SAE MEDIA GROUP

SATCOM Cybersecurity Challenges and Scalable Solutions

08 October 2024 Dr. Vincent Lenders,
Director of the Cyber-Defence Campus - Swiss Federal Department of Defence

Addressing Vulnerabilities and Enhancing Protection for Critical Infrastructure

Satellite communications play a critical role in global telecommunications infrastructure, providing essential services for a wide range of applications including military operations, navigation, weather forecasting, and broadcasting. However, the increasing reliance on satellite systems has made them a significant target for cyber threats. This presentation explores the cybersecurity challenges facing satellite communications, outlining key vulnerabilities, potential impacts of cyberattacks, and strategies for enhancing security.

Satellite communication systems are complex networks involving satellites, ground stations, user terminals, and control centres. Each component in this chain presents unique cybersecurity challenges. The primary vulnerabilities arise from the inherent exposure of satellite systems to external attacks due to their broad coverage area and the use of wireless communication links, which are susceptible to interception, jamming, spoofing, and unauthorized access. Additionally, the legacy infrastructure of many satellite systems, which may not have been designed with modern cybersecurity considerations in mind, further exacerbates the risk.

One of the significant threats to satellite communications is signal jamming, where an adversary disrupts the communication link by overwhelming it with noise. This can lead to a denial of service, impacting critical operations such as military communications or emergency response coordination.

Spoofing is another major threat, where attackers deceive satellite systems by sending false signals, potentially leading to the misrouting of data, incorrect positioning information, or even taking control of the satellite. Cyberattacks on ground stations, which serve as the command-and-control centres for satellites, can result in the loss of control over satellite operations, causing significant disruptions in services.

The potential impacts of successful cyberattacks on satellite communications are vast. They can range from the interruption of television broadcasts to more severe consequences like the loss of critical military or navigation capabilities. In the worst-case scenario, cyberattacks could lead to the physical damage of satellite systems, either through the manipulation of satellite controls or the triggering of destructive commands, resulting in the complete loss of a satellite. To mitigate these threats, a multi-layered approach to cybersecurity is essential. This includes implementing robust encryption protocols to protect the confidentiality and integrity of data transmitted over satellite links. Moreover, incorporating advanced intrusion detection and prevention systems can help identify and thwart cyber threats in real time. The adoption of strong authentication mechanisms for access control to satellite systems is also vital in preventing unauthorized access.

The Cyber-Defence Campus, part of Switzerland's Federal Office for Defence Procurement (Armasuisse), has been actively conducting research since its creation in 2019 to enhance the cybersecurity of satellite communications. The Campus focuses on identifying vulnerabilities in satellite systems, such as those in signal transmission, communication protocols, and satellite software. It develops advanced cryptographic techniques to secure communication links and protect against threats like spoofing and unauthorized access. Additionally, the Campus collaborates with international partners, leveraging a network that combines expertise in cybersecurity, aerospace engineering, and data science. Through simulations, testing, and real-world experiments, the Cyber Defence Campus aims to create robust defence mechanisms and establish best practices that can be applied across military and civilian satellite operations, ensuring the resilience of these critical infrastructures against emerging cyber threats.