Testimony before the U.S.-China Economic and Security Review Commission

Hearing on China's Advanced Weapons

February 23, 2017

Submitted by Todd Harrison

Director of the Aerospace Security Project and Senior Fellow

Center for Strategic and International Studies

The U.S. military's space capabilities provide an extraordinary advantage in war fighting. Military space systems are the backbone of the United States' power projection forces, allowing the military to conduct operations virtually anywhere in the world with precision and speed. This has not always been the case, however, as the role space systems play in military operations has evolved significantly since the end of the Cold War.

Evolving Military Uses of Space

Throughout the Cold War, space systems were largely focused on supporting nuclear forces. U.S. and Soviet military space systems provided valuable intelligence on each other's nuclear arsenals, early warning of a surprise missile attack, and command and control of nuclear forces. Space-based intelligence and surveillance capabilities were particularly important because they created a verification mechanism that underpinned arms control treaties and ultimately eased tensions.[1] Because military space systems were so closely associated with nuclear forces during the Cold War, both sides viewed an attack in space as a prelude to nuclear war. It would have been unthinkable for one side to attack the other's space assets in a conventional conflict. Thus, military space systems enhanced nuclear deterrence and were a stabilizing factor in the broader U.S.-Soviet competition.

Since the end of the Cold War, however, a gradual change has been underway in how the military uses space and how attacks on space systems are viewed globally. The 1991 Gulf War marked the first time space-based capabilities played a major role in conventional military operations. Operation Desert Storm demonstrated the force multiplier effect of U.S. military space systems for tactical command and control (C2), precision navigation and timing (including the use of GPS-enabled smart bombs and cruise missiles), and theater missile warning to detect and track SCUD missile launches.[2]

Since then, the military uses of space have grown exponentially. Space systems are now considered critical enablers across the full spectrum of military conflict, from counterterrorism operations to high-intensity conventional conflict with a near-peer adversary. The U.S. military relies on space-based capabilities for imagery, strategic and tactical missile warning, communications, signals intelligence, precision navigation and timing, and weather and environmental monitoring, among many other missions. Space-based communications and navigation in particular have fundamentally altered the way

[1] See Pat Norris, *Spies in the Sky: Surveillance Satellites in War and Peace* (Berlin: Springer Praxis Books, 2008).

[2] Lt. Gen. Ellen Pawlikowski, Doug Loverro, and Col. Tom Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," *Strategic Studies Quarterly*, Spring 2012, p. 32.

the U.S. military fights by allowing a high level of precision and coordination across great distances that otherwise would not be possible.

Other nations have taken note of the significant advantages space provides for the U.S. military in conventional conflicts. Some have attempted to replicate U.S. space capabilities to provide similar advantages for their own forces. Others have developed counterspace capabilities to reduce or eliminate the advantages space provides for the United States. China appears to be pursuing both strategies. It is developing more advanced space systems that mirror U.S. space capabilities in many areas, such as its own constellation of satellites for precision navigation and timing known as Beidou. At the same time, it is also making advances in many counterspace technologies that could threaten U.S. space systems.

Threats to Space Systems

The threats U.S. military space systems face from China and others can be divided into four categories: kinetic, non-kinetic physical, electromagnetic, and cyber. Kinetic attacks attempt to strike a satellite directly, detonate a warhead in its vicinity, or disable critical support infrastructure on the ground. The 2007 Chinese test of a direct-ascent anti-satellite (ASAT) weapon against one of its own satellites in low Earth orbit (LEO) provides a stark example of the effects kinetic attacks can have. This ASAT test produced thousands of pieces of debris, many of which are still in orbit more than a decade later.[3]

