Paper ID: 78845
student

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: Mr. Edward Koellner
University of Mississippi School of Law, United States, ed.koellner@gmail.com

SECURING THE FINAL FRONTIER

Abstract

As humanity continues to stretch its reach into space, cybersecurity becomes a subject of increasing importance. As more satellites, probes, and other spacecraft are launched, the requirement for secure networks to protect spacecraft from malicious actors is essential. Transmission signals are susceptible to cyber access, loss of control, disruption of services, and tampering with or deletion of data are numerous dangers in cyber space activities. Protections need to be put in place to protect space assets from adverse actions of foreign nations trying to obtain confidential information or interfere with space-oriented operations. Identifying the risks involved with space cybersecurity and engaging proactive measures will enable space exploration and cybersecurity to align to ensure a safe and secure future for human space exploration.

The commercialization of outer space is resulting in an exponential deployment of satellites supporting communications, navigation, and military services. Cyber vulnerabilities in space resulting from this interaction have not yet been comprehensively addressed. While there is no explicit regulation, existing treaties and improved cyber strategies regarding international cyberspace law can be a good place to start and build upon.

Cyberspace law is crucial in the regulation governing outer space cyber operations. Malevolent uses of cyberspace pose hazards to space activities. This article will begin with a discussion of definitions before describing the technological nature of cyberspace and addressing the subject of how cyberspace law may affect activities in outer space. Then, topics regarding the applicability of international law and space law to cyber activities and strategies to mitigate the effects of cyber-attacks on the space infrastructure will be discussed.

The purpose of this research paper include: (1) a background to the convergence of the commercialization of space and the escalating need for a focus on cybersecurity; (2) evaluate cyber-attacks affecting space assets and the applicability of the Outer Space Treaty and the Liability Convention; (3) discuss the new US White House released National Cybersecurity Strategy regarding fundamental shifts in allocated roles, responsibilities, and resources in cyberspace and (4) how this cybersecurity strategy can be implemented for the commercial space environment.