IAC-24-D5.4.11
57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES
Cybersecurity in space systems, risks and countermeasures

Authors: Mr. Nick Tsamis
The MITRE Corporation, United States, ntsamis@mitre.org
Mr. Harvey Reed
The MITRE Corporation, United States, hreed@mitre.org
Dr. Ruth Stilwell
Aerospace Policy Solutions, LLC, United States, office@aerospacepolicysolutions.com

THE ROLE OF LOCALIZED COMMUNITIES OF INTEREST IN STANDARDIZING COORDINATED RESPONSES TO SPACE CYBERSECURITY THREATS

Abstract

This paper explores the development of a local communities of interest (COI) cybersecurity standardization approach for the space domain that focuses on cyber resilience within and across COIs. The authors propose a paradigm shift from individual responsibility to respond to cybersecurity threats to a collaborative information sharing based approach to address common cybersecurity needs. This approach examines the space domain through a "neighborhood norms" (COI-centric agreement to normal behavior), cybersecurity-centric lens.

Here, localized COIs (LCOI) refer to stakeholders unified by common cybersecurity challenges and objectives across common operations performed within the space environment, e.g., Space Traffic Management (STM). For example, a community associated with providing Space Situational Awareness (SSA) to support STM may share intelligence on cyber threats and collaborate on countermeasures specific to SSA operations. This local COI model may be exportable to other stakeholder groupings with common operational concerns.

This approach aligns with USSF "Partner-to-Win" strategy, emphasizing strategic partnerships for enhanced cyber defense within the space domain. The COI model fosters a multi-entity approach to space cybersecurity, sharing the burden of responsibility for threat detection and response. Further, the approach enables optimized, community-specific solutions ensuring cybersecurity concerns are accounted for and addressed across affected community participants, ensuring the magnitude of data and number of parties with access are operationally relevant.

The paper will outline how these communities can categorize and align around foundational cybersecurity challenges, enabling stakeholders with common goals to address shared threats. It will also introduce the role of decentralized technical capabilities to facilitate the secure information sharing infrastructure necessary to build trust within and across these communities.

This paper further posits that equipping COIs with decentralized technical capabilities provide a means to securely manage responses to cybersecurity threats against complex space operations (e.g. STM). This enables COIs to maintain data and workflow integrity and execute consistent and traceable actions using community-developed response playbooks.

COIs using this decentralized infrastructure are empowered by efficient information sharing, including coordinated threat intelligence. This in turn allows for coordinated mitigation of impacts arising from in-progress cyber-attacks. The decentralized infrastructure facilitates information sharing using a Minimum-Viable Information (MVI) approach to increase the probability and utility of information being sharing within and across COIs. Sharing MVI sets allows individual members within localized COIs group to take informed and practical actions to secure their assets and contribute to the overall resilience of community needs. This coordinated defense approach promotes new normal behaviors across individual stakeholders in response to cyber incidents, resulting in space domain security through community vigilance and response.

Keywords: information sharing, cybersecurity, operational playbooks, minimum viable information, community of interest, security cooperation

1. Introduction

As the domain continues to grow, congestion and debris increases as well, and with it, the risk of conjunction between operational space objects. This requires increased interaction between operators, and due to shrinking time scales for decision-making, an increased reliance on automated systems. While conjunction risk can grab public attention and resources, it is important to take a broader view of space operations in general, and cybersecurity response in particular. Further, the nature of space operations is becoming more multi-party, including a diverse variety of stakeholder organizations (refuel, debris removal, etc.) and are thus complex. These complex interactions require trusted information sharing to perform the operation, and increases the importance of cybersecurity deterrence and response, which can in turn also use trusted information sharing for notifications and executing playbooks.

A diverse variety of stakeholder organizations and their actors must rely on information from external sources in their decision making. This challenges the existing paradigm for efficient decision making. For example, in a traditional conjunction analysis model, the operator is dependent on sensor-based information about a debris object on a ballistic trajectory. If the sensor information is accurate, the collision risk can be calculated for the operator to make a maneuver decision. When we consider conjunctions between operational space objects, they are not necessarily following a predictable ballistic orbit, and more information is needed including the intent and capability of the operators of both objects. As operations in space become more complex, the amount of information associated with these events also increases. Overcoming barriers to information sharing is essential to safety and security in an increasingly complex space domain. A Communities of Interest (COI) structure for information sharing can be instructive and useful in developing repeatable patterns of organization and information technology to overcome this barrier.

The concept of developing COIs is well-established in various academic fields from sociology to political science used to align stakeholders and foster collaboration, including the means to influence and organize behaviors within groups that align to common goals or a shared identity. This paper introduces the concept of Localized COIs (LCOI) to capitalize on the construct of self- organization in smaller (i.e. 'localized') subset communities with shared interests and demonstrated trust. This results in increased trust in the information shared within these focused LCOIs compared to that attainable in a single, larger and more diverse, community. In addition to increasing trust, the Minimum Viable Information (MVI) approach, introduced in Section 4, serves to lower the risk of sharing information regarding privacy and intellectual property, within and across LCOIs.

Borrowing from the closely related concept of Communities of Practice (COP) (Wenger, 1998), the use of these communities provides a useful paradigm to align and coordinate diverse varieties of stakeholder organizations in the increasingly complex space domain. This COP model enables the set of stakeholders to organize and align common operational and cybersecurity needs, encourage cybersecurity awareness, and adopt effective cybersecurity response practices. Specific differences exist between COPs and other communities, including COIs. However, for the purposes of this paper, we treat the foundational concepts as broadly applicable without distinction. In Cataldo's review below, three structural elements referenced are "inherent" to COPs and form the basis for the LCOI definition in this paper:

> "domain: the common ground and sense of shared identity; community: the people who care about this domain; and practice: the specific knowledge a community develops, shares and maintains" (Cataldo, 2009)

When applied to cybersecurity needs in the space environment, the domain (the space environment, itself) and community (space-faring stakeholders participating in similar activities [e.g. space sensing, or rendezvous]) are both clearly defined and well understood. The third element, practice (or interest), is the topic of this paper's further development. Increased understanding and definition of trusted information sharing, use of trusted information security to support cybersecurity needs, and effective cybersecurity knowledge curation will serve to benefit individual stakeholders and foster an overall increase in space domain security.

