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: Mrs. Aurélie Trur
Graduate Institute for Policy Studies GRIPS Tokyo, Japan, aureliessp@gmail.com

SPACE, CYBERSPACE, AND ARTIFICIAL INTELLIGENCE (AI): WHICH GOVERNANCE MODELS FOR A SUSTAINABLE FUTURE?

Abstract

Just last year in 2022, new artificial intelligence (AI) tools and growing instances of cyberattacks have highlighted their disruptive potential towards sustainable space activities and international stability and remind of the height of the Cold War. Cyber technologies literally affect everyone from nations to commercial entities, to all the citizen of the world, thus calling for debates at the highest international political levels. Starting as far back as 1998, discussions about cybersecurity threats to space activities under the United Nations are not exactly new. Since 2018, the debate gained momentum with the Space 2030 Agenda debate, the proposal for an agenda-item under the Legal Subcommittee of the UN Committee for the Peaceful Uses of Outer Space (COPUOS), and Groups of Governmental Experts initiatives leading to developments such as the Long-Term Sustainability Guideline number 18 covering cyberthreats, or the GGE on Advancing responsible State behavior in cyberspace in the context of international security (GGE-Cyber), a parallel debate to outer space discussions. The rapid pace of these technological changes and the magnitude of the threats affecting everyone demands a serious rethinking of governance mechanisms at the nexus of space and cyberspace domains, to maintain a sustainable future for space operations and international stability. Can norms help fill current governance gaps? Could an advisory body reporting to COPUOS be devised as a platform supporting the emerging normative progress as was the case for debris mitigation efforts? How to consolidate and institutionalize the emerging cyber norms involving both states and non-state actors in the debates? Could additional UN-led cyber initiatives such as Open-Ended Working Groups (OEWG) lead to the emergence of a new permanent body in the form of a Committee for the Peaceful Uses of Cyber Space (COPUCS) considering cyberspace as its own domain? This article explores the current regimes addressing space and cyber threats and looks for lessons to be learned from debris governance, early space governance and arms control efforts, as well as other cyberspace governance initiatives at the international level including the United Nations' system.