Paper ID: 50992
oral

52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Ms. Helena Correia Mendonça
Vieira de Almeida & Associados, Portugal, hcm@vda.pt

Mrs. Magda Cocco
Vieira de Almeida & Associados, Portugal, MPC@vda.pt

SECURITY-COMPLIANT CYBER MEASURES FOR SATELLITE SYSTEMS

Abstract

Satellite systems play a central role in society so much so that their disruption through cyber-attacks can have broad and serious impacts. Cybersecurity in satellite systems is therefore increasingly relevant. However, the security of satellite systems is not only dependent upon technical and operational measures independently defined by operators, but requires compliance with regulatory obligations stating who in the satellite value chain shall implement what security measures. And it so happens that the stakeholders in the space value chain may fit in in a number of regulatory classifications leading to varied security obligations under different regulatory frameworks. Indeed, the mandatory security requirements that must be met within the satellite value chain is dependent upon several factors such as how space actors are qualified under each framework, the type of services they provide, and where the operators, their services and resources are located (due to the possible territorial or extraterritorial application of regulations, all the more important given the international reach of satellites' value chain). IoT and M2M raise new challenges, together with AI, given the increasing regulatory attention paid to them including on liability, and the number of stakeholders involved. This paper analyses how satellite systems can and/or must guarantee their cybersecurity throughout the system lifecycle and the relevant value chain, also considering the different types of threats and their targets. The analysis is done in light of regulatory requirements: indeed, technical and operational cyber measures need to be derived from the applicable regulatory obligations, otherwise they risk being non-compliant. In this respect, note is taken that, in addition to specific cybersecurity, critical infrastructures' and cybercrime regimes, the frameworks for telecommunications and for personal data are central in this respect, as they also usually cover security requirements. The paper focuses on the EU regime given the recent Telecommunications Code and the GDPR and proposed E-privacy Regulation. These regimes contain provisions on cybersecurity or that have an impact on security (e.g., security-by-design, privacy-by-design, notification/disclosure requirements). A comparison with the US approach is done. The final goal is to assess and clarify how security obligations apply to satellite systems so that space stakeholders are able to define and implement cyber-compliant security measures. The paper will conclude by assessing whether new or different regulatory requirements should be set up to specifically deal with satellite systems and, if yes, how such an effort should be taken out, at the international and national levels