

## CHAPTER 7

### TECHNOLOGIES AND BEHAVIOURS OF CONCERN: WHAT THREATENS LONG-TERM SPACE SECURITY AND HOW CAN THESE THREATS BE MONITORED?

Laura Grego

As we look forward toward addressing security concerns in space by using laws and agreements, we must work on the practical counterparts to these laws. To do so, one would like to answer a number of questions, for example: What are the technologies of concern and how could they be limited? What are the roles of verification and inspection? When does it make sense to monitor behaviour rather than limit technology? What is the value of monitoring behaviour if it cannot guarantee that no attacks are made? Does assigning responsibility for rule breaking increase security? Are there technical bottlenecks that are suited for arms control, in analogy to the control of fissile materials for nuclear weapons arms control?

I will not attempt to answer these questions in depth or with finality but, rather, I will support the discussion by giving an overview of the most important threats to space security and what some possible methods for monitoring and mitigating them might be, with an emphasis on technical solutions.

There are four basic categories of things that threaten the sustainable, secure use of space. The first, space-based weapons, comprises ground attack weapons, missile defences and anti-satellite (ASAT) weapons based in space. The second, ASAT weapons, includes those weapons that interfere with or harm satellites, whether the weapons are ground-based or space-based. These two categories are the most provocative and deservedly receive the most attention. However, there are other issues that also need to be addressed in order to keep space secure. This includes the third category: dual-use technologies and latent capabilities. These are systems designed to perform a peaceful or defensive task, but which can also function as space-based or ASAT weapons. Inspector satellites and defender

satellites are examples of this category. And last, there are other things that are not weapons at all, but which can increase tensions and make space difficult or more expensive to use. These include unintentional or naturally occurring interference with satellites and lacunae in the legal framework that covers space. Examples include spill over onto neighbouring satellites of communications signals intended for a specific satellite, debris generation and leaving decommissioned satellites in orbit instead of de-orbiting them or moving them to “graveyard orbits”.

We intend to focus our energies on the most pressing concerns. We are unlikely to see in the near or mid-future space-based ground attack weapons systems, as they are enormously expensive when compared to ground-based alternatives. Nor will there be a large-scale space-based missile defence in that time frame, as such a system is also very expensive, and serious flaws render such a defence ineffective. There is little serious interest in the United States for fielding full-fledged systems of these types, and so we do not spend time on them here (although “test” assets for these systems may be the leading edge of space weaponization and can have a dual use as ASAT weapons).

Rather, it is likely that interference with satellite systems, rather than attacks on ground targets or missiles from space, will be the central security problem. The presence of a huge military space capability (some estimate that the US outlay on military space represents about 90% of military space spending) supporting conventional war-making presents a complex problem and arguably the central challenge to our work here. In a sense, these systems, by virtue of their great military value, have already drawn space onto the battlefield.

We are speaking of those systems that are not active weapons systems themselves, but that support military missions with targeting, intelligence and navigation information. Satellites providing these capabilities have had tacit approval, having no strongly voiced objection by other states, perhaps because other states may want this capability for themselves in the future. However, in a crisis, states in conflict may want to be able to deny such capabilities to their adversaries. Additionally, in the future, some of this “support” capability may be dual use and able to perform in a weapons capacity as well. The international community must decide what bounds, if any, to put on these capabilities and how to deal with the ensuing tensions. This has led to interest both in developing ASAT weapons and to banning

---

them. In any case, the use and denial of the use of satellite systems are likely to be the central space security issues in the near future.

We will look at the most likely types of ASAT interference and how they might be controlled or monitored and try to identify the areas that deserve the most attention. Interfering with the broadcast and reception of satellite signals is a simple way to frustrate the use of communications satellites. “Downlink” jamming interferes with signals sent from a satellite to the ground. The interference is local in scope, as the jammer is ground-based and is jamming ground-based receivers. Downlink jamming is generally quite simple, especially jamming unprotected systems, and such actions by state and non-state actors have been reported frequently.

There are means to mitigate such an attack. In many cases, the location of interference can be identified using radiolocators and the interference stopped through diplomatic channels or by military action—that is, destroying the jammer. The law covering downlink jamming is unclear, but it is unlikely that a high compelling case can be made that a state must not interfere with the reception of satellite signals it finds dangerous. This, and the fact that this jamming is so simple to do, and that it does not interfere with the satellite itself but only with localized ground based receivers, makes it a low priority for security law.

Uplink jamming is a bit of a different case. Uplink jamming interferes with signals sent from the ground up to the satellite and can affect the performance of the satellite on a global basis, rather than just locally. There have been numerous instances of this, particularly with commercial satellites, which do not make a high priority of including anti-jamming equipment on their satellites.

Again, there are means to mitigate this interference. Commercial businesses have been developed that specialize in locating the source of such interference. Presumably, states are developing this capability for themselves as well. Identifying the source of jamming is not the difficult part; the trick is in identifying the legal and diplomatic channels for resolution of the interference. This can be more complicated than for downlink jamming, as the uplink jammer could be located in a state that is neither the primary sender nor receiver of satellite’s real signals.

Another simple way to interfere with satellites is “dazzling”, that is, using a bright light source such as a laser to make it difficult for a satellite to take an image of the ground. The power needed to mask a small area are small; to dazzle an area of 10 metres, a laser no brighter than a laser pointer is needed. However, to mask an area of significance, such as 1km in diameter, then more powerful lasers are needed on the order of 10 watts, which can start to damage the satellite’s sensor. At this point, when permanent damage is done, the term used is “blinding”. In both cases, the light source likely will be ground based and the interference will be eminently attributable, but difficult to prevent because the technology is readily available commercially.

