Paper ID: 83839
oral

IISL COLLOQUIUM ON THE LAW OF OUTER SPACE (E7)
Artificial Intelligence and Safe Space Communication (3)

Author: Ms. Elina Morozova
Intersputnik International Organization of Space Communications, Russian Federation

MITIGATING CYBERTHREATS TO SPACE COMMUNICATION SYSTEMS: OPERATORS, USERS AND REGULATORS PERSPECTIVES

Abstract

The significant role of space communication systems in everyday life on Earth, including for critical space applications and commercial gain, makes such systems a target as a matter of when, not if. In any space communication system, it is customary to distinguish several segments, in particular space, ground, link and user. Obviously, attacking ground infrastructure is easier than attacking spacecraft.

Cyberattacks are often used to interfere with space communications: complex supply chains and layers of stakeholders with different cybersecurity standards open up many opportunities for intrusion. Cyber equipment is available at a relatively low cost, while the use of traditional hardware and software in space communication systems is familiar to attackers. Cyberattacks can achieve a variety of malicious results, from causing non-destructive and reversible damage to damage comparable to that of a powerful physical attack. Common ones include stealing, deleting and altering data, disabling operations temporarily or permanently, and even hijacking control over a spacecraft. Cyberattacks are difficult to detect and investigate, and even more difficult to attribute. Thus, they allow achieving a malicious goal with relatively little effort and without being held accountable.

The changing landscape of space communications exacerbates cyberthreats. These are, first of all, technological and operational aspects, such as the transition to a new architecture of space systems with a preference for satellite constellations, mass production, miniaturization, simplification and digitalization of space technology, and strengthening its integration into terrestrial applications. Market conditions are also changing: the number of space players and competition in the space industry is growing, forcing manufacturers of space technology and communications equipment to give preference to speeding up production and reducing costs. The lack of cybersecurity standards internationally and nationally means that cybersecurity often falls on the shoulders of private entities. Some may have limited budgets and even less expertise in countering cyberthreats and make trade-offs that affect the vulnerability of space systems.

This article will highlight the perspectives of operators, users and regulators on mitigating cyberthreats to space communication systems, and recall the key role of Article VI of the Outer Space Treaty, which allows states to introduce necessary and sufficient cybersecurity requirements into the licensing of national space activities.