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. Marceau Brigant
Eutelsat, France

Ms. Chehineze Bouafia
Eutelsat, France

HOW ABOUT A CYBERSECURITY FRAMEWORK TAILORED TO SPACE ACTIVITIES?

Abstract

As an essential component of the modern economy, the space sector is vital to many industries, including telecommunications, navigation, and national security. States increasingly rely on commercial satellites communication providers and recent geopolitical events such as the Ukrainian-Russian war have highlighted this paradigm, with space technologies being used in all facets of the conflict. In the early hours of the Russian invasion, a combination of jamming actions and cyber-attacks affecting the Viasat's KA-SAT satellite network provoked a satellite service outage Europe with several thousand terminals disconnected. Such incidents are no longer science-fiction and are likely to reoccur, whether initiated by states or non-states entities. This calls for governments to develop enhanced legal frameworks to ensure space assets cybersecurity and resilience.

Yet, satellite operators are already subject to various regulations on cybersecurity, either at national, regional, or international level. At EU level, the NIS2 directive recognizes space as a sector of high criticality, subject to its most strict cybersecurity requirements. These regulations have been transposed into national law (French Defense Code, the German BSI Act...) with some variations. In the UK, the Telecom Security Act came into force in 2022, tightening requirements for all electronic communications service and network providers, including satellites operators. In the US, the Infrastructure Asset Pre-Approval Program (IA-Pre) is a cyber framework dedicated to commercial satellite communications operators providing services to the US military.

Although these regulations aim at guaranteeing a high level of security, only a few directly address satellites. However, the digitalization of space systems and their rather complex architecture (space segment, ground segment, link segment, user segments) create specific challenges for ensuring the physical and digital security of infrastructures.

There is a need for an enhanced and tailored cyber framework on space assets, and this research aims to discuss policy options for its implementation. Indeed, satellite operators have inherently an international coverage and ensuring compliance with cyber frameworks of different states is often complex, intrusive, costly, and sometimes includes conflicting or divergent requirements between countries. A path towards harmonized standards, such as the upcoming "EU Space Law", could be taken, at least at regional level. Governments could also conclude mutual recognition agreements on standards to link key big size markets, in the same vein as the EU General Data Protection Regulation. Finally, information sharing through common hubs of cooperation such as the EU and US Space ISAC could be beneficial.