

## **Responding to Asymmetric Threats in Space**

James A. Lewis

House Armed Service Committee,

Panel on Asymmetric and Unconventional Threats

Center for Strategic and International Studies

November 1, 2005

Space is an area of American military advantage. No nation or group of nations now has the capability to challenge U.S. predominance in space. The basis of this predominance rests on more than one hundred satellites for remote collection of images and signals, for communications and navigation, and a ground infrastructure to process, analyze and disseminate information from space assets. The U.S. military space program is a critical component of U.S. national security.

However, the current military space system, while superior to any in the world, faces new demands, new missions and new risks. Potential opponents recognize that U.S. military advantage rests in part on access to space services provided by satellites for intelligence, communications, intelligence collection, weather forecasting and navigation. Disruption of these services would degrade American military capabilities and provide a symbolic victory. We know that potential opponents either have contemplated or have efforts underway to disrupt U.S. military space capabilities.

The need to mitigate these risks should help shape U.S. planning and acquisitions for national security space. This asymmetric threat to space assets is, in many ways, not a conventional military problem, and it requires a different kind of response from the U.S. The goal of this response should be to ensure the continued delivery of adequate space services to military and intelligence operations despite disruption or destruction by hostile action. Measures to produce this result fall into three categories: redundancy, hardening and innovation.

### **Risk Mitigation Through Redundancy**

Redundancy ensures that even if some satellites or ground facilities are damaged or destroyed, there will be sufficient assets to allow the continued provision of space services. The Internet is a useful model for thinking about redundancy. It, and the telecom backbone it uses, were designed to allow continued communications even if a major node in the network had been destroyed in a strategic nuclear exchange. The internet automatically reconfigures and routes around damage to provide continued service. We should similarly think of space operations as a network built on multiple military, commercial and even foreign satellites. Adopting this network approach could provide the capability to quickly reconfigure space assets in the event of an attack so as to ensure continued access to critical space services.

Building redundancy into military space operations has several components. Redundancy comes from having access to multiple sources of space services. Developing these multiple sources can be done achieved through several approaches that will provide the ability to rapidly replace space assets. In the past, the U.S. has stockpiled some assets. This,

combined with a rapid space launch capability (that would allow the U.S. to replace satellite in orbit) could provide redundancy. However, stockpiling is an expensive approach and other, lower cost alternatives are more attractive.

One alternative approach is to use commercial space services in communications and imagery. Our opponents can use the availability of commercial space services for military advantage. The U.S. should make use of these services as well. The U.S. already relies on commercial communications services for military operations and it is increasingly reliant on commercial space imagery for geospatial intelligence. This reliance is not a vulnerability, but an advantage.

There is an innate proclivity among agencies to prefer to harden assets under U.S. control rather than build redundancy. The military services, naturally, would rather own a satellite and have complete control and access to its services. This could weight decisions in favor of spending more on programs rather than exploring alternative commercial sources. Satellites that are wholly owned and operated by the military must form the backbone of our national security space system, but this backbone can be reinforced by commercial services. In its review of space programs, Congress may wish to take this into account.

The use of foreign space service providers by the Department of Defense is also an advantage. While the provision of space services by foreign companies requires a greater emphasis on the security and integrity of data, it greatly expands the number of satellites available to a military space network. The use of foreign space assets also complicates the planning of a potential opponent, in that they will need to attack the assets of neutral third parties in a conflict to disrupt services. Attacking U.S. space assets in a conflict is one thing, but attacking French or other European assets could create serious diplomatic problems that may deter a potential attacker.

The U.S. can increase redundancy within its own satellite fleet by making use of a mixture of platforms. The most important development in this regard is the progress made in the capabilities of small satellites as reinforcement for the large, sophisticated (and expensive) satellites that now make up the bulk of the U.S. fleet. Small satellites, in combination with a rapid launch capability, could reinforce damaged elements in a space architecture made up of larger platforms that are more sophisticated, if one of these large, primary platforms was removed from operation by an attack. The use of a constellation of small (or smaller) satellites in place of a single large platform also complicates an attacker's task. Damaging one satellite in a constellation of three or four will degrade, but not eliminate, the service being provided and will require multiple attacks to gain an advantage.

Small satellites and pseudo-satellites cannot yet duplicate the range or sophistication of services provided by the larger satellites used by the US. What they offer is a cheaper and more responsive set of alternatives. Their potential utility, however, should be conditioned on the assumption that the U.S. will continue to accelerate development of space and sensor technology. Advances in technology that improve small satellites will help mitigate the risk of an asymmetric attack by making it easier for the U.S. to respond and replace damaged capabilities.

The use of ‘pseudo-satellites’ can also provide redundancy. A pseudo-satellite is an aerial vehicle that provides the same or similar services as a space-based platform. Unmanned aerial vehicles that provide imagery and sigint can take the place of or reinforce space platforms. Pseudo-satellites could also provide communications or navigation services. A UAV or aircraft can orbit a conflict area, collecting information or broadcasting data. Current UAVs can only linger for a relatively short time over a conflict area, but research programs are developing platforms with greater capabilities.

The ideal military space architecture would allow the U.S. to take a core of high value military space satellites and combine them with civilian, commercial and foreign space services, and with pseudo-satellites to respond to potential attacks. If, for example, an imagery satellite was blinded by enemy action, the U.S. wants to be in a position where a combination of pseudo-satellites, commercial services and special purpose small satellites can be rapidly assembled to fill the gap.

