

## Section II: Overview of Interfering with Satellite Systems

This section gives an overview of some of the means of interfering with satellite systems—both military and civil. Military satellites may be the most obvious targets, but civil satellites perform many essential support functions for military and political operations, such as communications and reconnaissance, and loss of some civil satellites could cause economic distress or enough disruption to make a political point.<sup>1</sup> Military and civil satellites may have different vulnerabilities to some kinds of interference, so that assessment of the tradeoffs associated with protecting them may differ markedly.

Anti-satellite (ASAT) attacks can take a variety of forms and serve a range of goals. For example, they may cause temporary, reversible interference, or they may be intended to cause permanent damage. They may target the satellite, the ground station, or the links between them. They may be overt, or they may be intended to be covert and thus not attributable to the attacker.

The ASAT system may be based on the ground or in space. It may be relatively simple or require sophisticated technology appropriate to a space-faring nation. It may be able to interfere only with satellites in low earth orbit, or it may reach all the way to geostationary altitude.

Different methods of attack provide the attacker different levels of confidence of success. For some, success may be evident, while for others ascertaining whether the attack met its goal may be difficult. Some types of attack are easier to prevent or defend against than others.

This section includes information about these aspects of interference, organized (approximately) by the persistence of the effects. This arrangement traces fairly well the gradation from technically simple to technically demanding.

Preventing a satellite from accomplishing its mission temporarily, reversibly, or nondestructively is commonly called *denial*, while permanent disabling is called *destruction*. However, the distinction is not perfectly clear: whether a technique accomplishes denial or destruction can depend on a situation's details. For example, some denial techniques, such as dazzling a sensor

1. An estimated 60% of the military's satellite communications during U.S. operations against Afghanistan in 2001 (Operation Enduring Freedom) went through commercial satellites (Futron Corporation, *U.S. Government Market Opportunity for Commercial Satellite Operators: For Today or Here to Stay?* April 29, 2003, 4, <http://www.futron.com/pdf/governmentwhitepaper.pdf>, accessed December 17, 2004). The U.S. government was concerned about the availability of high-resolution commercial satellite images during the 2002 war in Afghanistan and used "shutter control"—buying exclusive rights to the Earth images taken in certain parts of the Ikonos satellite's orbits—during the first months of the conflict (John J. Lumpkin, "US Loses Edge on Spy Satellites," Associated Press, April 9, 2002). And state-sponsored satellite broadcasts in Iran and China have been jammed by political opponents. (Safa Haeri, "Cuba Blows the Whistle on Iranian Jamming," *Asia Times*, August 22, 2003; "China to Launch 'anti-jamming' Sinosat-2 satellite in 2005," *Xinhua News Agency*, March 4, 2004.)

with a laser and the use of high power microwaves to disrupt electronics, become destructive at higher powers; below we discuss reversible and permanent effects together for these systems.

Temporary and reversible interference with a satellite system is likely to be less provocative than destructive attacks. Such interference can, in some cases, be plausibly deniable. And it would not damage the space environment by generating debris. These techniques seem to be favored by military planners in the United States and elsewhere. Moreover, temporary interference with a satellite's mission, particularly over one's own territory, is likely to be perceived as defensive and legitimate in a way that permanently disabling the satellite would not.

Note, however, that impairing an individual satellite does not necessarily impair the mission of the constellation of which the satellite is a part. In a system that includes redundancy, back-ups, and alternatives in its design, the vulnerability of individual components need not lead to vulnerability of the system.<sup>2</sup> This point is discussed further in Section 12.

The following discussion considers active interference with a satellite system, but some satellite missions can be frustrated with passive measures. For example, hiding, camouflaging, or moving valuable assets may deny a remote sensing satellite the ability to acquire information about them. Similarly, for satellites designed to attack ground targets or other satellites, adding protection to those objects can deny the satellite that ability.<sup>3</sup>

#### ELECTRONIC INTERFERENCE: JAMMING AND SPOOFING

As discussed in Section 10, satellites communicate with ground-based stations or receivers for a variety of purposes. Signals sent from the ground to the satellite are referred to as the *uplink*; those from the satellite to the ground as the *downlink*. *Jamming* refers to disrupting communication with a satellite by overpowering the signals being sent to or from the satellite by using a signal at the same frequency and higher power. The jamming signal may simply be meaningless noise that drowns out the real signal at the receiver. *Spoofing*, however, mimics the characteristics of a true signal so that the user receives the fake (or spoofed) signal instead of the real one.<sup>4</sup>

To be effective, the jammer or spoofer must be within the *broadcast/receive area* (the area from which broadcast signals can be sent so that they can be received by the receiver) of the receiver it is trying to jam, and it must be able to direct its signal to the receiver.

2. This issue is also discussed in Bruce M. DeBlois et al., "Space Weapons: Crossing the U.S. Rubicon," *International Security* 29 (fall 2004): 1-34.

3. For a discussion of denial and protection, see DeBlois et al..

4. To successfully spoof a receiver, the power of the spoofed signal at the receiver must be nearly the same as that of the true signal. If it is stronger, then the receiver will be jammed rather than spoofed; if it is weaker, the receiver will ignore the spoofed signal in favor of the true signal. T.A. Spencer and R. A. Walker, "A Case Study of GPS Susceptibility to Multipath and Spoofing Interference," 2003, [www.eese.bee.qut.edu.au/QUAV/Unrestricted/Postgraduate/GPS%20Interference/Conference%20Papers/AIAC\\_03.pdf](http://www.eese.bee.qut.edu.au/QUAV/Unrestricted/Postgraduate/GPS%20Interference/Conference%20Papers/AIAC_03.pdf), accessed January 16, 2005.

### *Jamming or Spoofing the Downlink*

By jamming the downlink, an attacker prevents a ground station (or ground-based receiver such as a television, radio, or GPS receiver) from receiving a usable signal from the satellite. In the case of spoofing, the receiver receives a usable but false signal. Some receivers are designed to receive signals from satellites located anywhere in the sky, because this precludes the need to track the satellites or to orient the receiver in a certain direction and allows the receiver to be less complex and expensive. Placing a jammer or spoofer in the broadcast/receive area of such a receiver could be accomplished relatively easily by, for example, placing it on a hill or on an airplane.

The size of the area a jammer or spoofer affects depends in part on the power of the jammer and the strength of the satellite signal. A ground-based jammer or spoofer has the significant advantage of being much closer to the ground-based receivers than the satellite is, so the diminution of the signal by distance is not as pronounced and the jammer or spoofer needs to transmit much less power than the satellite does. And because the jammer or spoofer does not need to be positioned close to the receiver to produce a modest signal, the attacker does not need to know with great accuracy the location of the receiver(s) it is seeking to jam or spoof.

Simple jammers are inexpensive to make or to buy. For example, GPS jammers on the commercial market can reportedly interfere with receivers 150–200 km away, and instructions are available on the Internet for building a homemade GPS jammer inexpensively.<sup>5</sup> Spoofing devices are much more technically complex, since they must be able to mimic in detail the true satellite signal. However, GPS simulators that could spoof GPS receivers can also be purchased. (Jamming and spoofing of GPS receivers is discussed further in Section 12.)

Downlink jamming can be countered in several ways. Any antijamming technology makes it more difficult for an attacker to predict how effective jamming will be.

In some cases it may be possible to increase the power of the satellite's broadcasted signal. The downlink signal can be encoded, thus allowing the receiver to distinguish the real signal from the interference by comparing the incoming signal to a template known only to the user. However, these fixes add complexity and cost to the satellite and receiver system.

The receivers on the ground can be designed to receive signals only from the direction of the transmitters they are to communicate with and to reject signals from other directions. However, such antijamming features can increase the cost and weight of the receivers and, particularly for handheld

5. A *New Scientist* article describes an Air Force team that built a jammer to work against an ultrahigh frequency satellite, with just an Internet connection and \$7,500 worth of materials. It would be fairly simple to adapt the same technique to the GPS frequency. (Paul Marks, "Wanna Jam It?" *New Scientist*, April 22, 2000.)

receivers such as GPS receivers, may in the end make the receivers less usable.<sup>6</sup>

Another method to counter jamming is to have the satellite concentrate its power in a small frequency band and the receiver filter out all other frequencies. If the jammer does not know what frequency the system using, it must spread its power over a much broader range of frequencies to make sure it covers the frequency that is actually being used; such *broadband jamming* can require much higher power. This antijamming technique is a simple version of the more complicated signal manipulations performed in antijamming systems. Such systems may jump between frequency bands using a pattern known only to the legitimate user, making it difficult for the jammer to discover the frequency band being used for transmission fast enough to jam it. However, by forcing the satellite system to use only a small frequency band to transmit information at any one time, jamming or the threat of jamming can significantly reduce the rate at which information can be transmitted to and from the satellite even if it cannot stop transmission altogether.

In principle, a downlink jammer could be placed in low earth orbit to jam transmissions from satellites in high orbit. Since such a jammer would be 50 to 100 times closer to the receiver than a satellite in geosynchronous or semi-synchronous orbit, it could generate significantly larger signals at the receiver. However, since the jammer would move rapidly with respect to the Earth, such schemes are likely to be impractical since they would require a large number of orbiting jammers to keep one in the receive area of the ground user. Increasing the directionality of the receiver's antenna would increase the number of jammers required.

Finally, if a jammer can be located, it can be attacked directly—which is likely to be seen as a legitimate action during a military crisis. A stationary jammer, particularly one sending out a strong signal to, for example, jam receivers over a large area, will be relatively easy to locate and disable and is likely to cause only limited interruption of communication. During the 2003 Iraq war, for example, the GPS jammers used by the Iraqi forces were readily identified and destroyed by the U.S. forces. (Section 12 discusses an alternative approach to GPS jamming that may be more difficult to counter.)

To counter spoofing, the signal from the satellite can be encrypted—scrambled before it is sent and unscrambled after receipt. Because sophisticated techniques such as encoding and encryption add complexity and reduce the amount of data the satellite can handle, commercial satellite operators are unlikely to find a financial case for adopting such techniques unless

6. Many of the troops in the field in the 2003 Iraq war carried their own commercial Global Positioning System receivers rather than those issued by the military, because the commercial receivers were significantly lighter and consumed battery charge at a slower rate, or because they were not issued military receivers (Entry for May 8, 2003, <http://www.coldsteelinfantry.com/iraqi%20freedom%202.htm>, accessed January 17, 2005, a resource website for the soldiers and families of the 2nd Battalion of the 113th Mechanized Infantry Regiment, 42nd Infantry Division, United States Army; Joshua Davis, "If We Run Out of Batteries, This War Is Screwed," *Wired*, June 2003, [http://www.wired.com/wired/archive/11.06/battlefield\\_pr.html](http://www.wired.com/wired/archive/11.06/battlefield_pr.html), accessed January 17, 2005).

the threat scenario changes significantly. For sensitive military and other missions that require dependable and secure links, the tradeoff may, in some cases, make sense.