The space domain is in a period of rapid change that extends beyond the increasing number and size of satellite constellations. We are rapidly moving from complicated operations to complex operations requiring interactions between diverse variety of stakeholder organizations. Emerging trusted information sharing, operational and knowledge models, and cybersecurity playbooks can be useful in addressing increasing challenges, including physical threats and cyber threats which affect defined LCOIs.

2. Value Proposition

This paper defines LCOI generally and extends the concept into a Cyber LCOI (or potentially a set of Cyber-enabled LCOIs). Since multiple new concepts are being introduced to achieve a Cyber LCOI, the progression of value-add steps is described below, showing how the concepts build upon another. These concepts are framed together to present an overall value proposition. The general LCOI construct can facilitate trusted information sharing to reduce risk and enable complex space operation outcomes, through updated tools for information discoverability, understandability, and data integrity to achieve improved domain-wide Defensive Cyber Operations (DCO) mission outcomes.

The LCOI has two Implementation Aspects:

LCOI technical support for improved information sharing, increasing trust in data and information for all participating stakeholders, and

LCOI social and governance support to both:

- define and use precise shared language (ontology), and
- define, adopt, and execute playbooks during cybersecurity incidents.

This paper covers the above topics in sections as follows:

Complex Space Operations: operations with a diverse variety of stakeholder organizations, highly dependent on trusted information sharing, requiring shared awareness where critical actions (e.g., maneuvers, grappling, refueling) are potentially high risk, and dependent on timely trust in information sharing.

Technical Challenges to Cybersecurity Information Sharing: define technical aspects of trusted information sharing in the construct of a general LCOI.

Social Challenges to Coordinated Decision Making: define social aspects of trusted information sharing in the construct of a general LCOI. For example, agreement of forming and using local language (ontology) in trusted information sharing.

Maturity Model for Cybersecurity Information Sharing: define the range and extent of trusted information sharing required in a general LCOI to support cybersecurity defensive operations in a Cyber LCOI, and in coordination with other LCOIs.

Standardizing Responses to Cybersecurity Threats in the Space Domain: define the scope and use of Cyber LCOI to operationalize Cyber Playbooks, mitigating adversary actions and coordinating effects during a cyber incident.

3. Complex Space Operations

Complex operations are defined in this paper as operations in orbit (or transiting) in which a diverse variety of stakeholder organizations participate and require coordination beyond basic space situational awareness to accomplish. Each stakeholder organization makes independent decisions and requires trusted data and information to inform decision making, in coordination with other relevant stakeholders.

In a complex operation, when the mission requires coordinated action, the contributing action of each stakeholder must be based trusted information that all relevant stakeholders are sharing. This forms a dependency of that action on prior decisions, and further to prior input data to the decision. In cases such as cyberattacks of complex space operations, the tempo of trusted information sharing is rapid, requiring transitive trusted information sharing, and understanding of the information by other stakeholders to be similarly rapid. Thus, LCOI language elements (ontology) must be well-defined -- a critical function of the LCOI social aspects explored in detail later.

Some examples of complex space operations may include:

(a) docking between objects for the transfer of humans, cargo, and other resources,
(b) on orbit servicing to extend mission life through repair and refuel,
(c) orbital transportation services to remove or reposition objects,
(d) active debris removal, and
(e) recovery of recyclable materials.

These example operations represent a subset of what is referred to in the U.S. as In-Space Servicing, Assembly and Manufacturing (ISAM) is described by the U.S. National Science and Technology Council as:

> *ISAM capabilities enable specific activities, in the areas of servicing—the in-space inspection, life extension, repair, or alteration of a spacecraft after its initial launch, which includes but is not limited to: visually acquire, rendezvous and/or proximity operations, docking, berthing, relocation, refueling, upgrading, repositioning, undocking, unberthing, release and departure, reuse, orbit transport and transfer, and timely debris collection and removal; assembly—the construction of space systems in space using pre-manufactured components; and manufacturing—the transformation of raw or recycled materials into components, products, or infrastructure in space.* (Executive Office of the President National Science & Technology Council, 2022)

In May 2022 in the House Space and Science Subcommittee, Dr. Moriba Jah testified about the emergence of ISAM complex space operations[1] (Jah, 2022):

> *"The US White House recently delivered a strategy on In-Space Servicing, Assembly, and Manufacturing. The need for continuing supervision could not be more important than this developing space sector. In order to meet the needs of this community, there must be an unambiguous and distributed immutable ledger of who did what to whom when and where. As of this very testimony, I would challenge any government to demonstrate that it is currently capable of delivering such a capability. More complaints of harmful interference, damage, and threats will be raised whilst we are left ill prepared to assemble the evidence required to assess and quantify space events and activities."*

Jah's testimony emphasized the importance of both trusted information sharing and information provenance and archiving to support ISAM, which is a broad category of complex space operations.

From Complicated to Complex

The increasing interactions between growing numbers of space stakeholder organization objects move the environment from complicated to complex.

Complicated is used here to describe the current state of the environment due to the difficulty of tasks being performed within the domain. A key characterization of this complicated environment is that predictable activities can be largely managed and coordinated by a single stakeholder organization, through simple rule-based interactions.

In a near future however, complexity becomes a defining characteristic of the space domain.

