was significant concern that the move would result in interference on adjacent satellite communication systems already in place.

- In early 1997, the South Pacific island nation of Tonga accused Indonesia of deliberately jamming APT's Apstar-1A, which had been moved to the 134-degree east orbital slot. (APT leased the slot from Tonga.) Publicly, Indonesia denied the charges. However, Tongan officials claim that Indonesia boasted about the jamming during talks to resolve the dispute in March.

- Recently, Japan lodged a complaint with the ITU accusing Indonesia and the Philippines of operating the Agila 2 geosynchronous orbit communication satellite in violation of ITU rules. Agila 2 and Japan's Superbird C communication satellite were both operating at the 144-degree east orbital slot. Agila 2 was supposed to operate in G band, to avoid interference with Superbird

[78] Ibid., p. 10-12.
[79] Ibid., p. 13-14.

C's J band operations. However, Agila 2 was operated at J band, apparently causing interference on Superbird C. As a temporary fix, the Philippine government moved Agila 2 to 146 degrees east.

More sophisticated technologies for jamming satellite signals are emerging. For example, Russia is marketing a handheld GPS jamming system. A one-watt version of that system, the size of a cigarette pack, can deny access to GPS out to 50 miles; a slightly larger version can jam up to 120 miles.[80] Both are compact and powerful enough to jam an aircraft's GPS receiver signal, which could disrupt military missions or create havoc at a civilian airport.

Military communications sent via commercial communications satellites (COMSATs) are particularly susceptible to jamming. This is largely due to the fact that off-the-shelf satellite communication (SATCOM) equipment can and has been used to easily jam commercial COMSAT links. The problem is that most commercial satellite communications equipment currently operates in a very few internationally mandated frequency bands, primarily the G and J bands. According to an open source report, 90% of all communications between the U.S. and the Gulf during Desert Shield/Desert Storm went through communications satellites—roughly half of these went via commercial systems. The percentage of inter- and intra-theater communications conducted via commercial satellite communications services will increase, as will the counterspace electronic attack threat, as U.S. military use of commercial communications satellites increases.[81]

V. Impact of Counterspace Operations

The employment of space systems increases the effectiveness of terrestrial warfighters by acting as a force multiplier. Space-based systems provide imagery of targets on earth and in space, accurate timing and navigational data, critical weather information and command and control capabilities. If an adversary is able to employ offensive counterspace operations to deceive, disrupt, deny, degrade, or destroy U.S. space systems, the force multiplication effect would be reduced or eliminated. This could lead to more expensive victories or even to defeat.[82] The U.S.'

[80] "Anti-Anti-GPS," Aviation Week & Space Technology, 20 November 2000, p. 25.
[81] Department of Defense Studies, 2000, p. 14.
[82] Ibid., p. 4.

reliance on space, coupled with the growing amount of information available about our space systems, increases the likelihood that our adversaries will employ counterspace weapons technologies.

As harmful as the loss of commercial satellites or damage to civil assets would be, an attack on intelligence and military satellites would be even more serious for the nation in time of crisis or conflict. Some examples of the potential impact of deception, disruption, denial, degradation, or destruction of specific space systems by foreign offensive counterspace operations include:[83]

- Impairment or elimination of reconnaissance satellites that would reduce situational awareness and could lead to military surprise, underestimation of enemy strength and capabilities, less effective planning, and less accurate targeting and battle damage assessments.

- Impairment or elimination of missile launch detection satellites that would degrade the US's ability to perform missile launch warning, missile defense, and would increase the psychological impact of the adversary's ballistic missiles.

- Impairment or elimination of satellite communications systems that would disrupt troop command and control problems at all force levels.

- Impairment or elimination of navigation satellites that would make troop movements more difficult, aircraft and ship piloting problematic, and could render many precision-guided weapon systems ineffective or useless.

- Impairment or elimination of Earth resource and weather satellites that would make it more difficult to plan effective military operations.

Threatening or attacking the space capabilities of the U.S. would have domestic, economic and political consequences and could provoke international disputes about the origin and intent of an attack. Such ambiguity and uncertainty could lead to excessive forbearance when action is needed or to hasty action when more or better information would have given rise to a broader and more effective set of response options.

[83] Ibid.

There are a number of possible crises or conflicts in which the potential vulnerability of national security space systems would be especially worrisome. During these situations, the President, his senior advisors and military commanders would be dependent on information from U.S. satellite systems to help manage the crisis, conduct military operations or bring about a resolution to the conflict. If the performance of U.S. systems were reduced, the diplomatic and military leverage of the U.S. could decrease, the position of an adversary could be improved, and the cost and risks associated with achieving U.S. objectives would increase.

VI. Countermeasures—Strategies for Enhancing Survivability

The U.S. is more dependent on space than any other nation. Yet the threat to the U.S. and its allies in and from space does not command the attention it merits from the departments and agencies of the government charged with national security responsibilities. Consequently, evaluation of the threat to U.S. space capabilities currently lags in the competition for collection and analytical resources.

