Cybersecurity's role in supporting Space Situational Awareness

Mr. Nick Tsamis
The MITRE Corporation
Mr. David Vivanco
The MITRE Corporation
Mr. Harvey Reed
The MITRE Corporation

Space operations continue to grow in complexity due to the increased participation and population of on-orbit space system assets. New operational activities within space require a re-evaluation of the methods and processes we use to define a clear understanding of the domain. As operations grow in complexity, the space domain requires more efficient and accurate information to support a consistent and trusted common understanding of space situational awareness.

The current space ecosystem is continuing to expand, leading to organizations now finding themselves in a situation where large amounts of data needs to be processed and analyzed for current and future space activity. The expansion leads to an increase in computing systems required and complexity of the architectures used to support system-to-system communication, potentially spanning across different physical regions. From a cybersecurity perspective, this can be viewed as a significant increase in the attack surface that must be addressed – increasing the challenges to cybersecurity practitioners in facilitating trustworthy data exchanges among space community stakeholders.

The space domain is not immune from cybersecurity threats. As a quickly developing critical infrastructure, space remains an attractive target for cyber adversaries. Risks from a cyber-attack that has ability to disrupt accurate space situational awareness affects not only a single space stakeholder, but rather all space faring participants. These risks impose consequences far beyond the cybersecurity community, threatening the safe, endured, and sustainable access to space resources. Aligning and integrating cybersecurity solutions based on common operational space activities, e.g. tailored specifically to support space situational awareness, can yield solutions that will allow space operators to more effectively address these risks.

Traditional approaches to cybersecurity often do not consider the unique operational functions carried out within the domains into which they are integrated. Identifying such operational activities from the space situational awareness community can be an effective enabler in guiding a tailored approach to cybersecurity. As approaches, methodologies, and policies to cybersecurity are all actively being developed and implemented, it is now a valuable time to ensure the solutions being developed are indeed effective and useful to space domain stakeholders.

By better understanding cybersecurity needs unique to the functions carried out in the space domain, solutions can be integrated to support real-time operational activities more effectively and efficiently. As a step towards better understanding the domain's needs, it is proposed to start with a common vernacular to describe space domain operations. Using a common space language helps align cybersecurity goals (e.g. outcomes) and requirements (e.g. implemented controls) to space functions generically, rather than overfitting solutions to a single user or implementation. This allows cybersecurity solutions developed to be highly applicable across mission sets, yet tailored where necessary, to accommodate mission-specific constraints.

While not an end solution for all the challenges faced, using a common language to describe space operations reduces the overfitting to individual stakeholders' perspectives and allows for solutions to be effectively coordinated across the domain, incorporating a diverse set of operators and users. A characterization of space missions can then be described in a more consistent and concrete way. Further, by characterizing different missions, identified *similarities in space functions needed presents a ripe opportunity to take a consistent and modular approach to cybersecurity.*

Future efforts to help further coordinate defense in the domain can make use of a common understanding to develop more standard cybersecurity playbooks (i.e. sets of standard operating procedures) for effective multi-stakeholder monitoring, protection, and response. From this perspective, cybersecurity can serve as a conduit to increased collaboration amongst space domain stakeholders in helping to define interfaces, standards, and new normative measures for driving towards a clearer and more trustworthy picture of space situational awareness.

Starting with the application of such a common lexicon proposed, a more effective means to communicate across stakeholders provides a clearer understanding of space situational awareness cybersecurity success criteria. The need for space domain-integrated cybersecurity can serve as a call to action for overall increased community collaboration, ultimately moving the domain towards agreement on acceptable performance standards facilitating more sustainable, if increasingly congested, space domain activity.

1. INTRODUCTION

As the space ecosystem continues to expand with increasingly complex mission architectures, space mission forces are challenged to effectively defend space systems. A key aspect of this challenge is a high degree of diversity in how space mission operations are described and communicated. This results in a high degree of ambiguity for space mission owners to concretely articulate cybersecurity needs to be ultimately used by specialized cyber workforces.

Stakeholders of space systems are faced with the growing challenge of identifying applicable cybersecurity needs and addressing them with appropriate and effective controls. Consider Space Situational Awareness (SSA) and all the coordinated functions required to continuously accomplish the mission – determining data and access control requirements alone presents a significant challenge. Can SSA stakeholders today communicate more efficiently via a shared common description language?

Security guidance exists in the domain today and it is understood that tailored overlays of existing security tools, processes, and industry frameworks can be combined to articulate challenges and opportunity areas for cybersecurity into space missions. We propose that a common description language to 1) describe functional operations, 2) identify relevant data flows & components, and 3) define cybersecurity needs, can serve to provide a standardized way for space mission owners to coordinate the needs for and implementation of cybersecurity solutions. We demonstrate the effectiveness such an approach can have in coordinating needs and responsibilities across cyber and space mission forces. This provides an enabling pathway for existing cybersecurity forces to operate effectively within space domain systems.

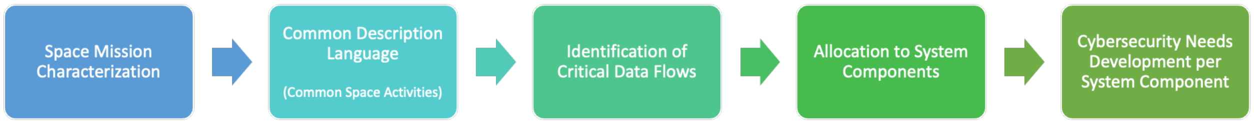

Space Mission Characterization
Common Description Language
(Common Space Activities)
Identification of Critical Data Flows
Allocation to System Components
Cybersecurity Needs Development per System Component

Fig. 1 – Overview to Identifying and Coordinating Cybersecurity Needs

2. PRIOR WORK AND CHALLENGES

Space Domain

Categorization of the space domain differs across different users' perspectives, but broadly, operations have been traditionally organized into four physical "segments": *Space*, *Ground*, *Link*, and *User*. GPS.gov, for instance, collapses this characterization into three segments: *Space*, *Control* (i.e. Ground), and *User* [1]. While other models consider inclusion of fifth segment, *Development* -- not necessarily aligned to a physical boundary -- to account for pre-deployment and maintenance activities.

