27th 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

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

Abstract

Once governed as separate and distinct areas by treaty frameworks established within the UN system, outer space and cyberspace are emerging nowadays as an increasingly inter-meshed governance regime also beyond conventional legal mechanisms: 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.

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. In the initial reflections about a possible policy development some basic principles appear to be widely accepted. Information sharing on threats and vulnerabilities should ultimately develop into public-private partnerships. However, many points still remain to be clarified such as the assessment of the nature of an incident, its attribution. In this context, practical rules to cope with imminent challenges in the two domains should be adopted at the earliest possible opportunity. Although rule-making in the UN is widely viewed as legitimate, it is also very difficult to achieve. An alternative approach, such as developing norms outside the UN and subsequently expanding the number of supporting countries, could be a pragmatic alternative.

This paper presents 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 address physical elements, personnel, 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.

Finally, think-tanks and respected international fora world-wide should be instrumental in facilitating the dialogue among the stakeholders and international partners, raising the level of awareness about the blurring legal distinctions defining the outer space and cyberspace, and paving the way to the development of a governance needed to guarantee a sustainable use of outer space in an ever more contested, congested and competitive cyber-security environment.