Paper ID: 85548
oral

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. Pietro Santoriello
Partners4Innovation, Italy

Dr. Annamaria Nassisi
Thales Alenia Space Italia, Italy
Dr. Stefano Mele
Gianni & Origoni Law Firm, Italy
Ms. Laura Camardelli
Gianni & Origoni Law Firm, Italy

PROTECTING SPACE ASSETS: CYBERSECURITY IMPERATIVES FOR FUTURE MISSIONS

Abstract

In an era defined by an unprecedented reliance on space technologies, cybersecurity emerges as a critical element in safeguarding the integrity of infrastructure vital to space missions. This reality is underscored by the escalating interest of cybercriminals in targeting space assets. The allure of cybercrime stems from the potential for devastating consequences, not only to infrastructure and sensitive data but also to global security and the economy at large. Targeted attacks have the capacity to disrupt essential communications, manipulate navigation data, or even seize control of satellites, posing significant threats to both national and international security. These attacks span a spectrum of tactics, from jamming to spoofing, and encompass compromises of collected data and malicious exploitation of ground control systems. In response to this challenge, space organizations are heightening security measures during the planning and development phases of new missions. The implementation of effective security measures necessitates a delicate balance between protection and practicality, coupled with the imperative to remain vigilant against evolving cyber threats. Exploring the landscape of emerging cyber threats, this paper delves into what constitutes a 'cyber-secure' space mission and examines how awareness of cyber risks is reshaping the approach of corporate entities in designing and operating space missions. The objective is to underscore the importance of proactive security assessment strategies and the adoption of best practices to mitigate risk. Furthermore, the paper discusses the integration of security frameworks specifically tailored to the unique challenges of the space environment. By analyzing existing standards and frameworks, this study aims to identify optimal practices at both international and corporate levels. It proposes a roadmap for fostering a cybersecurity culture within space agencies and private sector entities, advocating for international collaboration in developing global standards, sharing best practices and proposing a legal and protection framework to enable secure cooperation across corporate and international boundaries. In conclusion, this publication emphasizes the necessity of prioritizing threat prevention from the inception of future space missions.