8 June 2021

English only

Committee on the Peaceful Uses of Outer Space
Legal Subcommittee
Sixtieth session
Vienna, 31 May–11 June 2021
Item 15 of the provisional agenda*
Proposals to the Committee on the Peaceful Uses of Outer Space for new items to be considered by the Legal Subcommittee at its sixty-first session

The proposal of the Ukrainian delegation on the establishment of a new item on the agenda of the Legal Subcommittee on the cybersecurity of space activities

Submission by the delegation of Ukraine

I. Legal background

The Committee on the Peaceful Uses of Outer Space in the Report "Space2030" agenda and the global governance of outer space activities (A/AC.105/1166)[1] stated that owing to the critical importance of space-based infrastructure and its direct relevance for resilient societies, the protection of space assets, space systems and ground infrastructure, including related critical infrastructure, should be a matter of international discussions. The consideration of critical space infrastructure at the international level, including with a view of studying cyber-security issues related to space activities, should be initiated at the level of the Committee on the Peaceful Uses of Outer Space. This idea was recalled within UNISPACE+50 at the UNGA event "Space2030: Space as a driver for peace", namely, consideration of critical space infrastructure at the international level, including cybersecurity issues related to space activities was recognized as a new agenda items that could be considered[2].

There are a lot of international documents devoted to setting legal models for responsible behaviour in cyberspace. Under the auspices of the United Nations General Assembly were prepared the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 July 2015)[3], Resolution 73/27 on 5 December 2018 on the report of the First Committee (A/73/505) - Developments in the field of

* A/AC.105/C.2/L.317.
[1] https://www.unoosa.org/oosa/oosadoc/data/documents/2018/aac.105/aac.1051166_0.html
[2] https://www.unoosa.org/oosa/en/aboutus/director/director-statements/2018/director-speech-2018-permanent-missions-briefing.html
[3] https://undocs.org/A/70/174

information and telecommunications in the context of international security[4], Resolution 73/266 on 22 December 2018 on the report of the First Committee (A/73/505) - Advancing responsible State behaviour in cyberspace in the context of international security[5], Resolution 75/240 established an Open-ended Working Group on the security of and in the use of information and communications technologies 2021-2025[6].

Besides the UN, there are more than 20 international organizations, intergovernmental and nongovernmental arrangements that focuses also on cybersecurity and as a particular the cybersecurity of space activities. For instance, ITU promotes cybersecurity through the Cyber Security Index initiative, the Council of Europe elaborated Convention on Cybercrime, Working Group 3 (WG3) of ISO/TC20/SC14 develop and maintain space system standards in the following areas: cyber protection and cybersecurity[7], representatives of academia prepared Tallinn Manual which covers an overview of the application of treaties governing States' use of outer space. On this ground, some States recognize the necessity to elaborate or have elaborated national policy and legislation, concerning cybersecurity of space activity.

II. Cyber threats and their consequences for sustainable space activities

The need to provide the resilience of space systems to cyber threats is growing exponentially due to the increase of their reliance on information systems and networks from design conceptualization through launch and flight operations. Unauthorized interruption into the transmission of command and control, signals, or information between space vehicles and ground networks can deny, degrade, and disrupt space activity. The malicious cyber activities, like jamming or sending unauthorized commands, spoofing sensor data; corrupting sensor systems; injecting malicious code, and conducting denial-of-service attacks, pose a comprehensive danger to space systems comprises to four segments: space, ground, link, and user.

There are some examples of the cyber-attacks on the space technologies: in 1998, the German-US ROSAT space telescope inexplicably turned towards the Sun, irreversibly damaging a critical optical sensor, following a cyber intrusion at the Goddard Space Flight Center of NASA in the US; on October 20, 2007, and on July 23, 2008, Landsat 7 experienced 12 or more minutes of interference; 2015 - alleged interference with Globalstar's asset-tracking systems, etc.

Cyber threats capable to aggravate the several issues that cover by the Legal Subcommittee agenda items, i.e. space debris proliferation, space traffic management. Without taking into consideration possibilities of unauthorized access to space objects at least the liability for damage due to fault and identification of State of control may be accompanied by omissions and errors that can cause irreparable damage to capacity-building and long-term sustainability of space activities. Thus, cyber threats to space activities are a mature and acute problem that not limited by technical issues and goes beyond the mandate of the Scientific and Technical Subcommittee. It deserves detailed consideration of the Legal Subcommittee at least through the prism of the issues of control of space object, identification of liable State, transparency and capacity-building mechanisms.

This is the evidence of the maturity of the issue of ensuring the cybersecurity of space activities and the necessity to study relevant legal aspects under the auspice of the Legal Subcommittee of the COPUOS.

[4] A/RES/73/27 - E - A/RES/73/27 -Desktop (undocs.org)
[5] A/RES/73/266 - E - A/RES/73/266 -Desktop (undocs.org)
[6] https://undocs.org/pdf?symbol=en/A/RES/75/240
[7] https://www.unoosa.org/res/oosadoc/data/documents/2020/aac_105c_1/aac_105c_1118_0_html/V2006834.pdf

III. Provisional workplan

First stage

To collect policies, principles, rules, and best practices of States concerning ensuring the cybersecurity of space activities from design conceptualization through launch and flight operations and cooperation and coordination due regard in the cases of detection the malicious cyber activities concerning their space systems.

Second stage

Preparing the materials (compendium, guidelines, etc.) and spreading them among States as recommendations for formulating common approaches in managing cybersecurity threats to space activities.

Nataliia Malysheva

Anna Hurova