AMOS Conference 2022
Maui, HI, USA

Sharing operationally relevant space cyber information

Mr. Nick Tsamis
The MITRE Corporation, ntsamis@mitre.org
Dr. Ruth Stilwell
Aerospace Policy Solutions, LLC, office@aerospacepolicysolutions.com
Mr. Harvey Reed
The MITRE Corporation, hreed@mitre.org
Dr. Nathaniel Dailey
The MITRE Corporation, ndailey@mitre.org

Cyber threats pose a risk to every industry, space is not immune. As an emerging critical infrastructure, space operations become a more attractive target. The risks from a cyber attack, particularly a loss of control, have consequences that reach far outside the cyber community and put all operators in shared orbits at risk. Under existing structures, information necessary to identify such risk may not be able to be shared with the operational community in a timely manner. Challenges associated with information sharing became apparent in Table Top Exercises (TTX) conducted by the Space ISAC (Information Sharing and Analysis Center) in 2021. This paper formulates an approach to determine operationally relevant space information, and the means to broadcast this information to stakeholders. The approach leverages an assessment of workflows used in prior TTXs in which existing data types and willingness to share is analyzed against operational needs and risks. Further, this approach includes a process intended to encourage space stakeholders to engage in operational impact mapping, data sanitization, and information sharing with an international community, balanced against proprietary and nation-sensitive concerns.

Establishing an accepted space cyber information sharing process encourages definition and agreement of information sharing norms within the space community. The approach produces Minimum Viable Information (MVI) sets of operationally relevant space cyber information suitable for broadcasting to the space community. Such an approach seeks to build upon the current state of cybersecurity information sharing in the domain, which is heavily reliant on public-released hardware and software vulnerabilities, superficial information regarding cybersecurity incidents with ambiguous applicability to the space domain, and general cybersecurity news.

Removing ambiguity, minimizing required interpretability, and providing concrete guidance on how to broadcast and consume shared operationally relevant space cyber information will increase space stakeholders' ability to understand potential operational risk, and incorporate that understanding in their decision processes. This, in turn, enables the international space community to actively and authoritatively collaborate towards addressing cybersecurity issues threatening the space domain.

The paper closes with a call to action, to identify a subset of data with which to prototype an example of broadcasting and consuming operationally relevant space cyber information. Such a prototype can leverage work done in the SISE (Space Information Sharing Ecosystem) effort and would serve to validate our understanding of both current and future needs regarding both the content of, and the infrastructure supporting, shared space cyber information.

1 INTRODUCTION

Information related to the cyber state of operational space assets provide unique insight into risks presented to the space domain. Challenges with broadcasting or sharing such information present a systemic barrier to ensure a collaborative and secure shared space environment. Without efficient structures in place to encourage and facilitate information sharing, the space community remains vulnerable to silo mentality, and delayed response to critical events.

Participation in tabletop exercises (TTX) conducted by the Space ISAC (Information Sharing and Analysis Center) in 2021 provided a unique window into the need, current state challenges, and next step goals of the value cybersecurity information shared can provide to the operational community. As the cybersecurity community exercised addressing immediate threats related to a cyber attack, it became apparent that cybersecurity information relevant to the operational community was not easily transferable.

Insight gathered from these hands-on demonstrations paired with information from active engagement with space community participants and cybersecurity stakeholders culminated in the identification of needs for effective cyber information sharing within the space domain. Extending upon prior work, the concepts presented below are intended to align and interface with ongoing initiatives and be used as guiding principles to support the space community's drive in responding to current and future space cyber threats.

2 SPACE ISAC EXERCISES

Space ISAC is a sector-based information sharing and analysis center and a member of the National Council of ISACs. NASA, US Space Force (formerly Air Force Space Command), and National Reconnaissance Office sponsored the first space-dedicated ISAC in response to public and private sector dialogues in the 34th and 35th Space Symposia. At the Space ISAC's launch in April 2019, several representatives from public and private sectors spoke out about the importance of protecting the domain's critical space assets. [1] Since then, the Intelligence Community Commercial Space Council has also partnered with the Space ISAC.

