IAF SYMPOSIUM ON SPACE SECURITY (E9)
Cyber-security threats to space missions and countermeasures to address them (2.D5.4)

Author: Mr. Hamza Hameed
Unidroit, Italy, h.hameed@unidroit.org

Ms. Nadia Khan
University College London (UCL), United Kingdom, nadia.r.khan@live.com

THE NEED FOR MULTILATERAL CYBERSECURITY SPACE REFORMS TO MITIGATE THE RISKS POSED BY CYBERSECURITY THREATS AND VULNERABILITIES IN LOWER EARTH ORBIT.

Abstract

The NewSpace era is being defined by companies working towards establishing mega satellite constellations in lower Earth orbit to become providers of low-cost easy access high-speed 5G broadband, and other services. The arrival of these services not only bolsters connectivity, but also increases peoples dependence upon global systems of space enabled communication and infrastructure. Many companies are competing in these areas, which has meant that they have adopted cost-efficient measures at every level of their product development supply chain to ensure that their satellite constellations reach lower Earth orbit at the fastest possible speed, and lowest possible cost, to meet market demands. The lack of regulation around satellite manufacturing and a lack of international standards poses a real threat to this industry and to the States involved in it.

A reliance on satellites developed without enhanced regulations and standards increases the risk of communication failures and disruptions, particularly through cyberattacks involving satellite spoofing and jamming. Satellite hacking is not a new phenomenon, and can have a large impact on the industry. Several reports published by governments detail incidents of hacking involving critical State related satellites, and outline the risk that cyberattacks pose to the efficacy of space enabled services and critical infrastructure. Such reports illustrate how mission critical satellites are vulnerable to cybersecurity threats. Presently, international space law through the Outer Space Treaty largely regulates the traditional weaponization of space, rather than giving proper consideration to cyberwarfare. This causes uncertainty and requires additional clarification.

Besides highlighting how a lack of cybersecurity standards and regulations for small satellites in the NewSpace era poses a threat to the national security of space faring nations, as well as to the entire industry, this paper will examine the steps which States may take to mitigate and manage cybersecurity in space. The paper will consider existing legislation on cybersecurity and will provide recommendations for multilateral reform which could be considered to improve cybersecurity standards across the entire industry.

Additionally, this paper will provide a risk model which show cases how commercial space companies have a greater disposition to cybersecurity threats as a result of their cost-effective, high-speed production and launch of small satellites. The model will provide a forecast which policymakers and legislators may utilise when developing legislation around cybersecurity and threat mitigation in outer space.