Chapter 21

Space System Threats

Maj Brian Garino, USAF, and Maj Jane Gibson, USAF

Most US military operations are touched in one way or another by space—we are more dependent on space than any other nation.[1] This dependency has opened up critical vulnerabilities that must be addressed. Aircrews, mission planners, director of space forces (DIRSPACEFOR) staff members, and all personnel involved with combined air operations center (CAOC) planning and air tasking order (ATO) development should understand the threats to space operations and space support functions, as well as the intelligence, surveillance, and reconnaissance (ISR) threat from other nations' space-based systems. Regarding threats to space systems and associated links and nodes, the presented threat will more than likely influence the effectiveness and/or efficiency of other friendly-force operations. This effect will not only affect planning timelines but could also result in the loss of valuable military assets and human life. Space threats include, but are not limited to, (1) tracking and monitoring satellites and their transmissions; (2) electronic attack (EA) against space-based services at the transmission site, the satellite, and the user' s equipment; (3) physical attacks against actual satellites and spacecraft; and (4) the use of space for adversary force enhancement and adversary intelligence preparation of the battlefield. These threats could cause communication problems in disseminating and executing the ATO, impact the successful guiding of weapons and aircraft to the target, cause the loss of national overhead and air-breathing ISR systems, compromise operations security (OPSEC) and information security (INFOSEC), and impact force protection posture.

Vulnerabilities can be exploited by focusing attacks on any one of the three segments that make up our space capability—ground, communication (link), and space. The ground segment includes fixed and mobile land, sea, or airborne equipment used to interact with the space segment. The link segment is the data transmitted between the ground and space segments. The space segment includes satellites, space stations, or reusable space-transportation systems. The ability of our space systems to fulfill their missions can be augmented through various methods including redundancy, hardening, maneuverability, denial, and passive defense.

Ground Segment Threats

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. The ground segment is defined by ground station operations to include telemetry, tracking, and commanding (TT&C) of the space nodes and space-launch mission functions. DOD satellites are network-controlled at Schriever AFB, Colorado, via the Air Force Satellite Control Network (AFSCN). The ground segment includes satellite communications (SATCOM) transmission and reception devices, such as GPS receivers. These specialized facilities are critical to the continued operation and effective use of satellites. 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.[2]

These nodes are the most vulnerable to direct attack, network attack, or jamming. Many satellite tracking and control stations are lightly guarded, but their remote locations provide some measure of protection. Many of our satellite communications, launch, data reception, and control facilities are described in open-source materials. With the proliferation of bomb-making techniques and explosive materials, our continental United States (CONUS)–based facilities are at an increased risk. This includes domestic and international terrorists, as well as traditional state actors. An attack on a fixed ground facility can stop data transmission, kill skilled analysts and technicians, render launch facilities unusable, and prevent control of satellites. A single incident or a small number of incidents could significantly impact our space systems for years.[3]

Research, sustainment, integration, and test facilities are also vulnerable. The lifecycle of a space system is processed through commercial facilities that are well-known and are susceptible to physical attack. For example, on 10 May 1992, two individuals scaled the fence surrounding the Rockwell facility in Seal Beach, California. Using false identifications, the individuals penetrated a clean room where a GPS satellite was being assembled and attacked it with axes. They caused several million dollars worth of damage before being subdued.[4]

Network attack against ground nodes is a growing threat, as many countries have developed dedicated cyber-attack or hacking capabilities. Hackers routinely probe DOD networks and computers. Detected probes and scans are increasing, access to hacking tools is becoming easier, and hacking techniques are growing more sophisticated.[5]

Communications (Link) Segment Threats

Both the ground-segment and the space-segment nodes are tied together by information conduits called links. These links are identified as control or mission links. Control links command the satellite and its sensors. Mission links describe the operational data transmitted to or from the satellite. These links are vulnerable to multiple types of electronic attack.

Electronic Attack

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.[6] US space systems could be functionally neutralized by jamming and/or spoofing.

