22nd IAA SYMPOSIUM ON SPACE DEBRIS (A6)
Policy, Legal, Institutional, Economic and Security Aspects ofDebris Mitigation, Debris Remediation and STM (8-E9.1)

Author: Dr. Bruce Chesley
Teaching Science and Technology, Inc (TSTI), United States

Prof. Pam Magee
Teaching Science and Technology, Inc (TSTI), United States
Dr. Jerry Sellers
Teaching Science and Technology, Inc., United States

# THE CONVERGENCE OF SPACE DOMAIN AWARENESS AND CYBERSECURITY: IMPLICATIONS FOR FUTURE WORKFORCE DEVELOPMENT

**Abstract**

The Space Domain Awareness (SDA) mission area is evolving rapidly in scope and implementation, including tools for analysis and action. The scope of SDA is evolving from a military focus to include civil and commercial capabilities as well as international elements. These additional areas stretch the traditional military-focused missions of Space Situational Awareness (SSA) and SDA to address areas such as Space Traffic Management (STM), Proximity Operations (Prox Ops), and In-Space Servicing, Assembly and Manufacturing (ISAM) with a growing number of international and commercial actors.

In this expanding context, the implementation of SDA systems and services relies more than ever on a foundation of trusted data and collaboration to create the actionable knowledge required to predict, avoid, deter, operate through, recover from, and attribute cause to interrupted or degraded space capabilities and services. The integrity of this knowledge is dependent on cyber secure data sources, information delivery and trusted processing that vary by organization and mission.

In this tightly coupled multi-disciplined, multi-mission context we elaborate on the importance of cybersecurity as a foundational enabler of collaboration, data sharing, distributed analysis, and trusted processing environments as they relate to SDA mission success. We stress that data sharing occurs at multiple levels of analysis: at high levels to support integrated threat assessments (such as conjunction alerts and STM), as well as low levels (including sensor track data, and individual sensor measurements with their associated covariance and trustworthiness). We propose a framework that supports a balanced approach that accounts for both measurement accuracy and cybersecurity risk when assessing the trustworthiness of SDA mission architectures.

We discuss the emerging need for International Space Traffic Management (ISTM) coordination mechanisms as a case study highlighting the need for data sharing, risk assessment, data confidence, automation, trust, and cybersecurity. This case study highlights the overlapping interest of SSA/SDA and cybersecurity. We discuss cybersecurity in the context of SDA, where uncertainty and inaccuracy of data are key concerns, as well as the relationship between cybersecurity and space situational awareness that must be considered when incorporating data from outside sources, such as space weather and radio frequency (RF) interference. The paper concludes with a summary of the authors' experiences with training and workforce development in both the SDA and cybersecurity domains.