International Collaboration Framework for Space Domain Awareness

Sarah Law, Jared Stallings, Steve Thilker, Christy Cox, Liam Weston
Raytheon Technologies

ABSTRACT

As more and more entities enter into satellite operations, nations have a need to maintain Space Domain Awareness (SDA) including understanding any factors within the space domain that could affect space operations from a protection as well as defensive position . Space operations have become vital to many nations' security, safety, and economy by providing services such as timing, positioning, weather, and imaging. Ideally, SDA is maintained through a large network of ground and space assets and can be enhanced through data sharing with trusted partners. In order to protect vital space assets, an international collaboration framework is needed that allows countries to use their own unique sovereign assets in addition to leveraging other users' (commercial, allies, etc.) assets. It must include capabilities for Processing, Exploitation, and Dissemination as well as archiving of data at multiple security levels.

We recommend applying this type of enterprise mission framework (EMF) to SDA, creating a space segment agnostic system that allows multiple countries to partner and create a robust SDA solution. Raytheon has extensive experience in SDA, and this paper will discuss how an existing EMF can support the SDA mission through an architecture that decouples the individual system components and allows tailoring to multiple collaborative missions. International collaboration on SDA can help avoid accidents or misunderstandings in space and improve the space operations environment for all participants.

1. INTRODUCTION

Previously, protection of space missions was not a driving factor for development and operations as the vastness of space, limited threats, and reliance on US capabilities for protection allowed focus of limited resources on the mission. Today and into the future, it is well-recognized that space is an increasingly congested and contested operational domain. In a spiraling fashion, recent commercial- and government-driven proliferation of satellites drives down the costs of launch and space systems, allowing increasing numbers of actors to launch increasing numbers of satellites and likewise threats to those systems. Whether these space capabilities support national security, drive commercial revenue streams or provide scientific data, organizations with space capabilities recognize the growing need to protect their interests in space.

Mission protection (MP) for space-based systems can be decomposed into two essential focus areas: threat-resilient architectures to deter threat events from occurring, and threat mitigation to eliminate negative mission effects from active threat events. Mission Protection is foundationally reliant on a robust and comprehensive space domain awareness picture. Threat-resilient architectures rely on an understanding of the types of current and future threats that may impact a given space system. Threat mitigation relies on real-time awareness that enables predictions of or alerts of active threat events. The responsibility to generate actionable SDA and protect operations in space starts with each individual mission and extends to the supporting organizations, countries, and ultimately the overall space community.

As the likelihood of threats to space missions have expanded, stakeholders across these layers are recognizing the need to expand capabilities to ensure continued freedom of action in space. With an evolving, complex threat environment, no one mission or organization can expect to tackle the whole of mission protection on their own. Interfaces and partnerships between entities enhance the collective Space Domain Awareness (SDA), creating more data sources with greater resiliency and redundancy. Each spacefaring nation has a unique combination of industry, academia, and government (civil and military) space capabilities, which when used together can improve the generation of actionable, timely awareness.

Despite the potential utility, collaboration and cooperation across the layers is challenging. Many existing systems operate within pre-existing stovepipes. Organizational and national boundaries drive political and policy differences. Many SDA and MP capabilities and data lie behind national security boundaries.

Despite these obstacles, there are steps that can be taken to improve mission, organization and space community space domain awareness and mission protection. This paper describes internal and cooperative actions that can be considered to improve any mission's MP stance.

While many mission protection responsibilities lie outside the scope, capability or jurisdiction of a given space mission, mission protection starts with the concept definition of the entire integrated space/ground system and includes design, development, and operations. The mission relies upon external supporting organizations to provide the broader data, services and capabilities outside of the mission scope.

Examining how a larger coalition of space missions can work together, it is clear that each unique mission and/or dataset requires coordination to leverage them to the greatest possible utility. Using open standards/interfaces as well as design concepts, will help systems to interoperate more closely, creating greater value for owners/operators as well as allies. Courses of action should be coordinated across mission assets for the lowest cost and highest information value. To meet this need, Raytheon has developed a space mission agnostic enterprise mission framework (EMF) that can support collaborative international SDA. Our architecture decouples the individual system components and allows tailoring to multiple collaborative missions. This architecture enables courses of action (COAs) that look across the coalition to optimize asset utilization.

Here, we discuss an approach to mission protection as well as how an international collaborative EMF providing a strategic mission management (MM) ecosystem supports enhanced mission protection across allied nations.

2. MISSION PROTECTION

Actionable threat information is only useful if it is acted upon. Each mission must have the ability to develop and evolve architectural threat resiliency and act to mitigate active threat events based on SDA pictures. This SDA information starts internally using mission data and information, and is augmented with data and information from the supporting layers.

