# A Space Information Sharing Framework

Scott Kordella[1]
*MITRE Corporation, McLean, VA, 22102, USA*

Ruth Stilwell[2]
*Aerospace Policy Solutions, Hallandale Beach, Florida, 33309, USA*

John W. Giles[3]
*MITRE Consultant, Burke, VA, 22015, USA*

Christian Zur[4]
*US Chamber of Commerce, Washington DC, 20062, USA*

**The current space operating environment relies heavily on manual activities for space situational awareness, using legacy processes that may be inadequate to accommodate the rapid growth in the satellite industry and placing unprecedented demands on the orbital environment. Information sharing among government regulators and space operators is a key requirement for successful operations, future commercial growth, and long-term sustainability. While there are a number of activities where information is shared, space lacks effective and efficient access to shared information by the space community. The operational value of information sharing in the space domain goes beyond the question of conjunction alerting and includes spectrum interoperability, cyber protection, and air/space launch/reentry integration. Information sharing must be created to balance between the protection of information to support one's own parochial issues, such as protection of proprietary information versus sharing for the common well-being of the operating environment. This paper examines existing concepts and launches an activity to develop a framework for information sharing in the space community that balances user concerns and allows for safe and sustainable growth in the space domain.**

**Keywords: information sharing, space traffic management, spectrum management, cyber protection, orbital debris**

## I. Introduction

It is widely accepted that the space operating environment is on the verge of dramatic transformation. At present there are just under three thousand operational satellites on orbit, but even conservative estimates project that number at fifteen or twenty thousand within ten years. In addition, the diversity of orbital activities and the dynamic nature of those activities is also increasing specifically with regard to increases in low Earth orbit satellite operations linked to rising consumer data demand for reliable, high speed, and extreme low latency system needs. Additionally, increased autonomous ground and aerial vehicles and maritime vessels will require connectivity resilience that will

[1] Senior Advisor, Space Systems, and AIAA Member
[2] Executive Director, Aerospace Policy Solutions, LLC, and AIAA Member
[3] Founder and Senior Consultant, John W. Giles Consulting, LLC
[4] Executive Director, Procurement and Space Industry Council

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2636. 'The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.'**

rely upon robust satellite networks. Very large constellations, commercial manned spaceflight, asteroid mining, in-space servicing, in-space manufacturing, and the coming increase in CIS-lunar activities will all change the space operating environment in ways we cannot yet fully appreciate. Perhaps the most pressing challenge created by this rapid expansion and increased diversity of operational space traffic is to render legacy concepts of space traffic management obsolete. In recognition of this coming transformation, the National Space Council developed Space Policy Directive (SPD) 3 which was signed by President Trump in June of 2018. This policy defines space traffic management as "the planning, coordination, and on-orbit synchronization of activities to enhance the safety, stability, and sustainability of operations in the space environment."[5] According to SPD-3, one of the foundational goals to achieve the required level of coordination and synchronization is to "improve SSA data interoperability and enable greater SSA data sharing."[6] In addition, information sharing is explicitly cited or implicitly assumed within all of the 21 Guidelines for the Long-term Sustainability of Outer Space Activities developed by United Nation's Committee on the Peaceful Uses of Outer Space (UN COPUOS, June 2019).[7]

A closer look at legacy STM concepts in light of the emerging operating environment highlights the critical need for a new information sharing framework. Today's operations are relatively low volume and static, lending themselves to a catalog approach of observation, orbital element calculation, catalog refresh, and conjunction notification. This paradigm of catalog information sharing will lag operations in a more dynamic operational environment of continuous thrusting and active maneuvering. Simply put, today's information sharing activities are decidedly insufficient when applied to the emerging and future operating environment. There must be an expanded vision for situational awareness of space operators and an expanded level of coordination and synchronization, including automated information sharing. Further, after an appropriate period of standards development and confidence building, safety-related information sharing among space operators should be obligatory. The obligation may be self-imposed by community agreements such as a collaborative decision-making MOUs with norms for data exchange when resolving issues between two operators. These can be limited exchanges not released to the public.

This imperative for a new level of information sharing will highlight the tension between the need to share for necessary preservation of the space operating environment and the need to protect sensitive mission information, and this is not limited to specific stakeholders. The global nature of space operations transfers risk of any single space operator to all other space operators, so a new information sharing framework must be a partnership between commercial, academic, national security, civil, and international communities. In other words, this problem is equally shared by government leaders, academic institutions, CEOs, regulatory agencies, and international bodies as well as consumers reliant on space-enabled data and network communications.

In recognition of this critical juncture in the evolution of space operations, the authors of this paper seek to generate thought among leaders of stakeholder organizations about information sharing, and to move the discussion forward with practical thinking about what and how information could and should be shared. Specifically, this paper will use insights gained from specific information sharing comparative models and conversations with space operators to propose a generalized information sharing framework that can be applied to various space mission applications to promote a safe, stable, and sustainable space operating environment.

