66th International Astronautical Congress 2015

58th IISL COLLOQUIUM ON THE LAW OF OUTER SPACE (E7)
Interactive Presentations (IP)

Author: Ms. Iulia-Diana Galeriu
Romania, galeriudiana@yahoo.com

# ARE OPERATORS PROTECTED FORM UNAUTHOSRISED CYBER ACTIVITIES UNDER THE EXISTING SPACE LAW?

**Abstract**

The degree to which humanity has come to depend on space-related services has greatly surpassed that in 1967. With an application spanning from defense, surveillance and reconnaissance, to communications, meteorology, global broadcasting, remote sensing and navigation, space activities, and especially that of satellites have assumed a crucial role in both the public and private sector. But are these services as reliable as we trust them to be? New technological developments can also open the door to new threats. Tampering with the normal functioning of these complex systems that seem to be placed out of reach does not always require sophisticated equipment. With sufficient knowledge and off-the-shelf components, cyber attacks on space objects have become a real threat to the peaceful use of outer space. For the time being, there is no specific legal instrument that touches upon the issue of unauthorised cyber activities in outer space, which raises the question: How vulnerable are operators in the face of such a threat? Can the existing space law instruments provide sufficient protection or would a *sui generis* regime be preferred? In answering these questions, this paper will firstly set the framework by introducing the threat of unauthorised cyber activities in outer space. Afterwards, it will highlight the loopholes existing in the *corpus iuris spatialis* and International Telecommunication Union instruments in terms of defining and taking legal action against an unauthorized cyber activity. With the proliferation of private commercial space activities, a certain shift is envisaged in terms of potential victims, from States to private entities. Therefore, the obstacles that the private sector could face when dealing with a cyber attack will also be pinpointed. Finally, the paper will discuss possible approaches to these issues, such as a more efficient international policy or an insurance coverage against cyber attacks, and will end with several concluding remarks.