Complex refers to increased system and stakeholder organization -level interactions occurring at scale and pace such that the interactions cannot be easily defined by a single organization by simple rules and expected results. The result of this complex environment is potentially unpredictable emergent stakeholder and system behavior.

Compounding the complexity of the operations, is the diverse numbers and types of stakeholders. The Cold War space age was dominated by two State actors, the US and the USSR, these two countries were responsible for 93% of all objects launched into space through 1990 and only 4% were commercial (Harrison, Cooper, Johnson , & Roberts, 2017). By 2021, the global space industry included over 10,000 companies and 130 State space agencies (Brockmann & Raju, 2022) and the commercial sector represents the majority of space objects; by 2023 over 90% of spacecraft were commercial (Bingen, 2023). This complex and diverse environment requires structure to ensure that trusted, understandable, and actionable information gets to the appropriate decision makers across stakeholder organizations.

4. Technical Challenges to Cybersecurity Information Sharing

Complex operations pose unique challenges to sharing trusted information. The challenges are exacerbated by the unique physical, technical, and social distributed and decentralized characteristics of space as an operating domain, for example the diverse variety of stakeholder organizations participating in complex space operations.

[1] Underlined emphasis is that of this paper's authors, and not of Dr. Moriba Jah

Space is physically a distributed and decentralized domain occupying more physical space than any other domain, with frequent interactions, under the authority of multiple governance structures, including diverse missions and interests. Stakeholder organizations are distinct, their space objects are distributed over space and time, and there is no central authority for operations. In this environment, competing perspectives can lead to conflicting interests among stakeholders. The inherent lack of centralization of the space domain adds challenges regarding data integrity, non-repudiation, and provenance, carrying significant risk associated with trust between stakeholders. Two key challenges are presented here related to data integrity and information provenance.

Data Integrity and Information Provenance

The first challenge is that there is no established uniform way to determine if information shared is genuine and from the purported sender. Sharing high priority information, including for cybersecurity purposes, frequently informs critical decision making, and follow-on actions, reinforcing the need for trust and data integrity.

Second challenge is that, in addition to uncertain data integrity of individual pieces of shared information, there is no established uniform way to determine information provenance, which tracks the use of shared information through decisions, actions, and outcomes. For example, in a cybersecurity response, if a decision to restrict certain accounts is received by one party who does restrict the accounts, leading to specific outcomes -- can the involved stakeholders trace the sequence of events back to source data which informed the original decision to restrict accounts?

Thus, both data integrity and provenance of information is important. Further, the ability to understand information is paramount if information is to be used to inform decisions and take actions. Fig. 1 overviews the complex operation of refueling and the importance of not only data integrity but also event precedence linking and provenance of information.

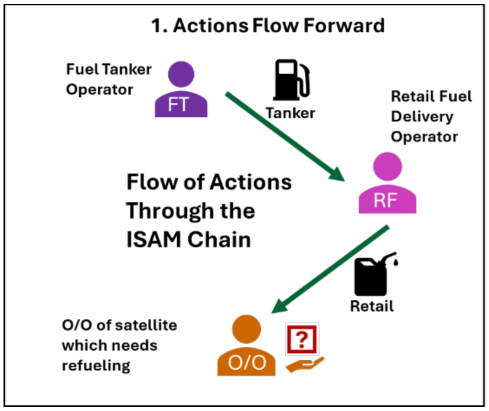
1. Actions Flow Forward
Fuel Tanker Operator
FT
Tanker
Retail Fuel Delivery Operator
RF
Flow of Actions Through the ISAM Chain
Retail
O/O of satellite which needs refueling
O/O
?

Fig. 1. Complex Space Information Sharing Sequence

In Fig. 1, in the complex space operation of refueling, the stakeholders are the Fuel Tanker Operator, Retail Fuel Delivery Operator and the Owner/Operator (O/O) of the space vehicle. Information is exchanged, for example the O/O calls for fuel from the fuel retailer who may in turn need to call for a “top off” from the tanker operator. After the call for fuel is issued (trusted information sharing), decisions are made, and actions are executed (fuel top off and then retail delivery) as depicted by the arrows. Ideally, actions will be performed in accordance with decisions made. Provenance of information and actions enable outcomes to be understood in context.

Fig. 2 illustrates the query activities required to traceback actions, to understand the chain of events, and the information sources used in those queries and actions in the complex space operation.

To be effective in a traceback, each piece of information needs to have provable data integrity, with the provenance sequence of information, decisions, actions, and outcomes must be clear, and the predecessor links must also have provable data integrity. At each step, the information must be accessible and understandable.

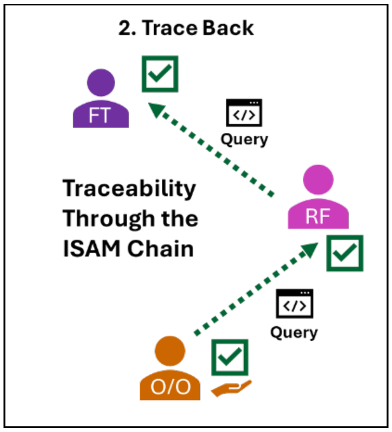

Fig. 2. Tracing Actions and Information Provenance

If stakeholders in a complex space operation cannot understand what happens in both successful and unsuccessful operations (information, decisions, actions, outcomes) then stakeholders will not be prepared to defend actions, assume and accept liability, and more. The scenario above, and potential outcomes supports Jah's cautionary testimony (Jah, 2022):

> *"As of this very testimony, I would challenge any government to demonstrate that it is currently capable of delivering such a capability. More complaints of harmful interference, damage, and threats will be raised whilst we are left ill prepared to assemble the evidence required to assess and quantify space events and activities."*

The trusted information sharing described above requires social agreement across the relevant stakeholders. The actionability of information is localized to stakeholders who participate in and must understand the relevant information. This localization of semantic understanding is the basis of the LCOI construct.