## II. Comparative Models

An information sharing framework that meets the needs of diverse users and provides reliable, current, and actionable data is needed. As with any surveillance system, increased data and precision can safely increase capacity. This has been demonstrated in the aviation community repeatedly. With each improvement in the quantity and quality of information, a given volume of airspace can accommodate greater demand, because the capacity of the airspace is increased. Participation from government, industry, and academia across the space community is necessary for successful implementation. Any information sharing system predicated on voluntary participation will encounter

[5] Space Policy Directive 3, The White House, June 18, 2018.

[6] Space Policy Directive 3, The White House, June 18, 2018.

[7] United Nations General Assembly Committee on the Peaceful Uses of Outer Space Scientific and Technical Subcommittee Fifty-sixth session, A/AC.105/C.1/L.366, Vienna, 11–22 February 2019.

barriers and concerns that should be addressed in the development stage. It is useful to examine existing models from other domains to derive insight into structural design that can be used to develop an appropriate information sharing construct. These models fall into two distinct categories: broad information sharing for operational benefit and safety reporting. Information sharing systems that seek to provide operational benefits include elements of safety reporting systems, but also include data that provides value outside the pure safety domain. Safety reporting systems tend to be reflective, allowing actors to benefit from the risks encountered by other system users, whereas broad information sharing for operational purposes provides actionable information to be used for both tactical and planning purposes.

### A. Aviation - System Wide Information Management (SWIM)

System Wide Information Management is concept in Air Traffic Management (ATM) consisting of standards, infrastructure, and governance for the management of ATM and the exchange of data between qualified parties.[8] The goal of SWIM is to provide the ability for diverse organizations with diverse systems to share information in an interoperable manner. The motivating purpose of SWIM is to improve the efficiency and capacity of global air traffic management. SWIM is built on a global interoperability framework with the following layers:

- SWIM Enabled Applications
- Information Exchange Services
- Information Exchange Models
- SWIM Infrastructure
- Network Connectivity

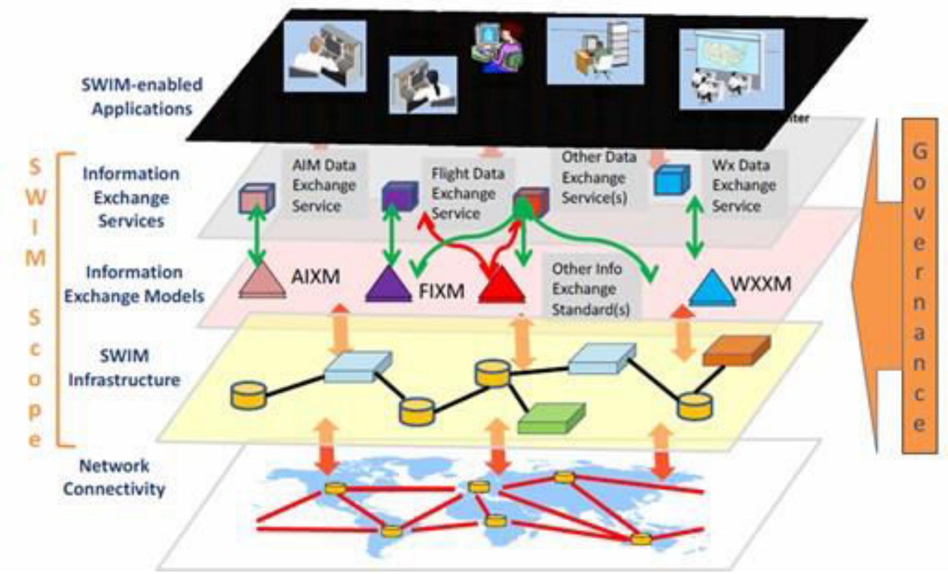

SWIM-enabled Applications
Information Exchange Services
AIM Data Exchange Service
Flight Data Exchange Service
Other Data Exchange Service(s)
Wx Data Exchange Service
Information Exchange Models
AIXM
FIXM
Other Info Exchange Standard(s)
WXXM
SWIM Infrastructure
Network Connectivity
SWIM Scope
Governance

**Fig. 1: SWIM Concept (Source: ICAO Doc 10039)**

The scope and governance of SWIM applies to the middle three layers, SWIM enabled applications are user defined and developed. In examining the purpose and principles of SWIM, we see very clear parallels to the information sharing needs of space traffic management. It is a secure architecture with trusted sharing of information

[1] International Civil Aviation Organization, Manual on System Wide Information Management Concept., online:https://www.icao.int/airnavigation/IMP/Documents/SWIM%20Concept%20V2%20Draft%20with%20DISCLAIMER.pdf [retrieved September 2020]

