48th SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

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

Mr. Stefano Zatti
ESA european space agency, Italy

PRELIMINARY REFLECTIONS ABOUT THE ESTABLISHMENT OF A CYBER-SECURITY POLICY FOR A SUSTAINABLE, SECURE AND SAFE SPACE ENVIRONMENT

Abstract

Outer space and cyberspace "together" constitute a unique technologically-created domain that is becoming a prominent locus for international strategic, political and economic power competition. However, while outer space is governed by treaty frameworks established within the UN system and by national laws, no agreed rules exist for cyberspace: it is thus needed to consider an inter-meshed governance regime able to address this specific situation, also beyond conventional legal mechanisms. Any policy development geared towards space security and cyber-security should take into account the significance of preserving open access to these two global commons whilst takling the respective relevant threats. In the initial reflections about a possible policy development some basic principles appear to be widely accepted as the fact that information sharing on threats and vulnerabilities should ultimately develop into public-private partnerships, or that any policy approach should also strongly consider the human factor as all technical elements and systems are managed by humans. However, many points still remain to be clarified such as the assessment of the nature of an incident or its attribution. In this context, practical rules to cope with imminent challenges in the two domains should be adopted at the earliest possible opportunity. This paper is based on the final results of an ESA preparatory activity encompassing two parallel studies aiming at raising awareness in the space community about the cyber-security issue. These studies address the entire spectrum of space missions falling within the remits of ESA, spanning the whole life-cycle. ESA intends to take into account the outputs and recommendations resulting from the two studies to develop technological solutions and an ESA-internal set of guidelines on cyber-security. The fields of application of these measures shall include non-technical procedures, supply chain control, computer and communications operating procedures. Already existing inter-institutional cooperation between ESA, the European Commission and the European Defence Agency could even be extended to include reflections and/or activities to enhance the cyber-security of the European institutional and commercial space missions. The on-going dialogue among the stakeholders and international partners is instrumental in raising the level of awareness about the increasingly blurring legal distinctions defining the outer space and cyberspace, and paving the way to the development of governance needed to guarantee a sustainable use of outer space in an ever more contested, congested and competitive cyber-security environment.