Organizing Information Sharing and Provenance in LCOIs

As introduced above, the LCOI is a venue for stakeholders to self-organize in subset communities with shared interests. This enables relevant stakeholders to decide on the terminology syntax and semantics of their shared information. Moreover, LCOIs provide a construct to share information about technical implementations.

This technical approach is introduced in the concept Space Information Sharing Ecosystems (SISE) and described in "Sharing Operational Risk Information in the Space Domain to Facilitate Norms." (Reed, Stilwell, Weedon, Dailey, & Tsamis, 2021). The premise is that LCOIs (ecosystems) provide a means for stakeholders to share the infrastructure of information sharing and to also agree on data definitions and ontologies. Note that sharing infrastructure in an LCOI (ecosystem) is a means to address the fact that a distributed and decentralized domain such as space acknowledges difficulty in achieving domain-wide concurrence using a legacy centralized approach. However, agreement in a smaller scale (LCOI) may be possible.

In the related distributed and decentralized domain of manufacturing supply chain, the NIST (National Institute of Standards and Technology) effort "Manufacturing Supply Chain Traceability with Blockchain Related Technology" (Pease, Stouffer, Reed, & Granata, 2023), the authors describe a similar concept of ecosystems which:

1. Enable stakeholders to self-organize as an ecosystem (LCOI) and define their shared language and types of information to share, events to record, and link applicable information in order of precedence.
2. Enable stakeholders to share information using interoperable infrastructure. Using blockchain technology for information sharing provides the highest degree of data integrity and thus trust in the data.
3. Enable ecosystems (LCOIs) to exchange information and provenance links across ecosystems.

Thus, the trusted information sharing, and provenance challenges of distributed and decentralized domains such as supply chain and space, can be mitigated through the use of LCOIs to organize stakeholders, and interoperate across LCOIs. Fig. 3 illustrates the conceptual relationship between reusable infrastructure (orange) and the independent functional use of that infrastructure to deliver information sharing contents (green). This figure is included to illustrate the role that the infrastructure plays in providing a trusted means for actual contents of information shared; de-coupling information sharing infrastructure needs vs content needs helps manage the complexity of future operational information sharing instantiations.

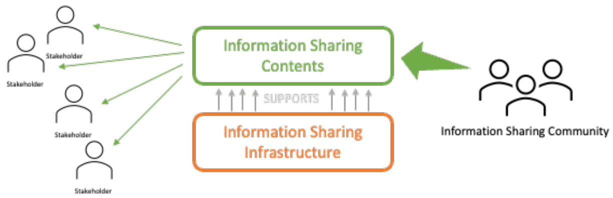
Stakeholder
Stakeholder
Stakeholder
Stakeholder
Information Sharing Contents
SUPPORTS
Information Sharing Infrastructure
Information Sharing Community

Fig. 3. Information Sharing Infrastructure vs. Contents

Challenges with Centralized Approaches

Thought leadership on information sharing in the space community has evolved over time. Some early concepts included a unified (centralized) “data lake” that would make large quantities of information available to large numbers of participants, but to date have not been realized.

Resistance to centralized information sharing ranges from the protection of intellectual property and privacy data to costs of providing the data to external sources. An effective trusted information sharing construct must deliver value to stakeholders that either or both provide or receive the information.

Centralization is not an effective information sharing strategy for the distributed and decentralized space domain. Thus, LCOIs may provide an effective model for trusted information sharing

a. agreements for language and data contents and
b. trusted information sharing supporting technical infrastructure.

Specializing LCOI (ecosystem) trusted information sharing further to cybersecurity is described in “Sharing operationally relevant space cyber information” (Tsamis, Stillwell, Reed, & Dailey, 2022). Here, cybersecurity information sharing emphasizes speed of sharing. Cybersecurity information useful for sharing may be large in magnitude, but also has a need for low-latency analysis (decision-making) and trusted information exchange to meet objectives.

Three Key Barriers

Tabletop exercises conducted by the Space ISAC[2] in 2021 highlighted specific challenges to information sharing that centered around data trust and protection. Three key barriers were identified:

1. Misunderstanding of information sharing constraints
2. Perceived low value of sharing information
3. Low confidence and willingness to trust external data.
(Tsamis, Stilwell, Reed, & Dailey, 2022)

Four Tenants of Cybersecurity Operational Relevance

While these barriers were systemic across many types of information sharing, cybersecurity information sharing limitations were specifically exacerbated due to perceived sensitivity, magnitude, and timeliness of information necessary to share. These concerns are repeated in other venues and reinforced in the AIAA Technical Collaborative Panel at AIAA ASCEND 2021[3]. The panel identified key takeaways focused on the need for actionable data from systems designed for decision support (The MITRE Corporation, 2021). Models developed to address these concerns in the cyber security community may be relevant other information sharing ecosystems. Four Tenants of operational relevance developed in the paper, Determining Operationally Relevant Space Cyber Information, illustrate how local COIs can serve to transform potentially large amount of data into information that is useable within and across COI’s (Tsamis, Stillwell, Reed, & Dailey, 2022):

Comprehensibility – information shared must be easily understood by the consuming organization. Removing the need for organizations to interpret intent enables organizations to comprehend shared information more easily. Performing this analysis before sharing maximizes efficiencies gained.

Applicability – all shared information will not be applicable to every consuming organization. Consideration must be taken prior to dissemination to equip organizations with the ability to determine what is or is not applicable for resource allocation.

Timeliness – information must be presented for action within appropriate time scales. Different data elements present risk or operational impact on different timelines. It is imperative that collection, analysis, and dissemination of shared information occur within the time constraints of possible impact based on the information under consideration.