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2636. 'The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.'©2020 The MITRE Corporation. ALL RIGHTS RESERVED**

on a system-wide basis that includes early provision of intent data, supports collaborative decision making, and highly automated access to information. It is built on the following principles:[9]

- Information is shared securely on a system-wide basis
- Information is available where and when it is required
- Information may be personalized, filtered and accessed as needed
- System includes all tenets of cyber security including confidentiality, protection of data, networks and control systems, continuity of operations, and secure interoperability
- Requires authentication for user access
- Information sharing can be adjusted to mitigate proprietary concerns

The FAA implementation of SWIM facilitates common situational awareness for aviation system users by sharing air traffic management system information to external users including airline operators. It provides a single point of access for aviation data for both providers and users of data. In addition to eliminating individual point to point connections to access different data sets, SWIM translates data from different sources into standard data formats to support global collaboration. Data provide through the SWIM network includes Flight and Flow data, Aeronautical data, and Weather Data. This provides airspace users with access to the same real time data used by air traffic control and traffic flow management to support collaborative decision making. SWIM consumers include Industry, Airlines, Non-FAA Government entities, Academic and Research Centers, Airports, FAA Facilities and FAA Program offices.

In examining the stated purpose and benefits of SWIM, we see clear parallels to the proposal for information sharing for the space community. SWIM was designed to reduce costs for all users of National Airspace System (NAS) data, improve aviation safety and efficiency through common situational awareness, deliver consistent information to all users types, both internal and external, and to provide a secure data exchange among the NAS user community.[10] In addition to serving as a model for the space community, an information sharing system for space situational awareness could include access to SWIM as a valuable data source for launch operators.

## B. Maritime Information Sharing Environment (MISE)

Within the Maritime domain, the US has developed a National Maritime Domain Awareness Plan that includes a Maritime Information Sharing Environment to provide a secure, collaborative, information sharing environment. This environment is comprised of four parts, trusted systems and their users, uses the National Information Exchange Model (NIEM) – Maritime data standards, common attributes for access control and an information sharing infrastructure.[11] The MDA recognizes information as a national asset that should be made available to relieve other agencies from duplicative efforts and support consumers access to a greater understanding of the maritime environment. In this way, MISE serves to coordinate efforts across government agencies with a common need for the information.

[9] Skybrary, Systemwide Information Management, online: https://www.skybrary.aero/index.php/System-wide_Information_Management_(SWIM) [retrieved September 2020]

[10] Federal Aviation Administration, SWIM Questions and Answers, online: https://www.faa.gov/air_traffic/technology/swim/questions_answers/ [retrieved September 2020]

[11] The National Maritime Domain Awareness Architecture Plan, December 2013

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2636. 'The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.'**

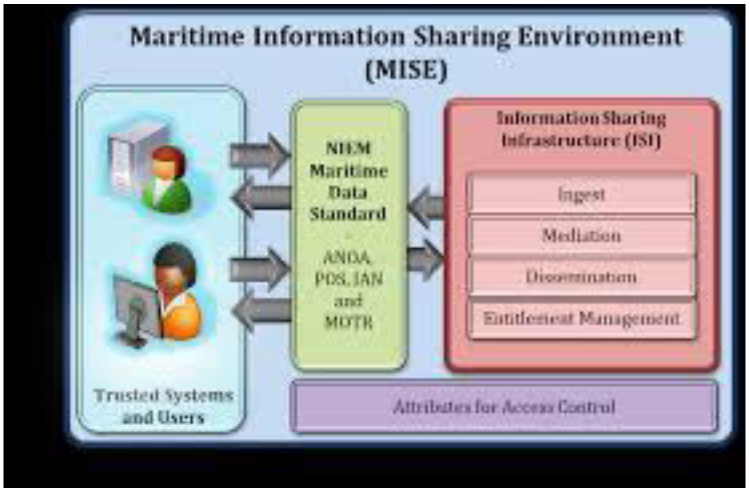

Maritime Information Sharing Environment (MISE)
Trusted Systems and Users
NIEM Maritime Data Standard
-
ANOA, POS, IAN and MOTR
Information Sharing Infrastructure (ISI)
Ingest
Mediation
Dissemination
Entitlement Management
Attributes for Access Control

**Fig. 2: Operational View of the MISE (source: National MDA Architecture Plan)**

The information sharing business process used to develop the MISE may prove useful to the space framework. The multistep information sharing process is:

1. Describe the operational use case being supported by the information sharing.
2. Identify the specific data elements required to support the use case,
3. Develop a standard definition, model or product for the information to be shared.
4. Identify and legal or policy driven constraints on the information.
5. Implement appropriate controls to ensure proper entitlement management.
6. Implement and monitor the sharing service.[12]

The maritime model also provides well defined steps for entitlement management and information management. Each system within the MISE is a trusted system, multiple agencies maintain separate systems but work together in a federation; trusted systems interact with the information sharing infrastructure but not each other, and the MISE is maintained by an independently governed entity. MISE uses an attribute-based access control model that uses information access policies to control which information is accessible by which users, this approach allows for the interaction with the system by diverse users without allowing access to more information than is necessary or appropriate.