Jammers usually emit noise-like signals in an effort to mask or prevent the reception of desired signals. All military and commercial satellite systems are susceptible to uplink and downlink jamming. In either case, the jammer must operate in the same radio band as the system being jammed. Uplink jammers on the ground 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. Since most satellites rely on uplinked command and control information from the ground for station keeping, payload management, and satellite health and status, attacking a satellite's uplink during critical commanding periods could seriously degrade mission performance. The effectiveness of electronic jamming, however, is

limited because of line-of-sight restrictions and increased satellite autonomy. Therefore, attacking the downlink is usually easier and more reliable.[7]

Uplink Jamming

There are two types of satellite uplink signals: signals for retransmission (payload signals such as TV and communications) and the command uplinks to the satellite. Uplink jamming against a payload signal is an attractive EA strategy because all recipients of the target transmission are affected. The jamming uplink signal is a radio frequency (RF) signal of approximately the same frequency as the target uplink signal. It is transmitted up to the satellite onto the same transponder as the target signal and affects the transponder's ability to distinguish the true signal from the jamming signal. Note that the target uplink source and signal are not affected; the inability of the satellite's transponder to distinguish between the signals results in a loss of downlink or corrupted downlink. The effectiveness of uplink jamming is extremely dependent on obtaining detailed information on the target signal. This can be done through formal signals intelligence (SIGINT) processes or (in some cases) open-source intelligence (OSINT) research. Once this is gathered and analyzed, the uplink jamming source must be able to acquire the proper satellite and transponder, as well as produce a signal with the correct characteristics and power necessary to overcome the signal to be jammed.

Targets of uplink jammers are the satellites' radio receivers, including their sensors and command receivers. Uplink jamming is more difficult, since considerable jammer transmitter power is required. However, its effects may be global, since the satellite or space system could be impaired for all users.

Downlink Jamming

There are two main targets for downlink jamming: SATCOM broadcasts and navigation satellite (NAVSAT) broadcasts. In a downlink jamming scenario, the objective of the EA is to disrupt or temporarily keep the spacecraft's transmission (communication or navigation signal) from being received by select ground users. A downlink jamming system accomplishes this by broadcasting an RF signal of approximately the same frequency as the targeted downlink signal but with more power. This jamming signal is transmitted toward a terrestrial (ground-based) or airborne satellite downlink reception antenna where it overpowers the satellite's signal. With smart jamming (vice brute-force jamming), the jamming signal attempts to emulate the satellite's signal and, if successful, can provide the targeted user with false data or information. The effectiveness of downlink jamming is dependent upon the jammer being able to operate within line of sight (LOS) of the ground site and within the field of view of the ground site's antenna; effectiveness is also dependent upon the jamming signal being processed by the SATCOM receiver. LOS restrictions can be overcome to a degree by utilizing an airborne platform; the altitude gained by the airborne platform expands the coverage and aids in overcoming ground-based obstacles. It is difficult to assess the effectiveness of downlink jamming as this normally requires monitoring the output of the targeted receiver (often not possible).

The targets of downlink jammers are ground-based satellite data receivers, ranging from large, fixed ground sites to handheld GPS user sets. Downlink jamming only requires a very low-power jammer, though its effects are local (from tens to hundreds of miles, depending on the power of both the jammer and downlink signal). Since downlink

Figure 21-1. Russian GPS jammer. (National Air and Space Intelligence Center photo)

telemetry contains the mission information and health and status information, successfully attacking the downlink directly attacks information flow and, therefore, has a more immediate effect on denying or disrupting the satellite's mission.[8]

Sophisticated technologies for jamming satellite signals are emerging. For example, Russia markets a handheld GPS jamming system (fig. 21-1). 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.[9]

Spoofing

Spoofing is the ability to capture, alter, and retransmit a communication stream in a way that misleads the recipient.[10] Attacking the communication segment via spoofing involves taking over the space system by appearing as an authorized user. Once established as a trusted user, false commands can be inserted into a satellite's command receiver, causing the spacecraft to malfunction or fail its mission. Spoofing is one of the most discreet and deniable forms of attacking our space systems.[11]

