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

Author: Mr. Evan Meyrick
Space Generation Advisory Council (SGAC), United Kingdom

Mr. Aaron Pickard
Space Generation Advisory Council (SGAC), United States
Mr. Tobias Rahloff
Deloitte Germany, Germany
Mr. Sebastien Bonnart
Space Generation Advisory Council (SGAC), United States
Mr. Antonio Carlo
Tallinn University of Technology, Estonia
Mr. Kathiravan Thangavel
Royal Melbourne Institute of Technology (RMIT), Australia

GROUND STATION AS A SERVICE: A SPACE CYBERSECURITY ANALYSIS

Abstract

Amidst increasing digitalization of space systems, cloud computing has expanded to the space domain by providing new data processing tools to satellite operators and end-users. Cloud computing is now going further by integrating ground station systems – Ground Station as a Service (GSaaS). Established cloud service providers such as Amazon and Microsoft are now delivering services allowing satellite operators to uplink and downlink data from their own satellites and spacecraft and process it within the cloud environment.

However, this novel architecture brings cybersecurity risks and an increased attack surface, and threat actors will undoubtedly benefit from this significantly lowered cost of entry to the space environment. Also, while GSaaS brings high cost efficiency through externalization, mutualizing antenna resources comes with a compromise in independence, and opens novel attack vectors.

This paper addresses the cybersecurity tradeoffs that Ground Station as a Service represents for the space industry, both from a technical aspect and also from legal and political perspectives. After presenting the GSaaS concept, characteristics, and market leaders, this paper outlines how GSaaS is representative of the new big data driven space economy. In addition, it assesses potential cyber risks affecting confidentiality, integrity, and availability such as data breaches, advanced persistent threats, and supply chain compromise. Finally, it analyzes cyber risk management from the standpoint of data sovereignty, legal compliance, and cyber policies.

Please note that the present abstract is submitted under the auspices of the Space Generation Advisory Council, as part of the activities of the Space and Cybersecurity Project Group.