[2] https://spaceisac.org/

[3] https://www.ascend.events/

Actionability – the value of information is ultimately limited by the actions it can support in an operational setting. Consuming organizations must know how to understand, and what to do with shared information. Providing sufficient information necessary to make decisions and execute requisite actions in an unambiguous fashion empowers organizations to fully respond to cyberattacks.

Making use of these Four Tenants, the Minimum Viable Information (MVI), comprises a set of information that is both:

1. minimally sensitive (maximizing stakeholders' willingness to share it) and
2. relevant to the parties it is shared with (substantive perceived value of the information received)

When enabled by shared infrastructure that provides a means to increase stakeholder trust and confidence in this information, a solution to address the three key barriers arises. Applied in such a manner, the MVI's agreed standardization and pre-definition of operationally relevant information elements allows stakeholders to collaborate effectively at the speed and scale necessary for cybersecurity information sharing to respond to cybersecurity incidents. This approach represents a significant change to the current status quo of information sharing methods in the domain. However, a Cyber LCOI and use of MVIs provides a scalable and achievable means to address future challenges presented by cyberattacks in increasingly complex space operations.

5. Social Challenges to Coordinated Decision Making

In addition to technical challenges, social constructs also present legacy barriers to overcome to inform coordinated operational decisions. Operational success for complex space operations requires coordinated decision making. This requires trusted, correct, and understandable operational details be shared for coordination. Coordinated decision-making among stakeholders remains an inherently social element.

As LCOIs are established, they can serve as effective tools to not only address technical aspects of information sharing through shared infrastructure, but also manage social challenges through governance. Forming language and practice agreements within an LCOI, may be more straightforward due to both a smaller number of stakeholders than the whole space domain, and a high degree of relevance by the interested stakeholders.

As domain operational complexity rises, stakeholders become more reliant on information sourced from and processed by other stakeholders. The distributed and decentralized nature of the shared space environment and of the complex space operations within, requires mechanisms be in place to efficiently exchange trusted and traceable information throughout the decision chain among participants to facilitate social collaboration. Without the assurance of traceable information integrity (provenance), social interactions are strained, stifling productivity and innovation in the space domain. Some key social considerations, and how cybersecurity can play a role, to be addressed by the LCOIs are discussed below.

- National security interests play a significant role in decision-making considerations. As countries prioritize the protection of their space assets and the prevention of espionage or sabotage, emphasis is placed on stringent cybersecurity rules. However, it can also lead to reluctance in sharing sensitive information with other nations, potentially hindering collective efforts to address cybersecurity challenges. Appropriate rules and governance structures to protect national security interests can be implemented while also considering increased domain security via the promotion of non-sensitive information sharing.
- Economic and commercial interests are another critical factor to consider, as the space industry increasingly comprises commercial entities. Companies are inherently de-motivated to share information it if presents any risk to protection of investments or the future sustainability of business operations. This desire to maintain competitive advantages and protect proprietary data can result in resistance to information sharing, complicating efforts to facilitate a trusted and collaborative environment. Cybersecurity and information assurance play an important role in finding the balance between what information may be broadly useful to an LCOI or the entire domain, while still respecting individual commercial stakeholder interests.
- Cultural and political differences between stakeholders may influence decision-making and affect willingness to rely on external

information. Diverse perspectives on and expectations of governance, proprietary data, privacy, and data protection can lead to varying levels of trust and willingness to collaborate. Incompatibilities in these differing levels may present a social barrier, impeding collaboration, or conversely, a new set of perceptions to learn from. Considering the potential implications here may be important to adequately incentivize and promote benefits across cultural and political boundaries.

- Differing levels of technology maturity among stakeholders may impact decision-making. It may be significantly easier for organizations that have achieved technologic parity for space operations to collaborate on decisions and actions in the domain. Alternatively, disparities in technology maturity may serve to reduce collaboration potential. Bridging this gap requires consideration of approaches that respect the unique needs and current capabilities of each stakeholder.

Diplomatic arrangements between State actors may be insufficient to address the complexities of a new space age. The emergent polycentricity (localized governance, such as LCOI) in space can serve as an effective tool to organize how data is shared and transformed via decision-making into actionable information shared with external entities and help overcome perceived barriers to information sharing. Established LCOIs are well-suited to address social challenges due to the self-organization of its participants that share common interests, risks, and threats.

6. Maturity Model for Cybersecurity Information Sharing

As LCOIs are established within the space domain and intra and inter -LCOI community collaboration develops, community needs for trusted information sharing, including cybersecurity responses can be addressed. Over time, LCOI participants increase willingness to trust, share, and uphold responsibilities set within the community. A maturity model is proposed, illustrated in Fig. 4, to provide a means to characterize the various states of coordination occurring both within individual LCOIs and in context of the entire space domain.

Maturity Model

Level 1. **Data for exchange is identified** – individual stakeholders enumerate and catalog data that is beneficial for exchange within an LCOI.

Level 2. **Data is exchanged within LCOI** – LCOI stakeholders establish protocol and technical means to exchange identified data. Trust relationships begin to develop within LCOI at this stage.

Level 3. **Information is shared within LCOI** – data is analyzed into operationally relevant information, then shared via traceable means (provenance) within the LCOI. Increased situational awareness and coordination within an LCOI begins at this stage. Decision-making begins to incorporate multiple perspectives from within the LCOI.

Level 4. **Information is shared across LCOIs** – information sharing is extended beyond a single LCOI. Collaboration and coordination across LCOIs, with provenance, are established and decision-making may be readily shared with or incorporate feedback from stakeholders in other LCOIs. Collective knowledge across the space domain is leveraged to address broad challenges facing the entire space domain.

Level 5. **Viable information is shared globally** – global situational awareness is possible with the provision of critical insights and necessary information to all space stakeholders. Standard behaviors begin to arise on a global scale within the space domain.