### *Jamming or Spoofing the Uplink*

The receivers on the satellite itself can be jammed as well, preventing them from receiving the uplink signal. Satellites use uplink receivers to receive command-and-control communications.<sup>7</sup> These links are normally well protected from jamming by encoding the signal and from spoofing by encrypting the signal. Nevertheless, a high-power jammer can defeat the protection provided by encoding by essentially creating too much noise to sort through.

Communications and broadcast satellites use uplink receivers to get signals from the ground they will subsequently retransmit. While military satellites may encode or encrypt these signals before retransmitting them, commercial satellites often receive and retransmit data with a minimum of processing. Such rebroadcast satellites essentially route information from one point on Earth to another; for this reason, they are sometimes referred to as *bent pipes*. It is relatively easy to jam such bent pipe receivers: a ground-based jammer for such communications and broadcast satellites is basically a higher power version of standard communications equipment. Even satellites in geosynchronous orbits can be jammed from the ground, as both the jamming signal and the true signal it is trying to overpower have to travel the same distance and so experience the same decrease in signal strength due to distance.

Commercial communications and broadcast satellites may be particularly vulnerable to uplink jamming and spoofing for another reason: they are designed to receive signals from users over broad ground areas, and thus there will be a large area from which it will be possible to jam or spoof the uplink.<sup>8</sup> (Many such satellites are in geosynchronous orbits, and the broadcast/receive area may cover a large fraction of the Earth's hemisphere.) Thus, a signal originating in one country could be jammed using a jammer in another country. In contrast, an attacker trying to jam the downlink signal from the satellite and to overwhelm the ground-based receiver would need to be somewhere near the receiver.

Jamming or spoofing attacks on commercial satellites could be a particular concern during a crisis for those countries that use commercial satellites to carry some or all of their military communications, including the United States.

Jamming communications broadcast satellites is not a purely theoretical threat. In July 2003, transmissions from the United States being broadcast via the Telstar 12 satellite to Iran were reportedly jammed by Iranians in Cuba,

7. Satellites may use cross-links to perform these functions, but this is uncommon.

8. Geoffrey Forden, "Appendix B: Anti-satellite Weapons," in *Ensuring America's Space Security*, Report of the FAS Panel on Weapons in Space, (Washington, DC: Federation of American Scientists, 2004) 75-81, <http://www.fas.org/main/content.jsp?formAction=297&contentId=311>, accessed January 17, 2005.

who used a ground-based jammer to jam the uplink signals from the United States to the satellite. The United States had recently begun broadcasting its Voice of America program in Farsi, and several private Iranian-American groups encouraging protests against the Iranian government had increased their broadcast programs. The jamming was discontinued after discussions among the interested parties.<sup>9</sup>

As a second example, the China Central Television broadcasts of the 2003 Shenzhou V manned spaceflight were reportedly jammed by the group Falun Gong, which is believed to have repeatedly used transmitters in Taiwan to jam broadcasts in the Chinese mainland by jamming the uplink to the satellite. The new generation of Chinese communications satellites (Sinosat) will reportedly be carrying antijamming equipment.<sup>10</sup>

Jamming uplinks to satellites other than communications and broadcast satellites in geostationary orbits is technically more demanding, since the attacker needs to locate and perhaps track the satellite. This would be the case for any communications networks based in low earth orbit (such as the Iridium system) and for any satellite not in geostationary orbit.

Without detailed knowledge of the satellite, the jammer or spoofer may not be able to promptly determine the success of the attack on a command link, as many satellites can perform autonomously for some time and the behavior of the satellite would not change suddenly. It would be easier to determine the effect on a communications or broadcast satellite, as the downlink could be monitored for changes.

The antijamming and antispoofing techniques discussed above for uplinks could also be used to defeat downlink jamming and spoofing. However, it is generally not feasible for commercial satellites to use a directional antenna, since they rely on being able to serve customers from widespread locations. Nor is it always practical for military satellites, which must often accommodate a large number of users with different uplink capabilities (from mobile field terminals to permanent command centers) whose locations may be unpredictable and widely dispersed. Moreover, it may be more difficult to locate an uplink than a downlink jammer since, in many cases, an uplink jammer could operate from anywhere within a large area.<sup>11</sup>

*Satellite-Based Uplink Jammers.* Any space-faring country could in principle place an uplink jammer on a small satellite close to the target satellite. Because the distance from the jammer to the receiver would be hundreds or thousands of times smaller than the distance from the ground station transmitter to the receiver, the space-based jammer would need tens of thousands of times less

9. Haeri. Iran has also placed strong restrictions on the ownership of satellite broadcast receivers, and the government jams many foreign broadcasts locally by jamming the downlink from the satellite.

10. "China to Launch 'anti-jamming,'" *Xinhua News Agency*.

11. Locating the source of satellite interference is the business of at least one company, Transmitter Location Services, LLC, based in Chantilly, Virginia. The company's website is <http://www.tls2000.com>, accessed January 17, 2005.

power in its signal to give equal signal strength at the satellite receiver.<sup>12</sup> If the jammer were able to orient itself so that its signal could be received by the satellite's antenna, it might be able to conduct effective broadband jamming with low power.

However, it may be difficult in practice to make effective space-based jammers. For the jammer to be in the broadcast/receive area of the satellite's antenna, it would need to be in an orbit below the satellite. Since its speed in that orbit would be greater than that of the satellite, it would quickly cross and move out of the antenna's broadcast/receive area.<sup>13</sup> Keeping a jammer in position to jam the satellite would require essentially continual maneuvering, significantly complicating operations.

A simpler arrangement would be to place a space-based jammer in the same orbit as the satellite, trailing it by a small distance, since it could then maintain a constant distance from the satellite. However, the jammer would be beside and not below the satellite, so it would not be in the main broadcast/receive area of the satellite's antenna. Satellite antennae do have some sensitivity to signals coming from directions other than in the main broadcast/receive area; these directions are covered by the *side lobes* of the antenna. However, the antenna's sensitivity in these directions is many factors of ten less than its sensitivity to signals coming from in front of the antenna. Moreover, once in orbit, the satellite may be able to control the shape and location of the side lobes to suppress them in the direction of a co-orbital jammer. This would result in lower sensitivity to jamming signals entering through side lobes and could easily eliminate the advantage of placing the jammer in space.

## LASER ATTACKS ON SATELLITE SENSORS

*Directed energy weapons*, such as lasers and microwave weapons, have a number of desirable features for an attacker. The beams reach their targets rapidly since they travel at the speed of light, and the delivered power can be tailored to produce temporary and reversible effects or permanent, debilitating damage. Directed energy weapons also have disadvantages relative to physical interceptors: they can only reach targets in their line of sight, unless relay mirrors are used, and simple shields of reflective, absorptive, or conductive material can be effective defenses.

Lasers are especially useful for directed energy attacks because they can emit a large amount of energy in a narrow beam and a narrow band of frequencies. In principle, these features allow the attacker to efficiently direct energy to the right spot on a satellite with the proper frequency to inflict damage; in practice, however, the frequencies that can be used are constrained

12. The signal strength decreases as one over the square of the distance from its source.

13. A jammer in an orbit 1 km below a satellite whose antenna was designed to view the entire section of the Earth below it would cross the broadcast receive area in 2 to 3 hours, whether the satellite was in low earth orbit or geosynchronous orbit. The jammer would spend proportionately less time in a smaller broadcast receive area.

by available technology and other considerations, such as the need to choose a frequency that penetrates the atmosphere in the case of a ground-based laser. Moreover, if the attack requires energy at a range of different frequencies, either multiple lasers that produce different frequencies, or a broadband source may be required, as discussed below.

Lasers can attempt to interfere with a satellite's sensors or to damage the satellite by depositing a large amount of energy. The latter requires much higher power than the former and is discussed later in the section.

Laser technology is mature, and a variety of laser materials and techniques have been developed with a range of power levels. Lasers fall into one of two general categories depending on whether they produce power continuously (*continuous wave (CW) lasers*) or in short, repeated bursts (*pulsed lasers*). The distinction between the two is important for ASAT effects. CW lasers deliver a continuous stream of energy. A simple tabletop CW laser can generate from tens to hundreds of watts; large commercial CW lasers can generate tens of kilowatts or higher.<sup>14</sup> The U.S. Army's Mid-Infrared Advanced Chemical Laser (MIRACL) is a CW laser described as being in the megawatt range.<sup>15</sup>

Pulsed lasers can generate very high power levels over small fractions of a second (referred to as *peak power*), while having modest average power levels (when averaged over seconds). The pulse length and total energy per pulse are also important parameters. The highest power commercial pulsed lasers<sup>16</sup> can deliver terawatts of peak power but only in very short pulses, giving an energy per pulse (average power times pulse length) of 20 J; such pulse energies are common in longer pulses.

As laser power increases, the lasers become larger and more complicated, since they require large power supplies, cooling, and, in some cases, exhaust systems. For example, the MIRACL is fueled by a chemical reaction similar to that used in rocket engines and requires the support of a large facility. The Air-Borne Laser being designed for missile defense with a goal of having power in the megawatt range will have a mass of about 100 tons.<sup>17</sup>

A laser ASAT system also requires a tracking and pointing system. A movable mirror can be used both to direct the laser beam toward the satellite and to focus the beam.

14. A 10 kW 1.315  $\mu\text{m}$  chemical oxygen iodine laser (COIL) costs about \$10 million (see, for example, <http://www.tokyo.afosr.af.mil/coil.html>, accessed January 14, 2005).

15. The MIRACL laser is located at the High Energy Laser Systems Test Facility (HELSTF) at White Sands Missile Range, New Mexico. Its beam has wavelengths in the 3.6 to 4.0  $\mu\text{m}$  range. (See, for example, the MIRACL system's homepage at the HELSTF website, <http://helstf-www.wsmr.army.mil/miracl.htm>, accessed December 20, 2004).

16. Coherent Inc. builds high power commercial lasers, including an Nd:Glass pulsed laser that produces 40 terawatts (TW) of peak power with 20-J pulses. See "Multi-Terawatt Systems," <http://www.coherentinc.com/Lasers/index.cfm?fuseaction=show.page&ID=726>, accessed January 11, 2005.

