56th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Nijanthan Vasudevan
Drexel University, United States, nijanthan.vasudevan@spacegeneration.org

Ms. Alex Thach
University of Maryland, United States, alex.thach3@gmail.com
Ms. Cassandra Paoli
United States, cassie.paoli89@gmail.com

DEVELOPING AN AI-ENABLED CYBERSECURITY MODEL TO PROTECT SATELLITE SYSTEMS FROM CYBER THREATS

Abstract

Satellite cybersecurity was shown by the 2019 Galileo attack. Due to the rise in cyber risks and attacks caused by connected devices and the internet of things (IoT), advanced cybersecurity models that can detect and respond to threats in real time are needed. AI can improve cybersecurity by enabling real-time cyberattack detection and response. This paper presents an AI-enabled satellite cybersecurity model to prevent hacks like the 2019 Galileo attack. Using satellite telemetry data, a deep learning algorithm detects satellite system behavior patterns and abnormalities. The application can detect and classify cyber threats such unauthorized access, malware infestations, and data manipulation and notify system operators in real time. Host and network-based intrusion detection systems may monitor satellite network endpoints. AI-based intrusion detection, firewalls, and endpoint security prevent cyberattacks. The firewall prevents unauthorized access, and the intrusion detection system monitors satellite network traffic for suspicious activities. Endpoint security can protect satellite system equipment and apps against malware and other cyberattacks. Vulnerability and patch management may update malware signatures daily. The simulation proved that the AI-enabled model can identify and react to cyber threats in real time, decreasing attack risk. Like Azure Sentinel, our AI will identify new threats, tactics, and mitigations. Integrating AI-based intrusion detection systems with satellite system telemetry data processing systems is recommended. New cyberthreats need model monitoring and updating. AI will enable cyberattacks as it improves. Reinforcement learning modifies AI-based intrusion detection. This paper presents an AI-enabled cybersecurity paradigm for satellites, spacecraft, and ground control stations. The technique may improve system security and resilience, reduce cyber-attack risk, and protect critical infrastructure. In conclusion, this study proposes a satellite cybersecurity paradigm with AI help that can detect and respond to cyberattacks in real time. Firewalls, endpoint security, and AI-based IDSs block cyberattacks. The strategy may improve satellite system security and resilience and prevent damage to critical infrastructure. Further study may combine the model with other space systems and construct cybersecurity models for AI-powered critical infrastructures. Threat intelligence, network segmentation, and cloud security may be covered.

Keywords: Cybersecurity, AI Model, Threat intelligence, network segmentation