Satellites in LEO, where many imaging satellites reside, are particularly vulnerable to the type of direct ascent kinetic ASAT weapons used in the Chinese test because lower altitudes are easier to reach. Missile defense systems can be adapted to serve as ASAT weapons, as the United States demonstrated in 2008 by launching an SM-3 missile to intercept and destroy a disabled U.S. military satellite that was projected to re-enter the atmosphere within days.[4] Attacking satellites at higher altitudes—such as medium earth orbit (MEO) where Global Positioning System satellites reside, or geostationary orbit (GEO) where many communications and missile warning satellites are located—requires a larger, more complex missile with multiple stages. Higher orbits also take longer to reach, providing greater warning for the satellite being attacked. For example, a typical launch trajectory to geosynchronous orbit takes more than 5 hours to reach apogee. China appears to be developing and testing missiles with the capability of reaching higher orbits.[5]

Satellites are also vulnerable to co-orbital threats where a satellite already in orbit can be deliberately maneuvered to collide with another satellite, dock with an uncooperative satellite, or detonate a small warhead in the vicinity of a satellite.[6] China appears to have the requisite technology to build and launch small satellites for these purposes, and recent activity in space indicates it may be testing these

---

[3] "Fengyun-1C Debris: One Year Later," *NASA Orbital Debris Quarterly News*, Vol. 12, Is. 1, January 2008, p. 3, http://orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv12i1.pdf.

[4] Department of Defense, "DoD News Briefing with Gen. Cartwright from the Pentagon," News Transcript, February 21, 2008.

[5] See Brian Weeden, *Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space* (Washington, DC: Secure World Foundation, March 17, 2014), https://swfound.org/media/167224/through_a_glass_darkly_march2014.pdf

[6] Brian Garino and Jane Gibson, "Space System Threats," *AU-18 Space Primer* (Maxwell Air Force Base, Alabama: Air University Press, September 2009), p. 277.

technologies.[7] Nuclear weapons can also be used as kinetic weapons against satellites by detonating them in space or at a high altitude to physically destroy a satellite or damage its electronics. A nuclear detonation in space, however, is indiscriminate in its effects because the highly charged particles created would affect all satellites in similar orbits.

Kinetic physical attacks tend to have catastrophic effects on the satellites they target by totally and permanently disabling them. Moreover, kinetic attacks create space debris that is indiscriminate and can affect satellites belonging to nations or companies not directly involved in the conflict. The Chinese anti-satellite weapon test in 2007, for example, produced more than 10 percent of the manmade objects currently being tracked by the Joint Space Operations Center (JSpOC).[8] Because kinetic anti-satellite weapons are largely attributable, create irreversible effects, and carry a high risk of collateral damage to other satellites, using these weapons in space would likely be viewed as a significant escalation in a conflict.

Rather than attacking the satellites on-orbit, an adversary could achieve similar effects by attacking the ground stations that support them. The ground segment is perhaps more vulnerable to attack because it is often highly visible, located in a foreign country, and a relatively soft target. Ground stations are vulnerable to direct physical attack by a number of means, including guided missiles and rockets, rocket-propelled grenades, and small arms fire directed at ground station antennas. Ground stations can also be disrupted by attacking the electrical power grid, water lines, and the high-capacity communications lines that support them.

Non-kinetic physical attacks can be used to temporarily or partially degrade a satellite with less risk of debris and without directly touching it. Directed energy weapons, such as lasers and high-powered microwave systems, can target space systems within seconds and create effects that may not be immediately evident beyond the satellite operator. A high-powered laser, for example, can be used to damage critical satellite components, such as solar arrays and sensors, but requires high beam quality, adaptive optics, and advanced pointing and stability control—technology that is costly and not widely available.[9] A relatively low power laser can be used to permanently blind or temporarily dazzle electro-optical sensors on satellites. In September 2006, China reportedly illuminated U.S. satellites using ground-based lasers in what may have been an attempt to blind or dazzle the satellites, an indication that this technology, while advanced, is not beyond the reach of potential adversaries.[10]

Electromagnetic attacks target the means by which data is transmitted rather than the physical satellite or ground support system. Satellites are dependent on radio frequency communications for command and control and to transmit data to the ground. Jamming is the use of electromagnetic energy to interfere with these radio communications. A jammer must operate in the same frequency band and within the field of view of the antenna it is targeting. Unlike physical attacks, jamming is fully reversible—once the jammer is disengaged, communications can be restored. Ground terminals with smaller antennas or omnidirectional antennas, such as GPS receivers, have a wider field of view and are

---

[7] "China's new Orbital Debris Clean-Up Satellite raises Space Militarization Concerns" *Spaceflight101*, June 29, 2016, http://spaceflight101.com/long-march-7-maiden-launch/aolong-1-asat-concerns/

[8] U.S.-China Economic and Security Review Commission, *2011 Report to Congress*, p. 218.

