Paper ID: 77662
oral
student

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: Ms. Laura Morelli
International Space University (ISU), Italy

Mr. Nicolas Peter
International Space University (ISU), France

CYBERSECURITY AND SPACE: A TRANS-ATLANTIC PERSPECTIVE

Abstract

Due to the exponential growth of technology development and data transfers, cybersecurity in the space field has become a topic of utmost relevance to all operators. For this reason, international and regional powers are developing policies and laws to better protect themselves and their data. Nonetheless, the term "Cybersecurity" has not been well defined in international law and there is little consensus on what it really entails. Entering a more specific field, cybersecurity in the space domain is necessary and often requested, but hardly explained.

This paper presents in detail the concept of "cybersecurity" and its application to the space sector. It first offers extensive research on the meaning of "cybersecurity". Secondly, it identifies the possible different types of cyber threats and cyber-attacks that can be experienced. To understand via a practical approach the necessity for space actors to carry out cybersecurity measures, a historical overview of past and present breaches of security related to space activities is provided. Many such breaches fall under jamming and spoofing, but there are some other mechanisms to take into account. For this reason, it is extremely relevant to understand that cybersecurity needs to be present throughout the entire information chain as to protect all segments of space activities that transfer, analyze or store data: space segment, ground segment and user segment. Furthermore, this work portrays a thorough analysis of international laws and policies related to cybersecurity. Additionally, it contains a specific comparative study between the United States and Europe, assessing differences according to units of comparison: US government and EU political institutions; as well as NASA and ESA.

The paper also provides recommendations, identifying current legal loopholes or further concepts that might not have been considered yet. Such recommendations can be used as a guideline for the United States, European authorities, or other powers to upgrade their space-related cybersecurity measures.