Paper ID: 79540
oral
student

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: Mr. Vinicius Guedes Gonçalves de Oliveira
Flinders University, Australia

CONSIDERATIONS ON AUSTRALIA'S SPACE CYBERSECURITY POLICY AND REGULATIONS

Abstract

Australia has a long history in space, being one of the initial members of the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) and one of the first to ratify all relevant international treaties. Although never asserting itself as a major space power, in recent years the country has renewed its ambitions in the sector, intending to double its space workforce and triple the size of its national space economy by 2028. In order to accomplish this goal, the government has recognised the need to cater a legal and policy framework that is able to incentive the development of new space demands while protecting its space assets against security threats. Among those, cyber threats are particularly worrisome for the country, which does not have a developed supply chain industry, and relies abundantly on COTS components. Australia also lacks a clear national space cybersecurity strategy, even though the growing risk of cyber-attacks on its space infrastructure has been already acknowledged by the government. Most of the documents that compose the Australian cyber regulatory framework are spread between different governmental branches and are limited to specific uses. Cybersecurity of the space assets is not the main focus of any of them. Building on extensive research conducted by Flinders University in cooperation with CyberOps, this paper will contribute to identify gaps in the Australian legal and policy framework regarding the cybersecurity of its space assets and propose recommendations to address them. The paper will first analyse what are the main domestic policies and legislations and the governmental bodies responsible for their creation, exploring the extant roles and responsibilities of different stakeholders. Subsequently, it will examine the interaction between the documents and identify gaps in the framework that requires to be addressed. By doing so, the paper will focus on legislation, strategic documents and policy implementation tools. Finally, recommendations on how to address such gaps will be provided. The value adding nature of this paper is that it will assist the development of the Australian space sector growth in a secure and responsible manner, providing actionable inputs to tackle the cybersecurity threats associated with space operations.