Paper ID: 90818
oral
student

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: Ms. Niki Giannakou
National and Kapodistrian University Of Athens, Greece

Prof. George (Georgios) D. Kyriakopoulos
National and Kapodistrian University Of Athens, Greece

THE ENVIRONMENTAL IMPLICATIONS OF CYBER ATTACKS ON SATELLITES: ISSUES UNDER THE OUTER SPACE TREATY AND GENERAL INTERNATIONAL LAW

Abstract

At present, space economy heavily relies on the operation of satellites in the Geostationary and Low-Earth orbits mainly by private entities. At the same time, satellite-based services are critical inter alia for telecommunications, Space Situational Awareness services, Wi-Fi services and remote sensing. Especially satellites with environmental monitoring applications are pivotal in terms of environmental protection and preservation on earth. Furthermore, the increased congestion of earth orbits with space debris and mega-constellations of thousands of satellites intensifies the risk of possible collisions and further debris contamination in case of satellite jamming.

Cyber-attacks against satellites can involve - but are not limited to - satellite control, satellite communications terminal hacking, and GPS spoofing. Such attacks are nowadays capable of generating large-scale environmental contamination, which is prohibited under Article IX of the Outer Space Treaty. For instance, a typical example of back contamination on earth might be caused by a cyber-attack against a satellite that provides navigation services for vessels at sea, which could in turn cause a marine accident and hence a catastrophic oil spill at sea. Another possible scenario of forth contamination in outer space could be a cyber-attack against a satellite used to provide SSA data for purposes of collision avoidance maneuvers. In such case, a collision among space objects in the already highly congested earth's orbits could generate millions of new space debris deteriorating even more the environmental contamination of the orbits.

n general, given that satellites are now in many cases providing support services to critical ground-based infrastructures, there is a serious possibility that a cyber-attack on the satellite could result in a significant disruption to the operation of such infrastructures. Examples of this have already been given above. Even if this damage is secondary or even tertiary in relation to the cyber-attack, it could still be attributed to the latter in terms of causality. This issue may become even more serious in the context of an armed conflict, in which the relevant provisions on the protection of the environment under international humanitarian law should be considered applicable, in accordance with Article III OST.

In this sense, the purpose of this paper is to examine the overall landscape of the environmental consequences of cyber-attacks against satellites within the entire available international legal framework, i.e. both under the Outer Space Treaty (lex specialis) and under general international law, international environmental law and the law of armed conflict (lex generalis).