Space Segment Threats

Spacecraft themselves are complex, expensive, and relatively fragile. They are susceptible to a variety of lethal attacks, including kinetic energy and directed energy (laser and high-powered RF). From the attacker's perspective, destroying a spacecraft using an antisatellite weapon (ASAT) may be preferable because target destruction can be complete and easily verified, although the political ramifications could be significant. Execution of most ASAT options requires detailed and complex information about the weapon system, the satellite, the ground infrastructure, and the command and control (C2) network. Such efforts are extremely expensive and easily detectable by dedicated intelligence organizations. As a result, ASAT development worldwide has been limited.

Kinetic-Energy Weapons

Kinetic-impact weapons cause structural damage by impacting the target with one or more high-speed masses. Small pieces of debris can inflict substantial damage or destroy a satellite. On 11 January 2007, China successfully tested a direct-ascent, kinetic-kill ASAT vehicle, destroying an inactive Chinese *Feng Yun 1C* (*FY-1C*) weather satellite (launched in 1999). The satellite was in a polar orbit at an altitude of 865 km (537 miles) and was attacked when it passed over the Xichang Space Centre in Sichuan Province. The satellite broke into more than 900 pieces, generating more debris

than any previous space event and threatening many operational spacecraft. The launch vehicle was probably a mobile, solid-fuel KT-1 missile, a version of the DF-21 medium-range ballistic missile (MRBM), with a range of 1,700 km to 2,500 km, although according to some accounts it was a KT-2, also mobile and solid fuel, based on DF-31 intermediate-range ballistic missile (IRBM)/intercontinental ballistic missile (ICBM) technology, with a range of more than 6,000 km. The launch vehicle and warhead were guided to the target by ground-based radars.[12]

The threat of hostile actions involving microsatellites (microsats) that can target US commercial space systems is of growing concern. Microsats offer the opportunity for a broad range of countries to enter space using off-the-shelf hardware to build inexpensive satellites and very affordable launch options to place them into orbit. Currently at least 40 countries have demonstrated some ability to design, build, launch, and operate microsats. Used offensively, maneuvering microsats can inspect and interfere with operations of orbiting assets. India, Russia, China, and Japan all have the ability to launch microsats as secondary payloads to low Earth orbit (LEO) and geosynchronous Earth orbit (GEO). "Parasitic" microsats/nanosatellites could also be launched inside the structure of primary payloads without the knowledge of the launch provider and deployed at GEO without detection.

Directed-Energy Weapons

Directed-energy weapons include laser, RF, and particle-beam weapons. Directed-energy weapons are considered "standoff" weapons because they are primarily either ground- or air-based systems that never get very close to their target. Most of these concepts are technically sophisticated and attack the target from longer ranges than most kinetic interceptors. In addition, these technologies are capable of engaging multiple targets, whereas interceptors tend to be single-shot systems. Additionally, if the geometric conditions are right, directed-energy weapons can acquire and attack their targets in seconds, whereas kinetic-interceptor engagement times tend to be much longer. Finally, standoff directed-energy weapons provide the enemy with a degree of deniability. This is because the attack is relatively quick—probably no intelligence indicators associated with it—and because the degradation of the target spacecraft may not be immediately apparent, making it difficult to figure out when and where the attack actually occurred.[13]

Laser Weapons. 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 absorption of this energy leads to several forms of thermal damage. Generally, an antisensor laser weapon 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 lethal power to the target. This results in demanding weapon-system requirements: high laser power (megawatt class lasers are required for most long-range, nonsensor blinding missions), high beam quality, large-aperture beam director, extremely stable beam pointing system, and so forth. These factors make laser weapons extremely complex.[14]

The effectiveness of a given laser system is dependent upon the specific operational elements of the laser. Due to the complexity of conditioning the beam to compensate

for atmospheric effects, space-based laser weapons have been studied for years, as alternatives to ground- and air-based laser weapons.[15]