Each of the examples provides useful insight for the space sharing framework. Many of the barriers to implementation, particularly with regard to industry concerns about proprietary data, are addressed in the models identified. In each implementation, the systems have provided value to both the consumer and the government.

## C. Safety Reporting Systems

Information sharing systems focused on safety reporting enjoy statutory protections in the US precluding the disclosure and use of that data for other than safety purposes.[13] In general, the data collected by safety reporting systems are held by a third party who de-identifies/anonymizes, analyzes, and aggregates the information for safety purposes. Often the third party is a non-government entity to further protect the data from disclosure under transparency standards like the Freedom of Information Act.

### a. Aviation Safety Information Analysis and Sharing Program (ASIAS)

[12] Ibid

[13] 49 U.S. Code § 40123.Protection of voluntarily submitted information

The Federal Aviation Administration ASIAS program is part of the aviation safety management regime. It uses voluntarily provided data from airspace users to evaluate known risks, evaluate deployed mitigations, and detect emerging risk.[14] The ASIAS database gathers electronic data from public and a proprietary data sources and increases the number and types of sources through a deliberate expansion plan. Members in the ASIAS program include commercial air carriers, general aviation operators, aircraft manufacturers maintenance providers, industry associations, training organizations, and government agencies including the FAA, NASA, and the Department of Defense. The data, particularly proprietary operator information, is protected through governance agreements with the owners of the data and databases to provide ASIAS safety analysts with access to relevant data.[15] De-identified safety data is maintained by a trusted third party provider and is made available to program participants. Authorized users are able to perform integrated queries across multiple databases to proactively identify safety issues. It is designed as a non-punitive, collaborative approach that is designed to provide data solely for safety purposes. Strong governance of the program is often touted as the key to the success of the program. In order to secure operator participation, the program had to overcome concerns that the information could be used to trigger enforcement action against the regulated industry. This barrier was overcome by limiting the access to the information by the regulator to aggregated information in addition to explicit standards that ASIAS data could not be used for enforcement action.

ASIAS creates a backward-looking data set for the purpose of analysis and identification of safety concerns targeting the prevention of accidents and incidents. While the purpose of the information sharing database may not provide a model for a space situational awareness information sharing regime, the structures of governance and incentives for voluntary participation is instructive for the space community. The use of de-identified data coupled with participant agreements that include restrictions on use, and the long experience illustrating confidence from the participants can serve as a model to build similar confidence from the space community. The existing model is able to identify issues after the fact, but aviation is working toward a predictive safety risk identification process that would provide insights in advance of potential accidents.

### b. Aviation Safety Reporting System (ASRS)

The ASRS program is a confidential, non-punitive, voluntary safety reporting system maintained by NASA as the responsible third party to capture, analyze, and report to the aviation community. This program provides for the input of qualitative data from the professional community. Reports cannot be used for enforcement purposes and the third party approach is used to ensure the anonymity of reporters under its statutory authority to do so. This is one of the older voluntary safety reporting programs of the FAA and is available to individuals in professions across the aviation industry including, pilots, air traffic controllers, cabin crew, maintenance, and others.

### c. Aviation Safety Action Program (ASAP)

The ASAP program is an agreement between the FAA and FAA Certificate holder organizations as part of an overall Safety Management System (SMS). It allows employees of an organization to report safety or security related events to the FAA without fear of reprisal. The two types of reports generally received are safety reports that involve a violation of regulations and reports of a general safety concern that do not appear to violate a regulation. This program was developed with the recognition that employees of certificate holders are resistant to providing safety information to the FAA if it is subject to public disclosure or enforcement action.[16] Participation in the ASAP program is voluntary.

## D. Common Elements

[14] Federal Aviation Administration, Fact Sheet – Aviation Safety Information Analysis and Sharing Program, April 12, 2016 online: https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18195 [retrieved September 2020]

[15] ASIAS, Welcome page, online: https://portal.asias.aero/ [retrieved September 2020]

[16] Federal Aviation Administration, FAA Order 8000.82: Designation of Aviation Safety Action Program (ASAP) Information as Protected from Public Disclosure under 14 CFR Part 193, Washington, DC, September 3, 2003.

