Space and Cyber Security

08 October 2024 Jessie Hamill-Stewart, PhD Candidate - University of Bath and University of Bristol

The Critical Need for Enhanced Cybersecurity in Satellite Systems to Protect Modern Life and Services

Space has become critical to today's modern world. Satellite systems, such as global navigation satellite systems (GNSS) provide positioning, navigation, and timing services on which critical industries increasingly rely, including finance, transportation and electricity. In addition, satellite broadband is providing internet access to growing numbers of users in remote areas globally. As this dependence grows, modern life becomes more vulnerable to disruption caused by a problem with satellite systems. Increasing commercial investment is driving wider use of satellite systems, extending

the potential attack surface, in turn increasing the importance of security for space.

Cyber attacks can be used to exploit attack vectors within space infrastructure and cause disruption to critical services which rely on satellites in order to function. Cyber attacks disrupt the IT networks of components, often leading to physical consequences and widespread disruption. The recent CrowdStrike error was not documented a cyber attack, but it demonstrated how one piece of faulty software can lead to global disruption, including delayed transportation and disrupted health systems. Considering the importance of space systems for other critical infrastructure, cyber attacks against space systems poses a particularly concerning threat.

Satellite systems comprise of user, space and ground segments. Each segment contains a number of components which contain unique vulnerabilities and threats. Cyber attacks pose a concern across all segments. Signals transmitted to receivers on vessels or aeroplanes in the user segment could be spoofed or jammed, perhaps to intercept critical positioning data and confuse crews. Satellites orbiting in the space segment could be targeted with a cyber attacks originating from another satellite, or the ground control infrastructure. The ground segment is especially concerning because this is where satellites are operated and monitored from, and if an attacker gains access to this segment, they could disrupt the position of satellites in orbit and extended ground systems too, such as internet modems.

Some cyber attacks and incidents have already been documented against satellite systems. A notable example was the disruption to ViaSat's Ka-Sat network in 2022, just before the invasion of Ukraine. The attack impacted the Ukrainian military's satellite ground communications, as well as thousands of modems for other critical facilities across Europe, including wind farms. There has also been disruption to GNSS, such as the Global Positioning System, Glonass and Galileo in the past, as well as documented nation state attacks against the ground infrastructure of satellite operators (1).

As the space industry continues to grow, cyber attacks may become more common. As such, raising awareness of the potential disruption cause by

attacks against space systems is a key aspect of demonstrating the importance of securing infrastructure. A cyber attack against any kind of space systems could potentially create wider disruption, so that increasing levels of security throughout the industry has become absolutely fundamental.

(1) For more information about cyber attacks against ground infrastructure of satellite systems, please visit: spacesec2024-87-paper.pdf (ndss-symposium.org)