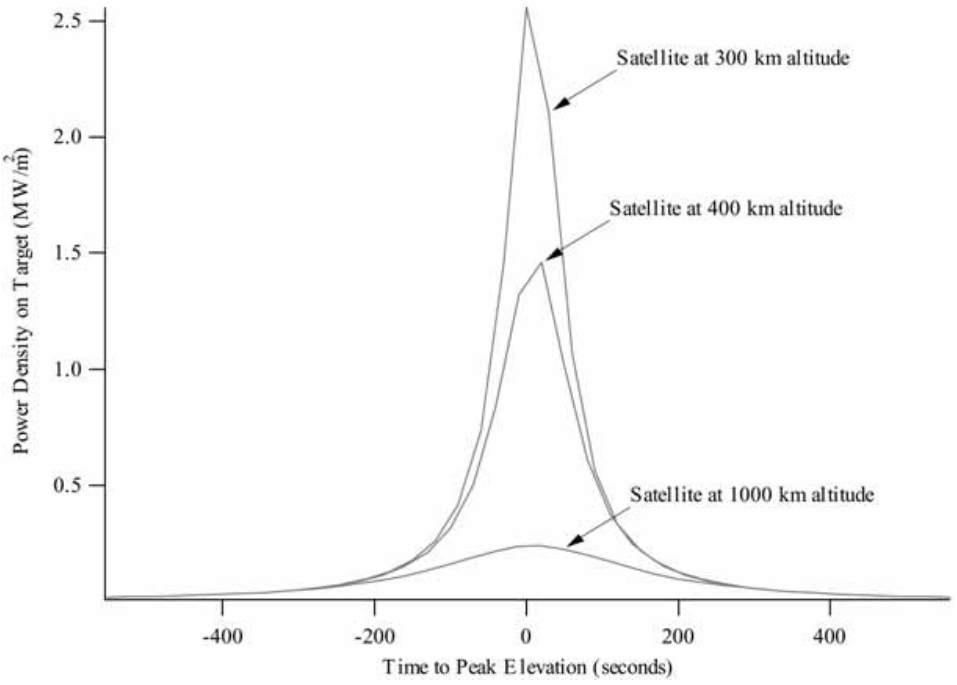
APPENDIX B

Anti-satellite Weapons
Geoffrey Forden

Laser Attacks against Satellites

In the past, both the United States and Russia have considered using lasers in missile defense systems. Such systems, if they were actually completed, have an inherent capability against satellites in low Earth orbit. In fact, the United States tested at least the aiming capability of a ground-based laser system against a satellite and there have been media reports that China is interested in using a laser system in an anti-satellite mode. It is straightforward to calculate the power delivered to a satellite as it passes a ground-based laser. The graph below shows the power delivered to satellites, assuming a three megawatt laser focused on the satellite using a mirror one meter in diameter.

Figure 1. The power density delivered to a satellite as it transits over a ground based laser for various orbital altitudes. The orbital motion limits the time the satellite is visible and changes the range of the laser, and hence the power delivered.



No atmospheric effects, which would certainly lower the effective power density at the satellite, have been included. However, the same adaptive optics techniques that are used in observational astronomy could be used to improve the power delivered.

The power densities at these relatively low Earth orbits, on the order of a megawatt per square meter, are enough to do significant structural damage to many of the exposed components on satellites. For instance, any pressurized tanks, such as fuel tanks for orbital maneuvering, could be exploded and structural members, such as solar panel support struts, could be weakened and potentially could break off if the satellite undergoes any motion during the attack. Of course, many optical instruments, such as the charged coupled devices (CCD) used to record images, would be destroyed if exposed to the laser beam.

Some might worry that satellites in still higher orbits, such as the GPS/NAVSTAR constellation at 20,000 km, might still be in danger of being incapacitated by other, more subtle, affects of a laser attack. For instance, it is possible that a laser could heat up a satellite's solar cells so much that they lose all efficiency of converting sunlight into electricity. Since a satellite's power budget is so finely tuned, it is possible that such an attack could send the satellite into a standby mode, effectively removing it from use for at least the time it is illuminated by the laser. The next figure below shows some of the quantities that determine the effectiveness of such an attack: the range to the satellite, which changes as the satellite approaches the laser, the elevation of the satellite as seen by the laser, which determines the atmospheric effects that have to be overcome, and relative orientation of the solar cells to the laser as they follow the sun.