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2636. 'The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.'**

Information sharing is a not a new concept and the barriers to implementation have been addressed in fields as diverse as homeland security and public health. The space community does not require a blank sheet of paper to accomplish this task. Both operational and safety information sharing regimes have certain common elements, including a need to balance the interests of the community with the interests of the individual operator. Common elements of an information sharing system answer primary questions:

- What data will be shared?
- Who will have access?
- Where will the data be shared and stored?
- When will the data be shared?
- How will users access the data?

An information system that seeks to move beyond superficial data provides protections to the participants and requires foundational elements that we see in the models discussed. This includes the protection and anonymization of data that may expose a vulnerability, clearly defined agreements for data protection and use, and well defined governance structures.

## III. Generalized Information Sharing Framework

In August 2020, the National Association of Public Administration published a Congressionally requested study that identifies key issues of data sharing and supports a conclusion that the US Department of Commerce should be the lead agency for Space Traffic management. Additionally, the Academy was required to report on related statutory, regulatory, and personnel funding matters, necessary information technology and data integrity initiatives, and national security considerations to support this mission. The Open Architecture Data Repository (OADR), under the direction of the Office of Space Commerce, and other data sharing mechanisms can support an information sharing regime. The study offers certain key principles, including:

- *For successful SSA/STM, data integrity, protection, and data sharing mechanisms must be supported by an incentive structure that promotes those mechanisms. Data security and competitive interests must be balanced.*
- *The major challenges to the successful establishment of open, networked approach to data management have less to do with technical obstacles than with difficulties in reaching agreement on issues such as the conditions under which data will be shared and how they will be paid for. In interviews with stakeholders, two major considerations were identified. These considerations are:*
  *1. What will be produced by the government versus purchased from commercial providers and provided by the government?*
  *2. What types of data will be provided, with whom will they be shared, and under what conditions will these data be shared?*[17]

This section introduces a framework to use for information and apply that framework to several mission categories that pertain to space operations. The aspiration is to use this framework in a consistent manner across multiple mission categories to encourage a greater practice of information sharing among space operators. The information types in the framework describe '*what* information is to be shared?', and the information sharing comparative models described in Section II provide insights into '*how* could the information could be shared'.

[17] National Academy of Public Administration, Space Traffic Management: Assessment of the Feasibility, Expected Effectiveness, and Funding Implications of a Transfer of Space Traffic Management Functions, Academy Project Number: 102252, Washington DC, August 2020.

Space Info Sharing Mission Categories (types of space activities)

Consider these four missions that are relevant to space operations, each cited in the recently published NAPA study on space traffic management[18]: 1) Space Traffic Management (STM); 2) Cyber security; 3) Radio Frequency Spectrum Management; and 4) Air-to-Space Debris ('Surface-to-Space') Management. There are certainly other mission areas that also pertain to space operations which could be included, but these four to allow a focused discussion of information sharing.

Space Info Sharing Data Types

For these four mission categories, we can generalize the kinds of information that could be shared among space operators. If all of the relevant information could be listed in a single column, such a list would have hundreds of elements, such as positional information, system status, system descriptions, environmental descriptions, and so on. The information would include the who, what, when, where, why? descriptions of the current system and future plans for that system.

Hard and Soft Data Concept

Consider two classes of data which could be provided: 1) 'hard data' – numeric description of a given situation, such as positional data using two-line elements (TLEs), satellite dimensions, remaining fuel, radio frequency power levels and many other quantitative measures; 2) 'soft data' – contextual information, such as planned maneuvers, general system health and status, general operating conditions in space, etc. Of course, most 'soft data' have 'hard data' descriptors, but there could be example where numerics aren't available or appropriate. Together hard and soft data provide a complete framework for potential information sources to be shared.

Tear Line Concept

In this study, we envision a set of hard & soft data that need to be shared to ensure safety of operations among all parties operating in a given space regime, such as LEO. Notionally, this information could be listed in a matrix and a line drawn between this information and other information that operators may be resistant or unwilling to share. We propose this distinction as a 'tear line' indicating that information below the line could be separated from the information above the line and retained by the operators. Information above the tear line would be shared by all operators for joint safety of operations.[*] Figure 2 illustrates the concept. We realize that the tear line is inherently 'fuzzy' and does not crisply define an unambiguous boundary. Generally, the community has come to agreement on what must be shared, but this boundary can change based on a given circumstance. The tear line could reside at one level for general system-wide sharing and could dive lower in cases where specific operators need to exchange additional information, for example, to work tactical resolutions to eminent threats.

