Sharing Operational Risk Information in the Space Domain to Facilitate Norms Development and Compliance Monitoring

Harvey Reed
The MITRE Corporation
Dr. Ruth Stilwell
Aerospace Policy Solutions, LLC
Dr. Brian Weeden
Secure World Foundation
Dr. Nathaniel Dailey
The MITRE Corporation
Nick Tsamis
The MITRE Corporation

ABSTRACT

The norm development cycle has an accepted pattern, norms emerge, reach a tipping point to norm cascade and finally, internalization. But we cannot reach the norm cascade without sufficient shared information to operationalize an aspirational norm. Determining the Minumim Viable Information (MVI) set to enable responsible norms of behavior in space is a necessary first step. Anthropogenic risks in the space domain include spread of cyber-attacks (especially loss of operational control), orbital densities, maneuvers, close proximity operations, and debris generating behavior. Characterizing these risks requires sharing and storing trusted and symmetric access to space information regarding RSO (Resident Space Object) orbital position, operational capability (e.g., ability to maneuver), reports of intent (e.g., intent to deorbit), and discrepancies / anomalies. This paper proposes a method to determine necessary information sharing, and a roadmap for experimentation to validate the approach and implementation in an international context.

The method to determine necessary information to share starts with determination of the Minimum Viable Information (MVI) set for each category (position, capability, cyber-attack, etc.) including bounded information that should be shared with the space community, and unbounded information that should not be shared due to proprietary or national sensitive nature. The MVI for risk categories must be shared and stored in a manner that assures trusted and symmetric information sharing in the context of the international space community, such as proposed in Space Information Sharing Ecosystems (SISE). SISE approach provides cryptographically provable attribution of data, with resilience and tamper-evident data qualities.

MVIs shared using SISE enable sensing data and reporting data to be recorded in such a manner that the space community can build a combined picture of operational awareness and risk. Critical anomalies can then be discovered as discrepancy between stated intents and observed behaviors. Such discrepancies between behaviors and practices can inform measures of liability and insurance risk.

The paper concludes with a call to action to pursue an MVI in a sustainability space information category as a starting point. This initial MVI can be implemented using a scaled down SISE prototype as a demonstration to the space community. Such a starting point can energize the space community to tackle more challenging MVIs and start building an operational risk characterization of the space domain. In turn, a trusted and symmetric risk characterization of the space domain can serve as a foundation for norms-based rules in the space domain.

I. INTRODUCTION

The Space Information Sharing Ecosystem (SISE) approach seeks to take the concepts of polycentric information sharing and apply them to the level of the global space community. We are no longer in the space race of the 20th century; State operations exist and exercise power side by side with corporate and civic space actors. The space community is enmeshed in a web of interdependent global social and technological networks.

Approved for public release. Distribution unlimited 21-03234-13

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Space information sharing ecosystems can be designed to match this very different world, taking the concepts of transdisciplinary information diffusion and innovation, understood at the level of a single organization and applying them at the multi-stakeholder and community level of the ever-growing interdependent global space domain. Space safety is not limited to the safety of any individual component or organization. Rather, space safety needs to consider how components interact within a complex space system, and how the operations of objects in space interact with each other.

II. SPACE INFORMATION SHARING ECOSYSTEM (SISE)

The space domain has a long history, with valuable legacy assets in use today. These legacy capabilities must be incorporated during the adoption of new approaches. For example, SISE relies on new decentralized information sharing technologies that can be used by existing legacy systems to coordinate and share information, and considers augmenting and building upon, but not replacing legacy capabilities. It is the goal of SISE to ingest selected data and information from SISE stakeholder organizational capabilities (e.g., sensors, data repositories), and make the data and information symmetrically available to other SISE stakeholders, each with a shared responsibility for preserving a safe and sustainable orbital domain [1].

Space information is currently exchanged between many space actors, generally by using bilateral arrangements between actors who are space information providers, space information consumers, or both. These bilateral arrangements serve to inform information sharing transactions between select stakeholders but fall short of a meeting multi and transdisciplinary information diffusion methods and components. (Figure I).

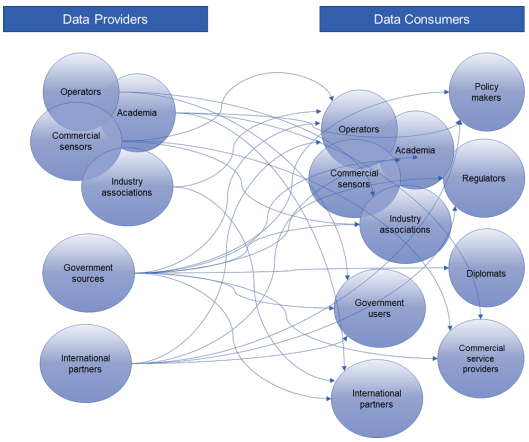

Figure I: Bilateral Information Sharing

The space community is not limited to bilateral agreements as industry consortia have formed to improve information sharing at the community level (Figure II). These consortia, like the Space Data Association and the EU SST, provide a framework for data sharing within the subset of member organizations, illustrating the need to expand information exchange outside individual space entities.