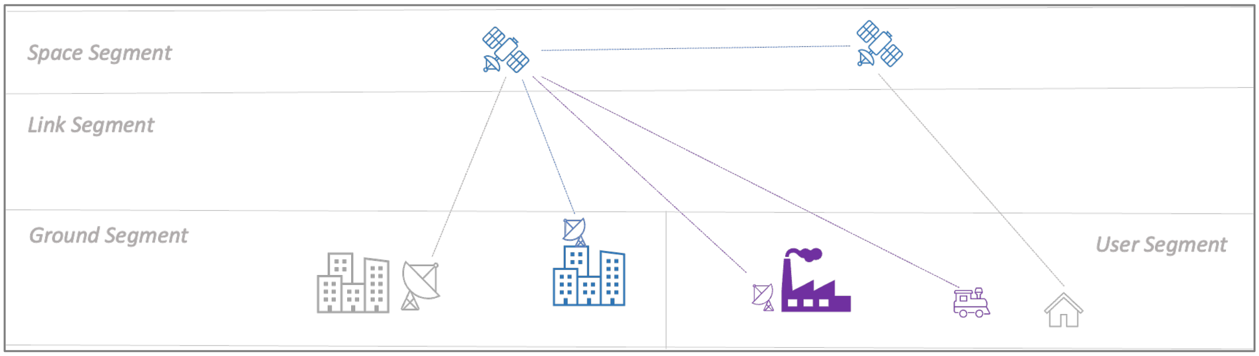


Fig. 2 - Traditional View of Space Segments

While segment-based categorizations can be proven useful for high-level descriptions of activities and their physical location, it does not always provide a useful reasoning framework to analyze security implications that may be better suited to an operations-focused perspective that inherently requires analysis across segments. Making explicit and enforced physical delineations at this level may not always be plausible or entirely useful based on analysis needs.

Consider the concept of autonomous satellite traffic management, where space vehicles can autonomously avoid collision based on SSA data received by entities part of space segment. From an SSA perspective, the space vehicle receiving SSA data can be considered part of the space segment, whereas the architecture supporting those data flows may be co-located across any of the Ground, User, or Space segments. Operational needs, and associated security needs, easily span across multiple domains. These segment boundaries do not provide an effective way to organize security goals or responsibility/cognizance over those needs.

Rather, by characterizing the operational functionality required, we can ensure that security goals better align to operations. Function-based frameworks and analytic methods are widely known and well-accepted practices across safety and security engineering disciplines. Similarly, the development of standardized lexicons used to describe domain operations is not a unique request. The call for common ways to communicate for increased effectiveness and ability to collaborate in the space domain remains a well understood need [2], [3].

Significant efforts in support of common definitions and descriptions exist in the space domain today and provide an excellent starting point to understand. The United Nations Institute for Disarmament Research (UNIDIR) specifically published a dedicated lexicon in August 2023 [4]. This report serves as a comprehensive reference for included definitions spanning space objects, orbits, services and activities and components (i.e., space segments). Similarly, the concept of unified "terminology" has been the subject of development for organizations like The International Academy of Astronautics (IAA), the International Astronautical Federation (IAF), and the International Institute of Space Law (IISL) for some time. At the International Astronautical Congress in 2022 [5], these three organizations authored a joint publication (executive summary referenced) [6] providing additional guidance to the space domain related to the use of unified language.

Cybersecurity Domain

The need to communicate consistently using abstract frameworks is a concept the cybersecurity industry has approached. Many frameworks, including MITRE ATT&CK® [7] and MITRE D3FEND™ [8], have been created and widely adopted to help coordinate the way cybersecurity is consistently described and communicated. Extensions provided by related projects tailor this guidance further to specifically describe operations within specific domains. The Aerospace Corporation's SPARTA framework [9] provides a dedicated reference to describe adversary actions associated with space segment operations. Future extensions and applications can provide similarly useful supplements for inclusion.

Many frameworks have been created and widely adopted to help coordinate the way cybersecurity is consistently described and communicated.

Approved for public release. Distribution unlimited 22-03937-5

These frameworks all contribute to helping the cybersecurity domain better organize and unify around cybersecurity concepts. Through experimentation with these combined frameworks, a challenge was identified in how to consistently leverage the various tools together when needed. For complex, multi-domain analyses, analysts have need for frameworks to be used with each other. This Systems-of-Systems analysis problem was the rationale for MITRE's Platform Independent Vectors of Techniques (PIVOT) [10] concept.

Function-based processes are not unique to the cybersecurity industry with several different varieties provided. One such example methodology, Mission-Based Risk Assessment Process for Cyber (MRAP-C) includes a Functional Thread Analysis (FTA) component focused on making use of a mission's operations distilled into more atomic functions to perform a function-based analysis [11]. As applied to the cybersecurity industry, they have largely been used: 1) in a reactionary manner, after system implementation, 2) not to define requirements pre-development, but to retroactively identify gaps or missed opportunities in the application of security controls during system design, and 3) using specialized analysis formats or mission-specific lexicons hindering transferability across diverse stakeholders, organizations, and missions. With the concepts presented here, the intent is to not overwrite or supersede approaches of well-defined methodologies, but rather provide a set of reference material that can be *incorporated* into existing analysis or assessment processes for enrichment.

Using the frameworks referenced allows for more consistent description of cybersecurity challenges and needs to be communicated, reducing misunderstandings, ambiguity, and effort needed for cybersecurity stakeholders to accurately create and validate selected solutions.

3. COMPLEXITY WITHIN SPACE DOMAIN OPERATIONS

SSA is defined in [6] as providing "foundational positional, electro-magnetic, and situational information on objects as a function of time. It also summarizes the overall state of the space environment, including debris and space weather conditions, upon which Space Traffic Management (STM), Space Traffic Coordination (STC), Space Domain Awareness (SDA), and Space Environment Preservation (SEP) actions are based." The publication further describes how security is challenged and complicated by "ever-blurring lines between commercial space systems and support to national security", and present across any number of active spacecraft and ground system components. This begs the question – can a function-based approach be taken to apply cybersecurity principles to ultimately secure mission objectives across all system components?

A real-world use-case of this complex dynamic between commercial space systems and their support to national security was demonstrated in Russia's recent aggression towards SpaceX's Starlink service in Ukraine. SpaceX, a commercial company, delivered Starlink terminals to Ukraine in February 2022 to assist the country in maintaining Internet access amid Russia's invasion. Shortly after, Starlink's service was impacted by purported signal jamming, a type of electronic warfare targeting the frequency band that Starlink operates on [12]. This event, ultimately targeting Viasat and Starlink systems, provides a clear example of the impacts faced due to the "ever-blurring lines between commercial space systems and support to national security." Are other commercial companies at similar risk by providing space services to contested areas?

