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, gued0002@flinders.edu.au

Ms. Clémence Poirier
European Space Policy Institute (ESPI), Austria, clemence.poirier@espi.or.at
Mr. Marco Aliberti
European Space Policy Institute (ESPI), Austria, marco.aliberti@espi.or.at
Prof.Dr. Rodrigo Praino
Flinders University, Australia, rodrigo.praino@flinders.edu.au
Dr. Daniel Floreani
Australia, daniel@cyberops.com.au

CYBER-SECURING AUSTRALIA'S SPACE INFRASTRUCTURE: AN ASSESSMENT OF THE POLICY AND LEGAL FRAMEWORKS

Abstract

As space assets continue to move towards the integration of more advanced information technologies, the entry points for cyber-attacks are inevitably bound to increase. Similarly, the globalization of the space supply chain, the proliferation of small satellites using COTS components and the possibility to operate space mission payloads across networks through public internet connectivity substantially increase the vulnerability of space systems to cyber-attacks. In the emergent Australia's space sector, these vulnerabilities are further exacerbated by the fact that the cybersecurity of the space infrastructure is scantly addressed at the operational and policy levels. Despite the rising efforts of the Australian Cyber Security Centre within the Signal Directorate and the Attorney-General's Department, numerous technology and policy gaps remain, including those pertaining to the definition of roles and responsibilities of the different stakeholders in case of cyber-attacks and those pertaining to policy guidance for RD and procurement activities by public bodies.

This paper will contribute to bridging these gaps by identifying cyber threats that exist within the Australian space market today, clarifying the policy and legal protection available to satellite operators in case of cyber-attack and recommending a set of security controls falling within the policy and legal dimensions. Towards this, the paper will first identify a representative set of cyber threats that Australia's space missions can be subject to throughout their lifecycle, from the manufacturing of satellite systems to their exploitation, passing through their launch and operations. The exercise will in turn enable the identification and assessment of vulnerabilities of the different space systems as well as the identification and assessment of risks associated to the identified vulnerabilities. Subsequently, the paper will complement the threat analysis with an investigation of the policy and legal frameworks that surrounds threats vectors. The paper will more specifically provide a thorough examination of the applicable policy and legal frameworks to safeguard the security of space infrastructure from cyber menaces. Particular attention will be devoted to both strategic documents (e.g., Australia's Cyber Security Strategy 2020, Defence Strategic Update 2020, International Cyber Engagement Strategy) and policy implementation tools (e.g., Australian Government Information Security Manual, Cyber Incident Management Arrangements, Cyber Cooperation Program, etc.). The project will likewise examine the extant roles and responsibilities of

different stakeholders in response to different types of incidents affecting the cybersecurity of the space infrastructure as well as the applicable legal framework. Based on the findings of this assessment, the paper will eventually identify a set of security controls to offset the identified gaps at the legal and policy level and enhance policy/legal protection available to Australian space operators. The value adding nature of this paper is that it will provide Australia's space companies and public stakeholders with actionable inputs to tackle the cybersecurity threats associated to space operations.