Paper ID: 99877
student

IAF SPACE OPERATIONS SYMPOSIUM (B6)
Ground Operations - Systems and Solutions (1)

Author: Ms. Mehriban Karimova
Azerbaijan State University of Economics, Azerbaijan

Mr. Elmar Bashirov
Azerbaijan State University of Economics, Azerbaijan
Mr. Khayyam Masiyev
Baku Higher Oil School, Azerbaijan

CHALLENGES, THREATS, AND SOLUTIONS IN ENHANCING CYBERSECURITY IN SPACE MISSION GROUND OPERATIONS

Abstract

The high complexity of space missions has placed significant demands on ground operations, requiring new, efficient, and secure systems for both preparation and execution. As ground systems manage mission-critical tasks such as spacecraft tracking, telemetry, and data processing, they have become prime targets for cyber threats. While advancements in the digital realm have enabled new capabilities, they have also introduced vulnerabilities exploited by malicious actors. The increasing reliance on digital infrastructure, cloud-based mission control, and inter-agency collaborations further expands the attack surface. Addressing these challenges is vital to ensuring the integrity, availability, and operability of ground operations. This research explores security challenges in modern ground operations, analyzes potential threats to mission-critical infrastructure, and proposes innovative solutions to enhance system resilience. Specifically, it examines cyber threats such as GNSS spoofing, data corruption, and network intrusions that could compromise mission execution. By evaluating existing security measures and identifying gaps, this study seeks to develop a framework for strengthening ground operations against evolving threats. A comprehensive approach is used to assess the security landscape. First, an extensive literature review is conducted, drawing from case studies involving organizations such as EUMETSAT, CNES, and NASA. Real-world cyber incidents targeting space operations are analyzed to identify common attack vectors and vulnerabilities. Additionally, network simulations and penetration testing are employed to evaluate system resilience under simulated attack conditions. Finally, a comparative analysis of cybersecurity best practices in aerospace and defense industries is performed to recommend mitigation strategies. Findings indicate that while ground operations employ sophisticated security measures, gaps remain in areas such as real-time threat detection, automated response mechanisms, and international collaboration. Emerging technologies such as AI-driven anomaly detection, quantum-resistant encryption, and resilient network architectures offer promising solutions, but their implementation requires coordinated efforts among governmental agencies, commercial operators, and research institutions. To ensure secure and efficient ground operations, a proactive cybersecurity approach is necessary. By integrating advanced security frameworks and fostering international cooperation, space agencies can safeguard mission-critical infrastructure against evolving threats. This research highlights the urgency of addressing cybersecurity in space operations and provides actionable recommendations to enhance system resilience.