Complexity is also presented to the space domain by today's modern system and mission architectures. Increasing amounts of data transmitted across the ecosystem is not easily understood or characterized by traditional segment-based views. To further illustrate a complex operation not easily binned by segment categorization alone, consider the graphic below making us of: ground-ground, ground-space, space-space, and space-ground communication flows. (1) a *User* entity requesting an operation or data stream from (2) a space service provider, *Ground* entity, resulting in a command to execute a (3) *Space* Operation. The operation results in required coordination (4) with another *Space* entity, perhaps to optimize downlink for ultimate (5) *User* receipt of the transaction.

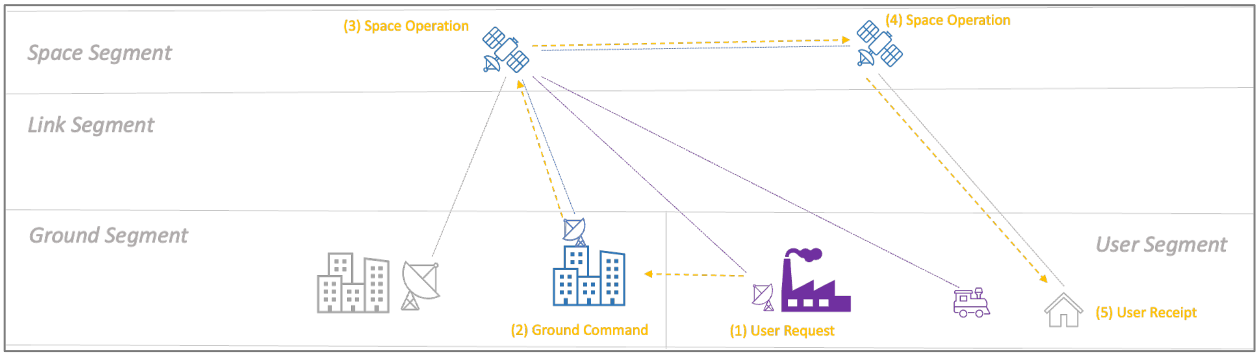


Fig. 3 - Complex Cross Segment Relationships

When considering this set of interactions from a cybersecurity perspective, several questions are illuminated for analysis consideration:

- *What threats do we need to consider when analyzing the protection of mission data?*
- *What data is at risk at which times throughout the multiple transactions occurring?*
- *Who is responsible for ensuring information security tenants are accounted for, at each step in the process?*
- *How can cybersecurity controls effectively be allocated to ensure end-to-end data flows are properly protected, commensurate with applicable threats?*

4. DESCRIBING FUNCTIONAL SPACE ACTIVITIES

While prior work exists in the domain today performed towards consistent terminologies for objects, orbits, and other space-based concepts, consistent emphasis on operational functionality is not always a key focus. Due to the constraints presented by a segment-based categorization, for analysis requiring modern cross-segment mission architectures, a common taxonomy (Common Space Operations Taxonomy) consisting of atomic functionality of space operations is proposed. **The taxonomy organizes functions that may span across multiple space segments, therefore removing the artificial boundary.** For each function, multiple subfunctions can exist to explain further detail.

Table 1 provides an example of what such a functional decomposition may constitute. The entries provided in the table are not intended to contain a complete picture of all common space operational activities nor form an exhaustive list of all functions/sub-functions associated with an identified activity. The information is provided to illustrate 1) the utility in using an agreed-upon language, and 2) how using such a function-based approach can be a useful guide in supporting complex cross-segment analysis. Using this approach provides a useful reference that overcomes challenges experienced with more traditional views of space domain characterization (i.e., characterization by space segments). With an understanding of what space functions are present within a given analysis scope, data flows can be more readily identified, providing an effective path to determining and managing cybersecurity needs.

Table 1 - Collection of Space-Based Operational Activity (Functional Taxonomy)

Common Space Operations			
Activity	Function	Sub-function	Definition / Exemplar Instance
Communicate	Command and Control	Receive Telemetry / Health Check	Facilitate collection and analysis of diagnostic data from space-based assets to infer health and operating status.
		Command Action	Dispatch active command to space-based assets to support mission execution.
Coordinate	Plan Mission	Facilitate Coordination of Resources	Perform peer-to-peer ground station hand-offs. Plan link budgets for transmitting payload data.
	Schedule Resources	Schedule Ground Resources	Orchestration of available system resources (physical and logical) to meet mission needs. Allocation of terrestrial-based assets to facilitate execution of mission.
		Schedule Space Resources	Allocation of on-orbit assets to provide capabilities in support of mission.
	Execute Mission	Dispatch Resources	Execute on resource allocation plans by dispatching system resources in support of mission goals.
Sustain	Maintain	Maintain Spacecraft Bus	Planned and unplanned maintenance activities associated with the computing components on-board space vehicle, including software updates & patches.
		Maintain Communications Infrastructure	Planned and unplanned maintenance activities associated with computing components supporting communications including software updates, patches, configuration changes, etc.
	Secure	Enforce Authorized Access	Authenticate and authorize access requests to resources. Resources may enforce user or machine -based accesses to services, computing resources, or data.
	Monitor	Provide Situational Awareness of SVs	Provide real-time picture including continuous updates on the health and status of on-orbit space vehicles.
		Provide Environmental Awareness	Provide real-time picture of on-orbit asset's experienced operating environment. May include spectrum management, conjunction potential, interference, or other environmental parameters that may pose a threat to normal operations.
Manage Data	Downlink	Maintain Transport for Payload Data	Sustain the ability for successful transmission and receipt of data from on-orbit application-specific payloads to external entities.
	Uplink	Update Payload Configurations	Sustain the ability for successful transmission and receipt of updated configurations, tasking, or instructions to on-orbit application-specific payloads, provided by external entities.
	Process Data	Facilitate Data Analysis	The management and provisioning of resources required to coordinate, process, and analyze data retrieved from on-orbit payloads to support user or mission needs.
…			

Four major high-level *Activities* are identified in Table 1: Communicate, Coordinate, Sustain, and Manage Data. These activities represent a highly generic operation, they are comprised of *Functions* that support the higher *Activity*. Functions help describe the various facets of the higher-level Activity. As an example, mission planning, resource scheduling, and mission execution are all individual components of (different ways of contributing to) the coordinate *Activity*. Finally, a third level of categorization (*Sub-function*), accompanied by a definition or exemplar instance, provides further detail on how each of the identified *Functions* is carried out.