[9] Garino and Gibson, "Space System Threats," p. 277.

[10] Vago Muradian, "China Tried to Blind U.S. Sats with Laser," *Defense News*, September 25, 2006.

more susceptible to downlink jamming. The technology needed to jam many types of satellite signals, such as GPS, is commercially available and relatively inexpensive. Jamming can also be difficult to detect and distinguish from accidental interference, making attribution and awareness more difficult.

Unlike electromagnetic attacks, which interfere with the transmission of data in the electromagnetic spectrum, cyber-attacks target the data itself and the systems that use this data. Like many other modern military systems, satellites can be vulnerable to cyber-attacks used to intercept data, corrupt data, or take control of systems for malicious purposes. Cyber-attacks can also target satellites, control stations, and user equipment on the ground. The effects of a cyber-attack on space systems could range from local disruptions that cause a satellite to temporarily go offline to widespread disruptions and potentially the permanent loss of a satellite. If an adversary were able to take control of a satellite through a cyber-attack, for example, it could shut down all communications and destroy the satellite by expending its fuel supply or damaging its electronics. Moreover, it may be difficult for controllers to know what caused a satellite to lose control, since accidental malfunctions are not uncommon. Attribution for a cyber-attack can be difficult to establish conclusively because attackers can use a variety of methods to conceal their identity.

Grey Zone Threats in Space

While kinetic threats to satellites often receive the most attention, they are not necessarily the most concerning. If the Chinese were to use a kinetic attack against U.S. military satellites, the source of the attack would be attributable, the damage to satellites would be irreversible, the attack and the orbital debris it created would be publicly known, and it would create the potential for collateral damage to other nation's satellites. In other words, it would be an unambiguous act of aggression. All of these factors make this form of attack less attractive for the Chinese to use except in the most serious contingencies because it would be regarded as highly escalatory.

What is more concerning are the less obvious and less escalatory forms of attack that are possible. These "grey zone" threats are particularly problematic in space because traditional methods of deterrence may have little effect. As in other domains of warfare, grey zone attacks in space may have ambiguous attribution, effects that can be reversible, and limited public visibility. For example, a jammer could be used to disrupt critical U.S. military communications. If this jammer is located on a mobile platform, such as a car or truck, and operates intermittently in a noisy electromagnetic environment, it would be difficult to geo-locate the jammer and attribute the source in a timely manner. The public (including other countries) may not even know the jamming is occurring. Moreover, if the jammer is operating in a third country, the range of actions available to neutralize the jammer could be limited. Jammers can be relatively inexpensive, making it possible for countries to field jammers in larger numbers and proliferate them to surrogates.

Beyond jamming, grey zone threats in space can include cyber-attacks, blinding or dazzling sensors with a laser, and high-powered microwave attacks, among others. In some respects, these threats are more insidious than an overt kinetic attack because they can be used even when conflict is not imminent. As in other domains, grey zone attacks can be used in space to test U.S. responses, to prepare the battlefield by degrading key space capabilities, and to deter the United States from becoming involved in a situation by signaling that key space assets are at risk.