Approved for public release. Distribution unlimited 21-03234-13

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

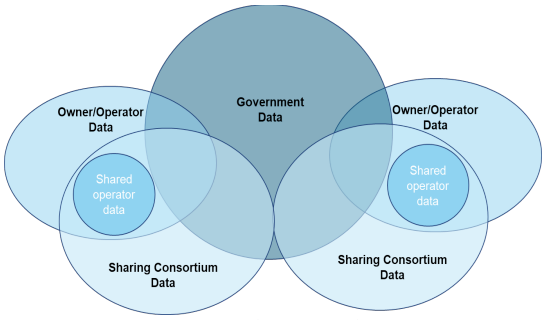

Figure II: Data sharing with consortia

The alternative to bilateral and consortia-based information sharing is a whole of ecosystem approach, to symmetrically share information that SISE stakeholders agree should be shared. Note, this is not the same as sharing all information with all actors in the space domain. Rather it is the identification of the appropriate subsets of information and the appropriate subsets of participants in a minimum viable ecosystem. The minimum viable SISE first establishes the minimal set of relevant data to share that has sufficient value to motivate stakeholders to participate. Second is to establish an initial set of decentralized sharing principles to assure information is both symmetric and trusted for all ecosystem participants. Finally, it is necessary to establish initial decentralized information sharing capability, constructed, tested, and operated in the open with transparency. The SISE model of information sharing maintains parity of information awareness among stakeholders. This information sharing protocol, is accomplished by reading prior posts of information, and making your own posts of new information, yielding a two-way conversation effect, viewable by the SISE stakeholders. Further, there may be need for more than one SISE ecosystem of stakeholders. For example, safety (as discussed above) is an obvious choice and may be best suited to start an initial prototype. However, there may be additional SISE ecosystems needed for other concerns such as supply chain, human health, etc.

Permissioned blockchain (Figure III) decentralized data technology can serve as a key enabler and has demonstrated utility across a variety of domains, including finance, supply chain, and logistics. The approach provides a foundational tool for a variety of activities across the space domain.

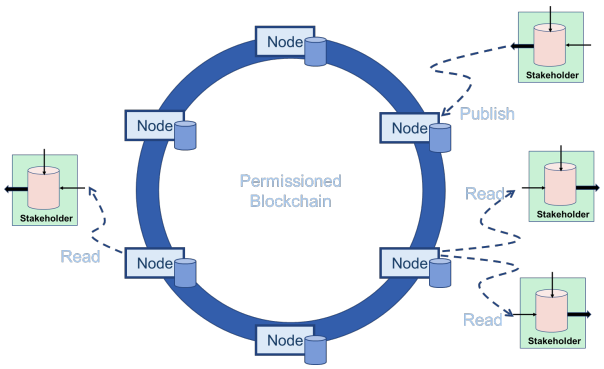

Figure III: Information Sharing with Permissioned Blockchain

The critical shift in cultural perspective required to implement this decentralized information sharing model, is to embrace the approach of incrementally growing (technical, governance, best practice) SISE ecosystems versus constructing a pre-defined system that is owned and operated by a single stakeholder. The barriers to information sharing in the space community have strong parallels to that of information silos inside complex organizations and relates to the difficulty of measuring the value of transparent systems as discussed above.

The adverse effects of information silos are measurable. Lost time and productivity due to silos are documented in multiple studies and affect most of the business [2]. Members of the space community are anecdotally aware that

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

limited access to information related to space domain awareness can frustrate their work, but the cost that information silos has imposed on the global space community has yet to be measured.

Taking concepts from productivity to safety is straightforward as the underlying principles are the same. However, the selection of enabling tools must consider factors that may not be of concern for internal systems. Intellectual property, corporate vulnerabilities, and business plans are not expected to be shared and users must be assured that the information is trusted. This is an advantage of the permissioned blockchain approach in the concept of a Space Information Sharing Ecosystem (SISE) as a tool for interdisciplinary and international cooperation to facilitate the development of norms and standards, cooperation, risk management, and information management.

The SISE approach recognizes this difference, particularly regarding the need to "translate" data so that it can be understood by diverse and disparate stakeholders. This became apparent in the discussion of cyber security incidents that may create an operational risk – how is the information shared from the cyber community to the operational community?

To address this barrier, the SISE approach adopts four tenets for shared information [3]. This focus is particular to determining operational relevance and the need to share, and the tenets provide foundational principles for information sharing at the community level (Figure IV).

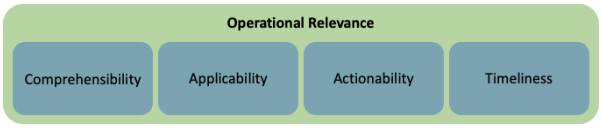

Figure IV: Four Tenets for Shared Information

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

Actionability – the value of information is ultimately limited by the actions it can support in an operational setting. Consuming organizations must know what to do with shared information. Providing complete sets of information necessary to address necessary actions in an unambiguous fashion empowers organizations to make informed operational actions.

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

Timeliness – paired with actionability, information must be acted on 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.

III. THEMES IN INFORMATION SHARING

The incentive for sharing information using SISE varies depending on the stakeholders' role in the space community.

The space community may implement instances of SISE tailored for various interests, such as reporting cybersecurity incidents, auditing manufacturing or in orbit repair, etc.