In 2021, Space ISAC conducted two tabletop exercises that included diverse industry engagement. Observations from these two TTX exercises provide insight into challenge areas within this information sharing in the space domain:

1) **Pandora's Gambit** – TTX event held on 20 July 2021 conducted with support from American Institute for Aeronautics and Astronautics (AIAA) and The MITRE Corporation. 7 teams from various space industry backgrounds participated in reasoning through a mock scenario in which an Advanced Persistent Threat (APT) successfully targeted and accessed operational satellite networks. All participants had to navigate impacts to space operations associated with Command and Control (C2), space vehicle telemetry, and mission planning. Cybersecurity concepts explored included malicious supply chain injects, Satellite Communications terminal compromise, disruption to cloud service providers, and others. [2]

2) **Pandora's Portent** – TTX event held on 15 November 2021 during the 2021 AIAA ASCEND Conference. More than 15 organizations participated in this exercise, specifically focused on ensuring appropriate space traffic coordination in the face of a cybersecurity attack. The scenario at play led participants through handling a compromised space vehicle, uncertainty around existing spacecraft command channels, and conjunction risk. [3]

Enormous value is provided to the space community by hosting exercises that test current protocols and channels for information sharing. Through these exercises, the space domain is provided valuable insight used to continuously improve the current state of practice. It is the hope that future exercises will continue to elicit participants from further diverse organizations with unique perspectives and contributions to the community. Promoting continued international engagement and increased participation will provide opportunity to exercise new workflows and challenges not readily experienced to date.

3 PRIOR WORK

Prior work analyzing the output of these engagements identified key information sharing infrastructure needs [4]. These needs called for the development of the following products:

- **Universally accepted space domain vernacular**
- **Common space mission function taxonomy**
- **Standardized set of operational playbooks aligned to information shared**

Multiple ongoing efforts across academic, industry, and government settings are working to address facets of these key needs with publication as a near term goal. As this work is further developed and shared for broad consumption and feedback, a core consideration is to prioritize use of existing frameworks, tools, and concepts can be re-purposed to address needs as they are identified and refined in more detail.

The topics explored in this paper refine space cyber information sharing needs starting from prior work. The analysis covered is derived from observations of mock information sharing interactions that provide realistic insight into the challenges with information sharing faced by space community participants (i.e., Space ISAC TTXs). Cybersecurity stakeholders have information that is important for the operational space community to ingest and act upon. The content explored within continues to refine the approach to providing cybersecurity stakeholders with appropriate avenues to effectively share this information with the operational space community.

4 GUIDING TENETS OF OEPRATIONAL RELEVANCE

Increasing the value, impact, and efficiency at which we can describe the operational relevance of shared information correlates to better informed decisions. Better informed decisions, in turn, result in increased understanding, certainty, and control of operations in the space domain, benefitting a coordinated and collaborative ecosystem [4]. The four tenets reviewed below provide a means to help inform and guide the selection of appropriate information to emphasize relevance to operations.

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

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

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

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

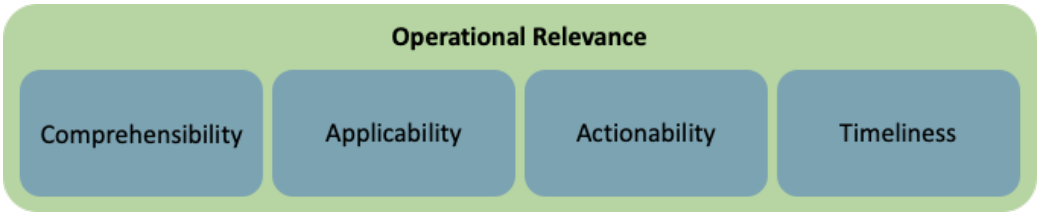

Fig. 1 - Four Tenets of Operational Relevance

Since its definition, the concept of the four tenets of operational relevance has been applied and extended to testing operational information sharing use cases, helping uncover gaps and opportunities to make shared information more relevant. Prior exercised use cases during TTXs were analyzed after the fact under the lens of these tenets [4]. Some data flows from these exercises were ultimately not agreed upon or proved insufficient support to stakeholders' operational missions. These exchanges were of particular interest for further analysis.

