55th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Dr. Paola Breda
HyImpulse Technologies GmbH, Germany, breda@hyimpulse.de

Dr. Adam Abdin
CentraleSupélec, France, adam.abdin@centralesupelec.fr
Ms. Rada Markova
Space Generation Advisory Council (SGAC), Austria, rada.markova92@gmail.com
Mr. Devanshu Jha
Space Generation Advisory Council (SGAC), India, devanshu.jha7@gmail.com
Mr. Antonio Carlo
Tallinn University of Technology, Estonia, ancarl@taltech.ee
Dr. Nebile Pelin Mantı
Space Generation Advisory Council (SGAC), Turkey, npmanti@gmail.com

CYBER VULNERABILITIES AND RISKS OF AI TECHNOLOGIES IN SPACE APPLICATIONS

Abstract

Artificial Intelligence (AI) is becoming a critical technology for space applications, and recently, AI has come into use in satellite operations, particularly to support the operation of satellite constellations, for relative positioning, communication, and end-of-life management, among others. AI systems are used in space applications to analyse Earth observation data, or telemetry data from the spacecraft. AI and Man-Machine Interface (MMI) are technological trends, which help to reduce the operational cost of satellite operations on the one hand, by optimizing the satellite trajectory, or by augmenting Space Situational Awareness (SSA). While the importance of AI is rising for new space assets, AI is vulnerable to cyber threats, and AI cyber security is becoming an important aspect of space safety and operational safety for both public and private actors. In fact, AI algorithms are not exempt from fundamental flaws, and these systems can be targeted by cyber attackers. This work aims to analyse how cyberattacks are targeted at space assets with AI technology integrated in one or more of their subsystems. Firstly, the paper examines and differentiate between vulnerabilities and risks specific to AI space systems. The analysis covers risks concerning satellite networks and ground operations as well as vulnerabilities concerning short-term and long-term missions. The dual use of AI is discussed by the authors as the worst-case scenario in a parallel paper. Secondly, a comparison between prevailing cyber-attacks in space and cyber-attacks targeting AI technologies is made. Different attack profiles are assessed, distinguishing between the local effects (on the system), the global effects (on the population and the economy), and the legal consequences of a cyber-attack. Based on this assessment, the paper recommends prevention and mitigation measures that are contingent on cyber resilience and a policy for security and safety of space operations focusing on AI-based space applications.