All the tenets and MVI considerations apply to each instance of SISE, regardless of the tailored ecosystem of interests, such as:

- Sensing
- On orbit operations
- Defensive cyber
- Etc.

Approved for public release. Distribution unlimited 21-03234-13

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Regardless of affinity group, each ecosystem will have a need to share information, with a common theme. The shared information will either be trying to prevent a negative event from happening (collision, on-orbit repair mishap, etc.) or mitigating an event once transpired (defensive cyber response to cybersecurity incident, etc.).

In either case, there occurs an event (T=0) used here as a starting point for proactive prevention or incident response/mitigation. Since there are many types of information sharing needs, there will be multiple T=0 events to consider.

For each T=0 event to prevent, or respond to once occurred, there are two dimensions of consideration:

1. (Pre T=0) → (T=0) → (Post T=0)
2. Tactical considerations vs Strategic considerations

Further, there are additional dimensions related to lifecycle of capabilities and processes, which we will not address at this time.

The two-dimensions related to an event, T=0 can be illustrated as a space information sharing T=0 Quad chart, below:

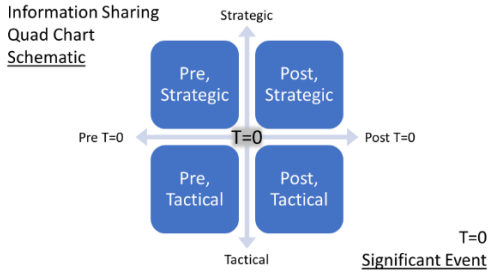

Figure V - Space Information Sharing Quad Chart

The T=0 Information Sharing Quad Chart shows that for any type of information sharing, there are at least four perspectives, and possibly more if lifecycle considerations are included (design-time, launch-time, on-orbit integration, software updates, etc.).

Consider a particular use case: on-orbit repair. This is in the news recently as the White House recently issued a strategy document "IN-SPACE SERVICING, ASSEMBLY, AND MANUFACTURING NATIONAL STRATEGY"[1] in April 2022. Shortly afterward, in May 2022, Dr. Moriba Jah testified[2] regarding manufacturing in space. Notably, he said on p.3 of his written testimony (emphasis by the authors of this paper):

> *"The US White House recently delivered a strategy on In-Space Servicing, Assembly, and Manufacturing4. 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."* [4] *(Moriba Jah)*

Consider what the Information Sharing Quad Chart looks like for On-orbit repair:

[1] https://www.whitehouse.gov/wpcontent/uploads/222/04/04-2022-ISAM-National-Strategy-Final.pdf

[2] Statement of Dr. Moriba K. Jah, The University of Texas at Austin to the Committee on Science, Space, and Technology Subcommittee on Space and Aeronautics United States House of Representatives on Space Situational Awareness: Guiding the Transition to a Civil Capability, May 12, 2022

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

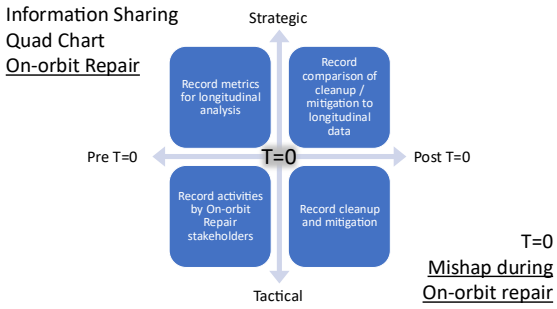

Figure VI: Quad Chart -On-orbit Repair Mishap

For on-orbit repair, there are at least four categories of pertinent information, as indicated by the quads. This type of high-level analysis offers insights as to the many types of stakeholder roles which may have an interest in each type of information sharing. Each stakeholder role will have concerns of:

- What incentive do I have to share information?
- What value to me is the information already recorded?
- What value does the information I possess provide to other stakeholders?
- How can I prevent oversharing my unique intellectual property and privacy-relevant information?

Ideally, for each type of information, the utility value of (information shared + constraints to avoid oversharing IP and privacy related information) is greater than (the effort to comply and record your information). The utility value may need to consider value provided directly to the sharing organization but also value to the ecosystem as a whole to which the information is shared.

The manufacturing / on-orbit repair example shows where information sharing is used to help coordination and avoid an event like a mishap. The goal of the information sharing is trying to forestall and delay the occurrence of T=0, while also aiding in post T=0 mitigation and avoiding unwarranted escalation due to misunderstandings.

In other cases, such as defensive cyber operations, the T=0 is instigated by outside forces, and the goal of the information sharing is to speed the mitigation, while simultaneously avoid unwarranted escalation due to misunderstandings. The information sharing focus is post T=0.

In the case of confidence building to grow acceptance of norms *all measures short of war* and conflict occur left of T=0 as strategic or planning sorts of activities. History tends to reflect a greater degree of instability during times of early paradigm phases and change, especially where strategic competition is involved. [5] Volatile uncertain complex and ambiguous (VUCA) transformative periods of change can greatly benefit from systematic means to ameliorate misinterpretations of intent.

Pre- vs. Post- T=0 Information Needs

Considering information needs pre- and post- T=0 (illustrated as a time-based horizontal axis in the Information Sharing Quad Chart), allows an organization to analyze and prepare for data needs prior to a real incident occurring. As an example, consider tactical actions that need be taken to execute system recovery. Ensuring the entire scope of an incident is properly understood is a key element in mounting effective and coordinated response and recovery plans.