For uplink and downlink jamming, as well as for dazzling and blinding, limiting technology is not a solution. The technology to mount such attacks is simple and widely available. All such attacks, however, can be attributed to their sponsor during and after the fact. The effects of the attacks, with the exception of blinding, are temporary and reversible. So, while these technologies are quite difficult to control, they also may be of the least concern for security. Qualitatively different from these are attacks that leave a satellite permanently disabled or destroyed. These ASAT techniques are considerably more destabilizing, but also provide more opportunities for monitoring.

At very high powers, lasers can be used to damage the physical structure of a satellite. These lasers could be ground or space based. Low-Earth orbiting satellites would be the targets from the ground or from low-Earth orbits. The distance to geosynchronous orbit (GEO) protects GEO satellites from such attacks. To generate the powers needed, they will be large and complex systems, and not simply bought off the shelf and generally not transportable on the ground. Hence, they may be identifiable with reconnaissance and technology limits may be useful. Additionally, verification sensors can be situated nearby to detect backscatter from the atmosphere if such highly powered lasers are used. These are not systems of the future, but are within today’s capabilities. In 1997, the United States tested a high-power laser and tracking system on a satellite, and a test of a laser using adaptive optics to illuminate a satellite is slated for 2007.

Kinetic Energy ASAT (KEASAT) weapons use the force of impact on a satellite to damage or destroy it. Ground-based direct ascent KEASAT weapons could be based on short-range ballistic missiles or air-launched

---

missiles with the ability to home in on satellites. It is not necessary to be a space-faring nation to develop these types of ASAT weapons, but advanced technical capability is necessary. These basic missile capabilities are dual use, but a distinction can be made between those used for ground targets and those that possess the ability to target satellites. This ability can be signalled by the inclusion of sensors that can home on satellites, for example, and the testing of such missiles in an ASAT mode will be evident and readily observed.

Space-based KEASAT weapons will need similar capabilities. Additionally, dual-use systems may also have KEASAT capability. Satellite “defender” bodyguard satellites and space-based missile defence interceptors would look and operate very much like a dedicated space-based KEASAT weapon. “Test” assets for a missile defence system, while not providing missile defence capability, would likely have significant ASAT utility. The pertinent technology is the ability to manoeuvre on orbit and accelerate rapidly and to be able to home in on a space object. So, restricting technology only for space-based KEASAT weapons, while making exceptions for missile defence or satellite defence weapons, is unlikely to be satisfactory for this reason.

Monitoring can be of some use in addressing the dual-use question. Once in orbit, it may be difficult to discern the abilities of a satellite, especially if some care were taken to disguise them, although imaging may be useful. Pre-launch inspections can provide some insight into the system’s capabilities, although this is, of course, invasive and not the likeliest of possibilities. Surveillance of the behaviour of the systems will allow ASAT-like behaviour to be identified and responsibility assigned. Excellent surveillance may also help satellites to evade an attack once it has begun. However, for space-based KEASAT weapons as well as ground-based ones, routine ground-based satellite surveillance is unlikely to detect an attack in time to prevent it and may not be sufficient to assign responsibility for it either; sensors specifically configured for the problem would be necessary.

Another space-based concern is micro-satellite-based ASAT weapons. These small satellites would closely approach another satellite, perhaps at a leisurely pace, and then use a simple measure to interfere with it at close range. The micro-satellite could also be in an orbit different from the target but which crosses the target’s orbit, and could make a last-minute diversion to approach. Micro-satellite and close approach technology is certainly dual

use, and technology limits are unlikely to be useful in this case. To monitor the behaviour of micro-satellites, one needs the ability to track all objects of a given size; the size of a functional micro-satellite will get smaller as technology improves. One would have to monitor it closely, perhaps in real time, to prevent an attack by last-minute diversion, but for a slow approach, the requirements are much more lax. However, real-time tracking of even the most important orbiting objects is out of reach currently and it is still a technical challenge to find small objects that manoeuvre. There are not sufficient surveillance assets currently in use to monitor a “keep out” zone around even the most important satellites. The establishment and verification of keep out zones do not themselves protect satellites from attack, but it does set norms and assigns responsibility for violations.

Long-term security will require the ability to monitor all space launches. Currently there are some two dozen fixed launch sites, from which launches are announced in advance. An unannounced launch from one of these sites would not escape notice for very long. As technology advances, however, it will become more complicated to monitor all space launches. The ability to launch satellites into orbit from mobile platforms exists: the Russian Federation has launched satellites from a submarine and is currently developing airplane-based satellite launch (as is the United States, reportedly), and there is no great technical barrier to using ground-based mobile launchers for satellite launch. To be assured of detecting all launches in a timely manner, one would need early warning-type capability.

In a regime where ASAT weapons have been developed and tested, it will be important to be able to distinguish between an ASAT attack and unintentional interference and naturally occurring satellite failure. Space is a hostile environment in which to operate and satellites partially and wholly fail at the rate of several per year; often the cause is never identified satisfactorily, and there are thousands of instances of unintentional signals interference to contend with. Additionally, in an environment where a large amount of debris is present, a collision with debris could be interpreted as a KEASAT attack. It can be difficult to distinguish intentional interference with unintentional interference; it is necessary to have on-board sensors and diagnostics, good space surveillance and a comprehensive debris catalogue.

In conclusion, there are verification options—technological limits and behaviour monitoring—that can help support important decisions regarding the security of space.