When analyzed forensically, the four tenets provided a useful framework to help analysts identify core reasons where some of these data sharing actions were unsuccessful. Analysis of these use cases continues to help uncover core issues experienced with intent to provide guidance for more effective space cyber information sharing exchanges (i.e. information sharing requests and responses). Researching the many information requests observed, analysts synthesized source data points into core systemic issues that provide insight into formulating better information sharing requests in the future. The following list provides a 'snapshot update' on some core themes identified from this in-progress analysis:

- Space and cyber -related elements are missing from exchanges – ***applicability*** or ***actionability*** is not well understood without inclusion of some needed data elements
- Pervasive perception of too much information being requested – information requested to organization is not ***comprehended***
- Past information requested is no longer time-relevant – new information uncovered at current time in incident response/analysis makes old information requested obsolete (***timeliness***)

It is expected that continued forensic analysis of demonstrated exercise use cases will yield additional insight. This insight will help to provide additional concrete guidance on shaping and standardizing future information requests, ultimately leading to increased probability of successful information exchanges. Specific outputs from this analysis are used explicitly in helping to define use case-specific sets of Minimum Viable Information, introduced and discussed in the following section.

5 ADDITIONAL INFORMATION SHARING NEEDS

Current means of sharing critical cyber information within the space domain face several challenges. Exclusive groupings of subsets of participants dominate over larger, more inclusive communities of participants, perpetuating the silo mentality. Further, the mechanism for sharing information remains maintained and operated within these smaller communities of interest, creating a high barrier of entry for new participants and trust silos. To maximize operational impact, the means of information sharing needs to scale to the whole space community and encourage increased participation. This requires wider agreement on the information shared, and the mechanism by which to share.

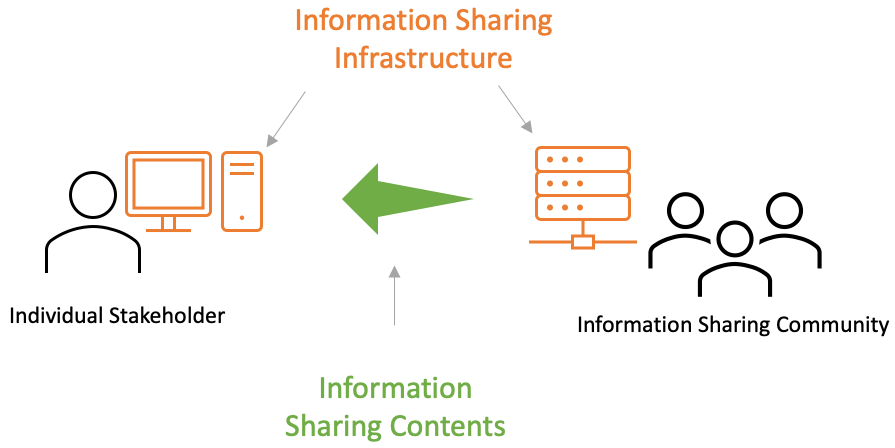

Fig. 2 - Information Sharing Infrastructure and Contents

Two different sets of information sharing needs must be considered:

information sharing infrastructure, referring to the mechanism of how information is shared amongst participants, and

information sharing contents, referring to information payloads being shared.

It is useful to de-couple these two categories of needs for appropriate system design, considering that each category will have unique attributes to consider for effective scaling to reach a wide stakeholder user base. Further, the differentiation between information sharing infrastructure and information structure/content allows for independent reuse and development of tools for the information sharing mechanism and information content definitions.

Prior work developed with the Space Information Sharing Ecosystem (SISE) concept [5] addresses the core information sharing infrastructure needs that support an effective means by which to share space cyber information with all participants in the space community. Additionally, SISE considers how to scale to reach a wide and international set of participants contributing to the build, maintenance, and operation of both information sharing infrastructure and information sharing contents. Further exploration of concepts that help define needs related to information sharing contents is addressed in the following section.

6 THE NEED FOR DEFINING MINIMUM VIABLE INFORMATION

A core theme from prior work described two key parameters which were responsible for reducing the potential for sharing information across organizations, inhibiting value to the operational community[1] [4].The two parameters are:

1) Magnitude of information shared for a requested exchange
2) Perceived sensitivity of information shared

