IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Ms. Giulia Pavesi
KU Leuven – University of Leuven, Belgium, giulia.pavesi@kuleuven.be

RECONCILING INTERNATIONAL AND EUROPEAN LAW TO ENSURE THE CYBER SECURITY OF SPACE MISSIONS

Abstract

In recent years, the spectrum of risks posed to space infrastructures has significantly expanded, both in terms of heterogeneity and of severity. Today, the safety of space systems is constantly threatened not only by environmental instability, due to upcoming large constellations, space debris proliferation and space weather interference, but also by signal interruption or disruption ascribable both to unintentional or intentional events, such as spoofing and jamming, as well as cyberattacks. This paper will exclusively focus on cyber-based security threats. Although the importance of cyber security initially emerged mainly as a technical and then policy problem, it is only in recent years that it has displayed all its criticalities from a legal perspective, both at the international and European level. While cyber dependency of space infrastructures has now been recognized by all space actors, including institutional players, national space agencies and the private sector, as a critical element in all the stages of the space supply-chain management, from the implementation to the downstream phase, such awareness has not necessarily translated into a comprehensive and coordinated regulatory response. First, this contribution will analyse the instruments provided by international law and directly addressing cyber security. In this regard, the possible implications of the agreed UN GGE reports of 2013 and 2015 for the cyber security of space infrastructures will be investigated, as well as the implications of the lack of consensus in the 2017 UN GGE report. In addition, the author will analyze and assess the effectiveness of the Open-ended Working Group (OEWG) in addressing cyber security as it relates to space. Second, with regard to the European perspective, it is a fact that in recent years the Union has increasingly acknowledged the potential spill-over effects affecting critical infrastructures and resulting from space service disruption (particularly Galileo) as a consequence of cyberattacks. In this regard, starting from the NIS Directive of 2016 and the Cybersecurity Act of 2019, this paper will address the implications and main novelties of the updated proposals of the NIS-2 Directive and the Proposal for a Directive on the resilience of critical entities, as well as on the possible opportunities presented by the 2021 Action Plan. Finally, this contribution will put forward possible mechanisms to coordinate responses among the different levels of governance in addressing cyber threats to space infrastructures, while ensuring that the interests of all the stakeholders involved, including the private sector, are represented.