Paper ID: 16989
student

26th SYMPOSIUM ON SPACE POLICY, REGULATIONS AND ECONOMICS (E3)
Assuring a Safe, Secure and Sustainable Space Environment for Space Activities (4)

Author: Mr. Luca del Monte
European Space Agency (ESA), France

TOWARDS A CYBER-SECURITY POLICY FOR A SUSTAINABLE, SECURE AND SAFE SPACE ENVIRONMENT

Abstract

Nearly every aspect of modern society depends upon information technology systems and networks. This interconnectivity creates vulnerabilities to cyber-threats. The space critical infrastructure is an enabler of this interconnectivity, but has now become both vehicle and target of cyber-attacks: its disruption would be critical to the whole society and would endanger commercial, institutional and defence activities. Space and Cyberspace are part of the Global Commons, physical and virtual domains that no State has sovereignty over, and that are available to everyone. Ensuring freedom and access to these areas is a key security challenge: it is likely that these commons will become an arena where political, economic and military rivalry will be played out. The issue of space security needs to be tackled in a holistic and systemic mode, through a methodology based on a strong cooperation between the public and private sectors.

In the past, 'civil' and/or 'scientific' space missions were unlikely objectives of malicious attackers, differently from military and commercial telecommunication missions that have traditionally been highly targeted. However, this view is now changing, as demonstrated by some serious security incidents which are progressively becoming publicly known.

With the objective of ensuring a safe and secure environment for its institutional missions, the European Space Agency, in consultation with the EU institutions, has started an activity supporting the potential development of a policy addressing cyber-security of space systems and encompassing the whole life-cycle of space missions including R&D, procurement, operations and decommissioning phases.

The perimeter of such policy should cover all those elements which may be targeted by ground-to-space, space-to-space or space-to-ground cyber-attacks including User segment, Space segment (satellite bus and payload, launcher on-board equipment, manned spacecraft or ISS's on-board equipment for life support and/or scientific experiments), Hosted payloads and Ground segment.

Within the scope of this activity, the addressed range of cyber-threats include highjacking/control of the spacecraft, intentional or unintentional destruction/damage of the spacecraft, signal interception, jamming, spoofing, eavesdropping, Distribute Denial of Service-type of attacks, and attack through the space mission supply chain (e.g. Trojan or latent virus).

This paper presents the preliminary results of an ESA preparatory study aiming at raising awareness in the space community about the cyber-security issue and at establishing elements of a policy allowing all stakeholders to define their own specific cyber-security requirements. This study addresses the entire spectrum of space missions falling within the remits of ESA.