17. "Extra Weight Will Not Affect ABL Test, Director Says," *Global Security Newswire*, March 7, 2003, [http://www.nti.org/d\\_newswire/issues/newswires/2003\\_3\\_7.html](http://www.nti.org/d_newswire/issues/newswires/2003_3_7.html), accessed December 20, 2004. The Airborne Laser System is intended to be carried by a modified Boeing 747-400F freighter airplane. See Boeing Integrated Defense System's Airborne Laser System webpage at <http://www.boeing.com/defense-space/military/abl/flash.html>, accessed December 20, 2004.

ASAT laser systems can be based on the ground, at sea, in the air, or in space. Ground and air-based laser ASAT systems would operate at visible and infrared wavelengths—wavelengths that can propagate through the atmosphere.<sup>18</sup> Powerful lasers can be readily made at these wavelengths, and light at these wavelengths can be aimed and focused at long distances using moderately sized mirrors. The atmosphere, however, is not perfectly transparent even at these wavelengths, and water vapor and other aerosols, as well as clouds and rain, will reduce the intensity of the beam.

Moreover, the ability to focus the beam may not be limited by the size of the laser's focusing mirror, but by the atmosphere. Turbulence in the lower atmosphere can disturb the transmission of the laser light and spread it out into a larger spot. For laser mirrors larger than a few tens of centimeters in diameter, the atmosphere limits how well the laser light can be focused.

Technical approaches to reducing atmospheric effects exist, such as adaptive optics, in which the mirror surface is rapidly deformed to compensate for atmospheric effects. These technologies are becoming more widespread, but they increase the complexity and cost of the mirror system. Moreover, using adaptive optics for this mission is more demanding than for typical astronomical uses.<sup>19</sup>

### *Dazzling*

Lasers are commonly mentioned as being useful for interfering with satellites that take images of objects on the ground. This section discusses the utility of lasers for temporarily interfering with the sensor a satellite uses for such imaging; such temporary interference is called *dazzling*. Just as a satellite's receiver can be swamped by a jamming signal, a satellite's optical sensor can be dazzled by swamping it with light that is brighter than what it is trying to image. Remote sensing satellites that take high-resolution images of the ground have important strategic and tactical importance and thus may be attractive targets for sensor interference.

To understand dazzling, it is useful to understand how an imaging satellite works. The size of the ground area that the satellite's imaging system can see is determined by the field of view of the satellite's telescope and the size of its sensor. This area is generally much smaller than the total area that would be visible from the satellite (see Figure 5.4). For a satellite taking high-resolution images, this region is only tens of kilometers across. An attack on the satellite's sensor must originate from within the field of view of the satellite's telescope, or else the laser light cannot reach the detector.

The satellite's telescope and optical system focuses an image of a section of the Earth in the telescope's field of view onto a plane called the *focal plane*. On

18. The relevant atmospheric transmission windows are from about 0.35-0.9  $\mu\text{m}$  (includes visible light and part of the near-infrared), 0.95-1.1  $\mu\text{m}$  (near-infrared), 1.2-1.3  $\mu\text{m}$ , 1.55-1.75  $\mu\text{m}$ , and 2.0-2.3  $\mu\text{m}$  (short-wave infrared), 3.5-4.1  $\mu\text{m}$  (medium-wave infrared), and 8.0-13.0  $\mu\text{m}$  (long-wave infrared).

19. DeBlois, 58.

the focal plane is a sensor (or detector), frequently a device made up of a very large number of small, light-sensitive elements called *pixels*. Each pixel generates an electrical signal proportional to the intensity of the light that falls on it, and that signal is sent to a computer.<sup>20</sup> Part of the image on the focal plane falls on the detector; other parts of the image may pass through the telescope, but not fall on the detector. The portion of the Earth corresponding to the section of the image on the detector defines the detector's field of view.

The detector may be a two-dimensional matrix of pixels or a long linear array of pixels. In the first case, the detector tracks and receives light from one rectangular patch of the ground to produce an image, then tracks and receives light from the next patch of ground (this is called a *step-stare* system). This type of sensor is used in the Hubble Space Telescope (though, of course, not pointed towards the Earth), allowing it to stare at a given region of space so that it can collect sufficient light from dim celestial objects.

Earth imaging satellites typically use linear arrays of pixels. As the satellite moves over the Earth, these arrays record the image a line at a time as they sweep over a continuous swath of the Earth. These individual images are stored and then stitched together by a computer to construct a two-dimensional image. (This is similar to the way scanners commonly used with home computers work.) This method of imaging is called *pushbroom* detection.

Thus each pixel corresponds to some small area on the ground within the satellite's full field of view and records the intensity of the light coming from that small area. The resolution of the satellite's imaging system is determined in part by how small an area on the ground corresponds to a single pixel, since the sensor will not be able to record variations of light and dark over smaller areas. For a satellite with a ground resolution of 1 m, for example, each pixel corresponds to regions on the ground about 1 m across.

For example, Space Imaging's IKONOS satellite, which has a ground resolution of 1 m, views a swath below it that is only 11 km wide. Its linear detector contains 13,500 pixels.<sup>21</sup> The French SPOT imaging satellite, which has a ground resolution of 2.5 m to 5 m, views a swath 60 km wide directly below the satellite.<sup>22</sup>

Consider a laser based on the ground that is attempting to dazzle a satellite with 1-m resolution. The laser uses a mirror to steer the beam and focus it on the satellite; that mirror might have a diameter of a few tens of centimeters. Since the satellite typically views a ground area that is tens of kilometers across, when this ground area is imaged on the satellite sensor, the mirror

20. This is the reverse of how a television or computer generates images on the screen. The screen is made up of an array of tiny dots, and the computer creates an image by controlling the brightness of each of these dots. The more dots there are in the screen, the higher the resolution of the image.

21. Gordon Petrine, "Optical Imagery from Airborne and Spaceborne Platforms," *GEOInformatics*, January/February 2002, 28-35.

22. "SPOT Image," <http://www.spotimage.fr>, accessed December 22, 2004. At an altitude of 832 km, the total observable ground area, as discussed in Section 5, would be a circle on the ground with a radius of roughly 3,000 km.

appears as a tiny point of light within that full area. If the satellite's optical system could create a perfect image of the mirror (ignoring effects of the atmosphere), that image would fall only on one or a few pixels on the detector, since each pixel would correspond to a ground area of 1 m across. In this case, if the laser is bright enough, it will dazzle those few pixels.

However, in a real (imperfect) optical system, the light coming from the laser is spread out over a larger part of the detector by several mechanisms. First, the fact that the satellite's telescope has a finite diameter leads to diffraction of the light, which spreads some of the light into a pattern of rings around the image of the laser's mirror. Second, small imperfections in any optical system tend to spread some fraction of the light passing through it out around the image. These imperfections have many sources, including errors in shaping or aligning the optics, distortions due to temperature gradients, and dust in the system. Finally, there may be bright reflections or glints off surfaces (such as edges of the optical elements) within the optical system. Satellite designers work to minimize this stray light and, under normal conditions, it may not be a problem. But stray light from a high intensity laser can be important.

The analysis in Appendix A to Section 11 gives a rough estimate of the laser power required to dazzle a portion of the detector of a high-resolution imaging satellite, assuming a ground-based laser with a 0.15 m diameter mirror. Note that the precise numbers depend on the laser wavelength used, the size of the laser mirror and satellite optical system, etc. Several important points emerge from that analysis. The first point is that because lasers can be focused into an extremely narrow beam, even low power lasers can dazzle small sections of a satellite's detector. However, if the satellite has high resolution, this section may correspond to a small region on the ground. For the situation considered in Appendix A to Section 11, a laser with a power of a milliwatt (mW)—roughly equivalent to that of a laser pointer<sup>23</sup>—appears to be able to dazzle a section of the detector corresponding to an area on the ground that is about 10 m in radius around the location of the laser.

Second, assuming the satellite's optical system is designed to control stray light as discussed in Appendix A to Section 11, the power required for dazzling larger areas of the detector increases rapidly. The calculation in the appendix suggests that laser power must be increased by a factor of 100 in order to increase by a factor of 10 the radius of the ground area obscured by dazzling. However, the required powers are within the range of commercially available lasers. The rough estimates in the appendix suggest that a 10 W laser could dazzle a region corresponding to a ground radius of about 1 km, and a kilowatt-class laser could dazzle a region with a radius of roughly 10 km. For a high-resolution satellite such as IKONOS, dazzling a 10-km region would dazzle essentially the full detector array.<sup>24</sup>

23. Because the beam from a laser pointer has such a small diameter compared with the mirrors considered here for a laser ASAT, the beam would be much less intense when it reached the altitude of the satellite than the ASAT beams, and the laser alone could not be used for dazzling.

24. At the large power required for dazzling a large area, the very intense light falling on pixels near the center of the diffraction pattern can damage those pixels, as discussed below.

Third, the actual power levels required for dazzling depend on the details of the satellite's optical system. It may be possible to design an optical system with lower levels of stray light that would increase the power required to dazzle a given area. On the other hand, satellites not designed to deal with high light intensities might have much higher levels of stray light and could be much more sensitive to dazzling.<sup>25</sup>

The ability to generate these laser powers does not necessarily mean that an attacker can keep a satellite from viewing objects on the ground. Imaging satellites typically carry multiple detectors and filters. Each filter allows only a small band of wavelengths to pass through and reach one of the detectors. The multiple images of the scene taken at these different wavelengths can then be combined to give a full-color image of the scene (a table-top scanner produces color images in the same way). For example, the IKONOS satellite collects light in four bands. The discussion so far has assumed that the laser is operating at a wavelength that can pass through one of the filters and reach one of the detectors. If so, it will be able to dazzle that detector as discussed above. However, the filters greatly reduce the amount of light from that laser that can reach the other detectors. This attenuation of the beam greatly reduces the detector area that can be dazzled, or may eliminate dazzling on these other detectors altogether. Dazzling large sections of all the detectors therefore requires the attacker to know the frequency bands of the various filters and to have lasers operating within each of these wavelength bands. If the attacker does not dazzle all the satellite's detectors, the satellite can still collect images of the ground.

Attempting to dazzle an imaging satellite with a space-based light source is difficult because of the requirement that the dazzler remain in the sensor's field of view, which is very small for the case of high-resolution imaging satellites. We do not consider this case in detail here.

To counter a dazzling attack, the satellite could change the direction it was looking or close a shutter to keep light from reaching the sensor. However, these both have the same effect as the dazzling attack: the satellite is unable to view the area of interest.