To illustrate this concept in a cybersecurity context, the need exists to validate that protective controls and detection means are both:

a) appropriate for identifying a cybersecurity incident and
b) effective in supporting planned response and recovery actions.

Reasoning about cybersecurity goals later in the incident timeline (further right on the Quad Chart) allows for the derivation of system requirements necessary to support those goals. If data elements needed for a given response action are not available to be collected based on an issue presented by the incident at hand, requirements can be defined

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

to ensure that data is provided another way; perhaps by providing a secondary and independent method to obtain necessary data or by ensuring the needed data is continuously collected to provide appropriate insight at T=0 based on last collection. An example illustrating the need for identifying cybersecurity requirements in support of space mission objectives using the NIST Cybersecurity Framework is discussed in [6].

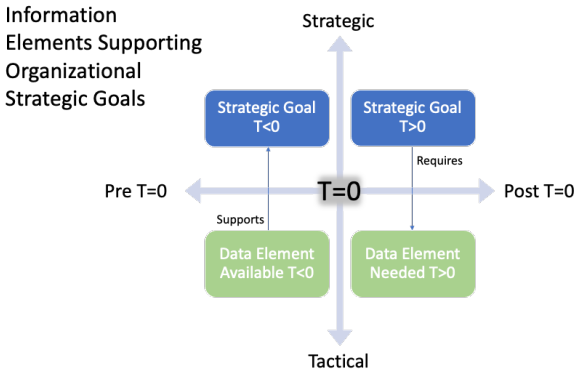

Figure VII: Information Relationships Across Goals

Tactical vs. Strategic Information Needs

The characterization of the second dimension presented, "Tactical vs Strategic" (illustrated as the vertical axis in the Information Sharing Quad Chart), identifies two noteworthy topics for further exploration.

1. First, different stakeholders have separate needs and thus impose different requirements to a space information sharing construct. It is imperative to understand what elements of information are applicable and requisite based on the audience intended to consume information shared.
2. Second, a relationship mapping between tactical and strategic information elements may be useful in organizing the various types of information available for relevant use across different needs. Due to the highly complex nature of space environments, leveraging digital means to capture and manage complex data relationships are increasingly required to support operationally relevant response actions to events, T=0.

To illustrate the relationship at work, consider an organization with a well-defined set of operational playbooks captured in a digital information management system. At T=0, this organization is better suited to thoroughly understand the situation for more effective response execution. Some questions this organization is equipped to answer include:

- Who are the right stakeholders within my organization to address this issue?
- Are we dependent on providers external to our organization to recover from this incident?
- Can we achieve our strategic goals for the specific incident encountered?
- What tactical remediation steps need be taken to support the strategic goal(s)?
- Do we currently have all appropriate data elements to support those tactical steps?
- Can an information sharing request external to our organization validate our understanding of the incident or enable more effective response?

What stakeholder(s) own which goals as well as the relationships between tactical data elements and strategic goals will be clearly defined for this organization, reference Figure . At time of incident, T=0, it may not be immediately apparent what tactical actions need to be taken to achieve desired strategic outcomes, but the organization is well equipped to understand what data elements are required may optionally further enable various strategic goals.

Having defined organizational relationships that capture an understanding of what data elements facilitate cooperation between goals and their appropriate stakeholders allows for the identification of what tactical actions to take to support strategic objectives desired. It may become obvious that effective capture and employment of these relationships soon becomes a complex undertaking. Leveraging SISE can effectively manage the complexity associated with these relationships, enabling personnel to focus on executing incident response actions rather than determining the appropriate actions need taken to support response during an incident.

Approved for public release. Distribution unlimited 21-03234-13

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Information shared across organizations can be leveraged more effectively when the need and utility of data elements are understood and agreed upon prior to incident, i.e. Pre-T=0. The complexity of these data relationships can be effectively managed through the employment of digital knowledge management systems to collect and organize the required elements of information necessary for sharing. This data set is termed the Minimum Viable Information.

V. MINIMUM VIABLE INFORMATION (MVI) USE CASES

Each subset of interest in the space community will have a set of information that is both valuable and relevant. Determining the Minimum Viable Information for each affinity must be determined by those stakeholders in the context of governance that includes disparate and diverse government, commercial, and international interests. An MVI agreed upon by stakeholders in an important step forward toward establishing norms. The agreed MVI establishes an important dichotomy of bounded information (the MVI) and unbounded information (everything else) which includes proprietary and national security sensitive information.

Full participation of stakeholders in establishing the MVI to share and sharing input and control over the means to share MVI requires a decentralized approach. Decentralized information sharing infrastructure is a key enabler to overcome the existing asymmetric access to trusted space safety information. Using decentralization approaches, the question of trust is addressed not by individual relationships, as is the case in bilateral arrangements, but rather through the trusted data integrity created by the decentralized information sharing infrastructure. This addresses the fact that no single stakeholder in the space community would be fully trusted to control information sharing. Coupled with governance and norms to encourage consistent sharing of critical safety-related information, the emergent effect is symmetrically sharing trusted space information (Figure VIII).