Many missions are operating or are being developed without mission protection as a driver. In the future, we envision that mission protection will become an essential function from concept development through end of life. Development and operational organizations will have mission protection integrated into organizational structures, roles and engineering processes.

However, even if MP hasn't been built in from the ground up missions can still improve their MP posture with the following recommendations:

- Develop and maintain a Mission Protection Plan that identifies the types of threats relevant to the mission and outlines the agreed upon resiliency and mitigation options for each threat type at the mission level. It also outlines the internal threat event responsibilities, reporting chains, decision points and authorities for prosecuting active threat events. This plan drives requirements, architecture and design activities.
    - Organizations may also create an organizational protection plan that defines their overarching responsibilities to its missions.
- Assign mission protection stakeholders with sign-off authority to ensure mission protection is properly addressed according to the Mission Protection Plan at key program milestones.
- Assign a mission protection role to the mission operational team to execute the Mission Protection Plan and coordinates mission protection activities for the mission. This role:
    - Maintains the current SDA picture
    - Oversees development, maintenance, training and rehearsal of protection related operational procedures
    - Ensures consistent, thorough monitoring of operations to identify potential threats
    - Receives and responds to external threat information and alerts

- Represents mission protection on anomaly teams
- Works with operational leadership to manage active threat events
- Documents and reports protection activities
- Identifies, analyzes and recommends mitigations to active threats

Whatever mission protection structures, organizations or processes are put in place, they rely on actionable, mission relevant information. Maintaining a current operational picture of the threat landscape starts with the internal monitoring of mission observables and is supplemented and supported by external organizations, systems and services. Missions maintain hyper focus on ensuring mission success. Their view of an understanding of the operational threat landscape is centered on their mission. The capabilities to provide broad, comprehensive space domain awareness and mission protection start in the organizational layers and move out to the national and international layers. In the end, these layers have the required scope of responsibility and breadth of capabilities to tackle the formidable challenges. As the operational environment becomes increasingly contested and congested, the ability to continue to ensure freedom of action in space can best be handled through increased collaboration and cooperation amongst willing partners.

3. PARTNERSHIPS FOR SDA

Ensuring freedom of action in space is a common objective for friendly nations as well as commercial companies; their incentives may vary between financial and national security, but there is an inherent self interest in mission protection. Relying on a single global supporting organization that has the charter and jurisdiction to ensure freedom of action in space is not realistic. It requires each mission to do as much as possible, as well as each supporting organization and nation. Obviously cooperation among friendly organizations and nations is a force multiplier that allows everyone a better chance to successfully operate their missions without harm.

Collaboration across organizations and especially across national boundaries is often difficult due to geography, policy/law, differing mission prioritization, language and existing capability. However, there are a number of steps that can be taken to increase collaboration. As each organization or nation considers what they are willing to do to increase the protection of their assets, they may be more or less willing to share private data. Creating an EMF that enables each entity to bring what they have and share with others as desired is key. Initially this may be a very loose ecosystem of data, apps and resources. The following is a roadmap to increasing collaborative SDA among affiliated entities:

1. Share Data

   The most basic step is to increase the sharing of data. No one mission, organization or nation can expect to be able to capture all data needed to identify, characterize and deter threats. While today basic space catalog data is available for most objects in space, it is based on optical and radar observations. Additional utility is provided through alerts of potential conjunctions. However, little of this data is generated or augmented with data from operational systems. Sharing operational information, such as ephemeris, vehicle status, planned maneuvers, anomalies, unexpected RFI events, can create great value across missions. With richer data sets available, AI/ML systems have more data from which to identify patterns of activity and predict or forensically identify potential threat events.

   For example, if a system encounters radio frequency interference and posts the times/locations, that data could be correlated across a variety of space operators and from the whole of the data you could start to identify patterns, likely causes, etc.

   The US Air Force Space Command Unified Data Library (UDL) which is open to US Allies [1] is being deployed to serve as a common data repository for SDA information. Working to overcome political, security or proprietary impediments to sharing data within a construct like the UDL is an important next step for each organization to consider. Another example is the Standardized Astrodynamics Algorithm Library (SAAL) that the US Space Force is sharing through Operation Olympic Defender [2]. Both of these examples are only shared with a limited set of partners.