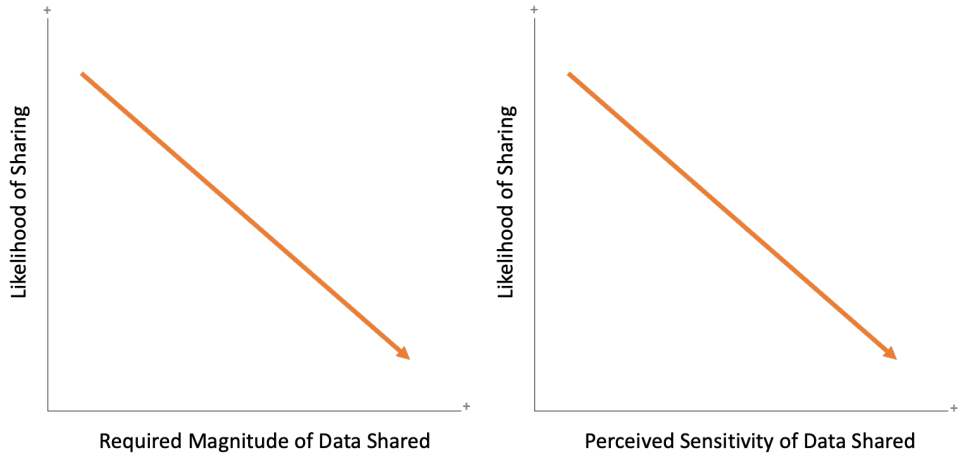

Fig. 3 - Observed Trend of Leading Contributors to Decreased Information Sharing

Using this concept enabled the enumeration of a minimal set of information elements that provide the necessary information for operational shareholders to agree to use and share with other operators in the space domain. To accommodate the two parameters referenced above, it was desired this set of data be minimal with respect to both size and sensitivity. This set of data is termed the Minimum Viable Information (MVI). In the context of space cyber information shared, the MVI is a set of at least space and cyber elements shared from one stakeholder to another that

[1] *This trend was consistently observed throughout the referenced TTX engagements; an increase in either the required magnitude or the perceived sensitivity of data requested for a sharing exchange trended with a decreased likelihood of the information to be shared.*

contains the data necessary for effective operational actions to be determined and, where applicable, performed, in a timely manner.

MVIs will differ based on the operational needs for which information will be used to share with other operators. For example, a simple advisory informing cyber stakeholders on the presence of increased reconnaissance activities against spacefaring organizations may define an MVI with a minimum set of cyber elements as suggested in the following notional list.

Example cyber elements for inclusion in an advisory-focused MVI:

- Information types targeted in reconnaissance
- Specific hardware or software packages targeted for information disclosure
- Techniques demonstrated by relevant threat
- Protocols used for exfiltration of data collected
- Known vulnerabilities leveraged

Many of these data elements can be readily described with well-accepted frameworks and schemas available today. For the elements included here, existing bodies of knowledge called upon will likely include Common Platform Enumeration (CPE) [6], Common Vulnerability Enumeration (CVE) [7], and MITRE ATT&CK® [8].

To support relevance to space mission operations specifically, additional space domain elements need be included in the MVI.

Example space domain elements for inclusion in an advisory-focused MVI:

- The space segment(s) targeted or potentially affected
- The space mission function(s) associated with targeted information
- Potential orbits at risk for future effects
- Affected individuals (satellites) or populations (constellations) that may be at risk

The MVI is the minimal set of information required to be viable for use among operators and other relevant stakeholders. In some instances, additional information may be need to maximize operational relevance. For these cases, additional requisite information may not fit neatly into the existing state of the MVI schema(s). Rather than preclude information from being shared, limiting the utility, these additional elements may need to be shared as a necessary addendum. If these circumstances arise, they provide a unique opportunity to critically analyze why additional information is needed, providing useful feedback in validating the current space, cyber, or other elements of the MVI as it exists in current form. These feedback loops are necessary to evolve MVI definitions as the space domain evolves, and are discussed further below.

