55th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Interactive Presentations - 55th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (IPB)

Author: Mr. Charles Mudd
Mudd Law, United States

Mrs. Svetlana Hanson
NASA, United States

CYBERSECURITY AND SPACE: ENSURING A SECURE SPACE AT THE OPERATIONAL SYSTEM LEVEL

Abstract

The future of secure space activity must begin at the operational level by ensuring systematic protection against cyber-attacks. To effectuate this, the space sector must increase awareness, adopt "security-by-design," increase regulatory support, implement data security principles, and cooperate domestically and internationally. Given the growth in commercial space and satellite activity, the space sector has become even more vulnerable to cyber-attack.

At the origin of computer networking, the corollary risk of network intrusion began. Given the prevalence of Internet use among the developed world, concerns about computer intrusions and hackers may be apparent to many in the general population. Within the technology sector, a more acute risk awareness and understanding exists. And, although intuitively it would be reasonable to expect those in the space sector to share this heightened perspective, reason does not always prevail. The absence of effective cybersecurity standards within the space and satellite sector reflect this disconnect. And yet, the risk of computer intrusions within the space sector and the potential harm to space operations could not be more pronounced.

From both state and non-state actors, space operations serve an attractive target for cyber attacks. At an exploratory level, the intruder intent could be limited to traversing computer systems without any clear objective. At an informational level, the intruders (whether human or bot) might be focused on the acquisition of specific documents, knowledge, or state or trade secrets. However, certain documents could clearly lead to more menacing objectives. Beyond the foregoing, more nefarious players could seek to threaten operations on the International Space Station, disrupt human spaceflight, redirect satellites, or worse. In fact, akin to ransomware, these criminal operators could hold returned normality ransom in exchange for demands.

To avoid or (at a minimum) minimize opportunities for intrusions, there is a need for awareness among and within the space industry, policy makers, and regulators.

This paper and presentation will define space cybersecurity concerns and provide proposals for increased awareness. The paper will also provide an overview of cybersecurity efforts in the United States and internationally. We will propose specific principles directly related to the space sector as well as emphasize on the need for communication and cooperation across governments, commercial operators, and other NGOs.