Paper ID: 64939
student

54th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Antonio Carlo
Tallinn University of Technology, Estonia, ancarl@taltech.ee

Ms. Francesca Casamassima
Italy, fcasamassima8@gmail.com

SECURING OUTER SPACE THROUGH CYBER: RISKS AND COUNTERMEASURES

Abstract

The space sector has witnessed, in recent years, significant changes in terms of technological innovation, emerging players, and new market dynamics, which further highlights the critical and strategic nature of the sector. Indeed, satellite services increasingly support critical functionalities in national and international infrastructures, making space assets attractive targets for cyber-attacks. In addition, within the past decades, new space actors have emerged and developed space and counter-space capabilities, leading to an increased commercialisation of space, along with the development of new market trends, that has thus shifted the focus on profitability rather than security. Though recognised as two different domains, the cyber and space domains share a variety of common security challenges ranging from increased militarisation, to a rise in dual-use technologies, which hinder the application of traditional arms control instruments, up to a lack of shared international treaties and guidelines. The space sector shares similar cybersecurity issues with other industries. However, given the intrinsic complex nature of the domain, risk mitigation is particularly challenging. In addition, both in outer space and cyberspace, Emerging Disruptive Technologies (EDTs) have become increasingly relevant. Rethinking the role of cybersecurity in protecting space assets and ensuring mission continuity, mostly by building resilience in the cyber supply chain, has therefore become vital. The paper will elaborate and analyse the importance of rethinking the role of cybersecurity in protecting space and ground assets, adopting security-by-design approaches in the early stages of system development and by developing Security Operational Centres (SOC). Moreover, this paper will evaluate the key challenge in advancing cybersecurity standards and regulations at a national and international level, fostered by international actors such as the EU and NATO as primary promoters of standardised cybersecurity practices in outer space.