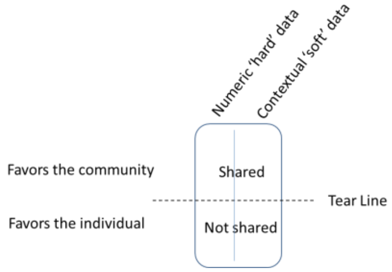


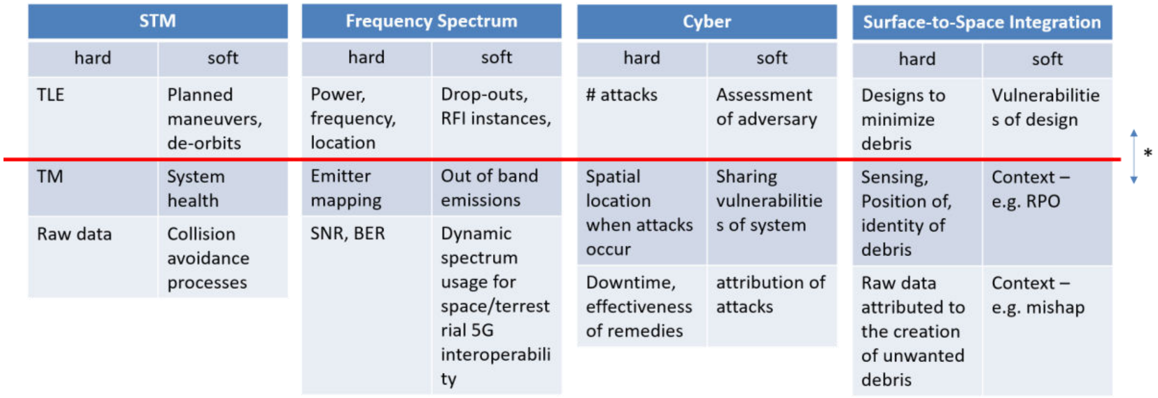
**Fig 2. Hard & Soft Data and Tear Line Concept**

[18] ibid

[*] *Note: in its conventional use, materials below a tear line are shared and information above the line are not. For the sake of our application, in which we focus on the information that should be shared, we have flipped the arrangement.*

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2636. 'The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.'**

Figure 3 shows representative information for the four space missions and a notional tear line (red). While depicted as a uniform straight red line across these missions, this is only notional. Again, this line is actually more ‘fuzzy’ than depicted and, as shown, can move up or down deeper into the information depending on the specific context.



| STM | | Frequency Spectrum | | Cyber | | Surface-to-Space Integration | |
|---|---|---|---|---|---|---|---|
| hard | soft | hard | soft | hard | soft | hard | soft |
| TLE | Planned maneuvers, de-orbits | Power, frequency, location | Drop-outs, RFI instances, | # attacks | Assessment of adversary | Designs to minimize debris | Vulnerabilities of design |
| TM | System health | Emitter mapping | Out of band emissions | Spatial location when attacks occur | Sharing vulnerabilities of system | Sensing, Position of, identity of debris | Context – e.g. RPO |
| Raw data | Collision avoidance processes | SNR, BER | Dynamic spectrum usage for space/terrestrial 5G interoperability | Downtime, effectiveness of remedies | attribution of attacks | Raw data attributed to the creation of unwanted debris | Context – e.g. mishap |

*Tear line could shift up/down depending on the operational context and timelines

**Fig. 3 Information Sharing Framework Applied to Space Mission Applications.**

According to SPD-3, Space Traffic Management is “the planning, coordination, and on-orbit synchronization of activities to enhance the safety, stability, and sustainability of operations in the space environment.” Its primary enabling objective is space situational awareness, which is “the knowledge and characterization of space objects and their operational environment to support safe, stable, and sustainable space activities.”[19] To achieve a future vision of effective coordination and synchronization, all space operators must commit to information sharing from the design phase through end of mission. The level of information sharing required to establish a basic level of traffic safety in space operations will change depending on where the mission is in its lifecycle, the health and status of the vehicle, and the external contextual environment. Applying the information sharing framework, the hard data above the tear line is the minimum current and projected orbital location data to prevent and mitigate conjunctions, and the soft data would be the contextual information related to that orbital location data. Although specifically what information would sit in each row/column intersection of the matrix of Figure 3 remains to be solidified, it is easy to see how, for each phase in a satellite lifecycle, specific information and contextual data would be required to perform STM. In the event a conjunction is identified or a debris-generating anomaly occurs, it is also easy to see how the tear line, which would typically protect sensitive information at a certain level, might shift downward with the increased coordinate required to respond to the event.

Cyber protection, as applied to space operations, is the effort to minimize vulnerabilities of space systems through effective design, maintenance, and operations, and to share information on existing and emerging threats in a way that allows stakeholders to mitigate the impacts of those threats. These efforts apply not only to the space segment, but also to ground systems and telemetry links. At the same time, the cyber landscape is constantly changing with bad actors probing for vulnerabilities and exploring new attack vectors. Cyber threats present risk to the entire space enterprise, so space operators have a common interest to share information to mitigate and defeat these threats.

