Paper ID: 44934
oral

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. Helena Correia Mendonça
Vieira de Almeida & Associados, Portugal, hcm@vda.pt

Mrs. Magda Cocco
Vieira de Almeida & Associados, Portugal, MPC@vda.pt

THE APPLICATION OF CYBER SECURITY LAWS AND PROVISIONS TO SPACE SYSTEMS AND SERVICES

Abstract

The protection of cyberspace is a central topic worldwide, given the escalation of cyber threats and their global impacts. Policy and regulatory measures aimed at dealing with the cyber world include not only frameworks exclusively focused on cybersecurity, but also on areas that, if cyber impacted, can have strong harmful effects on society. This paper looks at the international regime applicable to Outer Space (including specifically the Space Treaties and the ITU provisions), as well as at the Tallinn Manual, to determine their impact on cybersecurity from and in outer space, including their application to cyber-attacks to satellite data and other unincorporated elements (such as frequencies). The EU regime for cyber space will be then analysed as an example of a more concrete legal framework that can be applicable to space systems and services. This analysis will cover two main topics: first, the EU cybersecurity regime, which covers a set of strategies, recommendations, legal instruments and proposals on cyber and critical infrastructures. Secondly, two central regulatory blocks closely connected with cyber: the regime for telecoms (especially the proposed Electronic Communications Code) and the regime for privacy (mainly the GDPR and the e-Privacy proposal applicable to telecom operators). All these regimes contain provisions on cybersecurity or that have an impact on security (e.g., security-by-design, privacy-by-design, notification/disclosure requirements). Hence, the paper will assess to what extent space operators are subject to the obligations arising from the international and regional/EU provisions on cyber. Compliance with the latter obligations is dependent upon several factors such as how space actors are qualified under each of the above frameworks, the type of services they provide, and where the operators, their services and resources are located (given the territorial and material scope of application of the legal frameworks). This analysis will further take into consideration the discussions had at ITU and ENISA, including with relation to IoT and OTT. The investigation undertaken aims at determining to what extent space operators shall comply with current cyber obligations and to what extent space systems may be subtracted from the application of cyber laws (e.g., in case of EU/national laws with no extraterritorial effect or if extraterritoriality does not cover outer space). The final goal is to assess whether changes or a dedicated space cybersecurity framework is required given the key role of space systems in everyday life.