Paper ID: 65586
oral

IAF SYMPOSIUM ON SPACE SECURITY (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Prof. Andrea Harrington
Air University, United States

LEGAL FRAMEWORK FOR DAMAGE CAUSED TO SPACE OBJECTS BY CYBER ATTACKS

Abstract

When are cyber activities also space activities? To answer that question, it is necessary to consider the relevant language contained in the space treaty regime, including the Outer Space Treaty, the Registration Convention, and the Liability Convention. This paper contends that cyber activities do not rise to the level of space activities unless they involve the use of a space object that has been launched into space. Thus, cyber attacks against space objects using only ground-based assets would not be treated as "space activities" for the purposes of international space law.

Additionally, it is unreasonable to hold a State to the same level of responsibility for cyber actors as space actors under Article VI of the Outer Space Treaty. Cyber actors can operate clandestinely and anonymously with only a computer and an internet connection, while space activities inherently involve launches of objects into space which can be easily monitored even by amateur observers. However, if an entity were to use its own space-based assets to conduct a cyber-attack on another space object, it would rise to the level of a national (space) activity under Article VI of the OST, but may or may not cause damage to the second space object within the meaning of the Liability Convention. Even if damage is not caused under the definition presented in the Liability Convention, it may be possible to seek reparation under the Outer Space Treaty or general international law. This paper will analyze when State responsibility may be applicable to such cyber activities in these regimes. This analysis will help to identify gaps in the regime where further development is needed to safeguard space assets.

Finally, this paper argues that States have a higher level of responsibility under the space treaty regime to safeguard the command and control, particularly maneuvering, capabilities of the space objects they launch against cyber threats. While stealing, jamming, or spoofing the transfer of data can cause myriad problems, the maneuvering capabilities of satellites enable satellites to be used to interfere with other States' space objects and/or to cause damage to them within the meaning of the treaties. Thus, for a State to act responsibly under Article VI and with due regard under Article IX, and to avoid incurring liability under the Liability Convention due to fault in failing to protect such capabilities, States must use due diligence in protecting access to satellite maneuvering capability.