One potential reason for the lack of priority is that the signs of U.S. space vulnerability are not always so clear and therefore are not always recognized. Hostile actions against space systems can reasonably be confused with natural phenomena; space debris or solar activity can "explain" the loss of a space system and mask unfriendly actions or the potential thereof. They can be explained as computer hardware or software failure, even though either might be the result of malicious acts. Thus far the indicators have been neither sufficiently persuasive nor gripping enough to energize the U.S. to take sufficient defensive steps. In general, the U.S. is not well prepared to handle the range of potential threats to its space systems. However, there are courses of action and available technologies that could be used to counter these threats to U.S. space capabilities.

A. Reliable Threat Analyses

The Intelligence Community has begun to improve its collection strategy for threats in and from space. Its analytic efforts, however, need to give more attention to the technical and operational forms the threat might take. The Intelligence Community needs to account for the potential for

technology proliferation and services available on the open market to benefit those who would threaten U.S. space capabilities. Political and military leaders need to appreciate the nature of the threat and should seek and receive from the Intelligence Community the necessary information on the space-related threat.

Failure to develop credible threat analyses will have serious consequences for the United States. It could leave the U.S. vulnerable to surprises in space and could result in deferred decisions on developing space-based capabilities due to the lack of a validated, well-understood threat. Surprise, however, is not limited to the possibility of an attack on U.S. systems. The U.S. also could be surprised by the emergence of new technological capabilities in the hands of potential adversaries. Or, the U.S. could be surprised in the international arena by economic or arms control proposals it does not anticipate, or the importance of which it does not fully appreciate because of insufficient knowledge about the technical or operational capabilities of current or future negotiating partners.

B. Mobile Ground Control Stations

The goal of a mobile ground control station is to make it difficult for an adversary to apply a threat because of an uncertainty as to the location of the ground control station. The concept of operations might be to operate multiple ground control stations such that while one is controlling the satellite, the others might be relocating or in the process of standing up or down. Depending on the number of mobile ground control stations deployed, the cost of this system would be approximately two to three times the cost of a single large ground station.[84]

C. Autonomous Operations

For a satellite to continue to execute its mission, in the event that the ground control station is lost, it must be capable of performing autonomous operations. Autonomous operations require the capability for the satellite to perform autonomous orbit control (e.g. station keeping for geosynchronous orbits), momentum control, redundant unit control (fault

[84] Nordin, p. 226.

detection) and substitution. Analysts estimate that autonomous operations increase the total system cost by between three and eight percent of the total satellite cost.[85]

D. Hardening

Hardening of a space system's elements is the single most effective survivability measure.[86] The technologies to harden against damage from nuclear-weapons effects exist today. However, this level of hardening is reserved for a few, special mission military satellites, such as MILSTAR. Most of the hardening programs underway today are focused on providing electronic component hardening to protect satellites from natural environment effects. However, concepts such as reflective surfaces, shutters and non-absorbing materials have been proposed as a means of hardening against an attack by lasers. In the future, the U.S. must advance the state-of-the-art in hardening technology to include limiters, filters, Faraday cages, surge arrestors, waveguide cutoffs, as well as expand the use of fiber optic components to increase survivability against nuclear, high-power microwave and neutral particle beam weapons.[87] Analysts estimate that satellite hardening would increase the total system cost by between two and five percent of the total satellite cost.[88]

E. Proliferation-Redundant Nodes

The concept of orbit proliferation or redundant nodes involves placing multiple satellites, in a given orbit, with overlapping coverages. The premise behind this concept is that if one satellite fails then the other satellites will be available to execute all or some percentage of the essential functions of the mission. This forces the adversary to attack multiple space systems, driving up the complexity and cost of the attack. Continuing advances in micro-miniaturization of space systems and components and the compact, portable ground systems for controlling them will support the proliferation strategy.

[85] Ibid.
[86] Ibid., p. 221.
[87] United States Army, p. 11.
[88] Nordin, p. 226.

F. On-Board Systems For Attack Reporting

Many of the threats discussed here can reasonably be confused with natural phenomena such as space debris, solar activity, and computer hardware or software failure. In order for the U.S. to react appropriately to an attack on its space systems it must first know that it has been attacked and the nature of the attack. An on-board system for attack reporting would be able to record or report the time, intensity, or direction of a potentially hostile action against the satellite. I f combined with the ability to autonomously react, a system such as this would be effective for system survivability. Analysts estimate that employment of an on-board attack reporting system would increase the total system cost by between one and five percent of the total satellite cost.[89]

G. Maneuverability

While most satellites have thrusters for attitude control, station keeping and orbit changes, few have the thrust capability or carry the necessary propellant to maneuver. Thrusters which would enable a satellite to maneuver or dodge an ASAT threat would be powerful; generating higher structural loads to the spacecraft and requiring stiffer, stronger solar arrays and appendages, as well as, require additional propellant. These factors add up to weight penalties for the system. Analysts estimate that to add maneuverability to a satellite system would currently increase the total system cost by between ten and twenty percent of the total satellite cost depending on the satellite altitude (warning time), nature of the threat, and threat detection efficiency.[90]

However, this cost and the technology to implement maneuverability could be significantly reduced if the U.S. can develop the capability to refuel the space system on-orbit. Programs such as the Defense Advanced Research Project Agency's (DARPA) Orbital Express Program are developing and demonstrating the necessary technology and operations concepts needed to employ maneuverability.