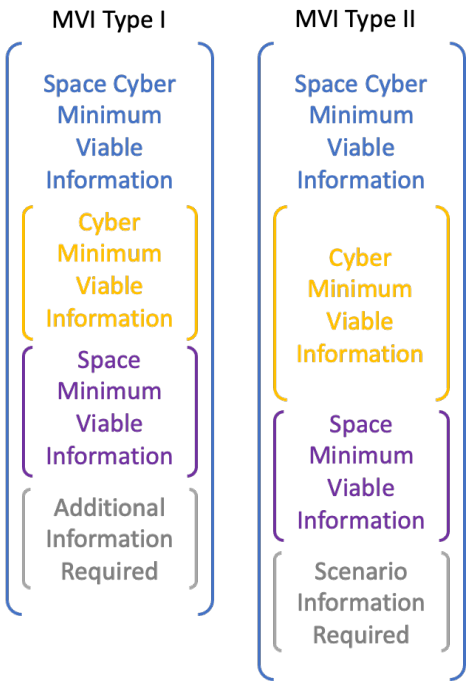

Fig. 4 - Illustration of Unique Sets of Space Cyber MVI

Once enumerated, these information elements contained within the MVI can be readily captured in a structured language that align with or extend, where feasible, existing standards such as STIX™, (Structured Threat Information eXpression) [9]. Domain-specific considerations are not always included in current state of cyber information sharing to date. As such, information elements shared may lack specific details that may be easily tailored for spacefaring organizations. While not explicitly required from a 'cybersecurity only' perspective, space domain specific data elements are included in the MVI as they can play a vital role in enabling more timely comprehension and determination of actionability for end stakeholders.

It is expected that different operational needs would be supported by different MVIs. As an example, information useful for providing insight into a cyber incident within Ground segment infrastructure will likely contain significantly different elements of data from an incident concerning within the Space segment itself. Thus, capturing the elements best suited to provide utility for each of these incidents, results in the description of different MVIs, each tailored to meet the intent of its associated operational needs.

With the MVIs defined, another challenge is addressed: the pre-planned agreement to and packaging of information shared prior to an incident occurring[2]. The concept offers a well-defined pre-packaged way to determine what can be appropriately shared amongst all sharing participants *before* that information is required to be shared. The goal is to arrive at an MVI that is usable and sharable by all stakeholders within an information sharing community. With these MVI constructs agreed upon and operationalized, practices and playbooks relevant to real-time space operations can be effectively developed and refined.

[2] *The challenge introduced here was directly experienced in TTXs prior. Information sharing potential was hindered due to a lack of pre-defined acceptance of sharing certain information. In the exercises, this was observed by a lack in understanding of what information was 'shareable' within or external to participating organizations. Understandably, organizations were not willing to participate in information sharing exchanges where the potential risks were not clearly understood and approved by a designated authority within the organization. Additional context is provided in [4].*

7 MEASURING THE VALUE OF SHARED INFORMATION

Significant challenges exist in measuring value for highly complex and dynamic environments including attempts to measure value related to intangible tasks or valuating costs of events that do not happen [10]. A starting point to approach this problem is to collect data that can be used for analysis; a mechanism to collect metrics to support measurement of the value of information shared is needed. To enable collection of feedback, information sharing infrastructure must support two-way communication. Consumers of information sharing products become feedback producers from which insight is collected and ultimately value can be measured from.