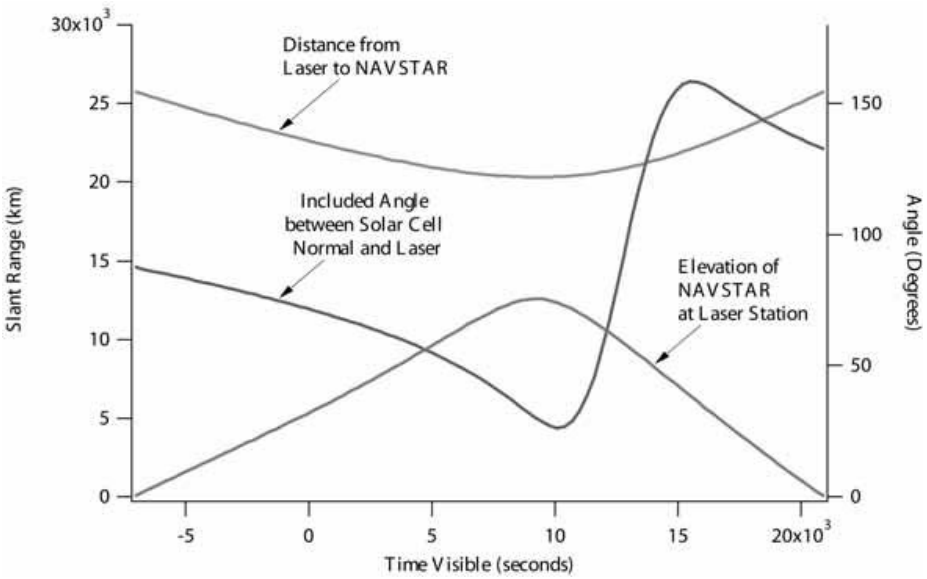


Fig.2. Quantities that determine the effectiveness of a laser attack on GPS/NAVSTAR

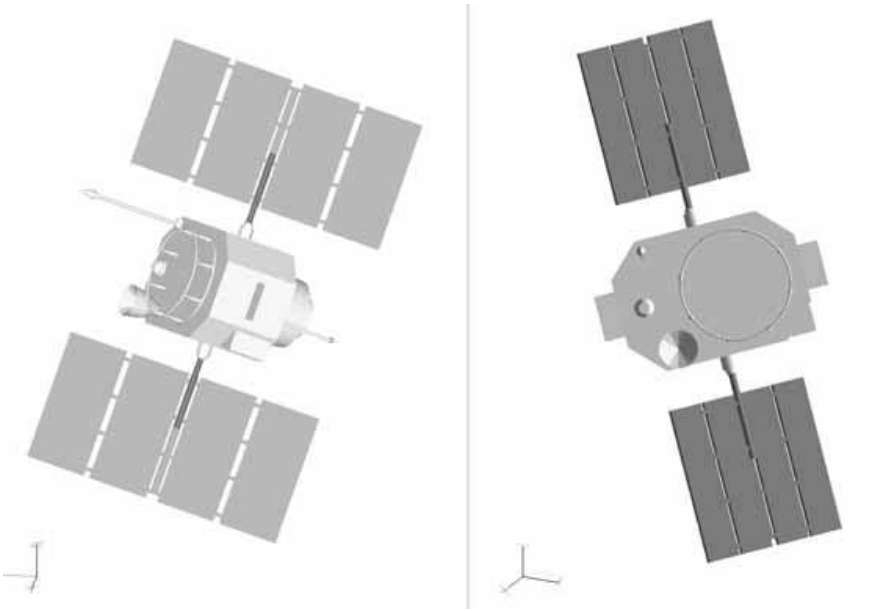


Fig. 3. The images show a GPS/NAVSTAR satellite, viewed from the sun's direction (left) and the laser's direction (right). In orbit, the solar panels change their orientation to keep the maximum area directed to the sun. Thus the power density delivered to the solar cells changes as the panels are turned away from the laser.