[89] Ibid.
[90] Ibid.

H. Rapid Reconstitution

The are two basic ways to rapidly reconstitute an on-orbit capability. First, spare or reserve satellites can be maintained on-orbit. Second, replacement satellites can be launched into orbit on short notice. In either case, an advanced commitment of resources is needed to provide this capability. Furthermore, the U.S. does not currently possess the capability to rapidly launch satellites into orbit, so a national level commitment to develop a rapid launch capability would be needed.

I. On-board Decoys

Decoys that credibly simulate the radar and optical signatures of the satellite are effective, potentially low-cost methods for diverting an ASAT attack from the actual satellite. The decoy would be located on or inside the host satellite and released at the precise moment for the most effective deployment. Decoys could also include lightweight optical or RF jamming systems to nullify or confuse an ASAT's homing system. Analysts estimate that employment of a decoy system would increase the total system cost by between one and ten percent of the total satellite cost.[91]

J. Self-Defense or Escort Defense Capability

The ability for a satellite to defend itself against an ASAT attack is a reasonable way to increase the survivability of a high-value space system. One method of self-defense would be to design a suite of optical or radar sensors and small, lightweight missiles into the satellite. Analysts estimate that employment of an on-board self-defense system would increase the total system cost by between ten and twenty percent of the total satellite cost.[92]

Alternatively, a small escort satellite carrying the same capabilities might be a more capable system, especially if the goal was to detect, track and intercept the ASAT while the primary satellite continued its mission. Analysts currently estimate that employment of an escort defense system would increase the total system cost by between twenty and forty percent of the total satellite cost.[93] However, with continued advances in

[91] Ibid.
[92] Ibid.
[93] Ibid.

technologies for capable microsatellites the cost of deploying such a system will decrease. In the more distant future, self-defense missiles might be replaced by a high-energy lasers or high-power microwave systems.

VII. Conclusion

As history has shown—whether at Pearl Harbor, in the killing of 241 U.S. Marines in their barracks in Lebanon, or in the attack on the USS Cole in Yemen—if the U.S. offers an inviting target, it may well pay the price of attack. With the growing commercial and national security use of space, U.S. assets in space and on the ground, offer just such targets. Widely dispersed counterspace threat capabilities coupled with space situational awareness platforms threaten the U.S. ability to freely operate in space. We can no longer look at traditional adversaries as the only threat as there will likely be various space threats from several nations.

History is replete with instances in which warning signs were ignored and change resisted until an external, "improbable" event forced resistant bureaucracies to take action. The question is whether the U.S. will be wise enough to act responsibly and soon enough to reduce U.S. space vulnerability. Or whether, as in the past, a disabling attack against the country and its people—a "Space Pearl Harbor"—will be the only event able to galvanize the nation and cause the U.S. Government to act.

Acknowledgments:

I would especially like to thank the National Air Intelligence Center and Defense Intelligence Agency for their efforts in support of this paper. I would also like to thank the 13 Commissioners and Dr. Stephen Cambone for their guidance and trust.

Although United States space systems have historically maintained a technological advantage over those of our potential adversaries, those potential adversaries are now advancing their space capabilities and actively developing ways to deny our use of space in a crisis or conflict. It is imperative that the United States adapt its national security organizations, policies, doctrine, and capabilities to deter aggression and protect our interests. Toward that end, the Department of Defense shall take actions under existing authority to marshal its space resources to deter and counter threats in space Space Object Tracking and Identification Capabilities. A. Non-Government Satellite Observers B. Optical Tracking and Imaging Systems C. Radar Tracking and Imaging Systems D. SIGINT and Passive RF Tracking and Characterization Systems. IV.Â Countermeasures--Strategies for Enhancing Survivability. A. Reliable Threat Analyses B. Mobile Ground Control Stations C. Autonomous Operations D. Hardening E. Proliferation-Redundant Nodes F. On-Board Systems For Attack Reporting G. Maneuverability H. Rapid Reconstitution I. On-board Decoys J. Self-Defense or Escort Defense Capability. VII. Conclusion. he United States is a global power with global interests. Scaling its military power to threats requires judgments with regard to the importance and priority of those interests, whether the use of force is the most appropri-ate and effective way to address the threats to those interests, and how much and what types of force are needed to defeat such threats.Â ll Defense of the homeland; ll Successful conclusion of a major war that has the potential to destabilize a region of critical interest to the U.S.; and. ll Preservation of freedom of movement within the global commons: the sea, air, and outer space domains through which the world conducts business. The geographical focus of the threats in these areas is further divided into three broad regions: Asia, Europe, and the Middle East.