Using a collection of common space operational activities can be directly mapped over a specific system architecture to disregard arbitrary constraints imposed by a segment-based characterization. A crude illustration provided in Fig. 4, shows how the *Activity* 'Manage Data' consists of *Functions* that span across three segments (Ground, User and Space). Using a traditional segment-based perspective, the data flows associated with Manage Data may be analyzed independently across Ground, User, and Space segments. Doing so may ignore the important interface between entities in each segment, presenting opportunity for gaps in analysis or security posture understanding. It is precisely these gaps that the proposed function-based approach seeks to identify to ensure interfaces are adequately defended in a coordinated manner. With a functional approach, cybersecurity overlays can now be attached to a set of (sub)functions spanning segments, reducing limitations presented by artificial boundaries.

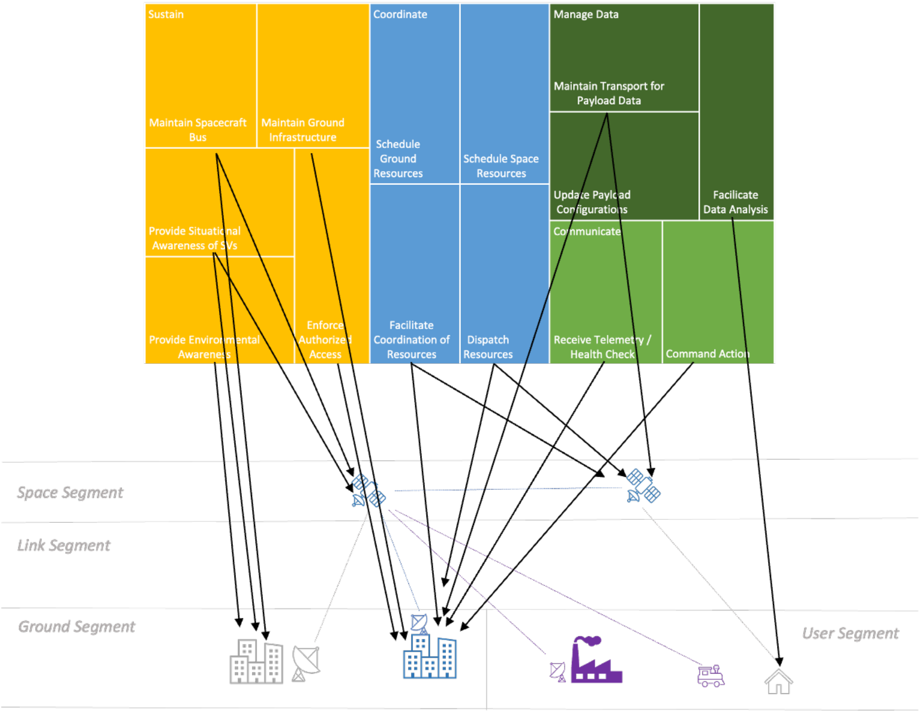

Sustain
Maintain Spacecraft Bus
Maintain Ground Infrastructure
Provide Situational Awareness of SVs
Provide Environmental Awareness
Enforce Authorized Access
Coordinate
Schedule Ground Resources
Schedule Space Resources
Facilitate Coordination of Resources
Dispatch Resources
Manage Data
Maintain Transport for Payload Data
Update Payload Configurations
Facilicate Data Analysis
Communicate
Receive Telemetry / Health Check
Command Action
Space Segment
Link Segment
Ground Segment
User Segment

Fig. 4 - Mapping Common Space Operations to Physical Architectures

5. APPLICATION TO SSA

As mentioned previously, SSA is defined as having the ability to summarize "the overall state of the space environment." SSA networks and architectures tend to be complex, often consisting of multiple systems in disperse geographical locations potentially contributing to additional missions. An example of this includes ground radars such as Millstone/Haystack – although primarily SSA focused, they all had a pedigree in missile warning from when SPADOC was located within Cheyenne Mountain. Eventually, it became clear that radars could be dual purposed to support SSA. Currently, the majority of the U.S. government's SSA network consist of inter-agency agreements to ultimately dual-purpose existing systems. Furthermore, existing efforts are underway to expand agreements with global partners, and even commercial entities [13].

Initial systems contributing to SSA consisted of ground-based radar and optical systems, categorized as ground segment components. However, due to weather, solar blind spots, and their geographical location on Earth [14], there was a need for a space-based system. In 2010, the U.S. launched the Space Based Space Surveillance System (SBSS) to contribute to the SSA mission with a clear and unobstructed view of space [14]. With the launch of SBSS 1, this has now expanded traditional ground segment functions for SSA into the space and link segment. While the system components and architecture changed over time, the core functionality of the mission did not change. A concept to be captured, and verified, in a function-based description.

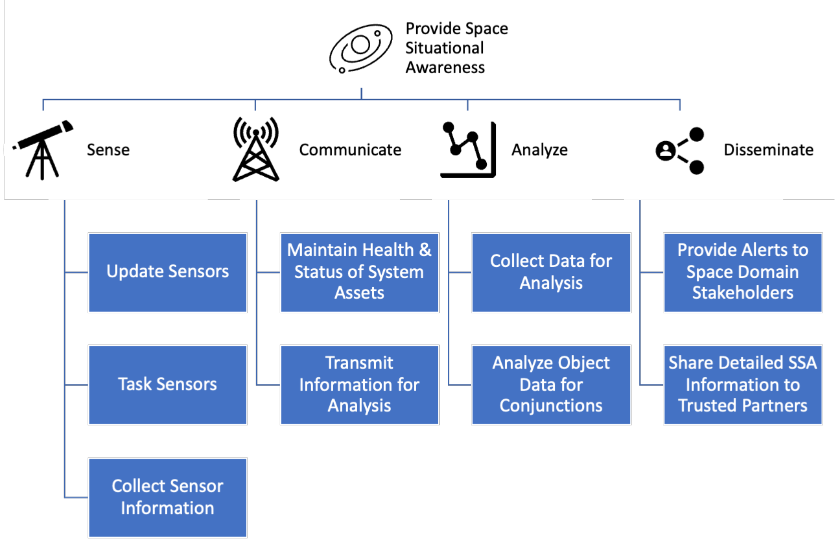

Provide Space Situational Awareness
Sense
Communicate
Analyze
Disseminate
Update Sensors
Task Sensors
Collect Sensor Information
Maintain Health & Status of System Assets
Transmit Information for Analysis
Collect Data for Analysis
Analyze Object Data for Conjunctions
Provide Alerts to Space Domain Stakeholders
Share Detailed SSA Information to Trusted Partners