[19] Space Policy Directive 3, The White House, June 18, 2018.

Applying the information sharing framework to cyber protection, even considering the sensitivities of cyber vulnerabilities and attacks, there is some level of information exchange regarding cyber threats and attacks that would fall above the tear line and support the concept of basic cyber protection.[20] Depending on the nature and circumstances of a particular threat or attack, particularly at specific times in a space mission lifecycle and geopolitical contexts, it is easy to envision a scenario where the tear line shifts to allow for increased coordination to defeat specific threats or avert greater impacts.

Spectrum interoperability refers to the efforts to prevent and mitigate frequency spectrum interference for communications in, from, and through space. A significant portion of this effort is through deconfliction in the licensing process, but because satellites operate in different orbital regimes, there is also increasing risk for situational signal conflict, particularly with the emergence of very large constellations. Information sharing in this environment will be key to establishing procedures and enabling innovative techniques of preventing and mitigating this interference. Basic broadcast information is already made public through the licensing process, so the foundation for hard data sharing above the tear line is already set. Expanding this foundation to apply to all operators, and adding amplifying information, or soft data, will increase the opportunity for developing innovative deconfliction techniques, and shifting of the tear line when appropriate will allow for improved mitigation techniques when interference does exist.

Surface to space (S2S) integration is the challenge of physical and spectrum traffic management during ascent and descent of space traffic through the atmosphere, primarily with aviation traffic. Increased launches, variation of flight paths and performance characteristics, and a multiplicity of geographical points of ascent is problematic even for a low volume of traffic. To ensure safe coexistence, accurate and timely tracking of aircraft and space systems into a single operational picture is essential. However, the manual processes used to manage space and airline traffic is unable to scale to accommodate this growth without causing undue impact upon the aviation industry.

This challenge is growing as new spaceports offer opportunities for launch from more and different locations. Tactics, techniques, and procedures are under development that will normalize traffic coordination and minimize traffic disruption for all types of traffic. Information sharing is and will continue to play a critical role in the S2S operating regime. Establishing above the tear line, hard data sharing for essential information is key to normalizing this traffic deconfliction. As in other mission areas, the tear line will shift under appropriate circumstances with stakeholder operators to ensure traffic deconfliction when baseline data sharing is insufficient.

Discussing Information Sharing with Industry

Through leadership provided by the US Chamber of Commerce, our team is conducting working sessions with several space system owner/operators and stakeholders to discuss the issues associated with information sharing. We will continue to conduct these working sessions going forward, and will provide an update of our findings at the ASCEND conference. We believe that this is a timely and helpful fresh-look at the general concept of information sharing considering information sharing mechanisms (Section II) and information sharing details (Section III) described in this paper.

Conversation thus far with industry revealed some interesting insights. First, there is value in clearly articulating the case for information sharing that can serve as a consensus perspective for operators, to include why it is necessary and the benefit to be gained in exchange. This is particularly true given the added expense associated with sharing and the potential risks of divulging information. Regarding the specific information to be shared, it is important to clarify what problem is being addressed and what data protections are in place. There may even need to be a provision for anonymous sharing where necessary. For anonymous sharing, there are numerous existing constructs in other domains from which to learn so it will not be necessary to start from scratch. Second, data sharing must be seen as part of the larger picture of national mission authorization, licensing, international relations, and support to the licensing nation's interests. In this respect, data sharing should be viewed more as a matter of incentive and benefit than carrot and stick. While asking companies to share information that could potentially impact their business or mission, there must be a way to incentivize them. In return, the companies should have the confidence the data shared voluntarily will not then be used punitively by regulatory agencies. Third, those we engaged with generally did not see a downside to information sharing, and could not identify a risk that outweighed the benefit. In fact, data sharing inspired an exchange of ideas that generally benefited all involved, and this applied across the space mission areas we

[20] Nayef Al-Rodhan, "Cyber security and Space Security", *The Space Review in Coordination with Space News*, URL: https://www.thespacereview.com/article/3950/1 [retrieved August 14, 2020].

