Paper ID: 45099
oral

51st IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Dr. Jana Robinson
The Prague Security Studies Institute, Czech Republic, jrobinson@pssi.cz

Mr. Jakub Pražák
The Prague Security Studies Institute, Czech Republic, prazak@pssi.cz
Ms. Lisa Perrichon
The Prague Security Studies Institute, Czech Republic, perrichon@pssi.cz
Dr. Martina Šmuclerová
The Prague Security Studies Institute, Czech Republic, smuclerova@pssi.cz

EUROPE'S MANAGEMENT OF UNCONVENTIONAL THREATS TO SPACE OPERATIONS

Abstract

Space-based services are now fundamental to the functioning of European societies. The disruption of space assets and the services they provide would almost surely cripple several key aspects of our day-to-day lives. Threats to space operations could result in the compromising of satellites, ground stations or links and trigger a cascading effect. Military systems represent the most obvious targets, but civil and commercial satellites offer many critical support functions for allied security communities (e.g. communications and reconnaissance), making them vulnerable to attacks as well.

Naturally, a number of safeguards and processes have been adopted in an effort to ensure the safety and resilience of these systems. Traditionally, however, the security architecture for civil and commercial space systems focused largely on mitigating risks related to the space environment and technical glitches.

While these remain valid concerns, the prospect of purposeful disruptions requires rather urgent attention and contingency planning, namely new unconventional (or hybrid) threats posed by certain spacefaring nations. These types of counterspace threats are designed to remain just below the threshold of requiring a meaningful retaliatory response and can span the security, civil, and commercial sectors.

Unconventional operations are being readied and, in some cases, deployed by Europe's competitors to project power, control, and influence in a manner designed to advance their strategic military, political and industrial objectives. While such practices are nothing new in other domains, the potential impact and knock-on effects of hybrid threats to space – including on the resilience of critical infrastructure (CI) – are less understood. Worst still, the formulation of political, and even military, responses to this new class of threats are inadequately developed in Europe.

This paper would first review the policy framework adopted to date at the Europe-wide level with regard to critical infrastructure protection and broader space security concerns. It would then assess the current level of preparedness to address space hybrid threats, both nationally and multilaterally. It would conclude with proposed measures to strengthen space crisis management architectures with regard to "grey zone" environments with imperfect attribution, including enhanced transatlantic intelligence-sharing and situational awareness as it pertains to counterspace threats.