49th 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. David Finkleman
International Academy of Astronautics, United States, dfinkleman@comcast.net

SHARING SPACE DATA BY DESIGN

Abstract

This paper describes structural models for space situational data pools based on successes in other disciplines. The International Organization for Standardization has created an environment for sharing orbit data through standard formats and content. Policy, legal, and data structural issues still impede sharing data that is essential for sustaining the space environment and managing orbital traffic. Ostrom's seminal concepts for governance of common pool resources has been extended to knowledge commons. Congress and Reichman suggest a spectrum of data pool architecture: fully centralized, intermediate distributed, fully distributed, and noncommons. Space data has inadvertently adopted the intermediate regime in which repositories are maintained separately but interconnected with shared service components and a common data exchange formats. Centralized paradigms suffer distrust and competition for centralized responsibility. Noncommons architectures lack common exchange formats and incur difficult interoperability and exchange across nations. Fully distributed architecture is most recommended in disciplines other than space. This paper will examine Willbanks models of informed consent and privacy protection developed to facilitate exchange of data subject to legal regulation and proprietary protection. Congress and Reichman suggest fundamental considerations that apply well to sharing space data:

How many repositories should there be? Is a common data portal feasible? Are data regulated or otherwise protected in participating jurisdictions?

Space data sources are public, private, and governmental. Data within the public domain might be produced by universities and research institutions. Private data might be produced by privately owned and operated instruments and organizations that operate satellites. Governmental data might include secure military information and data from civil satellite operations. There is currently no concept for managing or accessing what should be commons. This paper will suggest ways to overcome this diversity. It will begin with analysis of existing capabilities: the Space Data Center, Celestrak, and the USAF Space Track website. The SDC contains proprietary data from mainly Comsat operators. Celestrak adds value to openly available governmental data. Space Track owns data from government sensors and distributes a carefully selected fraction of its catalog. This diversity is unacceptable in the future.

The wealth of critical space object and orbit data required to manage and sustain a productive and safe near Earth space environment must be organized and shared according to a profound architecture. This paper might be the first foray into an optimal distributed architecture.