An example illustration is provided to depict these levels of maturity and how they relate to one another. It is important to note that the choice of illustration here is not intended to convey a drive towards, nor desire for full space domain centralization. Rather, the shape is used to convey that with increasing levels of maturity, decreasing magnitudes of information are needed for sharing across larger audiences. This is a natural result of federated information sharing across LCOIs.

For example, an individual LCOI's information sharing needs will be larger within the LCOI, than information sharing needs between two distinct LCOIs. In contrast, a single centralized authority over the entire space domain may not be a likely nor desirable means to implement such an information sharing construct. This is because space domain wide agreements, both technical and social, are not likely.

A federated approach can incrementally grow based on demand, driven by interested stakeholders.

Further, with this LCOI approach, individual stakeholder's can remain autonomous over their own actions and still maintain effective information exchanges throughout all maturity levels.

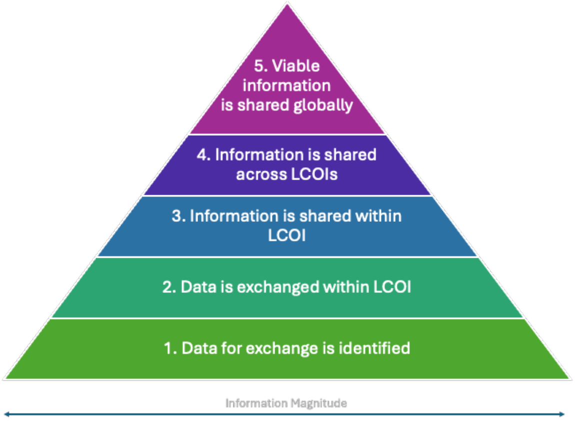
5. Viable information is shared globally
4. Information is shared across LCOIs
3. Information is shared within LCOI
2. Data is exchanged within LCOI
1. Data for exchange is identified
Information Magnitude

Fig. 4. Cybersecurity Information Sharing Maturity Model

Across the various levels of the maturity model, key transition points are identified.

Between Levels 1 - 2 - Compatibility and interoperability is first addressed. Large magnitudes of data are pared down to emphasize specific data exchange needs. Individual LCOI coordination is enabled after this transition.

Between Levels 2 - 3 - data is subject to standardized analysis means, yielding output products presented to, and agreed upon by individual LCOIs. Inter-LCOI coordination is possible beyond this transition point.

Between Levels 3 - 4 - synthesis and information integration occurs, providing insights across LCOIs that would not be readily understood by a single LCOI alone.

Between Levels 4 - 5 - advanced integration methods are employed to ensure all space-faring stakeholders are provided a minimum amount of information to meet expected duties of participating in the global space domain. Domain-wide collaboration is a possibility.

From the five levels of maturity presented above, three distinct phases emerge (reference Fig. 5), illuminating the intent and outcomes associated with their aligned phases.

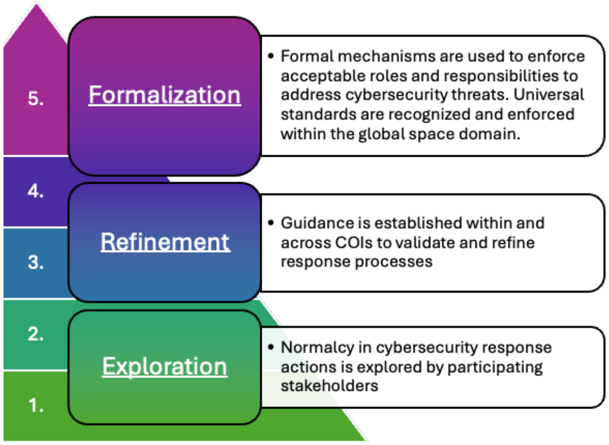
5.
4.
3.
2.
1.
Formalization
Refinement
Exploration
• Formal mechanisms are used to enforce acceptable roles and responsibilities to address cybersecurity threats. Universal standards are recognized and enforced within the global space domain.
• Guidance is established within and across COIs to validate and refine response processes
• Normalcy in cybersecurity response actions is explored by participating stakeholders

Fig. 5. Three Phases Organizing the Maturity Model

It should be noted that positive outcomes and benefit to individual sets of stakeholders and LCOIs are realized across all levels of maturity, not only at Level 5. Simply agreeing to what type of data is useful for exchange and implementing that exchange (Level 2) may represent a significant enhancement over the current status quo collaboration level among those same participants today.

7. Standardized Responses to Cybersecurity Threats in the Space Domain

To illustrate how this maturity model can be applied tangibly, the definition and evolution of Operational Playbooks -- that contain knowledge about defensive cybersecurity actions -- is explored below.

To support coordinated actions to against cyber threats in the space domain, response activities can be pre-planned (before they are needed) and tested to increase accuracy and maturity over time. While Operational Playbooks are an advanced topic for collaboration in the domain, work across all levels of maturity is necessary. Specific stakeholder activity and outcomes are outlined across the three phases.

- In the ***exploration*** phase, pre-planned activities may be specific to an individual organization and codified as an Operational Playbook containing a set of standard operating procedures (SOP). This SOP is specific to the organization and does not consider or include perspective from other similar organizations. Large opportunity exists in this phase to identify patterns, similarities, or redundancy across SOPs leveraging perspective and input from external organizations performing similar space activities or sharing cybersecurity needs.

- As Operational Playbooks undergo ***refinement*** and common information elements are identified and agreed upon across stakeholders, abstract response plans are shared across organizations to define "normal" actions within or across LCOIs. Specific details about exact tactical actions (i.e. SOP) taken are likely to remain exclusive to individual space operators, however the Operational Playbook's intent and outcomes will remain consistent and align across organizations and/or LCOIs. Operational Playbooks may both require specific Space Cyber MVI inputs to initiate and/or define specific output information (a separate MVI set) to be shared with other required stakeholders.
- Finally, when significant refinement has occurred and LCOIs agree to common guidance to respond to common cybersecurity threats, that guidance can undergo further ***formalization***. In this phase, a recognized universal set of standards and enforcement means can be identified for stakeholders to achieve and abide by. A high level of synchronization is required among all space stakeholders to recognize and maintain appropriate responses to cybersecurity threats. Individual organizations may uphold specific responsibilities based on their required role and rely on partner stakeholders to do the same.

