50th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Mr. Christopher Roberts
Institute of Air and Space Law, McGill University, Canada, christopher.p.roberts@mail.mcgill.ca

Mrs. Juliana Scavuzzi
Brazilian Association of Air and Space Law, Canada, juliana.scavuzzi@mail.mcgill.ca

EVALUATING THE EFFICACY OF LAW AND REGULATION IN PREVENTING CYBER-SECURITY THREATS IN OUTER SPACE

Abstract

As human presence and activity in outer space continues to increase at a rapid rate, so too does reliance on the sophisticated and complex technology that makes space missions possible, including, inter alia, vehicles designed to transport humans and cargo into space, satellites, telescopes, long-term orbital vehicles, and Earth-based (ground) installations which assist in the launching, operation, and re-entry of space objects. Because these technologies are dependent, at least in part, on computer networks and the internet in order to function, they are vulnerable to cyber-based threats, many of which have the potential to cause significant harm to public safety and security both in space and on Earth. For example, satellites and other spacecraft are susceptible to various forms of cyberattack such as hacking, data theft and corruption, hijacking, and interference with their transmissions in the form of jamming or spoofing, all of which can impede their operation and even render them inoperable. Despite these potentially negative consequences, however, few existing international or national laws and regulations specifically address the problem of cybersecurity in space, thus calling into question the necessity of promulgating a new legal regime in order to prevent these types of attacks. This paper will evaluate the efficacy of current international and national laws and regulations that could potentially prevent cybercrime in space including the United Nations space conventions, criminal laws which identify and prosecute cybercrime, and regulations regarding the oversight and prevention of intentional harmful interference, to name a few, and will assess whether interstices within these laws necessitate the implementation of a new legal and/or regulatory regime designed specifically to prevent space-based cyberattacks. In addition, because of the many conflicts and problems inherent in international cooperation, notably those pertaining to state jurisdiction and sovereignty, the authors will evaluate the role of alternative, non-governmental frameworks and methodologies in dealing with the problem of space cybersecurity. To take just one example, space-related industries and stakeholders could work collaboratively to create an international regime designed to develop, manufacture, and operate spacecraft that would be more resilient to cyberattacks. The authors will conclude that enhanced cooperation between private industry and actors on the one hand, and nation states and government institutions on the other, will likely provide the most effective approach in mitigating the risk of cyberattacks in space, in turn promoting an environment in which all space vehicles can operate safely for the benefit of all humankind.