IAC-22-D5.2.2

SPACE INFORMATION SHARING ECOSYSTEMS: DIGITAL KNOWLEDGE MANAGEMENT IN OPERATIONAL AWARENESS

Mr. Harvey Reed
The MITRE Corporation, United States, hreed@mitre.org
Dr. Ruth Stilwell
Aerospace Policy Solutions, LLC, United States, office@aerospacepolicysolutions.com
Dr. Nathaniel Dailey
The MITRE Corporation, United States, ndailey@mitre.org
Mr. Nick Tsamis
The MITRE Corporation, United States, ntsamis@mitre.org
Dr. Brian Weeden
Secure World Foundation, United States, bweeden@swfound.org

Modern space activity exists as a very different world than the Space Race of the last century. Today's space coordination information sharing ecosystems should be designed to match the very different world, where states exist and exercise power side by side with corporate and civil space actors, enmeshed in a web of interdependent global social and technological networks. Space safety is not limited to the safety of any individual component but must consider how that component interacts within a complex space system. This goes beyond engineering and should consider how the operation of objects in space interact with one another. Knowledge management centers on the concept of knowledge sharing but means different things to different stakeholders. This paper develops 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. Quality, safety, and security require trusted information as a foundation. The SISE approach starts with the determination of a Minimum Viable Information (MVI) set for each risk category 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 paper concludes with a call to action to pursue a SISE prototype exchanging MVI of a safety critical activity, such as reporting cybersecurity incidents. This initial MVI can be implemented using a small scale 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 can serve as a foundation for norms-based rules in the space domain.

I. INTRODUCTION

Knowledge management is commonly discussed at the organizational level. The Space Information Sharing Ecosystem (SISE) approach seeks to take the concepts of knowledge management 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.

Space information sharing ecosystems can be designed to match this very different world, taking the concepts of knowledge management, understood at the level of a single organization and applying them at the multi-stakeholder and community level of the 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. KNOWLEDGE MANAGEMENT

Knowledge management centers on the concept of knowledge sharing but means different things to different stakeholders. This is acknowledged within the ISO standard for knowledge management itself, which states: "Knowledge management is a discipline focused on ways that organizations create and use knowledge. Knowledge management has no single accepted definition and no global standards predate this management system standard." [1]

The Joint Inspection Unit of the United Nations produced a review of knowledge management in the system, recognizing knowledge as a strategic asset of the UN system and identified specific challenges in the adoption of knowledge management systems. The challenge of measuring the impact of knowledge management within organizations will be even more consequential to efforts to expand knowledge management to external systems that rely on voluntary participation. The inspectors found, "Measuring the impact is a major challenge in designing and implementing knowledge management strategies and policies as one cannot measure what has been prevented. Knowledge management prevents waste of money, waste of time and waste of human resources. However, it is difficult to quantify the time spent looking for the right information, or the cost of reproducing knowledge that already exists somewhere else or using obsolete instead of up-to-date information, or the money wasted in investing in technology without assessing its potential to improve the availability and accessibility of knowledge." [2]

Within the literature supporting the UN knowledge management area, it is defined as the process of capturing, storing, sharing, and effectively managing knowledge and experience across an organization. The purpose of the SISE concept is to take this concept beyond the organizational level and develop systems for capturing, sharing, storing, and making knowledge available across the global space community for the purpose of sharing knowledge to preserve a safe and sustainable space domain. The contributions SISE can make to results-based management system[1] for international efforts within a space related context thus span across not just knowledge management, but also strategic, operational change, and responsibility management; as well as fostering a culture of results and mutual accountability. For example, knowledge derived from SISE can comprise measurable information from before and after (*ex-ante/ex-post*) implementation of recommended practices or policies and relied upon for action due the nature of its transparency, accountability, and immutability attributes. (e.g., mass on orbit before vs after, number of reported incidents, number of COLA actions, transgressions from agreed upon behaviors, reduction in number of *note verbale*).