Fig. 5 - Example Mission-Specific Description of SSA

A rudimentary decomposition of the SSA mission is provided here to illustrate how mission-specific language could be translated. The decomposition identifies four major high-level activities as shown in Fig. 5: Sense, Communicate, Analyze, and Disseminate. Each of the activities is comprised of mission-specific functions (depicted in blue boxes) that fulfill SSA mission objectives, such as *task sensors*, or *provide alerts to space domain stakeholders.*

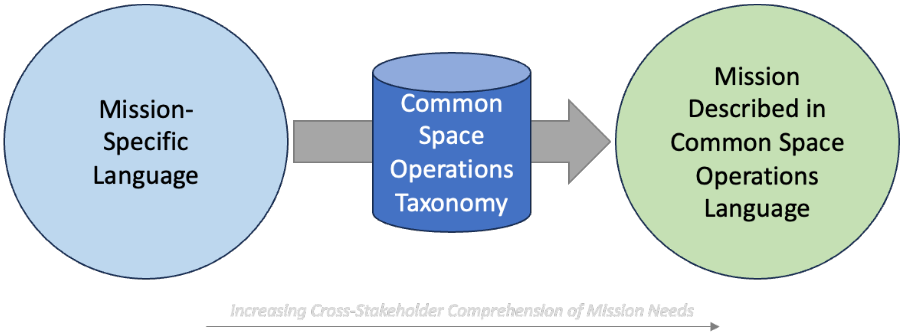

Mission-Specific Language
Common Space Operations Taxonomy
Mission Described in Common Space Operations Language
Increasing Cross-Stakeholder Comprehension of Mission Needs

Fig. 6 - Using a Common Vocabulary to Describe Mission Operations

The mission-specific activities and associated functions can now be mapped to the common space operations taxonomy as shown in Fig. 7. By performing the mapping, we are effectively able to characterize and define a given stakeholder's view of the SSA mission and their contribution through common functions, regardless of the physical location and segment categorization of their systems. When multiple stakeholders provide and share common views together, gaps in understanding or scope can be easily identified.

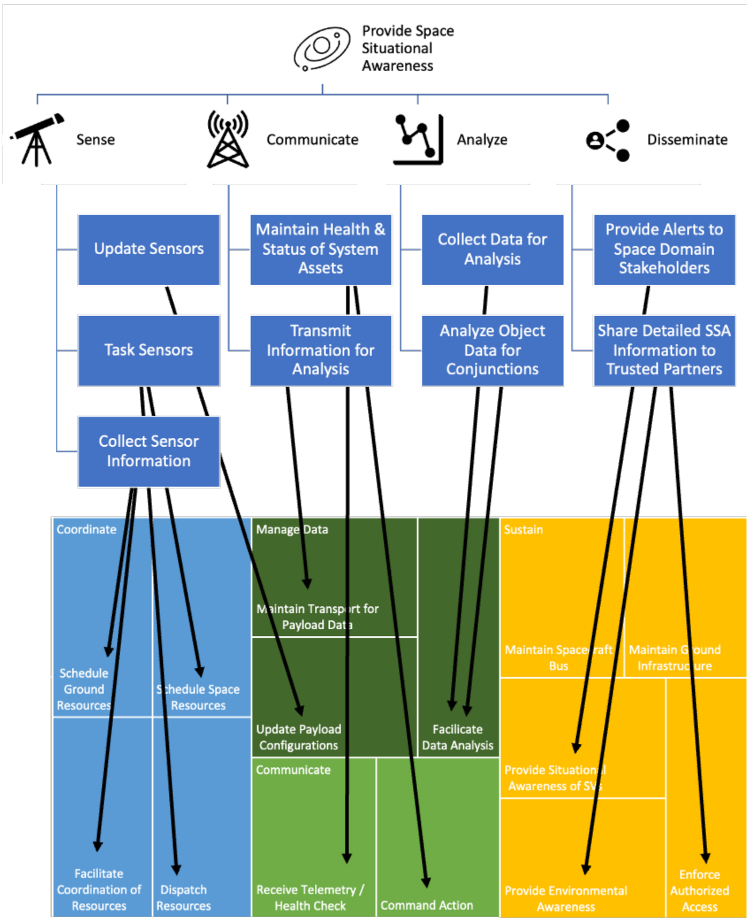

Provide Space Situational Awareness
Sense
Communicate
Analyze
Disseminate
Update Sensors
Task Sensors
Collect Sensor Information
Maintain Health & Status of System Assets
Transmit Information for Analysis
Collect Data for Analysis
Analyze Object Data for Conjunctions
Provide Alerts to Space Domain Stakeholders
Share Detailed SSA Information to Trusted Partners
Coordinate
Schedule Ground Resources
Schedule Space Resources
Facilitate Coordination of Resources
Dispatch Resources
Manage Data
Maintain Transport for Payload Data
Update Payload Configurations
Facilicate Data Analysis
Communicate
Receive Telemetry / Health Check
Command Action
Sustain
Maintain Spacecraft Bus
Maintain Ground Infrastructure
Provide Situational Awareness of SVs
Provide Environmental Awareness
Enforce Authorized Access

Fig. 7 – Describing SSA functions in Common Space Operations Language

The table below contains a mapping of the identified SSA activities with the common space operations language.

Table 2 - SSA Activities Mapped to Common Space Operations

Space Mission	**Mission Function**	**Mission Sub-function**	**Common Space Operations Language**
Provide Space Situational Awareness	Sense	Update Sensors	Update Payload Configurations
		Task Sensors	Schedule Space Resources
			Dispatch Resources
		Collect Sensor Information	Facilitate Coordination of Resources
			Schedule Ground Resources
	Communicate	Maintain Health & Status of System Assets	Receive Telemetry / Health Check
			Command Action
		Transmit Information for Analysis	Maintain Transport for Payload Data
	Analyze	Collect Data for Analysis	Facilitate Data Analysis
		Analyze Object Data for Conjunctions	
	Disseminate	Provide Alerts to Space Domain Stakeholders	Provide Situational Awareness of SVs
			Provide Environmental Awareness
		Share Detailed SSA Information to Trusted Partners	Enforce Authorized Access

6. CASE STUDY – VIASAT'S KA-SAT NETWORK

To illustrate real-world applicability of how a collection of common space activities can be used to describe cyber defense needs, a brief case study is reviewed: the cyber attack in February 2022 on satellite communications provider ViaSat's KA-SAT network. While this case study does not correlate exactly with specific functions comprising a typical view of the SSA mission, it provides a useful surrogate story to illustrate the utility of applying a common way to describe space activity for increased comprehension and collection of lessons learned using a real-world example.