### *Partial Blinding*

At sufficiently high intensities, laser light can permanently damage the sensors of imaging satellites. This report refers to such damage as partial blinding, since such an attack will damage only a portion of the sensor. The high intensity can cause the detector material to ablate or evaporate from parts of the detector. It can melt the material or its fragile electronic connections. In addition, the large temperature gradients produced by heat from the laser beam can produce thermo-mechanical stresses.<sup>26</sup>

25. During a test in 1997, a 30-W ground-based tracking laser reportedly dazzled an imaging satellite at 500 km altitude, although few details are available (John Donnelly, "Laser of 30 Watts Blinded Satellite 300 Miles High," *Defense Week*, December 8, 1997, 1).

26. A large body of literature investigating laser damage to detectors includes Vaidya Nathan, "Laser Damage in MWIR MCT Detectors," *Proceedings of SPIE* 2114 (1994): 726; F. Bartoli et al., "Irreversible Laser Damage in IR Detector Materials," *Applied Optics* 16 (November 1977): 2934–2937; Madhu Acharekar, et al. "Calculated and Measured Laser Induced Damage Threshold (LIDT) in Glass and Metal Optics," *Proceedings of SPIE* 3902 (2000): 85–96; and the literature referenced in *Laser ASAT Test Verification* (Washington, DC: Federation of American Scientists, 1991).

Like dazzling, a blinding attack would need to be mounted from within the sensor's field of view for the laser to reach the satellite's detector. However, unlike dazzling, the laser needs to be within the field of view for only a very short time to damage the sensor.

The satellite's optical system helps concentrate the laser energy reaching the satellite by focusing it onto the detector. As with dazzling, this leads to very high intensity at the detector, but restricts the region of high intensity to a small part of the detector, so that it may damage only a few pixels. Unlike dazzling, however, the damage is permanent and cumulative: additional parts of the sensor may be damaged by subsequent attacks. For a linear pushbroom detector, damaged pixels will result in missing lines in the image as the detector sweeps over the swath of ground below it. Such attacks may strongly discourage the country owning the satellite from viewing the area where the laser is located.

The fact that the satellite's optical system concentrates the beam is important for estimating the laser power needed for blinding attacks. The concentration can be estimated by the ratio of the area of the satellite's telescope (which determines how much light is being collected) to the area on the detector onto which this light is focused. For high-resolution imaging satellites, this ratio can be greater than ten billion (see Appendix D to Section 11).

A linear detector in a high-resolution imaging satellite passing over a  $1\text{-m}^2$  area on the ground or the mirror of a ground-based laser, collects light from that area on the ground for a very short time—a tenth of a millisecond—before moving on to adjacent areas. The laser would need to be powerful enough to deliver sufficient energy to damage the satellite's detector in that length of time. The required energy could be delivered either by pulsed lasers, which might have pulse lengths much shorter than a tenth of a millisecond, or by CW lasers, if they were powerful enough to deposit enough energy in the short time available.

Appendix D to Section 11 derives an estimate of the laser power required to damage a section of the detector of a high-resolution imaging satellite. This estimate is necessarily rough since it depends on details of the system, but it suggests a general scale of the power requirements. If the concentration of laser intensity by the satellite's optical system is high enough, even relatively low-power lasers—CW lasers with output powers of tens of watts or pulsed lasers with pulse energies of millijoules—appear to be capable of damaging small sections of a detector, corresponding to ground areas roughly 1 m in size (see Appendix D to Section 11). Damaging a larger section of the detector requires considerably higher power. The estimates in the appendix suggest that increasing the size of the damaged region by a factor of 10 requires increasing the laser power by a factor of 100. These estimates suggest that power levels available from commercial lasers could damage sections of a detector corresponding to tens of meters on the ground.

Partial blinding by a laser based in space is possible since the laser needs to be in the satellite's field of view for only a very short time. The shorter distance between the laser and the satellite in this case would reduce the laser power required relative to a ground-based laser.

Shutters can in principle protect satellite sensors from blinding, although the satellite system would need to detect the attack with enough time to react. For example, the satellite could include a sensor with low sensitivity to survey the ground area ahead of the primary sensors<sup>27</sup> or might detect a lower-power aiming phase prior to the attack. A nonlinear optical material that becomes opaque to beams with high intensity might be placed at an intermediate focus in the optical path to act as a switch to protect the sensor.

As discussed in the dazzling section, a laser operating at a particular wavelength could only deliver high intensity laser light to a satellite's detector if that wavelength fell within the small band of wavelengths that could pass through one of the detector's optical filters; otherwise, the intensity of the light reaching the detector would be sharply reduced. To damage the detector, the attacker would therefore need to know the filter bands. Even if this was known, a laser operating at a single wavelength could damage only one of the multiple detectors an imaging satellite would carry.

Predicting and confirming the success of a blinding attack may not be simple. Blinding is more difficult to perform confidently than dazzling. The energy needed for a dazzling attack can be determined by the local conditions and the sensor's resolution on the ground: the dazzling laser just needs to be brighter than the light reflected by the Earth within that area. In contrast, the amount of energy required for blinding can vary by large factors depending on details of the satellite's optics and sensor system.

For commercial and civil satellites, an attacker can gather details about the optical system and sensor design from public sources. For sensitive military and intelligence satellites, some information about the optics system (a modest guess as to the telescope aperture and focal length) can be gleaned from ground-based images of the satellites, and the sensor wavelengths can be surmised since the atmosphere limits the wavelengths that can be used and the wavebands are usually made as wide as possible so to increase the signal-gathering capability. Sensor materials and technology are well understood and a determined adversary may be able to make reasonable estimates of the effects a laser would have on them, although the details of sensor construction could be important.

## HIGH-POWERED MICROWAVE ATTACKS

A second directed energy weapon that could be used to attack satellites is a device that produces high-powered microwaves (HPM). Microwaves are electromagnetic waves with wavelengths shorter than radio waves but considerably longer than visible light.<sup>28</sup> They are commonly used by radars and for sending communication signals.

27. Ashton B. Carter, "Satellites and Anti-Satellites: The Limits of the Possible," *International Security* 10 (Spring 1986): 46-98.

28. Microwaves are typically considered to lie in the frequency band between about 1 GHz (corresponding to a 30-cm wavelength) and 300 GHz (corresponding to a 1-mm wavelength).

HPM attacks could in principle be directed at a satellite either from a ground-based or space-based HPM weapon. Ground-based HPM weapons would have to contend with long distances to the satellite, which limits their utility. Producing high intensity at the satellite requires high levels of emitted power and a large antenna for focusing the beam.<sup>29</sup> Moreover, the atmosphere limits the transmission of beams of microwaves with very high power.<sup>30</sup> For these reasons ground-based HPM anti-satellite systems appear less interesting than HPM weapons that attack at shorter ranges: those based in space or popped up using a suborbital missile.

Microwave radiation at high intensities, if they are able to enter and affect (or *couple* to) some component of the satellite, can disrupt a satellite's electronics and, above some threshold, permanently damage them. In a nondestructive attack, the microwaves may, for example, reset computers and garble commands, disrupting the satellite's function during the attack and for a time after. HPM attacks can permanently damage a satellite's electronics if the strength of the microwaves that couple to the system is large enough.

The coupling of HPM to the satellite's electronics is characterized either as *back door* or *front door*. Front door attacks couple to the satellite through the antennae used for broadcast and communication, which are designed to receive and amplify radio signals with frequencies in or near this range. Front door attacks are therefore mounted from within the area in which the satellite can broadcast and receive signals. Unlike jamming, however, HPM attacks use a short, high-power pulse and need be in the broadcast/receive area only briefly.

Microwaves can couple through the front door at any frequency that the satellite's receiver system accepts; the success of coupling is therefore more predictable if this information is known. The receiving electronics in the satellite are often designed to pick up faint signals, and overwhelming them with high intensity radiation can leave them permanently damaged if they are not properly protected. While front door attacks can potentially couple a large amount of energy to the satellite, if the satellite is designed to detect and block large signals from reaching the sensitive components, delivering an effective attack may be difficult. The effect on a satellite will not be predictable without information about the satellite's design.<sup>31</sup>

29. Since microwaves have wavelengths thousands of times longer than optical light, focusing them is more difficult than focusing optical light since it requires a much larger antenna. This limits the ability of an HPM system to focus radiation over long distances. See Appendix B to Section II for a discussion of antenna size and directionality.

30. At high intensities, microwaves will cause the air to break down and no longer transmit. For lasers, which have shorter wavelengths, the atmosphere will transmit beams that are thousands of times more intense before breaking down (Philip E. Nielsen, *Effects of Directed Energy Weapons*, [Washington, DC: National Defense University, 1994], [http://www.ndu.edu/ctnsp/directed\\_energy.htm](http://www.ndu.edu/ctnsp/directed_energy.htm), accessed December 21, 2004).

31. Damage thresholds are very uncertain, as they depend on the details of the system being attacked. H. Keith Florig estimates (in "The Future Battlefield: A Blast of Gigawatts" *IEEE Spectrum* 25 [March 1988]: 50-54) that a fluence (energy per area) in the front door of about 100 J/m<sup>2</sup> would damage unshielded electronics that were directly coupled to the satellite's antenna. Other damage threshold estimates are given in Nielsen and the references therein.

In back door attacks, the microwaves enter the satellite by some other means than an antenna. The metal casing of a satellite helps shield its electronic components from microwave attacks, but microwaves can enter the satellite through small seams in the casing or gaps around electrical connections. If microwaves enter the satellite in this way, they can interact with and damage a wide variety of the electronics inside the satellite. Since back door attacks do not enter the satellite through the antenna, they need not take place from the broadcast/receive area of the satellite and they need not be in the frequency band the satellite is built to receive.

The amount of coupling and the effects of back door attacks are, however, difficult to predict and will be a major source of uncertainty to the attacker. The ability of microwaves to find ways to enter the satellite may depend on factors such as the quality of construction and effects of aging. The frequency of microwaves that can couple through the back door will not be known since it depends on the dimensions of these openings. Coupling to the target can be increased by *chirping* the microwaves—emitting over a range of frequencies—to increase the chances that one of the frequencies will couple to a back door. However, spreading the power over a range of frequencies decreases the power at any one frequency, which may also limit the weapon's effect. Since the microwave signal is not collected and amplified as it is in a front door attack, the power levels required for a successful back-door attack are significantly higher.<sup>32</sup>

HPM technology is still maturing. The principal technical issues are generating high power from modestly sized devices and packaging the emitter in a useable and robust platform.<sup>33</sup> One of the more developed and compact HPM sources (called a vircator) can reportedly generate tens of gigawatts of microwave power at frequencies up to the gigahertz frequencies used by satellite communications. One report states that a 400-kg device could produce 2 to 5 gigawatts (GW) of HPM power in a short pulse.<sup>34</sup> This type of device generates its power using an explosive generator and so would be used only once. Such a weapon would have relatively short range: using a 1-m focusing antenna, it would need to be within about 1 km of an unshielded computer to disrupt it.<sup>35</sup> For a back door attack, poor coupling would decrease this distance; for a front-door attack, the distance could be tens of kilometers.