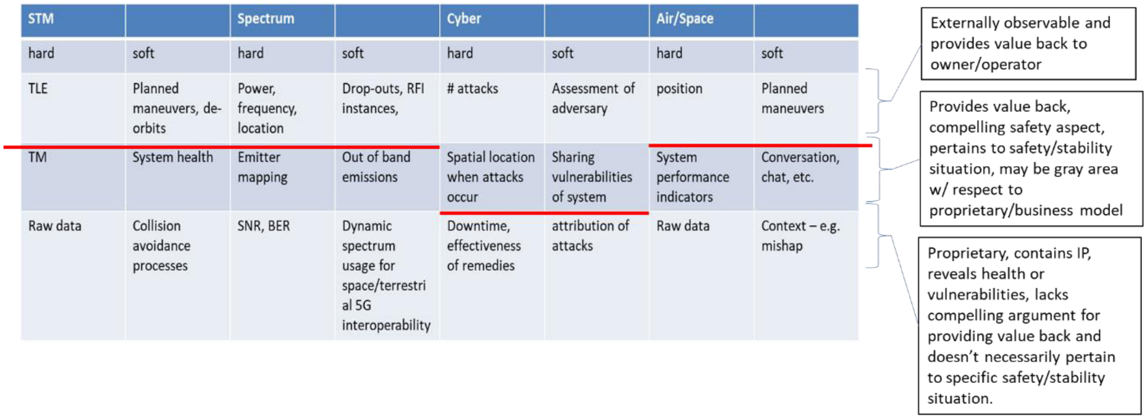
**Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2636. 'The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.'**

discussed. It was only when the information revealed vulnerabilities, details on health and status of systems, specific mission activities, or divulged intellectual property that data sharing was seen as a detriment rather than benefit. Clearly, the point at which data sharing crosses into these areas of concern may be different for each of the space mission areas. Cyber, for example, may have a fairly low threshold for sharing threat data before infringing on proprietary information, and this is an area where techniques like anonymous sharing and technology sharing agreements could play a role. Applying these themes to our matrix (Figure 3), we begin to see three regions described below and depicted in Figure 4:

Above the tear line
Generally, this is information that is also externally observable, such as position or emitted RF spectrum, provides value back to the provider, such as to avoid collision or interference, maximize launch window opportunities, and which relates to safety and stability of space operating environment.

In the vicinity of the tear line
Generally, this is information that addresses a compelling safety aspect, such as an anticipated conjunction, pertains to safety and stability situation, but may be gray area w/ respect to proprietary data, intellectual property or business model. Sharing data in the vicinity of the tear line also builds trust among and between providers/users of information.

Below the tear line
Generally, this is information that is proprietary, contains intellectual property, reveals health status or specific vulnerabilities, lacks a compelling argument for providing value back, and does not pertain to safety and stability of space operating environment.



| STM | | Spectrum | | Cyber | | Air/Space | |
|---|---|---|---|---|---|---|---|
| hard | soft | hard | soft | hard | soft | hard | soft |
| TLE | Planned maneuvers, de-orbits | Power, frequency, location | Drop-outs, RFI instances, | # attacks | Assessment of adversary | position | Planned maneuvers |
| TM | System health | Emitter mapping | Out of band emissions | Spatial location when attacks occur | Sharing vulnerabilities of system | System performance indicators | Conversation, chat, etc. |
| Raw data | Collision avoidance processes | SNR, BER | Dynamic spectrum usage for space/terrestrial 5G interoperability | Downtime, effectiveness of remedies | attribution of attacks | Raw data | Context – e.g. mishap |

Externally observable and provides value back to owner/operator

Provides value back, compelling safety aspect, pertains to safety/stability situation, may be gray area w/ respect to proprietary/business model

Proprietary, contains IP, reveals health or vulnerabilities, lacks compelling argument for providing value back and doesn't necessarily pertain to specific safety/stability situation.

*Tear line could shift up/down depending on the operational context and timelines

**Fig. 4 Information Sharing Framework with Industry Engagement Themes.**

## IV. Conclusion

Commitment to sharing "above the tear line" information necessary to maintain a safe and stable operating environment is key to addressing the challenges of the rapid increase in the volume and diversity of space activities. Consistent with SPD-3, improving SSA data interoperability and enabling greater information sharing should be a fundamental goal and stakeholder obligation in current and future SSA and STM efforts, and by extension other appropriate safety-related space mission areas. Recognition of this reality is just the beginning of the discussion to flesh out the specifics of that data sharing construct. Although there are unique attributes and challenges to space-related operations, the detailed information sharing discussion should begin with careful study of similar efforts, and adaptation of the lessons learned from those successful models wherever possible. The recently released NAPA study on Space Traffic Management endorsed Department of Commerce as the civil agency lead for STM, and thus the organization to lead development of an Open Architecture Data Repository and other data sharing mechanisms. The report further acknowledges "data security and competitive interests must be balanced" and lists as a major challenge the effort to determine "What types of data will be provided, with whom will they be shared, and under what conditions will these data be shared."[21] Now is the time for space operations stakeholders across the spectrum to accept the challenge of fleshing out hard and soft data that must be pushed above the tear line and working with Commerce to establish internationally recognized norms of safety-related information sharing.

[21] National Academy of Public Administration, Space Traffic Management: Assessment of the Feasibility, Expected Effectiveness, and Funding Implications of a Transfer of Space Traffic Management Functions, Academy Project Number: 102252, Washington DC, August 2020.

**Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2636. 'The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.'**