

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. Helena Correia Mendonça
Vieira de Almeida & Associados, Portugal

Mrs. Magda Cocco
Vieira de Almeida & Associados, Portugal
Ms. Cristina Miranda
Vieira de Almeida & Associados, Portugal

CYBER LAWS AND BEST PRACTICES FOR THE SPACE SECTOR – WHAT IS MISSING AND
WHAT IS NEEDED**Abstract**

The increasing number of cyber risks and incidents, together with the rising use of satellite systems in everyday life (notably in critical functions such as in transport or communications, including in 5G enabled IoT) and the use of technologies such as AI and cloud by satellite systems, is leading to the acknowledgment that specific policies and regulatory approaches to cybersecurity in space activities are required. The UN Space Treaties do not expressly cover this topic. However, some countries, such as the UK and the USA, have approved guidelines, directives or provisions addressing cybersecurity in their space frameworks. In other cases, though, it is the regulatory framework for cybersecurity itself and for critical infrastructures that covers, directly or indirectly, the space sector. This paper examines the most recent developments in the EU on cybersecurity and space, especially the new EU Cybersecurity Strategy, the Proposal for the Revised Directive on Security of Network and Information Systems (NIS2) and the Proposal for a Directive on the Resilience of Critical Entities (CER), whilst also taking into consideration the EU Cybersecurity Act and the proposed Cyber Resilience Act. It also examines the EU Regulation establishing the space programme of the Union, notably when it comes to cybersecurity requirements, as well as the general approach to cybersecurity arising from the EU Space Strategy. The analysis addresses the main aspects of the new EU policy and legal frameworks, noting that the NIS2 and CER cover the space sector for the first time. The analysis also makes a comparative analysis between the EU approach to cybersecurity in the space sector with selected existing approaches at the national level, with a view to determine best practices and potential shortcomings of the EU approach. Taking into consideration the analysis done, the paper issues recommendations aimed at ensuring that laws at the EU level can effectively tackle the challenges of cybersecurity in the space sector, including by promoting better alignment of applicable requirements given the borderless nature of space activities and in compliance with international space law principles and rules. With a view to better guide space actors in tackling cyber challenges and compliance obligations, this paper further issues recommendations for space organisations to develop and implement a cybersecurity strategy focused on resilience, cyber incident response, awareness and capacity-building, all under the principles of prevention, reaction and monitorisation.