54th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Edward Burger
Astrocast SA, Switzerland, edward.p.burger@gmail.com

STANDARDISED ENCRYPTION AS A HARD REQUIREMENT FOR SPACE MISSIONS' COMMUNICATIONS LICENSING?

Abstract

We are currently witnessing the development of new constellations of radically increasing sizes, while we also continue to see a high launch rate of non-constellation missions. Moreover, as a general trend we are seeing more powerful and more capable missions than even those performing similar activities from just a few years ago. The performance of propulsion systems is growing, while new propulsion methods are also in active development. And pristine, high-resolution EO, emerging SAR, and data service systems are supporting diverse space-based applications that possess high market and strategic value. And yet the myriad cyber threats to satellite missions remain, as ever, a cause for sobering concern, while the increase in the number of missions (and in the value of their data) and more capable propulsive systems only offer a wider variety of potential and increasingly severe risks to the entire sector and society more broadly.

In the face of the ever present and increasing risk of cyber threats to existing and new missions, this paper suggests that the mandatory implementation of standardised encryption techniques for space missions and their communications begins to appear as an essential next step in the evolution of national level regulatory frameworks. To investigate the necessary components and methods of implementation of such a requirement, this paper will first summarise the existing systems in place in the US (associated with NOAA and remote sensing licensing) and the UK (in the UKSA, concerning the traffic light system and the NCSC Guidance), as well as the provisions of the NIS Directive in the EU. The paper will also discuss how these represent important steps forward – in that they set the foundations towards implementing a more comprehensive global set of standard requirements – while it will likewise outline the specific directions in which they could be further developed.

Overall, the article aims to present a sketch of what a global and standardised set of requirements for the encryption of space mission communications could look like, to be implemented in national-level regulatory frameworks. The article, therefore, will consider the specific mission elements to be covered (and how), as well as propose a strategy for introducing this system with the widest possible global reach through appropriate governmental mechanisms and channels. It will lastly consider if this question should be addressed at the level of the ITU in the context of space and ground segment mission filings.