III. 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 gives principled consideration to augmenting and building upon, but not replacing legacy capabilities. It is the goal of SISE to ingest selected data and knowledge (referred to as information) from SISE stakeholder organizational capabilities (e.g., sensors, data repositories), and make the data and knowledge symmetrically available to other SISE stakeholders, each with a shared responsibility for preserving a safe and sustainable orbital domain [3].

[1] The pillars of the UN Framework for Results Based Management consist of 1. RBM conceptual Foundation, 2 Planning Programming and Budgeting, Monitoring Evaluation and Reporting, 4. Fostering a Culture of Results, and 5. Mutual Accountability.

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 knowledge management approach (Figure I).

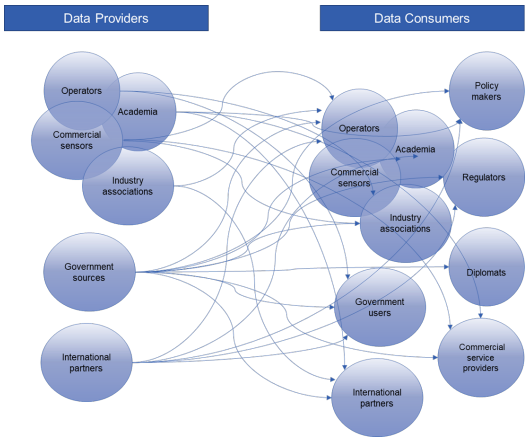

Figure I: Bilateral Information Sharing

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 knowledge management within the subset of member organizations, illustrating the need to expand knowledge exchange outside individual space entities.

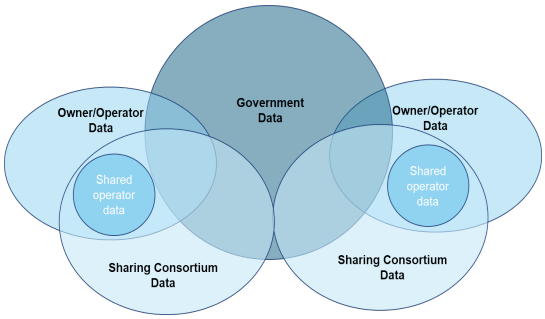

Figure II: Data sharing with consortia

Effective knowledge management requires appropriate tools that enable access to shared information. 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 / knowledge 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 knowledge management for a variety of activities across the space domain.

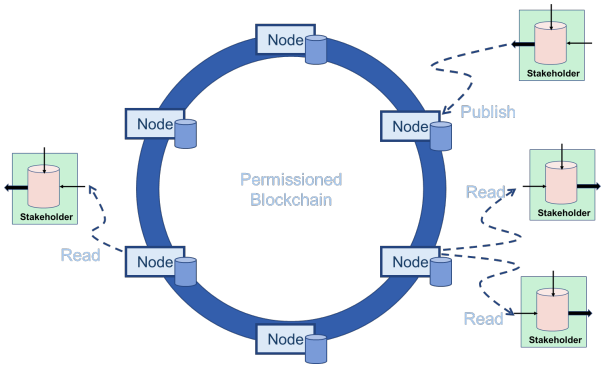

Figure III: Information Sharing with Permissioned Blockchain

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. This is where the lessons learned from organizational knowledge management can benefit space sustainability

at the community level. 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 knowledge systems as discussed above.

The adverse effects of information silos are measurable. Lost time and productivity due to knowledge silos are documented in multiple studies and affect most of the business [4]. Members of the space community are anecdotally aware that 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 knowledge management 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.

A key component of knowledge management is the recognition that sharing knowledge is not synonymous with sharing underlying data. 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 [5]. 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).

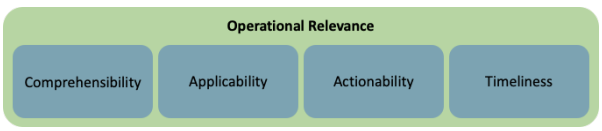

Figure IV: Four Tenets for Shared Information

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.