While the technology to create HPM exists and is likely to become more widely available, the effectiveness of these weapons will continue to be highly

32. Florig estimates that a back door attack might require a fluence a thousand times higher than a front door attack to cause the same disruption.

33. See reviews by Carlo Kopp, "The Electromagnetic Bomb—a Weapon of Electrical Mass Destruction," *Air & Space Power Chronicles*, <http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html>, accessed January 15, 2005, and Carlo Kopp, "An Introduction to the Technical and Operational Aspects of the Electromagnetic Bomb," Australian Air Power Studies Centre Paper 50, November 1996.

34. Kopp, "An Introduction."

35. This range assumes  $10^5$  J/m<sup>2</sup> is required to disrupt an unshielded computer and that the weapon creates a millisecond pulse (Florig).

uncertain, which limits their utility, especially against targets considered important enough to attack. Both the extent to which the microwaves couple to the satellite components, and their effects on the components if they do couple, will be uncertain. A given attack could be destructive, disruptive, or completely ineffective, depending on the details of the satellite's design. Although classes of systems should respond similarly to an HPM attack, it is difficult to predict with any certainty how any particular satellite will react without actually testing it. Moreover, electronics can be hardened against microwave attacks of moderate levels without great cost if the protection is incorporated into the initial system design; a hardened satellite could withstand orders of magnitude higher HPM flux than an unhardened satellite.

Space-based HPM weapons would be available only to space-faring countries. Since the HPM weapon needs to be close to the satellite, a co-orbital weapon is likely to be detected and identified as a threat. However, an HPM weapon in a crossing orbit intended for use as it passed close to the target satellite might not be recognized as a threat. Countries with short-range missiles could attempt to loft an HPM weapon to a high altitude and set it off near a satellite it wanted to attack. The attacker would need to be able to orient the weapon to aim it at the target satellite, and it would have to pass close enough to the satellite to be within the weapon's lethal range;<sup>36</sup> both of these factors could further increase the uncertainties in using the weapon.

The attacker may not be able to immediately determine if the attack was successful, apart from monitoring downlinks. If the satellite was permanently disabled, this might become evident over the course of a few weeks if the satellite's stationkeeping maneuvers could be monitored.<sup>37</sup> If the satellite was not updating its orbit correctly, the attacker might surmise that it was no longer functioning.

## DESTRUCTION

### *Attacks on Ground Stations*

Satellite operators command satellites from ground stations, which may be attacked with weapons from the outside, by agents from the inside, or remotely by hackers. Precautions that a satellite owner could take include screening employees' backgrounds, physically protecting the station with walls and gated entry, and making plans to transfer the ground station's operations to another facility in an emergency.

A successful attack on a ground station is likely to be disruptive for a period of time, but with proper planning by the satellite's operator, use of the satellite should be restored relatively quickly, by, for example, transferring

36. For a discussion of the difficulties of placing a lofted payload near an orbiting satellite, see Section 12.

37. For an example of how this could be used to determine the operational status of a satellite, see Pavel Podvig, "History and the Current Status of the Russian Early Warning System," *Science and Global Security* 10 (2000): 21-60, [http://www.princeton.edu/%7Eglobsec/publications/pdf/10\\_1Podvig.pdf](http://www.princeton.edu/%7Eglobsec/publications/pdf/10_1Podvig.pdf), accessed January 10, 2005.

control of the satellite to a backup station. Unlike a damaged satellite, damage to the ground station can be repaired.

### *Laser Attacks on Satellites: Heating and Structural Damage*

High-power lasers can subject satellites to large amounts of energy. The resulting heat can upset the delicate thermal balance of the satellite for long enough to damage the satellite's components or, if sufficiently intense, can damage a satellite's structure by, for example, weakening the hulls of pressurized tanks. Solar panels are also vulnerable to laser attacks.<sup>38</sup>

Since these attacks are not aimed at the sensor, the attacker is no longer confined to the satellite sensor's field of view, as in an attack intended to dazzle or blind. An attack can be mounted from any location that puts the satellite in the attacker's line of sight—from the ground, the air, or space—if sufficient laser power is available.

Compromising robust satellite components, such as the bus or non-sensor payload, requires powerful lasers. Studies of laser attacks on satellites estimate that for unshielded satellites in low earth orbits, ground-based megawatt class lasers could create this damage in a few seconds, and for the most fragile parts, kilowatt-class lasers could do the same in a longer period of time.<sup>39</sup> Laser attacks intended to disrupt the satellite by heating may require lower power. The altitude of geostationary satellites protects them from structural damage by lasers on the ground or in low earth orbits.

Developing a laser ASAT system for these kinds of attack is difficult and expensive, thus such attacks are restricted to technically sophisticated countries. Delivering high laser intensity to satellites requires a powerful laser, a large mirror for focusing the beam, and for ground-based lasers, adaptive optics to reduce atmospheric effects.<sup>40</sup> Currently, the technology does not exist to build a high-power space-based laser weapon.

There are some defensive measures a satellite could take, such as hardening exposed surfaces, building in redundancy, and deploying a protective shield against the laser light. (Satellites do not routinely carry shields today.) Such measures could allow the satellite to withstand the effects of the attack or could delay the onset of disruptive or lethal effects long enough to allow it to take other defensive actions. If the attacking laser were space-based, increasing

38. Damage of solar panels due to heating is discussed in FAS, "Laser ASAT Test Verification," 28 and in Forden, 75. Potential damage due to unequal charge across the panel is mentioned in Martin Unwin, "A Study into the Use of Laser Retroreflectors on a Small Satellite," 1995, <http://www.ee.surrey.ac.uk/SSC/CSER/UOSAT/IJSSE/issue1/unwin/unwin.html>, accessed January 15, 2005.

39. Detailed technical analysis of using high-powered lasers against space targets can be found in "Report to the American Physical Society of the Study Group on Science and Technology of Directed Energy Weapons," *Reviews of Modern Physics* 59 (July 1987): S1-S201 and in FAS, "Laser ASAT Test Verification."

40. Large mirrors are more technically difficult to produce and much more expensive than smaller ones. The cost of a ground-based telescope rises with diameter at approximately the power of 2.5; see for example, Aden and Marjorie Meinel, "Extremely Large Sparse Aperture Telescopes," *Optics and Photonics News*, October 2003, 26-29.

the time the satellite is protected is particularly significant since requiring the laser to operate for longer periods of time could exhaust the supply of fuel the laser needs to create the laser beam.

The success of laser attacks intended to cause structural damage to an unshielded satellite should be fairly predictable; success on a satellite that has taken defensive precautions may be unpredictable. Similarly, the effectiveness of other kinds of laser attacks, such as attacks intended to disrupt the satellite by heating it, may be highly uncertain. As with other types of attacks, its effectiveness may be difficult to assess. Structural damage to a satellite in low earth orbit may be visible from the ground using a telescope. Otherwise, the attacker may need to rely on monitoring changes in the downlinks or in the satellite's stationkeeping maneuvers.

### *Kinetic Energy Attacks*

Attacks that attempt to damage or destroy a satellite through high-speed collisions with another object are called *kinetic energy* attacks. Kinetic energy is the energy in the motion of an object. The faster two objects are moving relative to one another, the more kinetic energy is available to be turned into destructive force when they collide. Since satellites move at high speeds, a collision with even a small object can seriously damage them.<sup>41</sup> Even a collision that leaves the satellite largely intact could cause it to tumble.

*Ground-based Kinetic Energy Attacks.* Kinetic energy attacks that are launched from the Earth and attempt to destroy the satellite without placing an object into orbit are referred to as *direct-ascent* attacks.

Such an attack may use a homing interceptor. The ASAT would be launched on a missile that carries it above the atmosphere and releases it in the direction of the target satellite. The interceptor would then use its sensors to detect the target satellite and its thrusters to guide it to collide with the satellite. Shortly before intercept it might release a small cloud of pellets to increase the possibility of collision. Since the attack can be direct-ascent and does not require the interceptor to be placed in orbit, attacking satellites in low earth orbit requires only a relatively short-range missile to loft the interceptor to the satellite's altitude (see Section 8). Because of the difficulty of launching objects directly to geosynchronous altitudes, direct-ascent attacks are likely to be used only against satellites in low earth orbit.

For a homing ASAT, the attacker need not determine the trajectory of the satellite with high accuracy. It would need only to determine it accurately enough and deliver the interceptor into space accurately enough that the sensors on the interceptor could locate the satellite. The interceptor would also need to be close enough to the satellite so that its maneuvering capability is

41. The kinetic energy of an object with mass  $m$  and speed  $V$  is given by  $mV^2/2$  and, therefore, increases rapidly with the speed of the object. The kinetic energy of an object of mass  $m$  traveling at 3 km/s is roughly the same as the explosive energy of the same mass  $m$  of high explosive.

sufficient to guide it to intercept. The attacker would need the technical sophistication to build a simple homing device (which would include a sensor and the ability to maneuver accurately). If it can do these things, this method of attack has a high chance of success. Any space-faring country should be able to develop such an interceptor; simple homing systems using commercially available sensors should be within the reach of many other countries.

The United States successfully tested a direct-ascent interceptor against a satellite in low earth orbit in the 1980s. The interceptor was launched by a missile carried on an F-15 aircraft.<sup>42</sup> The interceptors being deployed as part of the U.S. ground-based midcourse missile defense system use direct-ascent kinetic energy interceptors to target ballistic missiles, and these could also be used to attack satellites throughout low earth orbit.<sup>43</sup>

If an attacker does not have the ability to develop a homing interceptor, but does have ballistic missile technology, it could instead try to launch a large cloud of pellets into the path of the satellite. The success of such an attack depends on various parameters, such as how well the attacker is able to determine the satellite's trajectory, how well the attacker can control the placement and dispersal of the pellet cloud, and what total mass of pellets the attacker's missile can loft to the orbital altitude of the satellite. This method is examined in more detail in Section 12, which finds that this method is unlikely to be an attacker's choice if other options exist. In particular, unless the attacker has accurate missiles and good tracking capability, the effectiveness of such an attack may be low, and the attacker could have little confidence in the attack.

