Paper ID: 61411
oral

IAF SYMPOSIUM ON SPACE SECURITY (E9)
Cyber-security threats to space missions and countermeasures to address them (2.D5.4)

Author: Mr. Douglas Wiemer
Rhea Group, Belgium

Mr. Gianluca Cerrone
Rhea Group, The Netherlands

CYBER RANGE SOLUTIONS AND SERVICES FOR SPACE ASSETS

Abstract

Cyber security is becoming increasingly challenging in the space sector. As advanced application services seamlessly leverage connectivity provided by space based communications systems, it is understood that space assets have gained increased attention of cyber adversaries. Seamless access to space-enabled applications services and reality of complex software results in increased cyber risks to space assets and downstream services. It is well known that several nation states have established doctrine including the identified need to interfere with, damage, and destroy reconnaissance, navigation, and communication satellites. The result of the increased and evolving cyber threat is a corresponding increased attention applied to cyber security risks in all stages of development and operation across the space industry. Among the promising approaches to improve cybersecurity preparation and risk reduction is the coordinated use of Cyber Range solutions and services. A Cyber Range provides an environment to train and equip cybersecurity professionals and system operators; perform cybersecurity related research and development of space systems and advanced prototype technologies; and perform tests and evaluations of space systems and architectures in a simulated operational environment. A full functioning cyber range supporting secure space assets development and delivery should encompass the following: 1. A scalable and flexible space assets emulation environment: In order to support independent security test and evaluation of space technologies, systems and solutions, the Cyber Range must be comprised of a system-of-systems solution involving a range of emulation technologies for mission control, ground station, and satellite systems across multiple mission types and covering both mission control and data segments. 2. An adaptable test harness with standardized interfaces: In order to conduct security testing of technologies within the emulation environment, it is essential that discrete components within the end-to-end service can be independently replaced by technologies under test. 3. A cyber simulation capability: Security test and evaluation of space assets requires a range of security testing capabilities. This will include static and dynamic application testing tools, and technical vulnerability assessment and penetration testing tools. RHEA has been actively involved in delivery of cyber range solutions since 2013. RHEA is the contracted authority delivery and operations of the ESA Cyber Range at the European Space Security and Education Centre. RHEA has since developed the CITEF, a next generation cyber range that greatly enhances the flexibility and adaptability of virtual cyber scenarios for any information technology or operations technology domain.