Boschetti, Gordon, and Falco provide an overview with detailed decompositions of the infrastructure at play and the specific methods used to disrupt various system component to execute the attack [15]. The various system components targeted in the attack are categorized by their segment location: *Space*, *Link*, and *Ground*. KA-SAT network operations are described in the report, allowing the following physical component model to be created, Fig. 8. Reviewing information related to the functions associated with each of these system components yields understanding of the functionality performed by each segment, Fig. 9.

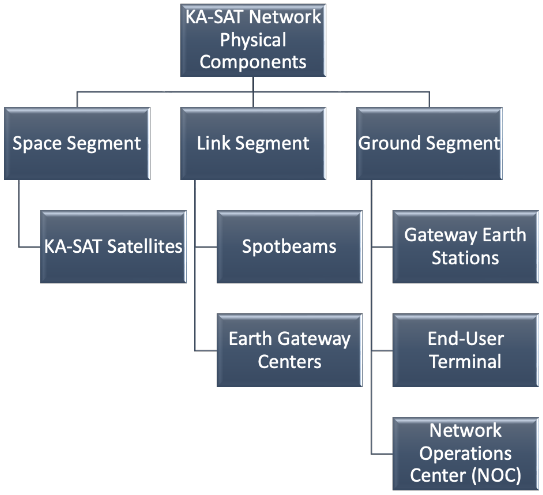


Fig. 8 - KA-SAT Network: Physical Components

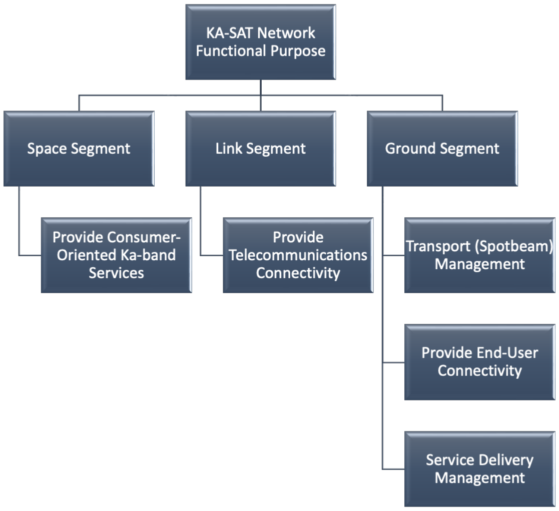

KA-SAT Network Functional Purpose
Space Segment
Link Segment
Ground Segment
Provide Consumer-Oriented Ka-band Services
Provide Telecommunications Connectivity
Transport (Spotbeam) Management
Provide End-User Connectivity
Service Delivery Management

Fig. 9 - KA-SAT Network: Functional Purpose

This decomposition provides a rough mission model onto which common space activity terminology presented can be mapped, illustrated in Fig. 10. By performing this activity, we can easily identify ask questions to determine what data flows are associated with the system's operations and potentially leverage other analysis or solutions used by in other systems supporting similar functions. When paired with a formulated threat model (references to inform this formulation can be found in the Prior Work section), cybersecurity protection needs can be more systematically identified. With this guiding information, we are able to ask more detailed questions than before (reference question list in section 3.

- *How is the spacecraft bus maintained to support telecommunications connectivity?*
- *What maintenance activities occur on ground infrastructure to support telecommunications connectivity?*
- *How is spotbeam management performed to allow for payload updates?*
- *How is authorized access enforced regarding end-user connectivity?*

- *What data is necessary to validate effective maintenance of transport for payload data supporting end user connectivity vs managing service delivery?*

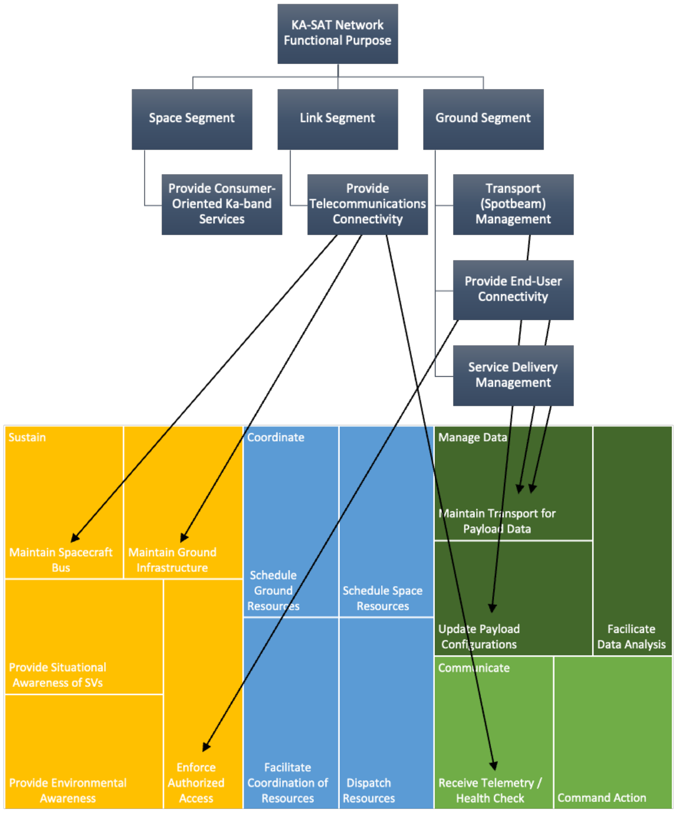

KA-SAT Network Functional Purpose
Space Segment
Link Segment
Ground Segment
Provide Consumer-Oriented Ka-band Services
Provide Telecommunications Connectivity
Transport (Spotbeam) Management
Provide End-User Connectivity
Service Delivery Management
Sustain
Maintain Spacecraft Bus
Maintain Ground Infrastructure
Provide Situational Awareness of SVs
Provide Environmental Awareness
Enforce Authorized Access
Coordinate
Schedule Ground Resources
Schedule Space Resources
Facilitate Coordination of Resources
Dispatch Resources
Manage Data
Maintain Transport for Payload Data
Update Payload Configurations
Facilicate Data Analysis
Communicate
Receive Telemetry / Health Check
Command Action

Fig. 10 - Describing KA-SAT Network Functionality in Common Space Activity Terms

With these questions illuminated for analysis, we use them to guide data flow identification. These data flows are the critical piece of information used in cybersecurity analysis to determine and integrate effective controls. Using the process demonstrated, when data flows are identified, they are inherently correlated to: the mission-specific language, mapping to common description language, and specific system components. This correlation provides important traceability for all included stakeholders to answer "why" security needs matter (mission objective) or "why" specific security controls are necessary for integration into a given component. This approach can align to and make use of artifacts from traditional space systems engineering development processes. Can such an approach provide unique insight into cybersecurity concerns for space systems ahead of need?