Finally, U.S. planning and exercises must include testing of alternative configurations and space architectures. The U.S. needs to have worked through scenarios where, if an opponent were able to successfully disrupt or destroy a space asset, we could reconfigure surviving (or alternative) assets to minimize any damage to military or intelligence operations. Having in place tested contingency plans will reduce the damage of an asymmetric attack.

### **Risk Mitigation Through Hardening**

Hardening involves making existing assets more difficult to attack and damage. Hardening makes space programs more expensive, something that could be difficult in a period of fiscal restraint, and policymakers will need to weigh the tradeoffs between hardening existing military space assets and building redundancy with commercial space services. There are also limits to the hardening of spacecraft. Given the weight limitations faced when putting a satellite into orbit, every pound devoted to hardening is a pound lost to mission capability. Armoring spacecraft, for example, is out of the question.

One controversial aspect of hardening involves stealth. Stealth makes sense if opponents will try to find and attack U.S. satellites. Some argue that with the end of the Soviet Union, we no longer face an anti-satellite threat. This is true now, but we cannot be sanguine about the next decade. Our potential opponents know they can gain an advantage by attacking our space assets. Any nation that can achieve space flight can attack satellites, and this includes Iran and North Korea. China reportedly has experimental anti-satellite programs to disable or destroy U.S. spacecraft. Further research on how to increase the stealthiness of future satellites would be beneficial.

Hardening is particularly important for ground facilities. Effective use of satellite services requires a support infrastructure of analysts and operators and the integration of satellite data and services into military plans and operations. Damaging these terrestrial support infrastructure can reduce the U.S. advantage from space and may be cheaper and technically less difficult for an opponent. One aspect of the hardening of ground facilities

that is easy to overlook involves information and network security. An opponent who can, using cyberweapons, disrupt the control of satellites, the flow of data from the satellites to the analysts and planners, or damage the integrity of that information can gain a real advantage at relatively low cost. Improved information and network security through the use of security and monitoring software, data encryption and authentication, is a crucial element for hardening the U.S. military space system against asymmetric attack.

Changes in the architecture for the distribution of space data could also reduce the vulnerability of ground infrastructure. A distributed model would reduce vulnerabilities. Current models for data distribution are, in many instances, centralized and stovepiped. Satellite data flows to a central collector. This collector distributes the data to several intermediaries who process, refine and inevitably delay distribution. While the situation has improved markedly from the time of the first Gulf War, when at first there were long lags between the time satellite data was collected and the time it came to Central Command, this centralized approach reduces the U.S. military information advantage and, by creating a small set of targets for attack, increases vulnerability.

GPS provides an alternative model for data distribution. In contrast to space intelligence, GPS data flows directly and immediately to the user. GPS uses machines and software rather than humans to process data. One goal for future space activities is to extend automatic processing to other kinds of satellite data. We would benefit from pushing data to the edges, to the combatants, and getting this data to them in as close to 'real-time' as possible. This will take considerable work in software development, to automate analytical processes that now require human intervention, but it is essential for improving the delivery of space services to military and intelligence operators. The primary advantage of this approach is that it extends information superiority. However, it would also help reduce the risk of asymmetric attack. If data flows directly from space to dozens, hundreds or thousands of operators, planners and analysts distributed among the military commands, it reduces the attractiveness to opponents of trying to attack ground facilities to disrupt the U.S. advantage from space.

### **Risk Mitigation and Innovation**

The ability to produce technological innovation more rapidly than potential opponents determines our ability to harden space assets and to develop cost effective approaches to providing space services. From many decades, the U.S. had an unquestioned lead in technological innovation. Today, that lead is being eroded. The technological leveling produced by globalization and economic interdependence give opponents new opportunities to seek asymmetric advantage. Nations and groups will exploit commercial technologies and services to mimic advanced U.S. military capabilities and to create or take advantage of vulnerabilities to gain asymmetric advantage.

Some of this erosion is inevitable, as other nations grow richer and are willing to spend on their own space capabilities. Some of it is the result of the increasingly sophistication of commercial technology. However, some of the damage is self-inflicted, by policies and regulations that reduce the productivity of U.S. research and the aerospace industry. A serious underinvestment in aerospace, physics, chemistry and engineering research erodes

the U.S. lead in space and reduces our ability to modernize our military space infrastructure in ways that will make it better able to respond to asymmetric attack. Maintaining the ability to innovate faster than our opponents is the best response, in many ways, to asymmetric threats.

Innovation in military space requires two components: a strong scientific base and a strong industrial base. The two overlap to a considerable extent. The scientific community provides not only new ideas and technologies, but also the trained technological workforce needed by defense industries. The defense industry itself is a significant source of research and development activities. Policies that strengthen the scientific community and defense industries will, over time, reduce our vulnerabilities to asymmetric attack.

### **Conclusion**

During the Cold war, both the Soviet Union and the U.S. explored the technology required for anti-satellite weapons. Although some systems on both sides reached the testing phase, none were deployed and an informal agreement between the opponents made space a neutral zone. We cannot assume that the opponents we face now or in the future will similarly accede to such informal agreements, if only because the U.S. advantage in space is so great, an opponent with few or no satellites has little to lose by initiating an anti-satellite campaign.

The U.S. spends more on national security space than all other nations combined, but this is not enough to guarantee security. The diffusion of space capabilities among potential opponents (and a growing awareness of U.S. space capabilities and the need to counter them) means that the advantage the U.S. gains from space will be placed at risk if we do not find new ways to mitigate risk. The measures here offer a few suggestions for reducing the risks from asymmetric attacks on space assets.