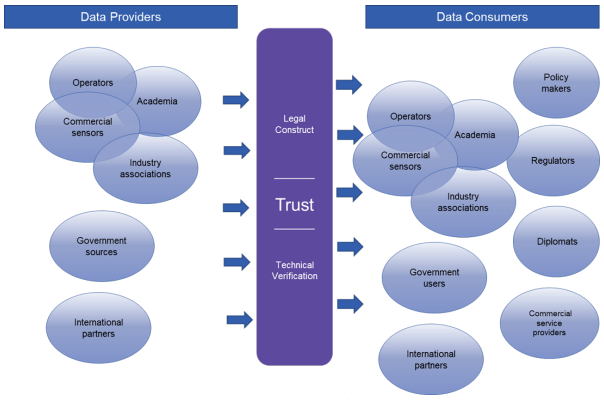

Figure VIII: Symmetric Information Sharing

Norms Based Behavior in Space

The global space community maintains a focus on the need for established norms of behavior in space. It is well established that, "Norms prescribe how to make decisions in social situations and play a crucial role in sustaining cooperative relationships and coordinating collective action" [7]. In asking actors to behave consistent with adopted norms, we must first ensure that they have access to sufficient information to apply the norm. This is the distinction between norms and aspirations.

Within the norms establishment field, this is a recognized barrier. Referring to the EU efforts to develop a code of conduct for outer space activities, the authors of Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity conclude "Even if the Code were to be adopted, the framework for broader information-sharing has not been created or demonstrated [8]". Information silos continue to be evident even in established systems to expand access to space domain awareness. For example, it is envisioned that the U. S. Department of Commerce Open Architecture Data Repository (OADR) will expand information exchange, but limitations remain. Dr. Moriba Jah, identifies this issue, "The most important aspect of the OADR is indeed being able to ingest sources of information that currently don't flow into the DoD and its catalog…not just industry, but international" [4].

Space Situational Awareness – sharing intent to maneuver

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Historically, space situational awareness (alternatively called space domain awareness) has relied on the collection of sensor derived data and operator voluntarily provided ephemeris. A missing component in shared space situational awareness is intent to maneuver. Interviews with subject matter experts in both government and industry reinforce the hypothesis that orbital and intent information can form the basis for the MVI for the universal set of space participants.

MITRE has been at the forefront of fundamental, applied, and formative research and development for Space Information Sharing Ecosystems (SISE) design concepts that enhance innovations in capacity development for space activities in ways that contribute to its responsible use and influencing positive behavioral norms. SISE includes consideration for such emerging and future technology innovations as artificial intelligence, shared vocabularies, capacity innovations, Blockchain immutability, consensus algorithms, Transparency and Confidence Building Measures (TCBMs), and benefits of polycentric information sharing designs that complement or enhance necessary bilateral arrangements with stronger collective mutual understanding mitigating misinterpretations of intent. The likes of SISE, such as an International Space Reference Architecture (ISRA), or Blockchain Enabled Space Traffic Awareness (BESTA), and SNARE all contribute to creating a full-scope picture, transparency, and trust by leveraging technologies and systems engineering to achieve normative socio-economic transformative impactful outcomes. Put succinctly altogether, they are socio-technological transformative mechanisms that provide an agnostic framework to serve space-related inter-discourse across national boundaries and allow the reconciliation of differences from across cultural divides. Like Defense mission objectives, so too can socio-economic and environmental impactful outcomes be architected with the help of technologies and systems thinking that is the hallmark of MITRE know-how.

In June 2019, the Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space were adopted (A/74/20, para 163 and Annex II) . They provide guidance on the policy and regulatory framework for space activities; safety of space operations; international cooperation, capacity-building, and awareness; and scientific and technical research and development. The Committee encourages States and international intergovernmental organizations to voluntarily take measures to ensure that the guidelines be implemented to the greatest extent feasible and practicable. [9] The following enumerates where SISE directly relates to implementation of those Long Term Sustainability Guidelines: A1, A2, A5, B1, B2, B3, B9, C1, C2, C3, C4

The De-escalatory Power of Clear Lines of Communication

One should not think that communication is unnecessary because conflict will not occur unless it is instigated by either one or both countries involved. It is when communication is absent that intent becomes fungible to the political insecurities and fears of the less powerful of the two countries. In the 1990s, the Chinese government believed that the United States had one of the most capable and advanced militaries in the world, backed by a superior intelligence apparatus. As a result, its leadership could not believe that the bombing of their embassy during the breaking apart of Yugoslavia was an accident. [10] It is entirely plausible that something similar could occur in the space domain today, as the United States is the more advanced and capable actor in the earth's orbit. In fact, recently the Kosmos-2558 satellite was launched from the Plesetsk Cosmodrome in Russia as a payload on the Soyuz-2.1v rocket. The Russian Ministry of Defense said Kosmos-2558 is a military satellite deployed into a Sun-Synchronous Orbit (SSO). Its exact purpose is unknown at present but has been described as an "inspector" satellite." [11]

"Initial data dictates that, in its current orbital path, Kosmos-2558 will pass within 80 km of the NRO's USA-326 satellite at about 14:50 UTC on Thursday, August 4 if neither of the satellites maneuver away from or closer to each other before then. McDowell does not expect that Kosmos-2558 will maneuver within 50 km of USA 326 as an observational mission can be accomplished from outside that distance, but that doesn't change the fact that the threat to U.S. orbital systems is growing very quickly" [11]

Without clear and effective lines of communication, a satellite malfunction, an accident, or an unintended signal could be wildly misconstrued by the opposing side. While it is an often-held truism that wars do not happen unless one or both sides want it to happen, the many near-misses to utter catastrophe the world faced in the Cold War should disabuse the policy maker of that notion.

