Paper ID: 78079
oral
student

56th 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

Dr. Nebile Pelin MANTI
Space Generation Advisory Council (SGAC), Türkiye
Dr. Paola Breda
International Space University, France
Ms. Maelys Rollinde de Beaumont
Space Generation Advisory Council (SGAC), France
Mr. Devanshu Jha
Space Generation Advisory Council (SGAC), India

TOWARDS A RESILIENT CYBER ARCHITECTURE FOR SPACE INFRASTRUCTURES: MITIGATING THE NEW ATTACK VECTORS

Abstract

After more than 60 years of space activities, ongoing scientic and technological progress alongside increased international cooperation, space security has also entered this eld, leaving its hallmark on what appears a new era of space activities. The space community is rapidly changing, and the world continues to face a growing need for dedicated space applications.

In cybersecurity, an attack vector is a method of achieving unauthorised network access to launch a cyber attack. Space assets, both military and civil, have been the primary target of cyber-attacks. It is highly recommended for commercial constellations to implement encrypted transmissions between the ground segment and the space segment - a compelled choice for military constellations instead. In both cases however, many of them are designed with no-further defences, such as permissions, intrusion detection, and mitigation, should an attacker manage to circumvent the encryption.

The growing dependence on space applications due to civilian and military interests requires maintaining control and continuity of space services. The security concepts therefore extend beyond cyber security, into cyber resiliency. A cyberattack in the space domain is a 'multi-dimensional' variant of a conventional cyber-attack. As the digitalisation of space systems rapidly increased in the past decades, the attack surface, or the types of system vulnerabilities accessible to a cyber attacker, have also expanded. Therefore, designing resilient system architectures for safeguarding and deciding upon the correct offensive security strategies for defending the cyber physical infrastructures becomes a more challenging task on the engineering, policy, and legal dimensions.

The paper will demonstrate that, given the ultra-hazardous nature of outer space and the growing dependence of society on space services, the conventional security concepts might extend beyond cyber security into cyber resilience. Furthermore, the paper will assess the effectiveness of a multi-layered cyber defence architecture and the need for shared measures and for international standards to augment resiliency and security of services. Finally, this work will provide an assessment of the actual existing cyber threats to on-ground and on-board space infrastructures, in order to propose tailored standards and policies at the right level based on the guidance provided by the international norms. Please note that the present abstract is submitted under the auspices of the Space Generation Advisory Council, as part of the activities of the Space and Cybersecurity Project Group.