Global Security Review

Russia and the Growing Danger of Satellite Cyberattacks

By

Alexis Schlotterback

To prove itself a formidable competitor in space, Russia is turning to space warfare. This includes anti-satellite tactics using cyber. Even in terrestrial cyber conflicts, Russia possesses the ability to engage in advanced denial-of-service, ransomware, and other types of malware attacks.

While no single agency oversees Russian cyberattacks, the amount of personnel involved in these operations continues to increase. There is a heavy reliance on criminal and civilian involvement to conduct offensive measures. Combining Russian interest in cyber and outer space has led to the "proliferation of handheld Global Positioning System (GPS) jammers, deployment of road-mobile jammers, and even development and testing of space-based jammers," as reported on by Sarah Mineiro. She also warns that Russia can hack American ground control systems for the GPS constellation.

Types of Satellite Cyberattacks

Though electronic means of interfering with satellite signals, such as jamming or spoofing, occur at a more frequent rate, attacks using cyber may prove to be more impactful and frequent in the next decade. Cyberattacks "target the data itself and the systems that use, transmit, and control the flow of data," potentially causing irreparable harm for military commanders and civilians reliant on communications and navigation systems for decision-making.

Like other cyberattacks, those on satellites and their networks require four main components: "access, vulnerability, a malicious payload, and a command-and-control system." Multiple methods and modes of attack can take out a satellite system or render it inoperable without using kinetic force. Adversaries can target the networks that satellites use, individual satellites, and the supply chains that produce satellite hardware and software. The Center for Strategic and International Studies describes three main types of cyberattacks: data intercept/monitoring, data corruption, and seizure of control.

First, there is data interception or monitoring, which is often seen as espionage. Adversaries may find spying to be a strategically sound decision to anticipate the next moves of the United States and leverage this knowledge in diplomatic or military channels. Secure World Foundation reports that many attempts of back door installations into American satellite networks were found in "Chinese electronics and Russian software packages."

Additionally, the communications from the ground to a satellite and a satellite to the ground often use "open (unencrypted) telecom network security protocols," Luke Shadbolt warns—making these systems vulnerable.

Second, data corruption, like a denial-of-service (DoS) attack, is accomplished through corrupting satellite data or even ransomware attempts to hold data hostage unless payment is received by the attackers. Secure World Foundation describes how a group of university students developed a DoS technique that causes GPS receivers to crash when they try to decode malicious signals. Reports in 1999 surfaced that an unknown actor hacked the United Kingdom's Skynet satellite, requiring payment to become operational again. Though the British Minister of Defense described the claim as "impossible" at the time, more of these instances may occur as computer systems advance and space networks fail to evolve with greater security.

Third, while American policymakers may focus mainly on protecting networks, defending against the seizure of a satellite remains equally important. Such seizures could result in the deliberate destruction of the spacecraft, creating considerable debris that threatens other systems on orbit.

Equally likely, a hacker could transfer ownership of a system, so the original user is completely locked out and the capability of a satellite is given to the adversary. In 1998, a German-American satellite was hacked and destroyed. Attackers fried the optics by turning the satellite towards the sun. Unfortunately, examples of hacked satellites continue into the twenty-first century. Bill Malik reports that "there are six known examples of hackers successfully interfering with or even commanding unauthorized maneuvers of NASA satellites before 2011."

Looking Forward: Addressing Cyber Threats

The US currently invests in multiple avenues to combat the possibility of satellite hacking, a challenge made more difficult by the same factors that affect other industries and targets. For general satellite protection, the Air Force Research Laboratory is beginning its fourth year of sponsoring a satellite hacking challenge to involve researchers across the country. The Hack-A-Sat competition opened for registration in February with this year's format involving the use of an on-orbit satellite for the first time.

"Space cybersecurity is a global issue, which is why it is so important that Hack-A-Sat is open to the global security research community," said Col. Kenny Decker. Across the Atlantic, the European Space Agency sponsors similar competitions with HackCYSAT.

Recently, the geospatial intelligence company, Orbital Insight, won a Department of Defense contract to identify intentional global navigation system disruptions. Orbital's platform aims to use artificial intelligence to detect spoofing operations. According to the National Security Agency's (NSA) Aaron Ferguson, it is a goal of NSA is to develop, "a way to characterize telemetry data so that as we deploy new satellites, we can make adjustments.” Finally, HDI Global Specialty argues that “the backbone of a cyber-resilient spacecraft should be a robust Intrusion Detection System (IDS).” Encryption and authentication must become priorities for the US government to implement in satellites and satellite systems.

Conclusion

Russia poses a large security threat to the United States even outside the future possibility of satellite hacking. Russian aggression in Ukraine demonstrated blatant disregard for Western ideals of a rules-based international order. It is no longer possible for policymakers to secure stability and prevent conflict by relying on post–Cold War paradigms.

Previous engagement through international communication channels is unlikely to reduce threats to critical infrastructure. As state-sponsored groups and proxy actors continue to target American assets, it is necessary to prepare for multiple modes of attack, especially in the space and cyber domains. A whole-of-government approach to defend against this new generation of conflict can increase reactivity in the event of an attack and aims to provide a deterrent against the targeting of satellites. As the twenty-first century evolves, implementing these solutions is one of the most important challenges the nation faces.