Decentralized space information sharing as a key enabler of trust and the preservation of space

Harvey Reed
The MITRE Corporation, 202 Burlington Road, Bedford, MA 01730, hreed@mitre.org
Dr. Nate Dailey[(1)], Dr. Ruth Stilwell [(2)], Dr. Brian Weeden[(3)]
[(1)] The MITRE Corporation, 7515 Colshire Drive, McLean, VA 22102, ndailey@mitre.org
[(2)] Aerospace Policy Solutions, LLC, 275 Commercial Blvd, Suite 210, Lauderdale-by-the-Sea, FL 33308, office@aerospacepolicysoutions.com
[(3)] Secure World Foundation, 1779 Massachusetts Ave. NW, Washington, DC 20036, bweeden@swfound.org

ABSTRACT

Preservation of space for its long term sustainable use requires stakeholders who not only want to preserve the usability of the domain for the benefit of all humankind but also with access to trusted and relevant information to make informed decisions and to take constructive actions. Space safety is a stakeholder-driven activity; there is no single controlling authority over space as an international domain. These stakeholders want to limit their own negative behavior, including the generation of space debris and other pollution while practicing positive behaviors to expand scientific and commercial activities by following recommended practices for launch, on-orbit, decommissioning, and reentry. This requires using trusted space data to self-synchronize activities individually. This trusted space data includes the position of space objects (during launch, in-orbit, or de-orbit), the activity of X (sustain orbit, maneuver, or decommission), and more. However, the challenge is that each stakeholder, including government, industry, and academia, has limited access to comprehensive knowledge of the space ecosystem, even though this information may be needed in their roles as producers and consumers of space-related information.

This paper describes the information-sharing infrastructure needed to ensure all stakeholders can benefit from equal access to symmetric and trusted information on the state of the space ecosystem. Symmetric information assures that all stakeholders have access to the same information. Trusted information means that it is attributed, available, has known pedigree and provenance, and is not controlled by any individual stakeholder or subset of stakeholders, and cannot be maliciously altered. The thesis of this paper is that when individual stakeholders have access to trusted data in a symmetric manner, then one of the emergent effects is the preservation of space. Further, beyond individual stakeholders, international partnerships can benefit from the ability to combine expertise by sharing trusted and symmetric space data as an opportunity to advance the preservation of space, which benefits everyone in the partnership. This approach recognizes similar considerations applied to commercial and academic relationships.

This paper explores building and using a decentralized space information sharing infrastructure to provide trusted and symmetric space-related data. This infrastructure can consist of implementation patterns, practices, and methods, as well as operational capabilities. This decentralized information infrastructure builds on nascent technical frameworks to support decentralized sharing of data, such as the ongoing Blockchain-Enabled Space Traffic Awareness (BESTA) effort.

This paper illustrates the decentralized information sharing infrastructure concepts in the form of use cases with a description of benefits to various stakeholder types. A use case template is introduced, which can be used to further scope ecosystem requirements. The goal of using a decentralized approach to building a space stakeholder trust model, built on a technical approach for decentralized information sharing, is to empower individual stakeholders to bring the space community closer to its shared goal of preserving the long term sustainability of space.

Keywords:
Space Traffic Management (STM), Space Surveillance Network (SSN), Space Domain Awareness (SDA), Persistence, SNARE, BESTA, GREAT

1. INTRODUCTION

The growing demand for space access and services on Earth provided by space activity is increasing congestion and leading to models of greater autonomy by space actors. In other domains, where activity is subject to a sovereign authority, this increase in activity is managed through centralized regulation and/or operational restriction. However, this is not realistic for the international orbital domain where individual states bear responsibility for the continuing supervision of objects launched from their jurisdiction, and operators are expected to operate in a manner that does not interfere with the actions of others in the shared domain. This shared responsibility requires shared information. This research paper addresses critical space information sharing topics necessary to advance space safety, increase the carrying capacity of the orbital domain, facilitate self-synchronization, and promote the long term sustainability of space. This research effort is funded by MITRE research, with numerous space Subject Matter Experts (SME) participation.

Information sharing is not new to the space community, and we have been using information sharing in one form or another since the early age of manned spaceflight. In 1975, the Apollo-Soyuz Test Project successfully joined two distinct space vehicles, with different designs, technologies, life support systems, and engineering from two countries who were not only in competition but critical of the other's engineering, governing, and political philosophy (Fig. 1). Considering the political posture between the US and Soviet Union at the time, it was not rational to believe either would share all their space technology. However, the "handshake in space" was successful, precisely because they were willing to identify and share the information necessary to achieve their common goal. In this case, the Apollo-Soyuz sharing was through a bi-lateral information-sharing agreement.