Approved for public release. Distribution unlimited 21-03234-13

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

It is with that in mind that a basic framework for information sharing and communication can be put forward in the space domain.

Table 1. A notional Maturity Model for Space-Related Polycratic[3] Communication

1. Routine contact across all relevant levels of government and multiple agencies regarding both security and peacetime uses of outer space, including permanent positions dedicated to maintaining the relationship and explaining misunderstandings.
2. Routine contact across limited levels of government and only a handful of agencies regarding both security and peacetime uses of outer space. Individuals may be designated as points of contact, but no institutionalized roles are present.
3. Limited and infrequent contact between the governments regarding the security and/or peacetime uses of outer space. A point of contact may be specified, but the exact nature of the communication will be unclear and informal.
4. Communication limited specific occasions, likely instigated by a particular action or event that mandates a meeting. Communication limited to most senior government or military officials.
5. Only informal communication occurs, and only on an as needed basis. Increased difficulty in communication is likely.
6. Emergency lines of communication only, perhaps limited to heads of state.
7. No lines of communication permanently open. This is the most dangerous tier.

An international space communication framework should include all willing countries, such as India, China, and Russia.

Democratic peace theory dates to at least 1795, to the philosopher Immanuel Kant, saying if rulers needed the consent of the governed to go to war, they'd weigh the decision more carefully. It is the closest thing we have in international relations to an empirical law. When scholars have done their statistical analyses, they've found that democracies almost never attack one another. When they do go to war, it's against autocracies (and even then, the democracies rarely initiate the fighting). While we call it the democratic peace, it is the polycentricity in these instances that matters, not just the elections or form of polity a nation chooses. All criticism of democratic peace theory aside, fundamentally most people think accountability comes from above or below and forget it can come from beside. "It arises from being flanked by many "piecemeal engineers", spreading out the ability to experiment and iterate." [12] Elinor Ostrom[4] called this system polycentric—decision-making with many centers. For Ostrom the focus was about effective government. However, the same checks and balances that promote peace can also make governance more adaptive and functional.

"*The goal of (applying) this research is to use Ostrom's theoretical framework for sustainable polycentric governance of CPRs to identify gaps in the current space governance structures and inform both current initiatives and potential future initiatives that foster the long-term sustainable use of outer space."* [13] – Brian Weeden

More specifically, of the 8 recommendations from Ostrom's work is to, "develop a system, carried out by community members, for monitoring members' behavior" directly relates to the concept for SISE.

A legitimate worry is that empowering other levels of government and civil society makes states weaker, not stronger. Thus, "polycentric" often heard in in many circles. But people tend to grant the state, governments, nonprofits, foreign agencies, and experts more power when they trust these authorities. Such trust comes from knowing they are limited and controlled. Making the center strong and making it more accountable run congruently.

---

[3] (politics) Governed by many people or groups. [from 20th c.]

[4] It was long unanimously held among economists that natural resources that were collectively used by their users would be over-exploited and destroyed in the long-term. Elinor Ostrom disproved this idea by conducting field studies on how people in small, local communities manage shared natural resources, such as pastures, fishing waters, and forests. She showed that when natural resources are jointly used by their users, in time, rules are established for how these are to be cared for and used in a way that is both economically and ecologically sustainable. Ref: https://www.nobelprize.org/prizes/economic-sciences/2009/ostrom/facts/

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Thus, holding power and desiring peace and stability involves a paradox: wield influence responsibly while also trying to give it away. [12] In the context of applying polycentricism to outer space information sharing however, it is ironic and advantageous that no such centralized power exists in the first place.

While incorporation of authoritarian nations may make consensus making more difficult, it is important to understand that the primary need for consistent engagement is not that it will enable sweeping international laws and policies to be passed that fundamentally solve all problems in orbital or cis-lunar space, but rather that steady communication at all levels of government is necessary to responsible statecraft in outer space. The need for this will only grow as the number of satellites proliferate in orbit, the rate of tourist and manned missions grow exponentially, and, perhaps multiple, stations are established on the moon. The relative fragility of space assets mandates extraordinary caution and highlights the need to ensure that information is shared across all governments, not just the two most likely to come to confrontation in the years ahead. It can be expected that in its most fully realized form, all countries with substantial stake and ownership in the space domain will be included in this communicative framework.
Not all communication needs to be through human intermediaries. At a certain point, a transition to a complete Space Information Sharing Ecosystem should be made. Such an ecosystem would include regular and routine multilateral communication among nations, but it should also include the proliferation of sensory capabilities in space. The purpose of this network of interconnected sensors would be that it is under no one country's control and the ability to access its data is publicly available for all to see. The deployment of thousands of such platforms will enable greater domain awareness, allowing for the easier identification and removal of debris.

