IAF SYMPOSIUM ON SECURITY, STABILITY AND SUSTAINABILITY OF SPACE ACTIVITIES (E9)
Cyber-based security threats to space missions: establishing the legal, institutional and collaborative framework to counteract them (2)

Author: Dr. Bruce Chesley
Teaching Science and Technology, Inc (TSTI), United States, bruce.c.chesley@gmail.com

Dr. Jerry Sellers
Teaching Science and Technology, Inc., United States, jerry.sellers@mac.com
Ms. Terri Johnson
United States, terri.akse@gmail.com

THE SPACE DOMAIN CYBER-SECURITY (SPADOCS) FRAMEWORK: A PROCESS FRAMEWORK TO ORGANIZE, UNDERSTAND AND EDUCATE

Abstract

The space and cyber domains have developed in parallel over the past several decades. The two domains evolved separately and have employed different architectural frameworks to guide their evolution. An example of this difference is the fact that space systems typically maintain distinct command and control networks that operate separately from mission data communications. Computer and cyber systems typically do not maintain separate networks. Establishing best practices for cyber protections and collaboration across space enterprises requires collaboration across the different architecture frameworks, terminologies and even cultures. We introduce the Space Domain Cyber Security (SPADOCS) framework to bridge the space and cyber domains with the goal of enhancing collaboration and information sharing across mission, company, international and government boundaries.

This paper describes the SPADOCS, beginning with the attack and defend value chains, summarizing the threat objectives and protection challenges. We then outline the aspects of the space domain that present challenges for cybersecurity, including a mentality that "It can't happen here"; inflexible, slow-changing (non-Agile) culture; hardware and software systems that were historically isolated from the internet; complacency (lack of a cybersecurity culture in civilian space); security requirements identified too late in the software development lifecycle; and patching and upgrading existing systems is difficult and expensive (and some cases impossible) with deployed space systems.

We then focus on the practical issues of developing and sustaining a secure cyber environment through all phases of the space mission lifecycle. We describe the SPADOCS framework to provide a comprehensive and systematic model for understanding and tackling all critical issues of cybersecurity in the space domain. An examination of the Key Objectives—confidentiality, integrity, availability—provides the foundation for the framework. From there, the space domain is examined layer by layer starting from the enterprise layer, then drilling down through mission, system and DevSecOps layers. Threats and vulnerabilities at each layer are highlighted. Finally, first principles of cybersecurity are discussed (domain separation, process isolation, and others) as well as key enablers (such as vision and strategy) to help frame plans for action to address the cybersecurity.

We conclude with a discussion of the SPADOCS framework as an element for increasing communication and collaboration to prepare for and respond to vulnerabilities, incidents, and threats. We describe our next steps include educating industry and government through organizations like the Space Information Sharing and Analysis Center to strengthen space mission performance through threat indicators, threat assessments and indicators.