Radio Frequency Weapons. RF 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.[16]

UWB weapons 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. The UWB enters through the satellite's antenna at its receive frequency, as well as through openings in the system's shielding. If enough power is applied, the received radiation may cause major damage to the satellite's internal communications hardware. However, in many cases, UWB weapons will simply cause system upset, which may persist only while the target is being irradiated or may require operator intervention to return the satellite to its normal state.[17]

HPM weapons 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.[18]

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 from overwhelming circuits with induced signals and high-power transients that penetrate the system's openings or cracks. It is difficult to close off these paths, since features such as openings and electrical wiring are essential to system operation. Because disruption and upset require only a few volts at extremely low current levels, the power levels needed to achieve these effects can be fairly small, and the matching of signal waveforms can be quite imprecise.[19]

Particle-Beam Weapons. Particle-beam 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, 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. Since these accelerated particles cannot penetrate the atmosphere, weapons using this technology against satellites must be based in space. 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 counterspace role appears limited. However, neutral particles can propagate long, linear distances in outer space.[20]

Interceptor Types

Interceptor 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 on board the satellite guide it to close proximity of the target satellite.[21]

Low-Altitude, Direct-Ascent Interceptors. Low-altitude, direct-ascent interceptors are launched on a booster from the ground or from an aircraft into a suborbital trajectory that is designed to intersect that of an LEO satellite. Because these interceptor systems are on a direct suborbital 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.[22] The US Navy's intercept of a failed US intelligence satellite in February 2008 is an example of a low-altitude, direct-ascent interceptor.

Low- and High-Altitude, Short-Duration Orbital Interceptors. A low-altitude, short-duration orbital system is an interceptor that is launched from the ground into a temporary parking orbit from which it maneuvers to attack a specific LEO satellite. A high-altitude, short-duration weapon is an interceptor that is launched from the ground into a temporary parking orbit from which it maneuvers to attack a high-altitude satellite. 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.[23]

Long-Duration Orbital Interceptors. The long-duration orbital system 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 attack the target satellite. The weapon may be stand-alone 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 targets 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, nonmaneuvering objects that are dispersed from one or more satellites in such a way that an artificial Earth-orbiting ring is created. Satellites flying through the ring are damaged or destroyed. Space-to-space missiles are rocket-propelled interceptors launched from an orbiting carrier platform into an orbit that intercepts the intended target.[24]

Nuclear Threat

A nuclear explosion can affect all three segments that make up the US architecture at the same time. Since the effects of nuclear detonation move out rapidly and permeate all space, no satellites have to be targeted directly. The aggressor can simply aim the weapon at an empty point in space, reducing the requirement for a highly accurate missile-guidance system. The environmental effects of a nuclear explosion have been divided into three categories: electromagnetic pulse (EMP), transient nuclear radiation, and thermal radiation. As for the success of a nuclear strike, it depends on three basic factors: the type of warhead (e.g., thermal nuclear, enhanced radiation, and yield), the altitude of the detonation, and the distance of the burst from its intended target.[25]

Electromagnetic Pulse

EMP affects the ground, communication, and space segments of our systems. The EMP threat is unique in two respects. First, its peak field amplitude and rise rate are high. These features of EMP will induce potentially damaging voltages and currents in unprotected electronic circuits and components. Second, the area covered by an EMP signal can be immense. As a consequence, large portions of extended power and communications networks, for example, can be simultaneously put at risk. Such far-reaching effects are peculiar to EMP. Neither natural phenomena nor any other nuclear weapon effects are so widespread.[26]

Within nanoseconds (billionths of a second) of a nuclear detonation, any electrical system is threatened by EMP. One significant factor in EMP effects is the amount of coverage desired. The area of exposure will depend on the size of the yield and the altitude of the burst. Based on the line-of-sight factor, the higher the burst altitude, the greater its coverage. Because of this factor, high-altitude electromagnetic pulse (HEMP) is the highest concern, as the entire electronic spectrum could be affected.[27]

