Paper ID: 87090
oral
student

57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Dr. Antonio Carlo
Tallinn University of Technology, Estonia

Dr. Nebile Pelin MANTI
Space Generation Advisory Council (SGAC), Türkiye
Mr. Bintang Alam Semesta Wisran AM
Skolkovo Institute of Science and Technology, Russian Federation
Mr. András Edl
University of Public Service (UPS), Hungary
Dr. Paola Breda
International Space University (ISU), France

# CYBER RANGE AND DIGITAL TWIN TECHNOLOGIES FOR SPACE RESILIENCY AND SECURITY

**Abstract**

Over the past decade, the number of civil and military assets operating in space has significantly grown, as the reporting of occurrence of cyber incidents has. Due to the criticality and interconnection of the space domain with the cyber domain, it is essential to guarantee the security and sustainability of their services.

To fulfil both tasks, Space Cyber Ranges is capable of providing a secure environment for product development and security testing of cyber technologies with the aid of tools such as Digital Twins (DT). In fact, DTs, as dynamic, virtual replicas of physical systems, present a transformative opportunity for satellite technology to enhance their accuracy, efficiency, and longevity. The integration and implications of DT technology to support space activities are investigated in regard to their contribution to space security, in particular, their use for satellite operations and their role in enhancing cybersecurity measures through space cyber ranges. Earth Observation cases as an example of current frameworks and models for implementing digital twins in satellite technologies are discussed, with the scope of establishing a comprehensive policy and technical framework for evaluation. In this context the paper shall examine the effect such a framework may have regarding operation of space assets from a compliance standpoint for companies in the private sector. By examining the security landscape faced by satellite systems, this work evaluates how DTs and Space Cyber Ranges act as pivotal tools in developing resilient defence mechanisms against cyber threats and, thus, how DTs are used within cyber ranges for proactive simulation and mitigation of cyber threats.

This research takes a multidisciplinary approach by combining examples from EO technologies and cybersecurity. It aims to contribute to ongoing discussions about improving the resilience and effectiveness of satellite operations through advanced DT technologies and cybersecurity solutions. Specifically, DT can be a useful tool for the space industry in developing adequate cyber capabilities.

Please note that the present abstract is submitted under the auspices of the Space Generation Advisory Council as a part of the activities of the Space and Cybersecurity Project Group.