Paper ID: 59367
oral

IAF SYMPOSIUM ON SPACE SECURITY (E9)
Cyber-security threats to space missions and countermeasures to address them (2.D5.4)

Author: Ms. Dimitra Stefoudi
Leiden University, The Netherlands

DO CYBERSECURITY LAWS UNDERSTAND CYBERSECURITY? - THE CASE OF THREAT AGAINST SATELLITE SYSTEMS

Abstract

The increasing reliance of space missions on cyber infrastructure along with the growing presence of cyber elements in the development of space applications are exposing space systems to greater cyber risks. Whereas satellite systems are elevated to major targets of cyber threats, space big data applications and satellite network connectivity require reliable satellite transmission and storage. Therefore, the appropriate level of preparedness against such threats is essential to the continuation and advancement of applications connected to space systems. Even though laws are in place to ensure the protection of cyber operations, their scope might not extend to cybersecurity in space activities. The existing framework, despite its attempt to regulate the evolving cyber domain, focuses on remediating the impact of cyber incidents rather than establishing protection mechanisms against cyber threats. The relevant regulations encourage post-threat cooperation in sharing information and notification of incidents, but do not outline specific measures for preventing such threats or for lack of compliance with the prescribed level of cybersecurity. Furthermore, the definitions of information networks and cyber infrastructure these regulations provide do not adequately cover space systems, which might be left outside their protective scope. Finally, the difficulty in identifying the location of the perpetrators of cyber incidents, combined with the lack of uniform standards across the different regimes, impedes the achievement of sufficient level of cybersecurity. This paper will advocate that existing cyber-related definitions do not take into account the growing convergence of satellite technology in network and information systems, hence do not provide adequate regulatory protection from threats against satellites. Its purpose is to identify the legal challenges with regard to cybersecurity in space activities and suggest methods in which existing and future regulations could approach the protection of space technology from cyber threats. Toward this end, it will elaborate on relevant national, regional and international legal documents, as well as the rights and obligations they introduce. Ultimately, it will support that attention should be shifted to security requirements prior to the occurrence of a cyber incident, since identifying and attributing a cybersecurity breach is challenging in terms of both practice and regulation. Aiming to propose an appropriate regulatory regime, the paper will highlight that the strong connection between the cyber and the space domains should form the basis of effective regulations and policy strategies.