IV. 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.

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:

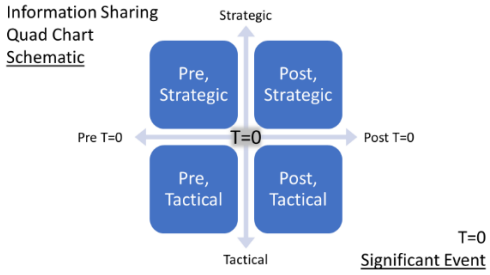

Figure V - Space Information Sharing Quad Chart

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"[2] in April 2022. Shortly afterward, in May 2022, Dr. Moriba Jah testified[3] 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."* [6] *(Moriba Jah)*

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

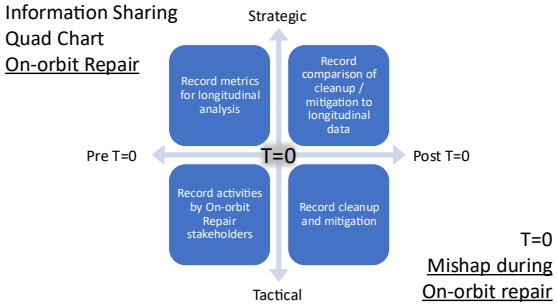

Figure VI: Quad Chart -On-orbit Repair Mishap

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

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

[3] 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

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. [7] 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 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 [8].

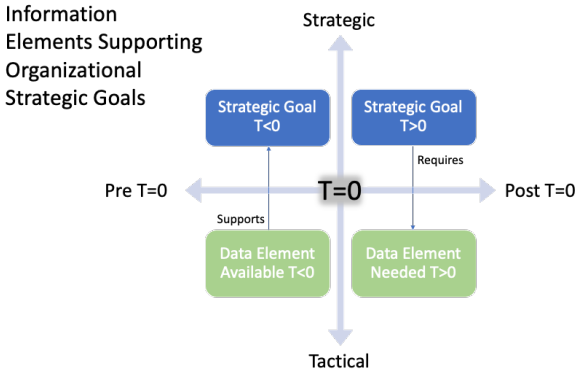

Figure VII: Information Relationships Across Goals

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 knowledge 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 a digital knowledge management system 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.

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. As discussed, 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).

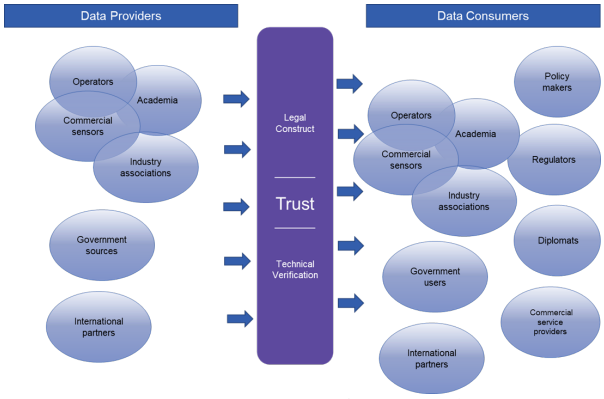

Figure VIII: Symmetric Information Sharing

VI. CALL TO ACTION: SISE PROTOTYPE TO IMPLEMENT DIGITAL KNOWLEDGE MANAGEMENT

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.

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[4] 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?

Such adversarial tests can increase confidence in decentralized capabilities such as SISE, by making the performance vs. degree of attack visible. Further, the

[4] caldera.mitre.org

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 : DIGITAL KNOWLEDGE MANAGEMENT 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 to inform KM practices and processes. 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 contributions SISE can make to results-based management system[5] for international efforts within a space related context thus span across not just knowledge management, but also strategic, operational change, and responsibility management; as well as fostering a culture of results and mutual accountability.

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.

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)

[5] The pillars of the UN Framework for Results Based Management consist of 1. RBM conceptual Foundation, 2 Planning Programming and Budgeting, Monitoring Evaluation and Reporting, 4. Fostering a Culture of Results, and 5. Mutual Accountability.

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] 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].

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

[3] 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.

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

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

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

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

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

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

[10] 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.

[11] 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].

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

[15] 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].