More than that, it would allow for the immediate identification of suspicious activity. The lack of transparency and predictability is a major contributing factor that "affects the potential for misinterpretation and miscommunication," to the point that "unpredictable or non-transparent operations conducted in deliberate proximity to other spacecraft may be viewed as posing a safety risk or a threat." In an information sharing ecosystem where all space platforms are easily locatable, aberrant behavior will be noticed almost right away. Suspicious platforms acting in a way inconsistent with past use could be raised for comment with the platform's controlling country long before any potentially hostile activity takes place. And, should such hostility occur, it would be immediately apparent whether this was one platform acting out of the norm or a coordinated effort on the part of a constellation of satellites. It can be hoped that radical transparency would make bad behavior significantly less likely. Barring that, it will at least allow everyone with access to the data the ability to track in real time the aggression of the state ordering the activity, thereby damaging their credibility when it comes to self-justifying narrative construction to explain their hostile acts.

VI. CALL TO ACTION: SISE PROTOTYPE TO IMPLEMENT TRANSDISCIPLINARY AND PLOYCENTRIC APPROACHES TO SPACE INFORMATION DIFFUSION

The need for SISE is manifest in several space related activities:

- Launch integration and orbit maneuvering
- Space traffic coordination / management
- Manufacturing and in-orbit repair, refueling, etc.
- Cyber threat information, mitigation

The common theme is that the entire space community needs to share MVI in a trusted and symmetric manner, so that independent space actors can make fully informed and coordinated, yet independent operational decisions. The SISE concept is ready for the next step of prototyping to demonstrate the following in an international context:

1. Stakeholders can cooperate by participating in the development, rollout, and operation of the SISE capability.
2. Diverse stakeholders can post data/messages, which all other stakeholders can view.
3. Stakeholders can trust that data/messages are resilient to tampering and destruction.

Approved for public release. Distribution unlimited 21-03234-13

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Cooperative SISE Participation

This type of information sharing ecosystem using blockchain is starting to be used in manufacturing supply chains, where the stakeholders are commercial firms as exemplified in NISTIR 8419, published April 2022. In this study, by NIST / NCCoE seven case studies in the manufacturing supply chain domain are analyzed regarding the use of blockchain to exchange traceability information. The SISE prototype will demonstrate that this mode of cooperation and information sharing can be extended to the space domain, to include nations and other international orgs exchanging safety critical and other information.

For this model of the prototype to be realistic, five to seven nations (or another recognizable international organization) are required to participate. The lower bound five is one greater than the minimum for multi-node consensus in blockchains such as Tendermint. The upper bound keeps the prototype nimble and accomplishable, although please note that a fully implemented SISE ought to accommodate hundreds of stakeholders posting and reading information.

The development and rollout of capability ideally should include all or many of the participating stakeholders, to at a minimum inspect work, if not also contribute code.

Decentralized Contribution to SISE

This aspect needs to clearly demonstrate the basics of information sharing, and the MVI concept. While all blockchains allow for stakeholders to post and others to view, this prototype needs to demonstrate this still works with decentralized control, and multiple parties hosting the blockchain nodes. Further, this prototype needs to show, at least in some small part, the embracing of the MVI and "Four Tenets" model to increase incentive to share, while reducing disincentive to share.

An advanced form of this prototype will demonstrate the information sharing capability even with larger files (text, audio, video). This will require using an external repository, which can also be decentralized. For example, IPFS (Interplanetary File System) from the Filecoin Foundation is a decentralized content store. This could complement a permissioned blockchain where hashes of the externally IPFS stored data/messages are hashed, with the hashes stored on the permissioned blockchain can be compared to the content stored in IPFS to maintain data integrity.

Trustworthy Sharing within a SISE

This aspect is perhaps the most important. Once the SISE capability can demonstrate information viability while operated by multiple international orgs/nations, there is still the question of data/message integrity (discussed above), even while under attack.

Prior MITRE research used a blockchain test harness, with cyber adversarial agents managed by MITRE CALDERA[5] to attack permissioned blockchains (e.g., Tendermint), and measure performance while network is degraded and the host machines for the blockchain nodes were attacked. The most important performance metrics for a permissioned blockchain are:

a. Rate of block production
b. How much network interference (dropped packets, delay, etc.) is needed to affect performance, and ultimately stop block production?
c. What is the rate of restitution? After network (or other) interference is stopped, how long before block production resumes?

[5] caldera.mitre.org

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Such adversarial tests can increase confidence in decentralized capabilities such as SISE, by making the performance vs. degree of attack visible. Further, the adversarial tests used to produce and measure effects as described above, can also be conducted in a decentralized manner, increasing participation of disparate stakeholders.

The permissioned blockchain adversarial testing using the blockchain test harness evolved into an emerging decentralized testing approach called Space Test Bed Network STBN that enables any number of stakeholders to host test nodes, where the test scenario executes over the nodes using prescribed and advertised services.

The primary hypothesis of the prototype is that by combining decentralized dev/rollout, usage, validated by adversarial stress test, the resulting prototype will be trusted, and stakeholders will agree to use the capability.

The secondary hypothesis of the prototype is that additional stakeholders will agree to join the effort for continuing decentralized dev/rollout, usage, and adversarial stress test, the resulting larger prototype will also be trusted, and more stakeholders will agree to use the capability.

This last point is key since a decentralized capability of this nature needs to be grown not specified in entirety in advance. Thus, not only do we need to prove an initial prototype works, but the model must also enable stable growth and adoption.