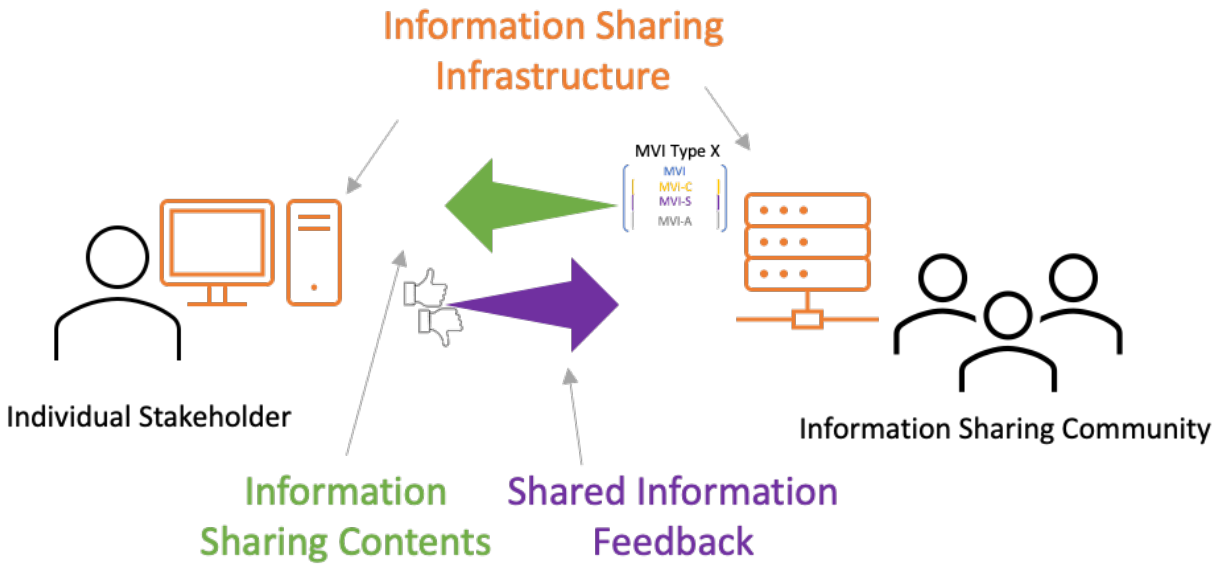

Fig. 5 - The Need for Two-Way Information Sharing

Feedback requested within a space information sharing construct can take many forms with varying levels of detail. Some feedback may require quantitative measures with objective metrics provided by participating organizations. Conversely, other feedback may be qualitative and highly subjective in nature yet still provide critical insight for the information sharing community. The nature of feedback requested will change based on the specific type of information shared. The set(s) of MVI shared for a given information exchange may provide a useful way to determine the type and/or level of feedback requested.

Even seemingly trivial feedback collected can provide significant value add and insight when aggregated at scale. Not all information will be relevant to all stakeholders within an information sharing ecosystem. Feedback collected from information consumers will help uncover what information is useful to a given set of stakeholders, but more importantly, start to identify potential reasons as to how information can be more valuable if shared in a different way. Implementation of simple feedback mechanisms allow information consumers to signal straightforward information back to the community (e.g. indicate if information is ‘useful’ vs ‘not useful’). This feedback alone can help easily uncover areas of opportunity for increasing value of shared information.

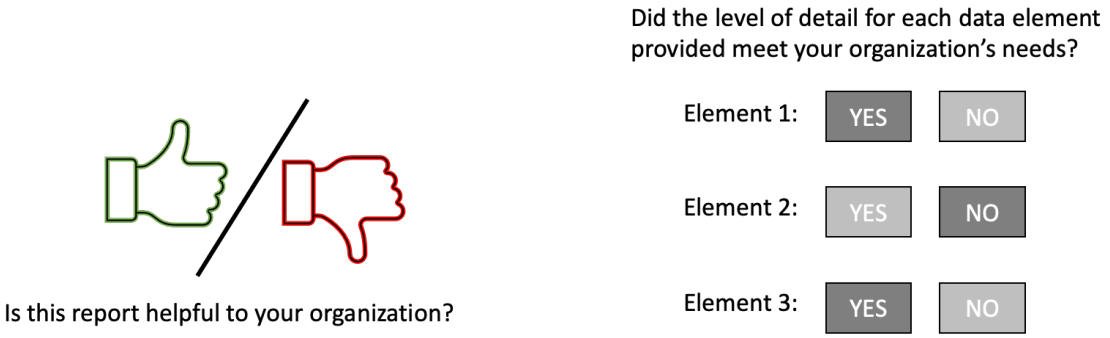

Fig. 6 - Example Metrics and Feedback for Low-Cost Collection

When feedback and metrics are collected, significant consideration must be given to requesting information that will provide insight into *why*. To help determine appropriate questions and metrics to request or collect, asking *why* serves to better identify stakeholder needs. Insight gained from this feedback may help uncover needs not readily addressed in the design and planning of the information sharing ecosystem. Why helps to identify methods to exact concrete and meaningful change immediately. A few example *whys* asked in analysis of prior events included for illustration:

- *Why* is this information specifically useful to your organization?
- *Why* did information shared yesterday not elicit the same level of utility?
- *Why* is the MVI, in its current form, insufficient?
- *Why* would inclusion of additional requested data elements provide increased benefit?

Ultimately, two-way information sharing elicits feedback that provides useful and direct input on future updates to information sharing definitions. Initially, starting with qualitative and low-cost feedback from stakeholders will provide a low barrier for participation, increasing the probability of future and more detailed feedback collection. Getting stakeholders comfortable and familiar with regularly providing feedback on information shared serves to increase amount of feedback collected over time, ultimately leading to gap identification and utility validation of information shared to the community.

