IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Mr. Peter Franke
Telespazio Germany GmbH, Germany, peter.franke@telespazio.de

Ms. Alexandra Weber
Telespazio Germany GmbH, Germany, alexandra.weber@telespazio.de
Mr. Jussi Roberts
European Space Agency (ESA/ESOC), Germany, jussi.roberts@ext.esa.int
Mr. Marc Niezette
Telespazio Germany GmbH, Germany, marc.niezette@telespazio.de

SPACE MISSION SECURITY MONITORING

Abstract

Space-based infrastructure has become increasingly critical to the functioning of our economy and society, with growing reliance on the communications, navigation and earth-observation capabilities it provides. However, this growing importance also leads to a growing threat and potential impact of cyberattacks against space missions. As a result, the various stakeholders of the space community share a need to increase the resilience of their infrastructure, consisting of ground IT and applications, on-ground operational technology (OT) and space assets. This also includes interplanetary assets forming deep-space communication networks ("Interplanetary Internet"), which are becoming more and more relevant with the increasing number of planned and ongoing unmanned or manned missions to the moon, mars or further destinations.

To increase the cyber resilience of these asset classes, different types of activities are being undertaken, including the development of security monitoring techniques, the establishment of cybersecurity centres to provide knowledge and training to personnel involved in various mission operation roles, fostering secure systems engineering processes, introducing penetration testing capabilities tailored to space missions, and the usage of quantum and post-quantum security technologies.

As they enable a swift detection and response to threats, sophisticated security monitoring techniques play an important part in the overall activities. This includes SOC (Security Operations Centre) capabilities incorporating the monitoring of on-ground operational technology and space assets, and hence going significantly beyond the capabilities offered by commercial solutions for monitoring terrestrial IT assets. Due to the increasing rate and sophistication of cyberattacks, analysing the vast amount of information collected to detect such attacks is becoming too complex for human operators alone to handle. To support them, the used security monitoring techniques must be able to process data at high speeds and automation levels. To this end, Artificial Intelligence (AI) techniques provide potential solutions which may be integrated into the security monitoring infrastructure, under consideration of additional security risks introduced by the use of AI.

In this paper, we describe a security monitoring architecture for space missions. The architecture includes monitoring capabilities for IT, ground OT and space segment assets involving state-of-the-art technologies. For each of the different segments, we elaborate on specific properties, like communication protocols, computing and networking technologies and physical location, that influence the required or feasible monitoring solutions. We also consider the issues that will be faced when monitoring interplanetary

assets and networks and providing SOC capabilities for these assets.