Some protection against attacks by small pellets can be gained by deploying shielding on the forward portion of the satellite, and modest maneuvering may be effective against a non-homing attack (see Section 12). However, neither shielding nor maneuvering capability could be expected to protect against homing interceptor attacks, since the mass of the objects hitting the satellite would likely be too large to shield against,<sup>44</sup> and the interceptor is likely to have more maneuvering capability than the satellite.

Damage from a kinetic energy attack to a satellite in low earth orbit is likely to be detectable from Earth using even a moderate-size telescope to image the satellite. Damage might also be assessed by monitoring the satellite's downlinks or tracking its stationkeeping maneuvers.

Destruction of a satellite by impact is likely to generate some persistent debris; just how much and how long the debris persists depends on the altitude of the satellite and the details of the collision. If the attacker has long-term interests in space, debris production may be a deterrent to using these types of weapons if other weapons are available.

42. Laura Grego, "A History of US and Soviet ASAT Programs," April 9, 2003, [http://www.ucsusa.org/global\\_security/space\\_weapons/page.cfm?pageID=1151](http://www.ucsusa.org/global_security/space_weapons/page.cfm?pageID=1151), accessed January 17, 2005.

43. See David Wright and Laura Grego, "Anti-Satellite Capabilities of Planned US Missile Defense Systems," December 9, 2002, [http://www.ucsusa.org/global\\_security/space\\_weapons/page.cfm?pageID=1152](http://www.ucsusa.org/global_security/space_weapons/page.cfm?pageID=1152), accessed January 17, 2005.

44. A homing interceptor that released a cloud of pellets as a kill enhancer shortly before intercept could use fewer, larger pellets than in a nonhoming attack, since the cloud would be much smaller.

*Space-Based Kinetic Energy Attacks.* Instead of using a direct-ascent approach, kinetic energy ASATs can also be placed in orbit prior to an attack. They may be launched shortly before the attack, as was the case with the co-orbital ASAT developed and tested by the Soviet Union in the 1960s to 1980s, which was intended to complete only a few orbits before attacking.<sup>45</sup> Space-based ASATs may also be deployed in space well before they are used; such ASATs are often called *space mines* (although the term includes ASATs that use other attack methods besides kinetic energy—see Section 12).

Like direct-ascent ASATs, space-based ASATs can use unguided clouds of pellets, or homing interceptors. A cloud of pellets would be released in an orbit that crosses the satellite's orbit or in the same orbit as the target satellite, but moving in the opposite direction so that the relative speed in a collision would be large. An orbiting pellet cloud may be more effective over time at destroying a satellite than a lofted cloud, since the orbiting cloud could be designed to pass near the satellite repeatedly; however, since it would constitute persistent orbital debris, it could threaten other satellites as well over time.

A homing interceptor could be placed in a crossing orbit to allow a high-speed collision. Or it could be placed in the same orbit, in which case it could approach the target satellite slowly and, for example, fire a small cloud of pellets to destroy it.

An ASAT placed in a low-altitude orbit could also be used for a kinetic attack on satellites in much higher orbits, including geostationary orbits, if it is given sufficient propellant for maneuvering. In particular, the discussion in Section 6 shows that an ASAT in orbit at 400 km could reach a satellite in geostationary orbit if it is designed to have a  $\Delta V$  of 2.4 km/s; the travel time to orbit in this case would be about 5 hours. If the  $\Delta V$  of the ASAT is instead 4 km/s, the travel time to orbit would be reduced to 1.5 hours. This issue is of interest since the space-based interceptors (SBI) that might be placed in orbit as part of a space-based ballistic missile defense system would require a  $\Delta V$  of this magnitude to allow them to swiftly engage a missile in its boost phase (see Section 9). The SBI could therefore be designed to have ASAT capability (if they are given the proper sensors, for example),<sup>46</sup> and a missile defense system would contain thousands of SBI—many more than the number of potential targets in high orbits. Even a relatively small number of SBI would represent a significant threat to satellites in geostationary orbit.<sup>47</sup>

45. Grego.

46. Wright and Grego.

47. Since an interceptor designed for attacking a satellite rather than a boosting missile would require less maneuverability for the homing process and for accelerating out of orbit, it could have significantly smaller mass. For example, using the same assumptions for the SBI as in the APS Boost-phase study (*Report of the American Physical Society Study Group on Boost-Phase Intercept Systems for National Missile Defense*, July 2003, [http://www.aps.org/public\\_affairs/popa/reports/nmd03.html](http://www.aps.org/public_affairs/popa/reports/nmd03.html), accessed January 16, 2005) but with  $\Delta V$  of 0.5 km/s for homing and 3 km/s for accelerating out of orbit (instead of 2.5 and 4 km/s), the SBI mass would decrease from 820 kg to 300 kg.

Because space-based ASATs must be placed in orbit, they are limited to countries with a space-launch capability. We discuss the possible advantages and disadvantages of ground- and space-basing for ASATs in more detail in Section 12.

Since both the target satellite and the kinetic energy ASATs considered in this section are in orbit, the speeds involved in a collision can be very high. While the speed and geometry of such collisions are likely to create persistent space debris, the amount and lifetime of that debris would depend on the details of the collision.

*Bodyguard Satellites.* Defensive satellites, often called bodyguard satellites, are sometimes discussed as a potential means of protecting high-value satellites from kinetic energy attacks.<sup>48</sup> How difficult this task is depends in part on what the bodyguard is intended to defend against. Defending against a co-orbital ASAT that approaches the satellite slowly might be relatively straightforward. Defending against ASATs in crossing orbits, however, could be difficult because the ASAT could approach at high speed and from a wide range of directions. A system of defensive satellites would require a capable surveillance system that could provide sufficient warning of an attack. For bodyguards using kinetic energy interceptors, even a successful intercept by the bodyguard could create debris that might damage the satellite it was defending.

Even if bodyguard satellites could be made to work against some kinds of threats, countries will not be able to rely on them to protect their satellites from direct attack or interference by a determined adversary. Their effectiveness against real-world attacks would not be known and they cannot be designed to defend against all possible threats to the satellite. Deploying bodyguard satellites does not preclude the need to take into account the vulnerability of satellite systems and to have back-up systems for any essential military capabilities provided by satellites.

### *Electromagnetic Pulse from a High-Altitude Nuclear Explosion*

A nuclear explosion at an altitude of several hundred kilometers would create an intense electromagnetic pulse (EMP) that would likely destroy all unshielded satellites in low earth orbit that are in the line of sight of the explosion.

In addition, the explosion would generate a persistent radiation environment that would slowly damage unshielded satellites in LEO.<sup>49</sup> The radiation

48. See, for example, William L. Spacy II, "Does the United States Need Space-Based Weapons?" School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, AL, 1998, 40-44, [http://www.au.af.mil/au/awc/awcgate/saas/spacy\\_wl.pdf](http://www.au.af.mil/au/awc/awcgate/saas/spacy_wl.pdf), accessed January 16, 2005; and DeBlois, 60.

49. For a discussion of these issues, see FAS, *Ensuring America's Space Security*, 23; and Defense Threat Reduction Agency, "High Altitude Nuclear Detonations (HAND) Against Low Earth Orbit Satellites (HALEOS)," briefing slides, April 2001, <http://www.fas.org/spp/military/program/asat/haleos.pdf>, accessed January 16, 2005.

environment could also make it more difficult for high-altitude satellites to communicate with ground stations (depending on their communication frequencies) and would last months to years. However, the extent of the damage the increased radiation could cause is uncertain, and shielding satellites against it is estimated to add only a few percent to the cost of the satellite. The designs of many military satellites incorporate protections against EMP and increased radiation.

Such an attack is indiscriminate and unlikely to be undertaken by an adversary with investments or aspirations in low earth orbit. However, because of the large area it could affect and the persistence of the radiation effects, detonating a nuclear weapon in space could be a highly effective terrorist-style attack by a country that had a nuclear weapon and a medium-range missile to launch it.

In principle, a nuclear warhead intended as an ASAT could be launched from the ground or based in space. However, the Outer Space Treaty prohibits the signatories from placing nuclear weapons in orbit. Moreover, a country with only a few nuclear weapons seems unlikely to place one into orbit for possible future use against satellites.

## Section 11 Appendix A: Laser Power Required for Dazzling

To dazzle an earth-observing satellite, the dazzler needs to produce a signal at the sensor stronger than the light reflected from the Earth. The brightness of this reflected light varies widely by time of day and by the surface from which it reflects.<sup>50</sup>

The intensity of sunlight reaching the surface of the Earth in a 1-micrometer ( $\mu\text{m}$ ) band around a wavelength of  $1\ \mu\text{m}$  is roughly<sup>51</sup>  $600\ \text{W}/\text{m}^2$ . To get a rough estimate of the intensity at the satellite of the sunlight that is reflected from the Earth, we assume that the full incident intensity is reflected diffusely, so that it is spread over  $2\pi$  steradians (sr). Under these assumptions, the scattered sunlight from  $1\ \text{m}^2$  of the Earth is roughly  $100\ \text{W}/\text{sr}$ . For this calculation, the satellite is assumed to have a ground resolution of  $1\ \text{m}$  and is assumed to image a  $1\text{-m}^2$  piece of Earth onto one pixel.

Now consider a laser on the ground of power  $P$  watts, operating at a wavelength of  $1\ \mu\text{m}$ , and assume the laser beam is focused by a mirror with diameter  $D_L$  meters. The diffraction limit of the mirror allows the beam to be focused into a solid angle of approximately  $(1.22\lambda/D_L)^2$  sr (see Appendix B to Section 11). Atmospheric effects also cause the beam to spread, and this effect may be larger than the mirror's diffraction. At optical wavelengths, the atmospheric effects are such that, unless adaptive optics are used, increasing the size of the mirror beyond about  $0.15\ \text{m}$  does not result in a more compact beam. A mirror of this size focuses the laser power into a solid angle of roughly  $10^{-10}$  sr.

As a result, if the laser uses a  $0.15\text{-m}$  diameter mirror, the power per steradian from the laser is roughly  $10^{10}P\ \text{W}/\text{sr}$ . Since the laser's mirror is smaller than  $1\ \text{m}$ , the satellite's optics focus the laser light onto one pixel.

