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. Nathaniel Dailey
The MITRE Corporation, United States, ndailey@mitre.org

Dr. Rick Randall
The MITRE Corporation, United States, rrandall@mitre.org

A METHOD TO EMPLOY A REGIME FOR A SPACE CRITICAL INFRASTRUCTURE ASSESSMENT FRAMEWORK

Abstract

The United States Space Priorities Framework makes clear that "access to and use of space is a vital national interest." Space Policy Directive 5 (SPD-5) notes: "Space systems enable key functions such as global communications; positioning, navigation, and timing; scientific observation; exploration; weather monitoring; and multiple vital national security applications. The proposed the 'U.S. Satellite Cybersecurity Act notes that need for a study on the actions the U.S. Federal Government has taken to support the cybersecurity of commercial satellite systems, including as part of any action to address the cybersecurity of critical infrastructure sectors. House bill titled, H. R. 3713 the "Space Infrastructure Act" directs the Secretary of Homeland Security to issue guidance with respect to space systems, services, and technology as critical infrastructure, and that 30 days after enactment the Secretary shall designate space systems, services, and technology as a critical infrastructure sector. To that end, and in the larger context of international space operations, this paper will enumerate recommended practices with which to ameliorate the problems associated with assessing risk to space as a critical infrastructure for general consumption among commercial satellite owner operators globally.

Good security practices necessitate traceability across numerous security practices, such as infosec, operational security, communications security, transport security and personnel security. The challenge with security is in how it is employed. If not properly implemented, a security profile with weak links will not protect commercial systems from more sophisticated bad actors. Minimal steps for security will not be effective against more sophisticated bad actors without the associated physical, personnel, trusted supply chain, cyber, certification and accreditation, mission assurance, safety management, security, and sustainability processes and procedures. Taken altogether, employing a regime for leveraging security standards and practices in the contexts of these other guiding principles provides the strongest means with which to assure a safe and resilient space critical infrastructure. This paper will provide a regime for international institutionalization of these recommended practices within and among commercial consortia, and further provide an assessment methodology with which to measure the applied impact of the recommended practices within commercial ventures and government programs alike.