57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Nick Tsamis
The MITRE Corporation, United States, ntsamis@mitre.org

Mr. Harvey Reed
The MITRE Corporation, United States, hreed@mitre.org
Dr. Ruth Stilwell
Aerospace Policy Solutions, LLC, United States, office@aerospacepolicysolutions.com
Dr. Nathaniel Dailey
The MITRE Corporation, United States, ndailey@mitre.org

THE ROLE OF LOCALIZED COMMUNITIES OF INTEREST IN STANDARDIZING COORDINATED RESPONSES TO SPACE CYBERSECURITY THREATS

Abstract

This paper explores the development of a local communities of interest (COI) cybersecurity standardization approach for the space domain that focuses on cyber resilience within and across COIs. The authors propose a paradigm shift from individual responsibility to respond to cybersecurity threats to a collaborative information sharing based approach to address common cybersecurity needs. This approach examines the space domain through a "neighborhood norms" (COI-centric agreement to normal behavior), cybersecurity-centric lens.

Here, COIs refer to stakeholders unified by common cybersecurity challenges and objectives across common operations performed within the space environment, e.g., Space Traffic Management (STM). For example, a community associated with providing Space Situational Awareness (SSA) to support STM may share intelligence on cyber threats and collaborate on countermeasures specific to SSA operations.

This approach aligns with USSF "Partner-to-Win" strategy, emphasizing strategic partnerships for enhanced cyber defense within the space domain. The COI model fosters a multi-entity approach to space cybersecurity, sharing the burden of responsibility for threat detection and response. Further, the approach enables optimized, community-specific solutions ensuring cybersecurity concerns are accounted for and addressed across affected community participants, ensuring the magnitude of data and number of parties with access are operationally relevant.

The paper will outline how these communities can categorize and align around foundational cybersecurity challenges, enabling stakeholders with common goals to address shared threats. It will also introduce the role of decentralized technical capabilities to facilitate the secure information sharing infrastructure necessary to build trust within and across these communities. This paper further posits that equipping COIs with decentralized technical capabilities provide a means to securely manage responses to cybersecurity threats against complex space operations (e.g. STM). This enables COIs to maintain data and workflow integrity and execute consistent and traceable actions using community-developed response playbooks.

COIs using this decentralized infrastructure are empowered by efficient information sharing, including coordinated threat intelligence. This in turn allows for coordinated mitigation of impacts arising from in-progress cyber-attacks. The decentralized infrastructure facilitates information sharing using a Minimum-Viable Information (MVI) approach to increase the probability and utility of information being sharing within and across COIs.

Sharing MVI sets allows individual members within localized COIs group to take informed and practical actions to secure their assets and contribute to the overall resilience of community needs. This coordinated defense approach promotes new normal behaviors across individual stakeholders in response to cyber incidents, resulting in space domain security through community vigilance and response.