Military systems must survive all aspects of the EMP, from the rapid spike of the early-time events to the longer-duration heave signal. One of the principal problems in assuring such survival is the lack of test data from actual high-altitude nuclear explosions. Only a few such experiments were carried out, and at that time the theoretical understanding of the phenomenon of HEMP was relatively poor. No high-altitude tests have been conducted by the United States since 1963. In addition to the more familiar high-yield tests mentioned above, three small devices were exploded in the Van Allen belts as part of Project Argus. That experiment was intended to explore the methods by which electrons were trapped and traveled along magnetic field lines.[28]

Effects on Space Assets

Perhaps the most devastating threat could come from a low-yield nuclear device, on the order of 50 kilotons, detonated a few hundred kilometers above the atmosphere. A nuclear detonation would increase ambient radiation to a level sufficient to severely damage nearby satellites and reduce the lifetime of satellites in LEO from years to months or less. The lingering effects of radiation could make satellite operations futile for many months. Even nuclear detonations in the 10-kiloton range could have significant effects on satellites for many months. To execute this mission, all that is needed is a rocket and a simple nuclear device. Countries such as Iran, North Korea, Iraq, and Pakistan possess missiles that could carry warheads to the necessary altitudes and either have, or are believed to be developing, nuclear weapons.[29]

Conclusion

Although we have historically considered our CONUS space facilities safe, the events of 11 September 2001 demonstrate that enemy tactics can affect us anywhere. As a result, we must consider the vulnerability of our ground segment throughout the spectrum of conflict—from peace to war. Easy access by anyone with hostile intent makes our ground segment more vulnerable—attacking the ground segment can be as easy as planting an improvised explosive device. Moreover, denying or deceiving the communications link segment is technologically achievable for any adversary we might face. On

the other hand, attack against the space segment requires money, know-how, and access, which limits the potential adversaries to a few countries. Increasingly, we are relying on commercial systems for our space operations, which are usually not "hardened" against potential threats as our military systems are. This further complicates the issue of insuring survivability of our space capabilities. In conclusion, our space systems must be regarded as a system made up of multiple parts—ground segment, link segment, and space segment. All of these are essential to the accomplishment of the space mission, and all must be survivable.

Notes

1. Commission to Assess US National Security Space Management and Organization, *Report of the Commission*, 11 January 2001, http://space.au.af.mil/space_commission/index.htm (accessed 11 May 2009), 13.
2. Tom Wilson, "Threats to United States Space Capabilities," prepared for the Commission to Assess US National Security Space Management and Organization, http://www.fas.org/spp/eprint/article05.html#10 (accessed 11 May 2009).
3. Ibid.
4. Ibid.
5. Ibid.
6. Ibid.
7. Col James G. Lee, "Counterspace Operations for Information Dominance," in *Beyond the Paths of Heaven: The Emergence of Space Power Thought*, ed. Col Bruce M. DeBlois (Maxwell AFB, AL: Air University Press, 1999), 281.
8. Ibid., 281–82.
9. Wilson, "Threats to United States Space Capabilities."
10. Dennis Howe, ed., *FOLDOC: Free On-Line Dictionary of Computing*, http://www.foldoc.org (accessed 11 May 2009).
11. Lee, "Counterspace Operations," 284.
12. Desmond Ball, "Assessing China's ASAT Program," Austral Special Report 07-14S, 14 June 2007, http://www.nautilus.org/~rmit/forum-reports/0714s-ball/fig1-schematic.html (accessed 11 May 2009).
13. Wilson, "Threats to United States Space Capabilities."
14. Ibid.
15. Ibid.
16. Ibid.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.
23. Ibid.
24. Ibid.
25. Ibid.
26. "Nuclear Weapon EMP Effects," Federation of American Scientists, http://www.fas.org/nuke/intro/nuke/emp.htm (accessed 11 May 2009).
27. Ibid.
28. Ibid.
29. Commission to Assess US National Security Space Management and Organization, *Report*, 21.