Once a secondary hypothesis is proven, then larger investments may be possible for a production version. But even here, care must be taken to avoid the natural tendency to centralize which reduces trust and may render the capability useless.

Beyond the primary and secondary hypotheses, further work is indicated in these areas:

1. More challenging MVIs. The examples given in this paper are a starting point. However, to have an impact on norms development and other areas, more challenging MVIs must be tackled, which will be a confidence boosting measure.
2. Build a more complete operational risk characterization. If the incentive to share is based on mitigating operational risk to the space community while minimizing each stakeholder's exposure (IP, privacy), this must be coupled by more sophisticated operational risk characterizations.
3. A means to first qualitatively, then later quantitatively, measure the value to space domain stakeholders provided by SISE. Metrics to measure increased capacity, timeliness, operational effectiveness, or other value add provided by SISE compared to current means of sharing information must be determined and enacted in SISE implementation.

VII. CONCLUSION : POLYCENTRIC INFORMATION GOVERNANCE CAN IMPROVE SPACE MISSION OUTCOMES

SISE is a socio-technical foundational for sharing trusted and symmetric information of interest to an ecosystem of stakeholders. SISE can be implemented using emerging permissioned blockchain and decentralized file storage technologies. SISE may have multiple instantiations for different interests, such as safety, and in-orbit manufacturing and repair. SISE develops systems for capturing, sharing, storing, and making derived knowledge available across the global space community for such purposes as preserving a safe and sustainable space domain.

The result is bounded information sharing ecosystems, similar to what is being observed today in manufacturing supply chains (e.g., NISTIR 8419) to share traceability information.

Once an ecosystem of interested stakeholders have a trusted and symmetric means to exchange information, this in turn can be the foundation for improving operations, coordination among independent operators, and overall space traffic management.

Approved for public release. Distribution unlimited 21-03234-13

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com

Further, once a trusted and symmetric information sharing capability is in use, stakeholders can then create shared language and metrics to describe risk characterization, which in turn can enable (but not drive) norms-based rules in the space domain. The driver for norms-based rules must be from a need to improve mission outcomes and avoid negative scenarios. SISE can be the socio-technological enabler.

A SISE prototype can validate the means of construction, testing, and operation by multiple stakeholders. This last point is critical in that a mechanism can only be trusted in an international environment if: (1) international stakeholders can operate the permissioned blockchain nodes themselves, (2) have access to the data on the nodes, (3) and have a demonstrable understanding of how the information sharing capability behaves under attack.

VIII. REFERENCES

[1] H. Reed, R. Stilwell , N. Dailey and B. Weeden , "SISE (Space Information Sharing Ecosystems): Decentralized Space Information Sharing as a Key Enabler of Trust and the Preservation of Space," in *AIAA ASCEND* , Las Vegas, 2021.

[2] Thrive , "Thrive Learning," [Online]. Available: https://www.thrivelearning.com/the-l-and-d-dictionary/what-is-a-knowledge-silo/. [Accessed 29 April 2022].

[3] N. Tsamis, R. Stilwell, H. Reed and N. Dailey, "Determining Operationally Relevant Space Cyber Information," in *8th Annual Space Traffic Management Conference*, Austin, 2022.

[4] M. Jah, Interviewee, *NOAA plans 'initial' civil alternate to DoD space tracking system by 2024: senior official.* [Interview]. 11 February 2022.

[5] T. Wright, All Measures Short of War, 2017.

[6] B. B. G. F. N. Tsamis, Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles, American Institue of Aeronautics and Astronautics, Inc., 2021.

[7] J. Gross and A. Vostroknutov, "Why do people follow social norms?," *Current Opinion in Psychology,* vol. 44, pp. 1-6, 2022.

[8] B. McClintock, K. Feistel, D. Ligor and K. O'Connor, "Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity," Rand Corporation, Santa Monica, 2021.

[9] "UNOOSA," [Online]. Available: https://www.unoosa.org/oosa/en/ourwork/topics/long-term-sustainability-of-outer-space-activities.html.

[10] T. Fox, "BOMBS OVER BELGRADE: AN UNDERRATED SINO-AMERICAN ANNIVERSARY," War on The Rocks, 7 May 2019. [Online]. Available: https://warontherocks.com/2019/05/bombs-over-belgrade-an-underrated-sino-american-anniversary/ . [Accessed 26 8 2022].

[11] E. Helfrich, "The Warzone," The Drive, 2 8 2022. [Online]. Available: https://www.thedrive.com/the-war-zone/game-of-chicken-with-u-s-and-russian-satellites-may-be-underway. [Accessed 26 8 2022].

[12] C. Blattman, Why We Fight, Penguin Publishing Group, 2022.

[13] B. Weeden, "The economics of space sustainability," The Space Review, 2012. [Online]. Available: https://www.thespacereview.com/article/2093/2 .

[14] Joint Inspection Unit, "Knowledge Management in the United Nations System," United Nations, Geneva, 2016.

[15] ISO, "ISO 30401:2018(en) Knowledge management systems — Requirements," 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:30401:ed-1:v1:en. [Accessed 28 April 2022].

Approved for public release. Distribution unlimited 21-03234-13

Copyright © 2022 Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) – www.amostech.com