2. Share Apps

Different users will have different interests in the shared data and will likely develop their own applications. Allowing open sourcing of capabilities can create opportunities for reuse and collaboration and avoids attempting to set up a single global processing capability that satisfies all users. Space operators should be able to open source development of key capabilities, or post their apps (source code, or containers). Other cooperative nations can help develop or just download specific capabilities, host them in their cloud and take advantage of the capability. This works well for self-contained applications, but may be more difficult with applications that have dependencies to COTS or other licensed capabilities.

An example of app-sharing is the SDA event tracker Metroid that is available to the FVEY Alliance [3].

All space operators have a need for situational awareness (SA) and it makes sense that this would be an early collaboration point among contributing parties. An ongoing and current understanding of the threat environment improves everyone's ability to operate safely. A common operating picture (COP) increases understanding across collaborating parties and needs to keep track of threat types and generalities, as well as real time information (active threat event detection). When threat events do occur, they must be tracked, including what indications and warnings (I&W) occurred, what actions were taken, and ultimately what lessons were learned. For example, Raytheon has developed Activity Based Intelligence (ABI) analytics and other Artificial Intelligence/Machine Learning (AI/ML) analytics that can correlate over these data sets to uncover 'unknown unknowns' and inform future decision making. Once this type of data is collected, it can be used to build automated triggers/alarms and newly informed COAs. These rich analytics are all enabled by a collaborative EMF with a rich data set.

3. Share Resources

Some nations have specific SDA resources that provide the ability to sense resident space objects (RSOs) and characterize them, while other users need to figure out what is happening to them (i.e. characterize a threat event or anomaly). Thus having a larger pool of cooperating resources can be greatly beneficial to participating entities. This can be accomplished technically through the use of common interfacing standards and technologies, although political and security boundaries may present additional impediments. One issue is how to share resources optimally across the ownership organizations needs and partners. A loosely coupled architecture can allow contributing parties to expose services into an EMF ecosystem and share what they want to, while maintaining positive control over their own assets and setting usage constraints as desired. Consuming organizations can invoke those exposed services through common standards and well-defined interfaces. This reduces the amount of infrastructure that participants need to stand up. Essentially, everyone brings what they have and exposes it for the coalition to utilize.

In addition, Raytheon has extensive expertise in implementing models such as prioritization schemes, tasking limits, economic models (bidding schemes) voting schemes among partners for prioritization of common tasks, etc. Different organizations may have different ideas about what equitable use of their and others' assets are, but highly optimizing asset use can help facilitate cooperation and reduce policy friction.

An example of sharing resources could be optimizing across multinational ground stations so that space-based SSA can be more quickly downlinked and shared across the coalition.

This ecosystem of shared data, apps and resources is enabled by an enterprise mission framework with the following characteristics:

- Modular Open Systems Approach (MOSA)
- Standards-based
- Containerized
- Agile development paradigms to facilitate integration

Raytheon has been working to develop a strategic MM ecosystem, or EMF, that supports collaborative SDA/MP as described above. It provides consolidated access to internal and inter-partner resources with a configurable policy that defines what is exposed to external users. Depending on the current threat posture, that policy may be

dynamically updated. This concept of a common, multi-mission tactical and strategic space mission system of systems can greatly improve MP for individual missions and reduce the cost of enhanced MP. From a tactical perspective, it allows individual space owner/operators to onboard and operate missions as they come online. From a strategic perspective it allows individual nations use of available resources. Additionally it allows allied nations or organizations collaborative use of available resource capacity.

The biggest hurdles for this type of path forward is security. Much of the data, applications and resources live behind levels and layers of security. Nations want to protect what they know and how they know it. This significantly limits the ability to work across organizational boundaries for the common good. However, multi-level security can be implemented using cross-domain solutions like the Forcepoint High Speed Guard, ensuring that as much data as possible is shared across allied entities.

4. SUMMARY

As space continues to become more accessible across the board, misunderstandings, accidents and ill intent are all increasingly likely to create mission threats. As a result, mission protection is an essential element of operations and ideally is built in from the ground up. All owners/operators and nations can improve their MP through collaboration. However, there are many obstacles, both technology-based and policy-driven, to creating interoperable systems. We recommend an incremental process to enhance multinational collaboration, culminating in a shared ecosystem of data, apps, and resources enabled by an enterprise mission framework shared across allied nations.

5. REFERENCES

[1] Hitchens, T. Crider: SSA Data ‘Library’ Will Open to Allies, *Networks & Cyber*, May 3, 2019.
[2] Strout, N. US Space Force to begin sharing technical space data with UK, *C4ISRNET*, Aug 18, 2020.
[3] Holland, M. Kobayashi Maru delivers ‘coalition friendly’ Platform, *SpaceForce.Mil*, May 8, 2020.