Beyond the exploration phase, maturity is achieved to include multiple stakeholders either within or across LCOIs. At this point, Operational Playbooks become a set of directions that both:

1. guide individual stakeholders on the explicit actions they can take based on specific input conditions (e.g. actively evicting a persistent cyber threat threatening the availability of a C2 link) and
2. coordinate and synchronize discrete actions across stakeholders to achieve outcomes desired by the LCOI(s).

In the refinement phase of Operational Playbook development, the LCOIs define and agree to overall structure or "templates" that can be applied and useful to organize active cyber defense response actions for all LCOI participants.

Activities Before and During a Cyber Incident

The concepts discussed above have specific roles across the lifecycle of a cyber incident. The following section (overviewed in Fig. 6) provides a categorization of what actions are necessary: before ("T minus 0"), at ("T=0"), and in response to ("T plus 0") an active cyber incident.

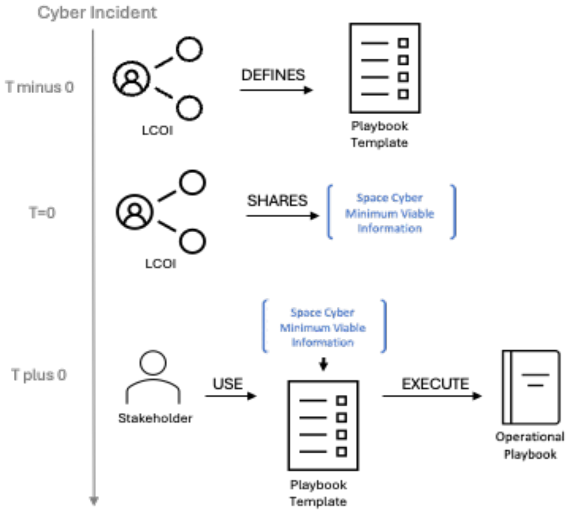

Fig. 6. Playbook Actions Before and During a cyber incident

A brief narrative scenario will be carried throughout the section below to illustrate tangible detail for reference. In this artificial incident, a cyber adversary is detected to be collecting information for use to execute a future denial of service attack via satellite communications availability denial.

<u>T minus 0</u> - Playbook Templates within LCOIs are defined ahead of need ("T minus 0") to effectively plan and coordinate the main components of cybersecurity defense response before it is required. At time of an actual incident ("T=0"), stakeholders will be actively managing and responding to the incident – having a plan on what actions to take already defined at this point affords defenders a significant aid by allowing for testing and validation of templates' assistance. Guidance captured in templates will define agreed-upon objectives and conclusions deemed as normal and expected cyber defense response actions based on the specific threat or incident they intend to counter.

A playbook template for the narrative scenario would cover information about, for example, how to gracefully failover communications to secondary (or more resilient) methods in the event of realized degraded availability for primary means of communication. Specific cybersecurity concepts may include establishing and exercising cryptography, transport, and application protocols independent of the primary channel of communications to provide a means of cyber diversity.

T = 0 - MVI elements are ideally shared at, or just after, a cyber incident is detected. A shared MVI will contain sufficient detail to allow a broad set of organizations in an LCOI (and related federated LCOIs as needed) to understand critical details about the incident to explore if they may also be affected (currently or at risk) by the incident. With templates already defined, the information shared here does not need to include the basic plan (templates) for stakeholders to follow.

The table below contains some sample elements of what information would be useful to include in the MVI including the specific space service affected, specific space courses of action to make stakeholders aware of, and detailed references to frameworks that multiple stakeholders can use for additional information. Included for example here are MITRE ATT&CK®[4], The Aerospace Corporation's SPARTA[5], and MITRE D3FEND™[6] cybersecurity frameworks.

The MVI elements are concise, provide limited sensitive detail but still allow stakeholders to explore if their systems may be subject to similar reconnaissance efforts.

Table 1. Example MVI Elements to be Shared[7]

Example MVI Shared		
Space MVI	Primary Space Segment	Space
	Space Service Affected	Deliver Telecommunications
	Space Specific Course of Action	Be prepared to activate secondary means of communication
Cyber MVI	ATT&CK Technique	T1592: Gather Victim Host Information
	SPARTA Technique	REC-0003: Gather Spacecraft Communications Information
	D3FEND Countermeasure	D3-MFA: Multi-factor Authentication D3-OTP: One-time Password

T plus 0 -

With MVI shared, an organization that receives the trusted shared information broadly understands the incident's activity but is not equipped with tailored detail to execute defensive actions against their specific operational systems. The organization will still need to fill-in specific details (likely sensitive details not useful outside the organization) to create specific tangible action.

Using the Operational Playbook template, and details shared in the MVI, organizations can add individual sensitive details (not to be shared) quickly to complete the Operational Playbook and dispatch cyber defense actions against system components. Specific procedures and artifacts are identified with organization-specific SOPs to suggest space or cybersecurity courses of action relevant to the threat or incident at hand.

