

61st IISL COLLOQUIUM ON THE LAW OF OUTER SPACE (E7)

The relationship between space law and cyberlaw, and other recent developments in space law (5)

Author: Ms. Dimitra Stefoudi
Leiden University, The Netherlands, dstefoudi@gmail.com

THE RELEVANCE AND APPLICABILITY OF CYBERSECURITY LAWS WITH REGARD TO DATA
STORAGE ON BOARD SATELLITES AND ON THE GROUND

Abstract

Cybersecurity is a growing concern in the space sector, with satellite transmission interference and unauthorised access to data being the most common threats against space systems. This paper will focus on the latter and on the cybersecurity laws that, albeit in their infancy, aim at protecting against such risks.

In particular, this paper will assess whether the existing cybersecurity regulations are pertinent to the protection of data stored on board satellite in outer space and on the ground. It will specifically refer to the context of the EU Directive on Security of Network and Information Systems (NIS Directive), the US Internet of Things Cybersecurity Improvement Act (IoT Cybersecurity Act), and the Tallinn Manual on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0), so as to assess their connection to the current methods of data storage. Towards this end, the relevance of the said laws and their competence in ensuring an adequate level of protection against cyber threats and security breaches will be argued. On the one hand, cybersecurity regulations are designed to safeguard the integrity of data systems from external tampering. . On the other hand, it has not yet been established whether the scope of these laws extend outside the territorial sovereignty of States or in outer space, while the element of cyber operation in the framework of space activities appears in various shapes.

The purpose of this paper is to determine whether the regulatory regime in force is able to address the challenges rising from the increasing connectivity of satellites and satellite systems, which make them vulnerable against cybersecurity risks. In doing so, it will mainly focus on the notions of information system, service provider, and cyber threat within the structure of space systems.