

Space Command 2.0

By Luther Martin – ISSA member, Silicon Valley Chapter



On August 29, 2019, the US government reactivated its [Space Command](#). The previous Space Command was created to coordinate the activities of the space forces of the US Army, Navy, and Air Force. It was created in September 1985 and deactivated in October 2002. The new Space Command is one of the American Unified Combatant Commands, which seems to suggest plans to prepare for aspects of future conflicts that will take place in space.

The reactivation of Space Command might have spurred the sale of “Make Space Great Again” t-shirts. It might also have spurred the creation of a new game in which people append “...in space” to fortune cookie fortunes in an attempt to get humorous results. Things like “Do not make extra work for yourself...in space” or “A new perspective will come with the new year...in space.”

But the reactivation of Space Command also gives us a good reason to think about the future of space conflict and how it relates to information security. The bottom line is that it looks like space combat might turn out to be more like the ongoing battle between hackers and corporate security departments than one involving the colorful beams of energy that we see in movies.

Some countries have tested anti-satellite weapons that can destroy other satellites using kinetic attacks, like destroying them through a collision with a missile. This might be a big part of what the new Space Command is thinking about, but it's probably very unlikely that we will ever see the use of such weapons in future conflicts. This is because of the problem of [space debris](#).

[According to the European Space Agency](#) (ESA), there are probably over 34,000

objects bigger than 10 cm (about 4”) in size in Earth orbit, of which about 23,500 are actively tracked. Objects that big pose a significant hazard to all satellites. Objects in low-Earth orbit move at about 17,500 miles per hour, and a collision with a 10 cm piece of space debris moving at that speed can easily destroy an expensive satellite.

If too much space debris gets created in Earth orbit, it's possible to get a catastrophic cascade of debris creation—debris created by one collision goes on to collide with other satellites and create debris which then goes on to destroy other satellites, etc. This is the [Kessler effect](#), named after the NASA scientist Donald J. Kessler, who along with Burton G. Cour-Palais first [noted](#) its possibility in 1978.

A runaway Kessler effect could deny the use of space to all nations for many generations. This would dramatically push back many technologies to where they were in the 1980s. (Although [current treaties](#) ban weapons of mass destruction from space, there are no limitations on the use of conventional weapons in space, like those that could do this.) Destroying an enemy satellite, either with a kinetic weapon or an energy weapon, will definitely create more space debris. It might even create enough debris to create a runaway Kessler effect.

That's probably not a risk that many nations would be willing to take. If an anti-satellite weapon is used to destroy a satellite, the amount of debris created can be significant. The ESA [estimates](#) that the Chinese FengYun-1C [anti-satellite weapon test](#) in January 2007 alone increased the trackable space object population by 25 percent. So, using even a few anti-satellite weapons could have dramatic consequences that would af-

fect the nations using the weapons as well as their targets.

A better way to control the use of space by other countries is to reduce or eliminate the effectiveness of satellites through cyber attacks. This may be fairly easy. Satellites are [notoriously non-secure](#), and both the constraints imposed by the cost of getting a satellite to space and the minimal amount of power that they have available means that many satellites look more like non-secure Internet of things (IoT) devices than advanced, space-age technology. A damaging cyber attack on a satellite could point its sensors at the sun to destroy them or even de-orbit the satellite and let it be destroyed by reentry into Earth's atmosphere, easily avoiding the problem of creating space debris in both cases. Less damaging attacks could temporarily disable or degrade critical systems.

IoT devices aren't as secure as we would like them to be, but we have a good idea of how to make them secure. Maybe the new Space Command can learn a lot from commercial security efforts in this area, like ETSI's [ES 103 645](#) “CYBER; Cyber Security for Consumer Internet of Things” standard and the work now being done by NIST's [Cybersecurity for IoT Program](#). They probably don't want to reinvent IoT security just because they're looking at it from a space point of view.

About the Author

Luther Martin is a Distinguished Technologist at Micro Focus. You can reach him at luther.martin@microfocus.com.