The intensity reaching the satellite from the laser ( $10^{10}P\ \text{W}/\text{sr}$ ) is therefore equal to the intensity from a  $1\text{-m}^2$  piece of the Earth ( $100\ \text{W}/\text{sr}$ ) for a laser power  $P$  of  $10^{-8}\ \text{W}$ . To ensure that the laser power overwhelms the reflected sunlight, we assume that the laser power should be 10 times the reflected light. By this estimate, a laser with a power  $P$  of  $0.1$  microwatts ( $\mu\text{W}$ ) could dazzle the pixel on which the light from the laser mirror was imaged. Since each pixel corresponds to only a size of  $1\ \text{m}^2$  on the ground, this is not useful to the dazzler since obscuring such a small area is unlikely to be useful.<sup>52</sup>

However, as noted in the text, the laser light is not perfectly focused onto one pixel, but is spread out over a larger part of the detector by several mechanisms. For this analysis, we assume that reflections off surfaces within the

50. A sensor may have settings that make it is less responsive to light when it is viewing bright areas and more responsive when viewing dark areas.

51. S.C. Liew, "Principles of Remote Sensing," Tutorial, <http://www.crisp.nus.edu.sg/~research/tutorial/solrdrn.gif>, accessed January 12, 2005.

52. If the intensity on a pixel is high enough to saturate it, the electrons it generates can overflow the pixel's storage bin. Depending on how the array is designed, these electrons can spill over onto neighboring pixels in a process called *blooming*. However, there appear to be ways to design the array so that electrons that spill over are carried away from the detector rather than affecting neighboring pixels.

satellite's optical system have been eliminated. Instead we consider light that is diffracted by the satellite's optics and light that is spread over the focal plane around a central peak by imperfections in the optical system. We write the intensity at a distance  $d$  from the central peak as  $I(d) = A(d)I(0)$ .

Following the discussion above, we assume that a pixel at a distance  $d$  from the central peak will be dazzled if the laser intensity reaching that pixel, which is smaller than the intensity at the central peak by the attenuation factor  $A(d)$ , is ten times greater than the light reaching that pixel from the ground. As a result, the laser power  $P_d$  required to dazzle pixels out to a distance  $d$  is roughly  $0.1/A(d) \mu\text{W}$ .

Due to diffraction by the satellite's circular mirror, the image of  $1 \text{ m}^2$  on the ground is focused to a spot on the detector with a diameter of roughly  $1.22 f\lambda/D_s$ , where  $D_s$  is the diameter of the satellite's mirror,  $f$  is its focal length, and  $\lambda$  is the laser wavelength; this length on the detector therefore corresponds to roughly  $1 \text{ m}$  on the ground. The central spot is surrounded by concentric rings that make up the diffraction pattern. The central peak contains roughly 84% of the light from the image;<sup>53</sup> the remaining 16% is spread into the diffraction rings. The diffraction pattern (including only the diffraction effect of the finite diameter of the satellite's mirror, but not the diffraction from the satellite's support structure and secondary mirror, which may comprise an additional few percent of the peak) can be approximated as a Fraunhofer diffraction pattern from a circular aperture, and the spacing and intensity of the rings can be calculated (see Appendix C to Section 11).

The maximum intensity of the first ring is  $0.018$  times the intensity of the central peak. By the fourth ring, which corresponds to a distance of about 4 meters on the ground, the intensity has dropped to less than  $10^{-3}$  of its value at the central peak. Far from the central peak, the intensity of the maxima in the diffraction pattern falls off as one over the cube of the distance from the central peak (Appendix C to Section 11).

Techniques exist for suppressing the intensity of the diffraction rings by modifying the optics. This process, called *apodizing*, may lead to some broadening of the central peak, which reduces the resolution of the system. It may also reduce the total amount of light that gets to the sensor, which may degrade the image. Whether it makes sense to reduce the intensity of the diffraction rings depends on the level of stray light in the system that comes from other sources.

The intensity of stray light from imperfections in the satellite's optical system appears to decrease more slowly with distance from the central peak than the diffraction peaks, and will therefore be the dominant source of light far from the central peak. Published studies of the Hubble Space Telescope and follow-on systems suggest that the intensity of stray light may decrease roughly as one over the square of the distance from the central peak.<sup>54</sup>

53. Max Born and Emil Wolf, *Principles of Optics*, 7th Edition (Cambridge, England: Cambridge University Press, 2003), 443.

54. John E. Krist, "WFPC2 Ghosts, Scatter, and PSF Field Dependence," August 9, 1995, <http://www.stsci.edu/software/tinytim/tinytim.html>, accessed December 15, 2004, and Pierre Bely et al., "NGST Optical Quality Guidelines," August 24, 2001, [http://www.ngst.nasa.gov/public/unconfigured/doc\\_0791/rev\\_04/monograph7\\_v10.pdf](http://www.ngst.nasa.gov/public/unconfigured/doc_0791/rev_04/monograph7_v10.pdf), accessed December 15, 2004.

To estimate the laser power required to dazzle pixels out to a given distance from the central spot, we assume that  $A(d) = 10^{-3}$  at a distance  $d$  corresponding to 3 to 4 m on the earth, as it would be for a pure Fraunhofer diffraction pattern, and falls off as  $d^{-2}$  for larger  $d$ , corresponding to the falloff for scattering due to optical imperfections.

This estimate suggests that, under the assumptions made above, a 1-mW laser, operating at a wavelength of  $1 \mu\text{m}$  and focused by a 0.15-m mirror, could dazzle a section of the satellite's detector corresponding to a ground image with a radius of about 10 m around the laser. One milliwatt is roughly the power of a standard laser pointer. Furthermore, under these assumptions, to increase the radius of the area that can be dazzled by a factor of 10, the laser power must increase by a factor of 100. Approximate results are given in Table 11.1.

**Table 11.1.** This table illustrates how the power of a ground-based laser needed to dazzle part of a satellite's detector increases with the size of the ground area corresponding to that section of the detector. This calculation assumes a laser operating at  $1 \mu\text{m}$  focused by a 0.15-m mirror, and a satellite with 1-m resolution.

Radius of Ground Area Corresponding to Dazzled Region of Detector	Required Laser Power
10 m	1 mW
100 m	0.1 W
1 km	10 W
10 km	1 kW

The discussion in Appendix D to Section 11 shows that by the time the laser power is high enough to dazzle a large section of the detector, the central peak is bright enough to damage the detector in that area. We emphasize that the values in Table 11.1 are approximate and depend on the level of stray light in the optical system, and will differ for specific systems.

## Section II Appendix B: Angular Size, Resolution, and Beam Divergence

### ANGULAR SIZE AND RESOLUTION

The apparent size of an object can be expressed in angular units and is called its angular size. Two sets of units are commonly used. A circle consists of  $2\pi$  radians (r) or 360 degrees ( $^\circ$ ). There are 60 arcminutes (denoted by ') in each degree of arc, and 60 arcseconds (denoted by ") in each arcminute. Angular sizes are related to physical sizes by the object's distance: the angle subtended by an object is proportional to its physical size and inversely proportional to its distance. For example, a bicycle viewed from 100 m subtends roughly the same angle as a bus viewed from 400 m. It turns out that the Sun, at a distance of  $1.5 \times 10^8$  km from Earth, subtends the same angle as the Moon, at a distance of around  $3.85 \times 10^4$  km, because the ratio of their physical sizes happens to be the same as the ratio of their distances from the Earth.

The angular size  $\Delta\theta$  of an object (for small angles) is given in radians by

$$\Delta\theta = l/d \quad (11.1)$$

where  $l$  is its physical size and  $d$  is its distance. For  $l$  in meters and  $d$  in kilometers,  $\Delta\theta$  is given in units of arcseconds by

$$\Delta\theta = 20.6'' \left[ \frac{l/10}{d/100} \right] \quad (11.2)$$

The angular resolution of a telescope depends on the diameter  $D$  of the telescopic lens or mirror and the wavelength  $\lambda$  of the radiation the telescope gathers. It is given in radians by

$$\Delta\theta = 1.22 \lambda/D \quad (11.3)$$

or in arcseconds by

$$\Delta\theta = 0.14'' \left[ \frac{\lambda/550}{D} \right], \quad (11.4)$$

where  $\lambda$  is measured in nanometers and  $D$  in meters.

The resolution improves as the wavelength gets shorter (visible light has a shorter wavelength than radio waves, and ultraviolet light has a shorter wavelength than visible light) and as the diameter gets larger. For example, an optical telescope (which gathers visible light) with a diameter of 10 m has an angular resolution of roughly 0.1 microradian ( $\mu\text{r}$ ) or 0.02", whereas a radio telescope of the same size has a resolution of roughly 0.1 milliradian (mr) or 20"—making it worse by a factor of 1,000.

The angular resolution indicates how far apart two objects have to be in order to be seen as separate objects rather than one object. A telescope with angular resolution of 20  $\mu\text{r}$  (4") could not distinguish two stars that are sepa-

rated by  $10 \mu\text{r}$  ( $2''$ ), but a telescope with an angular resolution of  $5 \mu\text{r}$  ( $1''$ ) could. The angular resolution also indicates how much detail the telescope can observe about an object at a specific distance. For an object at 500 km, a telescope with a resolution of  $2 \mu\text{r}$  ( $0.4''$ ) could see detail on the scale of 1 m; one with a resolution of  $20 \mu\text{r}$  ( $4''$ ) could observe details on the scale of only 10 m.

For an imaging satellite, the size of objects it can see on the ground depends on the altitude of the satellite and on the satellite's optics. The image of the ground is focused onto the focal plane, where the sensor is mounted. The imaging system is usually designed so that the physical size of the smallest object that can be imaged by the satellite (called the *resolution element*, given by the angular resolution multiplied by the effective focal length of the optics) matches the pixel size of the sensor, so that the resolution element falls onto one or a few pixels.

#### BEAM DIVERGENCE

The divergence of a beam transmitted by a telescope is closely related to the angular resolution of the telescope when it is used to observe an object. A telescope of a given diameter transmits a beam of approximately  $\Delta\theta = 1.22\lambda/D$ , where the size of the beam is given in radians and effects of the atmosphere are neglected. The size of the beam,  $l$ , at a given distance away can be found by multiplying the beam size by the distance,  $d$ , so that  $l = \Delta\theta \times d$ . For example, a beam of light with wavelength  $1 \mu\text{m}$ , being focused by a telescope of 1-m diameter, produces a beam of diameter 0.85 m at a distance of 700 km.