7. DATA FLOWS UNCOVER CYBER NEEDS

As mission-specific language is mapped to a common space operations vernacular, we are now presented with the opportunity to identify security needs to protect associated data flows. Recall the SSA function *task sensor* and its presence across multiple segments. Associated data flows may include space vehicle commands, acknowledgments (ACK) of the commands sent, or any commands/instructions (CMD) sent to the system components. Fig. 11 illustrates the process of uncovering what components are affected by the CMD and ACK data flows (red inset box). Four specific components (grey boxes) are identified, which then inherit data security needs associated with space mission operations.

Command and Control (C2) software, commonly known as Telemetry, Tracking, and Command (TT&C), is used across ground segments to initiate any command requests to space vehicles. After a command request has been submitted, it is received by a front-end processor (FEP). The FEP processes the command and any telemetry streams or packets such that it can now be received by radio frequency (RF) equipment (i.e., ground antennas). To protect against unauthorized eavesdropping, commands processed by the FEP are typically passed to an encryption/decryption device, otherwise known as the Crypto. Finally, the command is sent to a gateway, which acts as a direct interface with RF equipment.

Note: Expanding this analysis would require further detailed information on the pathway from the gateway to ground antenna, wireless infrastructure in place, the network architecture and physical configuration of the space vehicle itself, and beyond until the data's end destination. This more detailed information is omitted for conciseness and simplicity.

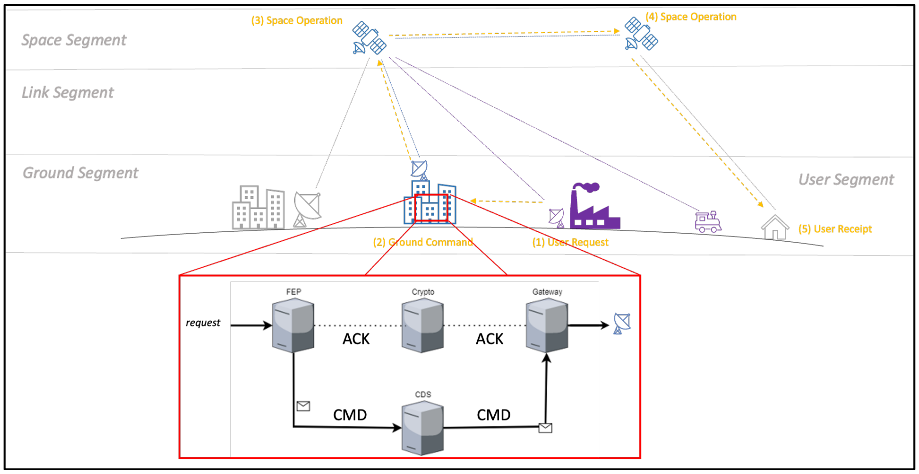


Fig. 11 – Example Subset Data Flow for Space Vehicle Commands

While this typical data flow may be well known to subject matter experts in the space domain, it is not always understood by traditional cyber forces because it involves specialized equipment and a unique architecture not commonly encountered. The decomposition of the data flow, which notionally represents requirements to fulfill a function, can now be presented to a cyber operator to provide a clear picture of what needs to be protected and why, completing the function-based identification of cybersecurity needs. In the case of the SSA function *task sensor*, cyber operators would be able to use the data flow to identify critical assets in the infrastructure that must be protected to ensure the success of a function and overall mission. As these needs can be described in terms cyber forces are likely to understand, they are enabled to leverage familiar tools and frameworks into the space mission system architecture.

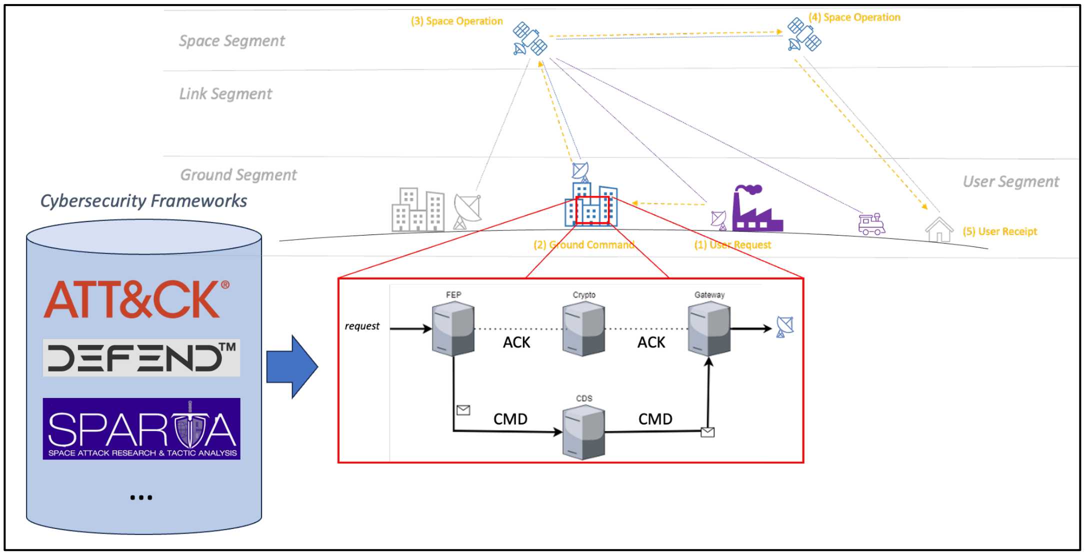
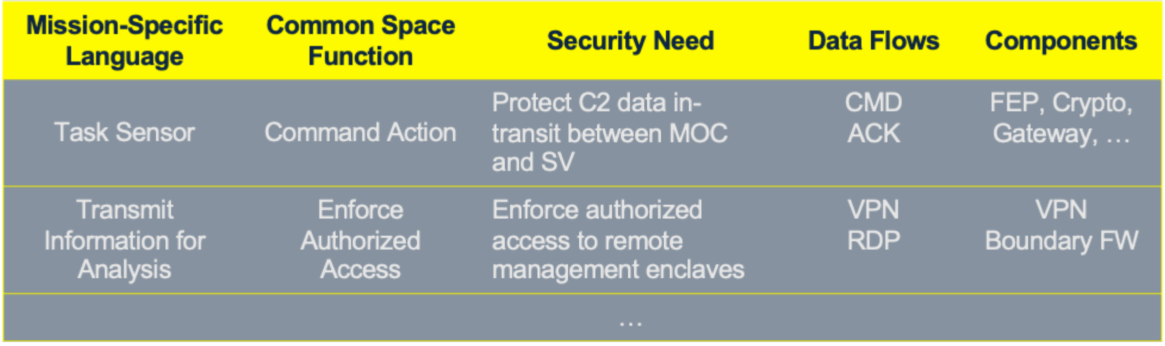


