49th 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: Ms. Helena Correia Mendonça
Vieira de Almeida & Associados, Portugal, hcm@vda.pt

Mrs. Juliana Scavuzzi
Brazilian Association of Air and Space Law, Canada, juliana.scavuzzi@mail.mcgill.ca
Mrs. Magda Cocco
Vieira de Almeida & Associados, Portugal, MPC@vda.pt

ADDRESSING THE INTERNATIONAL LEGAL FRAMEWORK FOR CYBER-SECURITY THREATS IN SPACE MISSIONS

Abstract

Cyber-security has become a major concern when it comes to space missions due to the critical nature of the satellite networks and services they provide. Increased reliance on space systems and competition over scarce space resources will only tend to worsen the cyber risks for both satellites and the data they transmit. In addition to the importance of guaranteeing that all stakeholders involved in the chain of satellite products and services adopt the technical, procedural and governance mechanisms required to address security concerns, a more structured approach from a legal point of view may also be required – otherwise, the efforts adopted in other areas may fall short of their goals due to the gaps or barriers created by the lack of a proper legal or regulatory framework. Indeed, a legal approach may contribute to set the minimum requirements for security and to clarify the legal tools that could help avoiding and or reacting to security breaches, thus contributing to creating a more trustworthy environment to the benefit of all, including States, operators, providers and end users. Currently, however, there seems that the cybersecurity threat has not been addressed in a systematic manner by regulators. On one hand, most cybersecurity strategies do not usually address satellite networks in an autonomous manner and satellite providers are not always identified as critical infrastructure suppliers in cybersecurity laws. On the other hand, the approach to attacks to data and other unincorporated elements (such as the frequencies) is still contested. This paper addresses the above issues, including the following questions: how attacks to non-physical elements of satellite systems should be dealt with and how the Tallinn Manual could contribute to defining a proper international legal regime; how can the protection of space systems be improved through legal and policy provisions, especially if cybersecurity strategies with a focus on space should be implemented; and how can regulators and authorities cooperate at the international level, including by analysing examples of international harmonisation of laws and cross-border cooperation for investigation and enforcement purposes. Lessons from the legal and policy approaches taken in cyberspace shall be learned but a specific approach shall nevertheless be considered due to the specificities of the space environment and the space law regime. A clearer approach on cybersecurity in space from a legal perspective may contribute to achieving the overall goals of security in outer space, including the promotion of its peaceful uses.