52nd 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: Mr. Samuel Visner
The MITRE Corporation, United States, svisner@mitre.org

Dr. Scott Kordella
The MITRE Corporation, United States, kordella@mitre.org

CYBER PROTECTION BEST PRACTICES FOR SMALL SATELLITES

Abstract

Securing our national and economic security is urgent, especially as LEO space is exploited in new ways. Private companies are orbiting payloads for research, communication and manufacturing purposes that enhance economic competitiveness and security. The commercialization of LEO is creating an information technology eco-system that serves many infrastructures (communication, transportation, education); these new infrastructures will feature far more connected devices (IPv6), highspeed interconnectivity (5G wireless) and AI-mediated management. As these infrastructures are introduced, their cybersecurity and resiliency will be of paramount importance. To the extent that this new information technology eco-system is support by LEO, the US Government and commercial industry needs to ensure cybersecurity for the emerging LEO commercial participants. Industry needs effective and affordable approaches, while the U.S. government must maintain effective oversight, licensing, and regulation of these companies and set international standards for all players. Like other industries, the need to balance effective cybersecurity with other factors will assume increasing importance. For example, exquisite – but expensive - measures for cyber protection could be required to allow companies to launch, but these measures might come at the expense of space commerce. What is an effective approach to ensure cybersecurity that respects the economics of small satellites and LEO? To meet current and emerging cybersecurity and resilience obligations without stifling innovation, a set of "resilient space best practices" guidelines should be established and made available. We envision a guidebook, developed in collaboration with government, industry, and other stakeholders. Such a guidebook would include straightforward approaches, such as the encryption of command/control channels between ground and satellite; the use of design practices to segregate major subsystems onboard a satellite to reduce system-to-system coupling vulnerabilities; and separation of downlinked mission data and ground-based processors using protected interfaces. Overall, these guidelines could convey one or more "reference architectures" that show builders and operators what technologies could be brought together and implemented to strengthen cybersecurity and resilience. These guidelines would include also the 'top N' things that must be done for a company to be allowed to fly, employing a prudent balance of cybersecurity and resiliency features. This concept has been adopted in other domains, such as wireless medical devices and threat-sharing. Real time operational coordination and use of an advanced information sharing infrastructure is being done in other critical infrastructures such as energy, transportation and manufacturing. In this paper, we tailor the principals used in these other applications to LEO.