Table 2. Example Suggestions from Operational Playbook

Example Operational Playbook Suggestions		
Cyber Course of Action 1	Technical Procedure	D3-LAM: Local Account Monitoring D3-AL: Account Locking
	System Component	Local Account Manager
	Artifact to Modify	d3f:Local User Account
Space Course of Action 1	Technical Procedure	Prepare backup communication channel
	System Component	Communications Transceiver
	Artifact to Modify	Communications Configuration

While the exact playbook will vary from stakeholder to stakeholder due to differences in individual systems, agreeing upon templates ahead of need and sharing a minimum set of operationally relevant information at time of need allows multiple stakeholders to align to common cybersecurity goals and outcomes. Through this sharing, disparate actions taken individually are synchronized through an agreed-upon common set of steps, resulting in a standard and coordinated response.

[4] https://attack.mitre.org/
[5] https://sparta.aerospace.org/
[6] https://d3fend.mitre.org/
[7] *Reference* (Tsamis, Stillwell, Reed, & Dailey, 2022) *for additional background.*

Conclusions

LCOIs play a key role in addressing cybersecurity threats in the space domain. By identifying, advocating for, and validating the exchange of specific information needs to address cyber threats, cyber-enabled LCOIs serve as the drivers of progress to achieve increased domain-wide cybersecurity. Cyber-enabled LCOIs provide the specialized support needed to effectively address defensive cyber needs associated with complex space operations. Specialized LCOIs may focus on specific cybersecurity concepts (e.g. alert management, operational playbooks, etc.) based on complex space operators' cybersecurity needs.

In this capacity, the LCOI's role in standardizing cybersecurity response is twofold: first, to manage the technical cybersecurity needs and solutions of its participants, and second, to understand and provide approaches to overcome social barriers among participants. The first aspect is technical, to define the information sharing technology used (e.g., blockchain or similarly trusted technology), and to cooperate with other LCOIs to define how information sharing between LCOIs is interoperable and preserving information provenance. The second aspect is social, enabled by governance to define and refine language (ontology) and practices of sharing trusted information.

The proposed maturity model offers a structured approach to measure the progress of both intent (social willingness) and ability (technical capability & infrastructure in place) for space domain participants to collaborate and defend against cybersecurity threats. This model emphasizes the importance of trusted information sharing through multiple ecosystems, overcoming identified barriers such as misunderstanding of information sharing constraints, perceived low value of sharing information, and low confidence and willingness to trust external data.

By leveraging the Minimum Viable Information (MVI) approach, stakeholders can effectively transform large amounts of data into operationally relevant information that is comprehensible, applicable, timely, and actionable. This facilitates efficient decision-making and coordinated responses to cyber threats, promoting new normal behaviors across individual stakeholders and enhancing overall space domain security through community vigilance and response.

Furthermore, LCOIs encourage more sharing within the domain by fostering and reinforcing a culture of trust and collaboration. With supporting decentralized infrastructure in place to support the secure exchange of information, LCOIs build confidence among participating stakeholders. This increased trust not only enhances the quality and reliability of the information shared within the LCOI, but, over time, improves the credibility of the products shared with other LCOIs. As trust and collaboration grow, the collective knowledge and situational awareness across the space domain are significantly enhanced, leading to more effective and coordinated cybersecurity responses.

Finally, the development and implementation of LCOIs, using the MVI approach, measured and driven forward by the presented maturity model provide a viable path forward to enhance cybersecurity in the rapidly evolving and complex space domain. This collaborative and decentralized approach ensures that cybersecurity concerns can be effectively addressed, fostering a resilient and secure space environment for future stakeholders.

Call to Action

The authors of this paper are preparing to prototype the concepts above, building a multi-LCOI environment, onto which information sharing and decision / action scenarios will be executed and analyzed. If you are interested in technical exchange and collaboration, please contact the authors.

References

Bingen, K. A. (2023, February 2). Launching Into the State of the Satellite Marketplace. *Statement before the House Energy and Commerce Subcommittee on Communications and Technology*. Washington, DC: Center for Strategic and International Studies.

Brockmann, K., & Raju, N. (2022). *Newspace and the Commercialization of the Space Industry: Challenges for the Missle Control Regime.* Sweden: Stockholm International Peace Research Institute.

Cataldo, C. (2009). Reviewed Work: Cultivating Communities of Practice: A Guide to Managing Knowledge by Etienne Wenger, Richard McDermott, William M. Snyder. *Academy of Management Learning & Education, Vol. 8, No. 2*, 301-303.

Executive Office of the President National Science & Technology Council. (2022). *IN-SPACE SERVICING, ASSEMBLY, AND MANUFACTURING NATIONAL STRATEGY.* United States of America.

Harrison, T., Cooper, Z., Johnson , K., & Roberts, T. G. (2017). *Escalation and Deterrence in the Second Space Age.* New York: Rowman& Littlefield.

Jah, M. (2022, May 12). Space Situational Awareness: Guiding the Transition to a Civil Capability. (S. a. House Committee on Science, Interviewer)

Pease, M., Stouffer, K., Reed, H., & Granata, S. (2023). *Manufacturing Supply Chain Traceability with Blockchain Related Technology.* Gaithersberg: National Institute of Standards and Technology.

Reed, H., Stilwell, R., Weedon, B., Dailey, N., & Tsamis, N. (2021). Sharing Operational Risk Information in the Space Domain to Facilitate Norms. *Advanced Maui Optical and Space Surveillance Technologies Conference.* Wailea, HI USA.

The MITRE Corporation. (2021, November 10). Applying Cybersecurity Lessons Learned to the Space Domain. *Technical Collaborative Panel Session, AIAA ASCEND 2021*.

Tsamis, N., Stillwell, R., Reed, H., & Dailey, N. (2022). *Sharing operationally relevant space cyber information.* Maui, HI: AMOS Conference.

Tsamis, N., Stilwell, R., Reed, H., & Dailey, N. (2022). Determining Operationally Relevant Space Cyber Information. *8th Annual Space Traffic Management Conference.* Austin, TX: The MITRE Corporation.

Wenger, E. (1998). *Communities of practice: Learning, meaning, and identity.* Cambridge University Press.