## Section II Appendix C: Fraunhofer Diffraction Pattern

The intensity  $I$  of the Fraunhofer diffraction pattern, assuming light of wavelength  $\lambda$  passing through a circular aperture of diameter  $D$ , is<sup>55</sup>

$$\frac{I}{I(0)} = \left( \frac{2J_1(x)}{x} \right)^2, \quad x = \frac{\pi Dd}{f\lambda} \quad (\text{II.5})$$

where  $I(0)$  is the intensity at the central maximum,  $J_1$  is a Bessel function of the first kind of order 1,  $f$  is the focal length of the satellite's telescope, and  $d$  is the distance from the optic axis on the focal plane, where the detector is located. The pattern is axially symmetric around the central maximum, which lies on the optic axis.

The maxima and minima of  $I/I(0)$  are given by the condition<sup>56</sup>

$$0 = \frac{d}{dx} \left( \frac{I}{I(0)} \right) = 8 \left( \frac{J_1}{x} \right) \left( \frac{J_1'}{x} - \frac{J_1}{x^2} \right) = -\frac{8}{x^2} J_1 J_2 \quad (\text{II.6})$$

The minima occur when  $J_1 = 0$  since this makes  $I/I(0) = 0$ . When  $I$  is non-zero,  $J_1$  must be non-zero; in this case Equation II.6 requires  $J_2 = 0$ , and this is the condition for the secondary maxima. For large  $m$ , the  $m$ th zero of  $J_2$ , and therefore the  $m$ th secondary maxima of  $I/I(0)$ , occurs approximately at  $x_m = (m + \frac{3}{4})\pi$ , where  $m = 1$  refers to the first secondary maximum.<sup>57</sup> The value of  $d$  at the secondary maxima is therefore linear in  $m$ .

For large  $x$ , the maximum values of  $J_1$  have the form<sup>58</sup>

$$J_1(x) \approx \sqrt{\frac{2}{\pi x}} \quad (\text{II.7})$$

so that the intensity at the secondary maxima has the form

$$\frac{I}{I(0)} \approx \frac{8}{\pi} \frac{1}{x^3} \quad (\text{II.8})$$

Table II.2 lists the locations of the secondary maxima of the diffraction pattern and the corresponding intensities.

55. "Fraunhofer Diffraction-Circular Aperture," <http://scienceworld.wolfram.com/physics/FraunhoferDiffractionCircularAperture.html>, accessed February 6, 2005.

56. The final equality uses Eq. 9.1.27 from F.W.J. Oliver, "Bessel Functions of Integer Order," in *Handbook of Mathematical Functions*, ed. Milton Abramowitz and Irene A. Stegun (Washington, DC: Government Printing Office, 1972), 361, online at [http://jove.prohosting.com/~skripty/page\\_355.htm](http://jove.prohosting.com/~skripty/page_355.htm), accessed February 6, 2005.

57. Oliver, 371, Eq. 9.5.12.

58. Oliver, 364, Eq. 9.2.1.

**Table 11.2.** This table shows the locations of the secondary maxima of the diffraction pattern and the intensity of those peaks relative to the intensity of the central maximum,  $I/I(0)$ . Here  $x_m$  is the argument of the Bessel function at the  $m$ th maximum,  $d/d_0$  is the distance (on the detector) of the maximum from the central maximum in units of  $d_0 = 1.22\lambda f/D$ , which is the distance on the detector corresponding to the angular resolution of the satellite's optics (see Appendix B to Section 11). For the case considered here,  $d_0$  corresponds to about 1 m on the ground.

$m$	$x_m$	$d/d_0$	$I/I(0)$
1	5.14	1.3	0.018
2	8.42	2.2	0.0042
3	11.6	3.0	0.0016
4	14.8	3.9	0.00078
5	18.0	4.7	0.00044
6	21.1	5.5	0.00027
7	24.3	6.3	0.00018
8	27.4	7.2	0.00012
9	30.6	8.0	0.000089

## Section II Appendix D: Power Estimate for Laser Blinding

To develop a rough estimate of the laser power required to damage pixels in a satellite's detector, we assume the damage threshold for a silicon detector is  $10^6$  J/m<sup>2</sup> of incident energy delivered in less than  $10^{-4}$  seconds. The damage threshold depends on the detector material; the value for silicon appears to be high compared with other materials.<sup>59</sup>

A ground-based laser of power  $P$  operating at wavelength  $\lambda$  and using a mirror of diameter  $D_L$  spreads the laser light over a disk with diameter of roughly  $1.22\lambda R/D_L$  at a distance  $R$ , giving an intensity at that distance of

$$I = \frac{P}{\pi \left( \frac{1.22\lambda R}{2D_L} \right)^2} = \frac{4D_L^2 P}{\pi(1.22\lambda R)^2} \quad (\text{II.9})$$

As in the discussion of dazzling in Appendix A to Section II, the laser light collected by the satellite's optical system is assumed to be focused onto one pixel. The optical system will concentrate the light by a factor  $C$ , which is roughly the ratio of the area of the satellite's telescope to the area on the detector onto which this light is focused. If  $D_S$  is the diameter of the satellite's telescope and  $f$  is its focal length, the ratio of these areas is  $D_S^2/[1.22\lambda f/D_S]^2$ . For  $D_S = 1$  m,  $f = 2$  m, and  $\lambda = 1$   $\mu$ m, this ratio is greater than  $10^{11}$ .

Over a time  $\Delta t$ , the energy incident on the pixel is then

$$\frac{\text{Energy}}{\text{area}} = CI\Delta t = \frac{4C D_L^2 P \Delta t}{\pi(1.22\lambda R)^2} \quad (\text{II.10})$$

The laser power required to damage the pixel on which this light is focused is found by setting this expression equal to the energy per area needed to damage the detector, taken here to be  $10^6$  J/m<sup>2</sup>. Assuming the distance to the satellite is 800 km, the laser wavelength is 1  $\mu$ m, and the concentration factor  $C$  is  $10^{10}$ , this equation gives a condition for achieving the damage threshold at the pixel onto which the laser is imaged

$$D_L^2 P \Delta t \approx 10^{-4} \text{ Jm}^2 \quad (\text{II.11})$$

The time it takes for the satellite to pass over a 1-m<sup>2</sup> area of the Earth is roughly  $10^{-4}$  s, so this will be the time the detector will have to collect light from that small ground area. Using this time for  $\Delta t$ , a CW laser with a mirror

59. Silicon has a damage threshold at an irradiation time of  $10^{-4}$  seconds of about  $10^{10}$  W/m<sup>2</sup>, for a total energy deposited of  $10^6$  J/m<sup>2</sup>. The damage threshold is similar for a range of incident wavelengths, from 0.69  $\mu$ m to 10.6  $\mu$ m. Other common detector materials have lower damage thresholds at this timescale: InSb and HgCdTe thresholds are around  $5 \times 10^4$  J/m<sup>2</sup>. See F. Bartoli, L. Esterowitz, M. Krueger, and R. Allen, "Irreversible laser damage in IR detector materials," *Applied Optics* 16 (November 1977): 2934–2937.

diameter of 0.15 m and a power of 40 W would therefore be able to meet the damage criteria in Equation 11.11. Using a 1-m diameter mirror with adaptive optics, the required power could be reduced to about 1 W.

For a pulsed laser,  $\Delta t$  is taken as the length of a pulse (as long as it is less than  $10^{-4}$  s) and  $P$  as the peak power. The quantity  $P\Delta t$  is then roughly the total energy per pulse. For a mirror diameter of 0.15 m, a laser that produces pulses with energy greater than about 4 mJ can satisfy the damage criteria in Equation 11.11, assuming the pulse width is less than  $10^{-4}$  s. For a 1-m mirror, a laser producing pulses with an energy of 0.1 mJ will satisfy Equation 11.11. If the pulse width and the time between pulses is short enough that several pulses are produced in  $10^{-4}$  s, then  $P\Delta t$  is the sum of the energies of all those pulses.

These numbers give a rough estimate of the power levels required for damaging a few pixels on a detector.

As in the discussion of dazzling (Appendix A to Section 11), we note that the optical system will spread some of the laser light over a larger part of the detector. Under the same assumptions as in the discussion of dazzling, the intensity of the laser light at a distance of about 10 pixels from the central peak of the diffraction pattern, corresponding to a ground distance of about 10 m, would be roughly  $10^{-4}$  times that maximum intensity. Delivering enough light to a pixel at that distance to damage it would therefore require a laser power  $10^4$  times larger than needed just to damage the central pixel, or 400 kW for the CW case with a 0.15-m mirror, and 10 kW for a 1-m mirror. While CW lasers with powers of 10 kW are commercially available, 400 kW lasers are not. Assuming, as in Appendix A to Section 11, that the intensity of the stray light in the detector falls off as one over the square of the distance from the central peak, increasing by a factor of ten the damaged area on the detector requires increasing the laser power by a factor of 100 (see Table 11.3).

For mirror sizes of 0.15 m and 1 m, a pulsed laser able to produce pulses with energy greater than 40 J and 1 J, respectively, with pulse widths less than  $10^{-4}$  s, would be able to damage the detector out to a distance of about 10 pixels from the central peak by the criteria used here. Commercial industrial lasers with pulse energies of tens of joules are sold for applications such as welding and drilling.<sup>60</sup> Using a 1-m mirror, a laser capable of producing 100 J pulses could damage a detector out to a distance of about 100 pixels from the central peak, corresponding to a ground distance of about 100 m, under the assumptions used here.

These results suggest that lasers with commercial-level power might damage the detectors of high-resolution imaging satellites over areas corresponding to tens of meters on the ground.

The power required for damaging the detectors of actual satellites depends on details of the detector and optical system, and may differ, perhaps significantly, from these estimates.

60. See, for example, U.S. Laser Corporation, "High Power Pulsed Nd:YAG Laser," <http://www.uslasercorp.com/pulsedspecs.html>, accessed January 14, 2005.

**Table 11.3.** This table illustrates how the required power (for a CW laser) or pulse energy (for a pulsed laser) needed to damage part of a satellite's detector depends on the size of the ground area corresponding to that section of the sensor, and on the size of the laser's mirror. This calculation assumes a laser operating at  $1\ \mu\text{m}$  focused by either a 0.15-m or 1-m mirror, and a satellite with 1-m resolution.

Laser mirror diameter $D_L = 0.15\ \text{m}$		
Ground distance corresponding to detector damage	Power (CW laser)	Pulse energy (Pulsed laser)
1 m	40 W	4 mJ
10 m	0.4 MW	40 J
Laser mirror diameter $D_L = 1\ \text{m}$		
Ground distance corresponding to detector damage	Power (CW laser)	Pulse energy (Pulsed laser)
1 m	1 W	0.1 mJ
10 m	10 kW	1 J
100 m	1 MW	100 J