Fig. 12 – Applying Cybersecurity Frameworks to Protect SSA Functions

Table 3 below contains two example mission-specific functions translated to a common space function, associated data flows and components, and paired with their identified security need. This table is a concise collection of important correlated information provided by the approach presented. Using the output included, cybersecurity forces are provided with a clear tactical path forward to identify what specific cybersecurity controls can meet the intent of each need related to the necessary components associated with each identified data flow.

Table 3 - Cybersecurity Needs Aligned to Space Functions, Data Flows, and Components



Mission-Specific Language	Common Space Function	Security Need	Data Flows	Components
Task Sensor	Command Action	Protect C2 data in-transit between MOC and SV	CMD ACK	FEP, Crypto, Gateway, …
Transmit Information for Analysis	Enforce Authorized Access	Enforce authorized access to remote management enclaves	VPN RDP	VPN Boundary FW
		…		

With the inclusion of common space function terms, templates or collections of cybersecurity tools and techniques can be created for re-use across mission sets with similar functional operations. **This provides a direct path forward to address the limited re-usability of the many function-based approaches currently available for cybersecurity analyses as applied to unique mission sets like SSA.** Further, success criteria for each security need can be identified based on the functional purpose it supports for its associated space mission. Lastly, when paired with a threat model, this information describing cyber needs can be explicitly defined and validated against to ensure adequate coverage to support an organization's risk assessment processes.

8. CONCLUSION

The approach presented intends to simplify the challenging task of managing cybersecurity needs for increasingly complex and complicated space systems. A key enabler of this simplification is to first get all stakeholders communicating more effectively using a standardized function-based language. The output of the approach proposed provides a concise means to systematically describe and manage cybersecurity needs while accounting for mission-specific outcomes. The presentation of cybersecurity needs of space systems in this context allows cybersecurity forces to better comprehend and actively participate in the integration of cyber controls appropriate for space system operational objectives.

From this perspective, a common and shared approach to cybersecurity can serve as a conduit to increased collaboration and earned trust among space mission and cybersecurity forces in the domain. For a critical function like space situational awareness, the time is now to integrate foundational enabling concepts into current development efforts to ensure that cybersecurity needs of the future can be supported. Trusted data exchanges supported by SSA today are paramount to the development of a trustworthy and sustainable space domain of the future. Using concepts presented here can help to proactively identify areas of cybersecurity concern before final fielding reducing resources required for remediation.

Future efforts can further domain collaboration by developing and sharing standardized cybersecurity playbooks associated with cybersecurity needs associated with common activities cataloged. This concept would provide enormous value to the space domain in allowing for coordinated multi-stakeholder monitoring, protection, and response to cybersecurity issues – an advanced cybersecurity concept still being actively addressed in the significantly more mature Enterprise Information Technology domain. By building upon these approaches and tailoring them to the space domain, the space community can benefit from decades of lessons learned -- starting first with clear communications and more effective cybersecurity needs description.

9. REFERENCES

[1] GPS.gov, "What is GPS?," [Online]. Available: https://www.gps.gov/systems/gps/.

[2] N. Tsamis, R. Dr. Stilwell, H. Reed and N. Dr. Dailey, "Determining Operationally Relevant Space Cyber Information," in *Space Traffic Management Conference*, Austin, TX, 2022.

[3] N. Tsamis, R. Dr. Stilwell, H. Reed and N. Dr. Dailey, "Sharing operationally relevant space cyber information," in *AMOS Conference*, 2022.

[4] UNIDIR, "A Lexicon for Outer Space Security," August 2023. [Online]. Available: https://www.unidir.org/publication/lexicon-outer-space-security.

[5] "About IAC," 2022. [Online]. Available: https://iac2022.org/about-iac/iac-2022/.

[6] The International Academy of Astronautics, International Astronautical Federation (IAF) and International Institute of Space Law (IISL), "IAF TC26 STM Executive Summary," [Online]. Available: https://www.iisl.space/wp-content/uploads/2022/09/IAF-TC26-STM_EXECUTIVE-SUMMARY-17SEP2022-1.pdf. [Accessed September 2022].

[7] The MITRE Corporation, "MITRE ATT&CK®," [Online]. Available: https://attack.mitre.org/.

[8] The MITRE Corporation, "MITRE DEFEND™," [Online]. Available: https://d3fend.mitre.org/.

[9] The Aerospace Corporation, "SPARTA - Space Attack Research and Tactic Analysis," [Online]. Available: https://sparta.aerospace.org/.

[10] M. Zuniga and M. Janson, "PIVOT: An approach for System-of-System Attack Path Analysis," The MITRE Corporation.

[11] M. Colonel Monroe and J. Olinger, "Mission-Based Risk Assessment Process for Cyber (MRAP-C)," December 2020. [Online]. Available: https://www.itea.org/wp-content/uploads/2021/02/ITEA_Journal_Dec20-Mission-Based-Risk-Assessment-Process-for-Cyber-MRAP-C.pdf. [Accessed August 2023].

[12] L. Laursen, "Satellite Signal Jamming Reaches New Lows," May 2023. [Online]. Available: https://spectrum.ieee.org/satellite-jamming. [Accessed August 2023].

[13] U. Col Mark A. Baird, "Maintaining Space Situational Awareness and Taking It to the Next Level," September 2013. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA625687.pdf. [Accessed August 2023].

[14] USSF SpOC , "Space Based Space Surveillance," [Online]. Available: https://www.spoc.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/2381700/space-based-space-surveillance. [Accessed August 2023].

[15] N. Boschetti, N. Gordon and G. Falco, "Space Cybersecurity Lessons Learned from The ViaSat Cyberattack," in *ASCEND*, Las Vegas, NV, 2022.