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

Author: Mr. PJ Blount
University of Luxembourg, Luxembourg , pjblount@gmail.com

CYBER-RISK ASSESSMENT IN THE SPACE DOMAIN: CATEGORIZING CYBER-RISK ACROSS SPACE OPERATIONS

Abstract

In the discourse over cybersecurity in the space domain, one of the oft repeated complaints is that there is a lack of industry level standardization for space operations. While this is true and development of standards and good practices at the industry level will be a significant step, this idea obscures the fact that cybersecurity is bespoke to each system. A university cubesat does not need the same level of cybersecurity as a GEO telecommunications satellite. Cybersecurity implementation for any system depends a great deal on the risks that result from a combination of technical, legal, and political factors.

Indeed, this is the stance taken by the cybersecurity community as a whole, which develops cybersecurity implementations based on risk management profiles of the IT systems employed in a particular enterprise. To this end, one of the first steps for the space industry when it comes to cybersecurity is assessing and categorizing risk categories of various space operations. This paper will do an initial analysis of the various factors that impose cyber-risk on space operations and attempt to categorize that risk for risk assessment purposes.

This paper will begin by giving a brief survey of the current discourse on cybersecurity in outer space. It will then discuss the role of risk assessments in the cybersecurity enterprise. Finally, it will develop a framework for categorizing this risk in such a way that it would be actionable for the implementation of a security concept.