Paper ID: 67116
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: Ms. Deborah Housen-Couriel
Israel, deb.hc@konfidas.com

INFORMATION SHARING FOR THE MITIGATION OF OUTER SPACE-RELATED CYBERSECURITY THREATS

Abstract

The growing realization on the part of lawmakers, policy experts and practitioners that cyber risks and cyber threat vectors have become a critical issue for all outer space operations requires all of these stakeholders to focus professional attention and resources on mitigating these risks and threats. Vulnerabilities in (for example) space-to-space, earth-to-space and space-to-earth communications; in satellite telemetry, tracking, and control (TTC); and other aspects of space operations arise because of the inevitable dependency of space-based activities on computer systems and wireless communications, which constitute key elements of cyberspace both on earth and in space. Additional cyber vulnerabilities are present in the terrestrial systems supporting space operations, including supply chains for dedicated equipment and services. The mitigation of cyber threats and vulnerabilities in the more traditional terrestrial context is a rapidly-developing area, as it works to meet the challenges posed by malicious actors whether they are cyber criminals, nation-states or hostile groups motivated by ideology. While the threat mitigation aspects of cybersecurity have by no means been resolved - hostile actors use increasingly sophisticated means to achieve their ends - there has been robust progress with respect to several measures and best practices that are recognized as critical to boosting cybersecurity. This presentation focuses on one of these: information sharing (IS) among trusted participants in a secure platform designed for the sharing of actionable cybersecurity data.A primary goal of IS is to reduce the informational asymmetry between the cyber attacker and the targeted entity, whether the latter is a state, a private company, or some other entity. Attackers leverage their knowledge of the the target's vulnerabilities, and they only need to be right on one occasion in order to cause damage that may be financial, operational and/or reputational, and that in some cases may impair the long-term functionality of an organization. Yet when a group of potential targets can pool the information that each has gathered separately through IS, the informational asymmetry is narrowed and cybersecurity improved. There are a number of conditions for optimizing IS, such as establishing trusted IS methodologies, which will be further detailed in this paper.Finally,in the context of outer space-related cybersecurity threats, the paper will argue that information sharing is crucial because of two elements: the aggravated asymmetry of cyber threat vectors in space; and their distinctive space-related characteristics A model IS platform for mitigating space-related cyber threats will be proposed in the paper.