# Cybersecurity for satellites is a growing challenge as threats to space-based infrastructure grow

February 21 2024, by Sylvester Kaczmarek

Credit: Unsplash/CC0 Public Domain

In today's interconnected world, space technology forms the backbone of our global communication, navigation and security systems. Satellites

orbiting Earth are pivotal for everything from GPS navigation to international banking transactions, making them indispensable assets in our daily lives and in global infrastructure.

However, as our dependency on these celestial guardians escalates, so too does their allure to adversaries who may seek to compromise their functionality through cyber means. A satellite's service could be interrupted, or at worst the spacecraft could be disabled. The expansion of the digital realm into space has opened new frontiers for cyber threats, posing unprecedented challenges.

This emerging battleground highlights the urgent need for robust cybersecurity measures to protect our space assets from sophisticated attacks that threaten global stability and security.

Recent cyber incidents, such as the 2022 attack on the KA-SAT network , highlight the immediate vulnerability of satellites. The network, owned by global communications giant Viasat, faced a sophisticated cyber assault that disrupted its services across Europe. While the perpetrators have not been officially confirmed, many suspect Russia's involvement.

As we witness an increase in state-sponsored attacks and the commercialization of hacking tools, the stakes for securing space assets extend beyond technical challenges to encompass potential disruption to the world economy and diplomatic relations between countries that operate satellite networks. The focus on space security has been thrown into the spotlight recently by the claim that Russia is developing a space-based anti-satellite weapon—possibly one that's nuclear-powered.

## Evolving threats

The shift from analog to digital has transformed space technology vulnerabilities, exposing them to a spectrum of cyber threats. Initially,

from the late 1950s onwards, concerns centered around physical tampering and espionage, but as the technology advanced, digital vulnerabilities became the forefront of security challenges.

With adversaries now employing artificial intelligence (AI) and machine learning to find new vulnerabilities, the complexity of attacks goes well beyond traditional strategies for defending satellites.

Early breaches such as the hacking of US-German satellites in 1998 were precursors to the complex cybersecurity landscape we navigate today. Modern adversaries leverage sophisticated techniques to exploit vulnerabilities in satellite communications and data transmission, aiming to disrupt, intercept, or corrupt the invaluable data they carry.

This evolution signifies a pivotal shift in how we must approach the security of space technology, underscoring the importance of anticipating and mitigating digital threats. This includes end-to-end encryption to make data transmission harder to hack or disrupt, and better detection of suspicious activity in advance of an attack. There's a cost to implementing these security measures, however, such as limitations on computer processing power and bandwidth.

## Vulnerabilities in the void

The isolation of satellites in orbit and their reliance on wireless communications expose them to specific threats such as signal jamming, spoofing—disguising communications from a suspicious source as those of a known, trusted source—and the interception of data.

Additionally, the limitations on processing power and bandwidth in space exacerbate the challenge of implementing routine software updates and patches, leaving systems vulnerable to exploitation.

Software vulnerabilities within satellite systems can be exploited from great distances, allowing attackers to potentially take control of them. This vulnerability is compounded by the ever-increasing complexity of satellites and their software.

The void of space does not shield these assets from cyber adversaries; instead, it presents a domain rife with unique challenges. These challenges require innovative solutions.

In response to these escalating cyber threats, a united front has formed among space agencies, technology companies and security experts. This effort is focused on developing robust defense mechanisms to protect satellites and other space-based technologies.

Key initiatives include establishing secure communication protocols, implementing end-to-end encryption for data transmission, and deploying AI-powered anomaly detection systems to identify suspicious activities in satellite networks. Beyond initiatives by Nasa and the European Space Agency (Esa), other international collaborations have taken shape, reflecting a widespread commitment to space cybersecurity.

Agreements among countries in the Five Eyes intelligence alliance (consisting of the US, UK, Canada, Australia and New Zealand) and partnerships with private-sector leaders in space technology underscore the global acknowledgment of the importance of securing space assets. These cooperative endeavors are crucial not only for safeguarding national security interests, but for ensuring the uninterrupted operation of the myriad services that rely on space technology.

## Cyber defenses in space

The development of AI-driven security protocols and quantum encryption is poised to revolutionize the protection of space assets.

AI-driven security offers the potential to predict and counteract cyber threats in real-time, continually adapting to new challenges. However, this technology is still under development and faces significant challenges, including the availability of limited data sets for training in the unique context of space.

Similarly, quantum encryption in theory offers impervious security by making use of the field of physics known as quantum mechanics. But this is still in the research and development stage for space applications—practical deployment of such technologies in space will require a great deal more innovation and testing.

## Global implications

Cybersecurity in space extends far beyond the technical realm, affecting international relations, cooperation, and competition. There is a drive towards greater protection for space infrastructure. International collaboration would be ideal to achieve this, but such an aim faces challenges due to competing interests and varying levels of trust between nations.

The economic repercussions of cyberattacks on space infrastructure are profound. A significant cyber incident could cost billions in damages, disrupting global services and requiring extensive resources for mitigation and recovery.

The complex interplay between the need for collective security measures, the hurdles in achieving global cooperation, and the potential for catastrophic economic impact underscores the intricate relationships between cybersecurity in space, international relations, and economic stability.

Progress in cybersecurity measures in outer space is not just a technical

necessity but a global imperative, to safeguard the future of space exploration and the integrity of critical space infrastructure. Addressing the evolving landscape of cyber threats demands ongoing vigilance, innovation, and a unified approach among all those involved in spaceflight.



Provided by The Conversation