These show that the solar cells' efficiency might be reduced by as much as 25% if the panels use silicon cells but only about 10% if GaAs cells are used. However, because of the worst-case assumptions made, a real attack will most likely be considerably less effective for either type of solar panel.

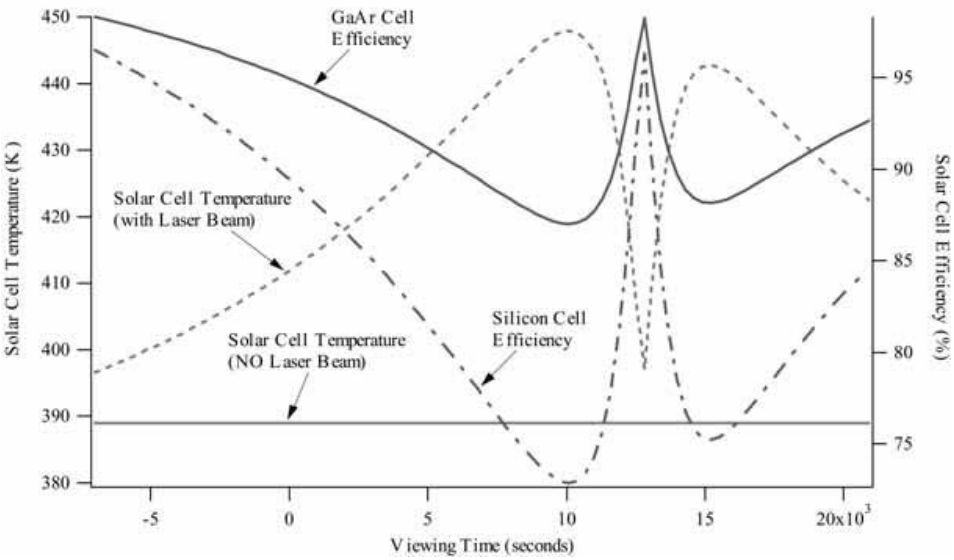


Fig. 4. Results of a 3 megawatt ground-based laser attack on GPS/NAVSTAR.

As this power is delivered to the solar cells, they heat up, decreasing the efficiency with which they can covert solar energy to electricity (it has been assumed that the laser is an infrared laser whose wavelength is below the threshold for producing electricity in the cells). We can assume a worst case scenario and assume that all of the laser beam is absorbed and that the panels reach equilibrium with a linear dependence on temperature (this produces a much higher temperature than the more realistic temperature to the fourth power). With these assumptions, the satellite's solar panels reach a maximum temperature of 450 Kelvin (normal operating temperatures are around 390 Kelvin). The two types of solar panels in use today would suffer different losses in efficiency, between 10 and 25%. It is possible that the power budgets of the GPS/NAVS- TAR satellites might be strained by

such a loss of efficiency. However, it is also possible that, since the effect could only last as long as the satellite was under attack (about four hours) that the satellites' batteries could make up the difference. Of course, it is highly likely that a more realistic calculation, and not using worst-case scenario used here, would indicate that the panels would suffer considerably less heating and therefore less loss of efficiency.

Jamming of Satellite Links

The U.S. military, as well as the entire world economy, makes extensive use of commercial satellite communications, which are essentially all based in geostationary Earth orbits (GEO). While such distant orbits make these satellites relatively immune from the physical threats lower Earth orbit satellites might face, their distance, coupled with the economic factors that drive the industry, actually makes them more susceptible to electronic jamming. Instead of jamming the receiver on the ground, the satellite-signal jammer attacks by trying to overwhelm the signal sent to the satellite, which then rebroadcasts that jammed signal back to Earth. The recent jamming, apparently by the Cuban government, of National Iranian TV (NITV), a station operated by an Iranian dissident group based in Los Angles, should act as a wakeup call.