8 FUTURE WORK

Rising complexity and scale challenges emphasize the need for information sharing constructs to prioritize machine-readability and ease-of-exchange in future state sharing infrastructure [11]. The concepts presented in this paper are prime candidates to capitalize on the opportunity to build these key priorities into future system design. Analysis into the efficacy of current schemas and methods used for machine-to-machine interactions, for instance, may uncover room for improvements as we look to extend existing information sharing solutions for addressing space domain challenges. Paying attention to how other domains/industries have historically approached unique challenges is likely to yield useful lessons learned for the space industry.

Further, with the rising integration of machine-to-machine interactions, it is imperative to not lose sight of the need for human operators in-the-loop in addressing cybersecurity concerns. Thought must be given to continuously re-evaluate that the processes put in place are optimized to account for human capacity and capability. This consideration may affect the feedback and metrics collected within operational space cyber information sharing implementations. Refining the approaches and methods used for feedback and metric collection is needed.

Future work is needed to identify the elements required for compiling MVIs necessary for operational use cases. Data elements can be agreed upon through the exercise of information sharing scenarios. Analysis on real test data from scenarios can help uncover where too much or too little information is shared for given use cases to verify the appropriate definition of MVIs.

Approved for public release. Distribution unlimited 21-03276-6.

Definition and agreement to operational playbooks for use in real time information sharing will be a future output. Standardized procedure sets to follow for various operational scenarios make use of shared space cyber information for operators to act with. In the future, the orchestrated execution of actions across space stakeholders translates shared information into tangible impact, allowing information sharing participants to collaborate towards a secure and sustained space community.

9 CONCLUSION

Defining consistent sets of information within well-defined interfaces serves to enable increased adoption, reduce the barrier to entry for sharing participants, and create new norms surrounding information sharing. Within a cyber context, the definition of common structures for space cyber information exchange can serve to foster increased agreement and participation in an information sharing ecosystem. Existing best practices, schemas, and frameworks can all be leveraged and, as needed, tailored to more effectively address unique needs for sharing operationally relevant cyber information in the space domain.

The next step to explore the utility of the information sharing topics discussed here entails piloting the concept in an information sharing environment (e.g., SISE) with multiple spacefaring organizations. Agreement to an MVI for an identified use case will define a usable product for test. With intent to facilitate an increase in both the magnitude and value of information shared within the environment, a pilot demonstration seeks to uncover areas of inappropriate implementation, insufficient functional capacity, or future growth opportunities. A live operational SISE and MVI prototype supports achievement of these goals:

1) Identify functional gaps between existing information sharing infrastructure and future needs
2) Validating the proper selection of space and cyber -specific data elements for MVIs
3) Enabling a SISE mechanism to both share MVI and collect feedback and metrics on the operational relevance of MVIs shared

Each of these three goals plays a key element today in defining the space domain's information sharing needs of the future. Such a prototype demonstration would serve to shift the current state of space domain cyber sharing to a more proactive mindset, enabling the domain to address the information sharing needs of future space activities. Further, with a proven demonstration, a re-evaluation of data sensitivity concerns can help foster new norms regarding space participants' willingness and ability to share, increasing the value of collaborative interactions amongst domain stakeholders.

10 REFERENCES

[1] "Space ISAC, About Space ISAC.," [Online]. Available: https://s-isac.org/about-us/.

[2] "TTX21-01, TTX Pandora's Gambit, After Action Report," Space ISAC, 2021.

[3] "Space cyber wargame exposes satellite industry risks.," [Online]. Available: https://readme.security/space-cyber-wargame-exposes-satellite-industry-risks-4c18bd234d5d .

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

[5] 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.

[6] "Security Content Automation Protocol; Common Platform Enumeration (CPE)," NIST, 2022. [Online]. Available: https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/Specifications/cpe. [Accessed August 2022].

[7] "About the CVE Program," 2022. [Online]. Available: https://www.cve.org/About/Overview. [Accessed August 2022].

[8] "MITRE ATT&CK; Getting Started," The MITRE Corporation, 2022. [Online]. Available: https://attack.mitre.org/resources/getting-started/. [Accessed August 2022].

[9] "Introduction to STIX," OASIS, [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.html. [Accessed August 2022].

[10] H. Reed, R. Stilwell, N. Dailey, N. Tsamis and B. Weeden, "Space Information Sharing Ecosystems: Digital Knowledge Management in Operational Awareness," in *International Astronautical Congress*, Paris, France, 2022.

[11] N. Tsamis, *Applying Cybersecurity Lessons Learned to the Space Domain,* The MITRE Corporation, 2022.