Paper ID: 78578
interactive
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: Dr. Nicolò Boschetti
Cornell University, United States, nbosche1@jhu.edu

Prof. Gregory Falco
Cornell University, United States, gjf24@cornell.edu

THE IEEE SA SPACE SYSTEMS CYBERSECURITY STANDARD: GOVERNANCE AND TECHNICAL ELEMENTS OF AN INTERNATIONAL STANDARDIZATION EFFORT.

Abstract

Global critical infrastructure is now inextricably linked to the space sector, making the need for space cybersecurity shared regulations and standards unprecedently crucial. To address this gap, the Institute of Electrical and Electronics Engineers Standard Association (IEEE SA) has recently approved the development of the Space Systems Cybersecurity International Standard.

This paper will describe the current state of space cybersecurity standardization and present the process of creating the IEEE SA Space Systems Cybersecurity Technical Standard. It will provide a review of existing international standards that can be applied to space systems to highlight the current gaps in the sector. Exposing the gaps, the authors will show why a technical standard is essential for the space community and how a globally coordinated technical standardization effort can be a robust solution to the darkening landscape of cyber threats.

Combining different stakeholders' expertise and priorities constitutes a complex policy and governance process. Therefore, the coexistence of institutional, commercial, and academic actors in the Working Group will be described to provide the community with an example of a complex governance and standardization framework. The complex multi-stage process for developing the standard will be described in addition to the relationship between the leading working group and subcommittees. In fact, the complexity of the effort will require the synergy of five specialized subcommittees, each focusing on a distinct segment of space operations: space, link, ground, user, and integration layer. Moreover, depicting such a complex framework will provide a case study for international space cooperation by harmonizing rules and practices.

This paper will help understand how the process of creating the IEEE Space Systems Cybersecurity International Standard has repercussions and connections with the global governance of space activities. Furthermore, the paper will show how the standard will significantly impact the space sector, ensuring long-term cyber sustainability and security. By providing technical guidance for cybersecurity in space systems, the standard will contribute to developing a more stable, secure, and sustainable space environment, supporting the continued growth and advancement of the space industry.

The authors (chair and secretary of the standard's Working Group) will carry out the study by merging space cybersecurity technical expertise and real-life experience of leading the standardization process. Therefore this paper will be of interest to both the policy and the technical communities, showing best practices and a process of governance and engineering international cooperation.