The distance to a geostationary satellite, roughly 35,000 km above the surface of the Earth, broadens the radio beams beamed up to the satellite. To avoid unintentional interference between adjacent GEO satellites, the world community has established rules that allocate both orbital positions (the longitude "slot" the satellite appears to hover over) and radio-frequencies both beamed up to the satellites and beamed down to the Earth. These frequencies are both known to the world at large and relatively unchangeable. Furthermore, companies that sell satellite services have equipped their satellites with technologies that have the capability of being accessed from large areas on the surface of the Earth. As will be discussed below, investigators working for the satellite's owner eventually determined that the signals jamming NITV were coming from a facility just outside Havana, Cuba. Figure 5 below shows the "gain", or sensitivity, of the uplink antenna for Telstar-12 (the satellite that was jammed in the most recent incident involving NITV); both Havana and the legitimate ground station outside Washington D.C. have similar reception gains.

Figure 5 Uplink gain for Telstar-12 (source: Loral Skynet Telstar 12 Technical Manual). The satellite has the same sensitivity to transmissions from much of Cuba, the apparent source of the most recent jamming, as the authorized uplink site near Washington D.C.

Most commercial telecommunications satellites have a battery of transponders, circuits that pickoff whatever signal is in a narrow frequency range from the receiving antenna, amplify it and retransmit it at a slightly different frequency to a different part of the globe. Unlike military satellites, there is little or no anti-jamming capability on commercial satellites since, at best, many of these technologies would increase the operating costs and could, in the worst case, reduce the number of users each satellite could service. There have been over 7000 incidents where an unauthorized signal has caused interference with satellite-based communications. Most of these have been unintentional interferences; commercial radio stations around the world have often caused unintentional interference with signals being beamed to satellites. However, recent years have seen a number of incidents where countries have intentionally interfered with these uplink signals.

NITV has been jammed on at least three different occasions, on at least three different satellites: Hotbird, Eutelsat W3, and most recently the Telstar-12. In the first two cases, the solution to the jamming problem was to switch satellites with the most recent change to a U.S. based uplink facility for Telstar12. In the first two

cases, the solution to the jamming problem was to switch satellites with the most recent change to a U.S.-based uplink facility for Telstar-12, which has a reception area far from Iranian jamming facilities. However, NITV's signal on Telstar-12 has been successfully jammed since 5 July 2003, apparently from the Cuban signals-intelligence facility at Bejucal. It is important to note that these incidents involve non-space faring nations, Iran and Cuba, disrupting significant space assets. There appears to be little or no recourse for current commercial telecommunications satellites other than to protest[1] the interference since instituting anti-jamming technology would severely impact their economic viability. This problem becomes more and more troublesome to the U.S. as more and more U.S. military communications bandwidth is sent over commercial satellites.

The world community could act to institute economic sanctions against countries that either sponsor or allow jamming from their territories. This might, conceivably, end the recent incidents of politically motivated jamming. However, it is doubtful that it would affect jamming against commercial assets used by the U.S. military in times of crises. One option, in that case, would be for the U.S. to consider such interference grounds to attack third parties, an action that might disrupt fragile coalitions. Or the U.S. could act now to reduce the susceptibility of civilian communications. For instance, the government of the United States could, in the future, introduce incentives to make commercial satellite communications less vulnerable to jamming. One such possibility might be to offer discounts on launch services to satellites that incorporate anti-jamming technology. (These would, however, have to be fairly steep discounts to compete with private launch services, such as SeaLaunch, or foreign launches like those provided by China.) The Government could also offer tax breaks to the owners of satellites if they incorporate anti-jamming technologies in their satellites or perhaps it could pay higher rates along with a guaranteed minimum
purchase of bandwidth to those telecommunications companies whose satellites do have anti-jamming technologies.

Even if private industry did switch to secure communications, it would be a number of years before these would become effective. Telstar-12, the victim of the most recent jamming, was launched in 1999 and has at least a 15 year lifetime. It is likely that a large fraction of the communications bandwidth the U.S. military relies upon will remain susceptible to jamming until at least 2015.