A grey zone attack in space could complicate a U.S. response in several ways. First, unlike a kinetic attack on satellites, non-kinetic, electromagnetic, and cyber-attacks may not provide a clear indication of overt hostilities. There is no precedent for determining when an attack in space rises to the level of invoking the right of self-defense or the mutual defense clauses of treaties. Second, it may not be clear what a proportionate response would be. Would an attack against U.S. military space assets that is reversible or non-lethal, such as jamming or dazzling, justify a kinetic and potentially lethal response on Earth? An attack that is covert or not readily visible to the public could put the United States in the position of taking military, economic, or diplomatic actions without a clear public justification. Depending on the nature of the attack and the space systems affected, the U.S. military may not want to disclose the full extent of an attack for fear of giving the adversary battle damage assessment and exposing weaknesses in U.S. space capabilities. Third, the escalation ladders of the United States and China are likely to be very different. Because the United States has more to lose in space, China may be inclined to escalate vertically by attacking other space assets while the United States may be inclined to escalate horizontally in other domains. For example, if the United States is attacked in space its best option may be to neutralize Chinese counterspace capabilities by striking targets on Earth, such as satellite tracking and command and control sites. This creates an escalation asymmetry in which the United States may be self-deterred because attacking targets on the surface—particularly if they are located in mainland China—could be viewed as provocative and politically unpalatable.

Recommendations

Advances in counterspace capabilities by China and others naturally raises the question of what the United States can do to adequately deter these threats. Deterrence holds when the perceived costs of an action exceed the perceived benefits. To maintain a credible deterrence posture in space, the United States should take steps to increase the perceived costs of attacking U.S. space systems and reduce the perceived benefits.

The United States can raise the costs of attacking its space systems by hardening its satellites, ground stations, and communications links. For example, the vast majority of military satellite communications is carried on satellites and communications links that are not well protected against jamming. The military could increase the capacity of its protected communications satellites, such as the Advanced Extremely High Frequency (AEHF) constellation, so that more of its critical communications links are protected. The communications payload on AEHF uses frequency hopping, interleaving, nulling antennas, satellite crosslinks, and on-board processing of signals to greatly increase its resistance to jamming.

The perceived benefits of attacking U.S. space systems can be reduced by making the military less dependent on individual satellites in key mission areas. Currently the U.S. military relies on a small number of large, expensive, highly aggregated satellites for missile warning, protected communications, narrowband communications, and other critical space-based capabilities. Each of these satellites is a juicy target for adversaries because disabling or degrading the operations of just one or two would have a major impact on the entire constellation. The military should instead transition to space architectures that rely on a large number of smaller satellites in a variety of orbits. This would reduce the benefits an adversary can gain by attacking any one of these satellites and make the overall constellation more resilient.

One of the most important step the United States can take to improve its position in space is to better understand Chinese space capabilities and intent. Many of the advances in Chinese space capabilities are dual-use in nature. For example, advances in on-orbit rendezvous and close-proximity operations can be used for peaceful purposes, such as on-orbit servicing of satellites and removal of orbital debris. But these same capabilities can also be used to interfere with the operation of other satellites and as co-orbital weapons. While the United States maintains a clear separation between its military and civil space programs, the Chinese do not. The comingling of Chinese civil and military space programs leads to greater uncertainty and suspicion.

Throughout the Cold War the United States maintained a level of cooperation with the Soviet Union on civil space programs. Like the Chinese, the Soviets did not have a clear separation between their military and civil space programs. U.S.-Soviet cooperation in programs such as Apollo-Soyuz Test Protect in the 1970s gave the United States greater insight into the largely secretive Soviet space program, reducing uncertainty and clarifying the intent of some technologies and programs.[11] Just as the United States partnered with the Soviet Union during the Cold War, the United States should partner with China on select civil space exploration programs. This would help provide greater insight into an otherwise opaque system, reduce the uncertainty regarding China's space activities, and encourage Chinese investment in more peaceful and stabilizing space capabilities. More importantly, government-to-government cooperation in civil space could create the opportunity for military-to-military contacts between U.S. and Chinese military space commands. This direct contact is something that is sorely needed and vital to stability and understanding in a crisis situation.

[11] Roald Sagdeev and Susan Eisenhower, "United States-Soviet Space Cooperation during the Cold War," *NASA Magazine: 50 Years of Exploration and Discovery*, http://www.nasa.gov/50th/50th_magazine/coldWarCoOp.html.