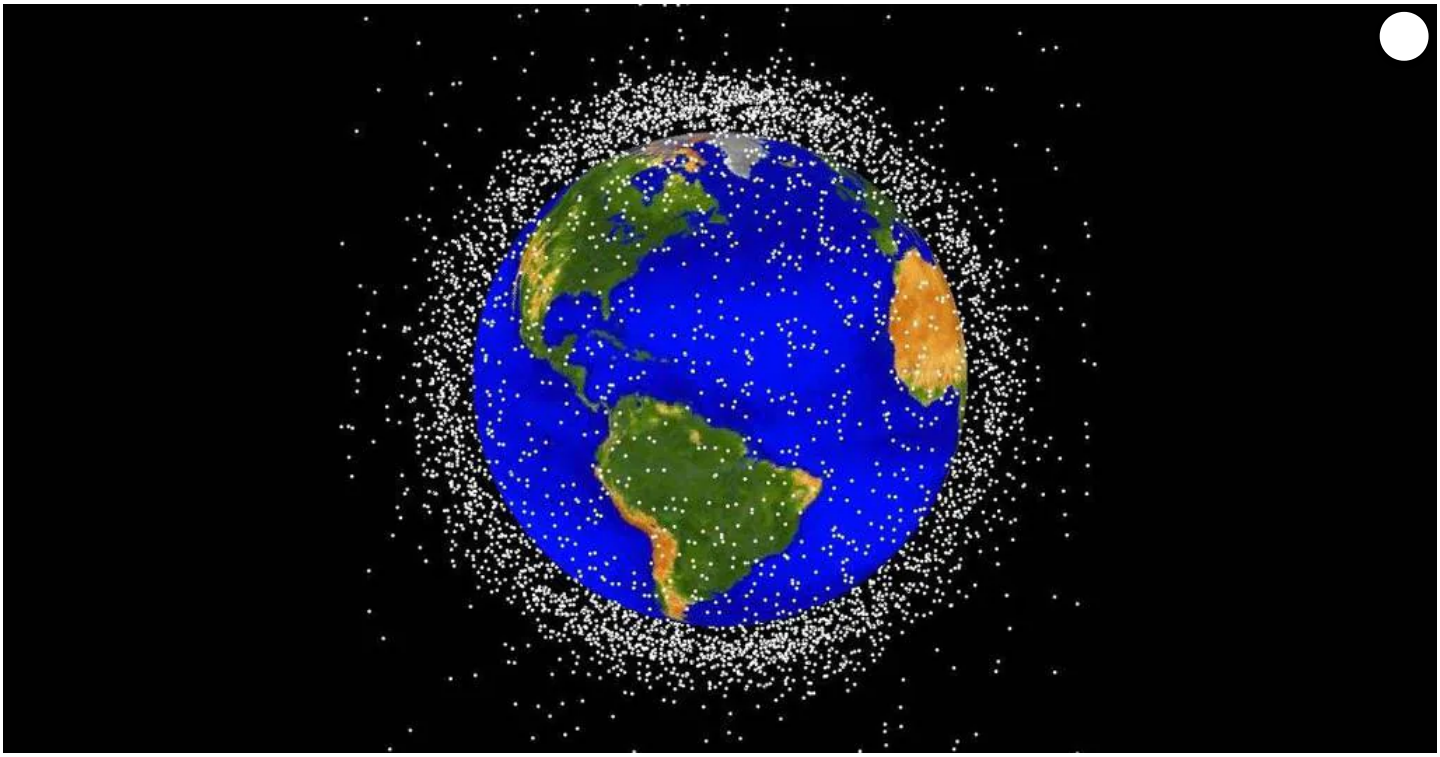
Why older satellites present a cyber risk

By **Jan Kallberg**

Dec 28, 2018



National security experts worry that an older satellite, one of thousands depicted above in this rendering of space debris, could be used as part of a cyber attack to harm U.S. satellites. (NASA image)

The most cost-effective and simplistic cyberattack in space, one with the intent to bring down a targeted satellite, is likely to use an older satellite now viewed as space junk that still has fuel and can respond to communications.

Hackers could then use that satellite to ram or force targeted space assets out of orbit. The benefits for the attacker are numerous.

Consider that the life span of a satellite is as long as 30 years, and even afterward it can still orbit with enough propellant for functional communications. Space contains thousands of satellites, both active and inactive, launched by numerous organizations and countries, hosting more than 5,000 space-borne transponders communicating with Earth. Every transmission is a potential inlet for a cyberattack. Older satellites share technological similarities, providing opportunities to exploit systems for control and processing. Satellites may be based on hardware and technology from as long ago as the 1980s and are unlikely to have been upgraded after launch.

But cyberattacks can exploit a single system, or a limited group of systems, within a larger group of satellites. These space-borne assets have a variety of operating systems, embedded software, and designs from disparate technological legacies. As more nations launch satellites with a variety of technical sophistication, the risk for hijacking and manipulation through covert activity increases. A satellite's on-board computer can allow for reconfiguration and software updates, which increase its vulnerability. For example, a satellite that will orbit for 10 years may be preprogrammed by a perpetrator for unauthorized usage when needed.

Even with the most-advanced digital forensics tools, tracing a cyberattack is complicated on terrestrial computer systems, which are physically accessible. Space-borne systems do not allow physical access, thus, lack of access to the computer system nullifies several options for forensic evidence gathering. The only trace from the perpetrator is the actual transmissions and wireless attempts to penetrate the system. If these transmissions are not captured, the trace is lost.

If the adversary is skilled, it is more likely the attribution investigation will end with a set of spoofed innocent actors whose digital identities have been exploited in the attack rather than attribution to the real perpetrator. Currently, nation-states are restrained by the political and economic repercussions of an attributed attack, but covert cyber war targeting US space assets removes the restraint of attribution.

A cyberattack resulting in a space collision would lack attribution and thus would be attractive to adversaries. A collision between a suddenly moving foreign satellite and a critical U.S. satellite would be neither a coincidence nor an accident. Or, even if a collision is narrowly avoided, a hacked satellite set on a crash course would force the targeted satellite to move – wasting fuel – and providing degraded service levels.

The easiest way to perpetuate this attack would be to hijack satellites from countries less technically advanced or from less-protected or outdated systems.

Post-mission disposal (PMD), the United Nations-led effort to remove satellites after their productive life spans, would require satellites to deorbit within 25 years after their mission ends. Naturally, this could happen faster, but it is drawn-out process and currently there are no tangible sanctions for noncompliance. If a satellite has a lifespan of 20 years, the additional 25-year allowance would increase the total number of years when the satellite can be remotely commanded for as long as 45 years.

Satellites launched in 1977, 1987, and 1997 are already technically outdated and several technology generations behind. The time between launch and end of the operation for a satellite is the foundation for its cyber vulnerability. It is a sound financial decision to use a satellite to the full extent of its lifespan. However, the question becomes: is it worth the risks? We must keep in mind technical leaps made since early space launches. Since technology today develops so quickly, PMD, in reality, increases the risk of cyberattack by hijacked satellites because it prolongs the time a satellite can be remotely commanded by signals exploiting obsolete and outdated communication equipment.

In a future near-peer conflict, one of the potential adversary's goals is to disrupt the United States' space capabilities. Cyberattacks in space are no longer science fiction; they are a valid concern.

Jan Kallberg is a research scientist at the Army Cyber Institute at West Point and an assistant professor in the department of social sciences at the United States Military Academy. The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute at West Point, the United States Military Academy or the Department of Defense.