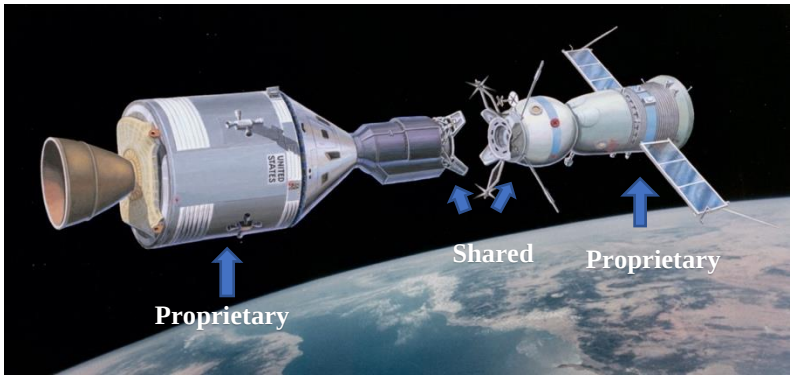

Figure 1: Apollo-Soyuz Test Project (image courtesy of R. Bruneau/NASA)

This demonstration of effective bi-lateral information sharing in Apollo-Soyuz led to greater information sharing in the Shuttle-Mir program and, eventually, the multi-lateral International Space Station. This evolution from bilateral information-sharing arrangements between adversaries to the multi-lateral ISS framework among friends, e.g., Canada and Japan, and competitors, e.g., Russia, is instructive for the challenge we are facing today.

The principles used in the Intergovernmental Agreement that governs the ISS inform a decentralized information sharing framework [1]. It is a cooperative framework that respects national jurisdiction, provides for the exchange of goods and services between participants without exchange of funds, and protects participants' intellectual property. The goal was to create a physical structure in space to provide a permanently inhabited trusted space station. The GREAT/BESTA decentralized information-sharing approach aims to create a permanently useable trusted data means in cyberspace [2].

This research assumes that the international model for space traffic management relies on decision making by sovereign, commercial, and non-profit actors and relies on space information including:

- Initial lifecycle events (launch, orbit insertion, maneuvers)
- Present observed orbit (awareness)
- Intention to maneuver (awareness)
- Computed possible conjunctions (collision prediction)
- Ongoing and terminal lifecycle events (collision detection, decommission)

Space information is exchanged between many space actors, in the role of a space information provider, consumer, or both, generally through bilateral arrangements, as shown in Fig. 2. This is a fundamentally asymmetric approach.

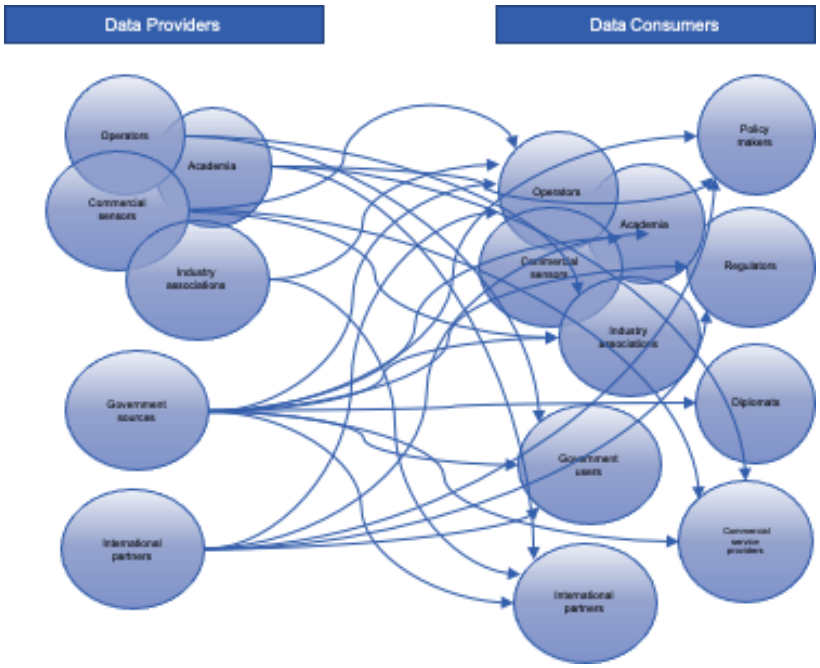

Figure 2: Bilateral Information Sharing

In the bilateral scenario, trust is established by the individual relationship between provider and consumer. This research assumes that rational decision-making in space traffic management among the independent sovereign, commercial, and non-profit actors, must use space information that is both symmetric and trusted. The risks carried by asymmetric information are well established in both economics and international relations. In financial markets, it is frequently identified as a cause of market failure as Mark J. Flannery, Chief Economist, and Director, Division of Economic and Risk Analysis at the Securities and Exchange Commission describes, “And often the market failure itself derives in some way from the fact that value-relevant information is costly to obtain and costly to evaluate” [3]. However, achieving symmetric access to relevant information across a global domain requires a mechanism to establish trust between those providing the data and those consuming the data (Fig. 3).

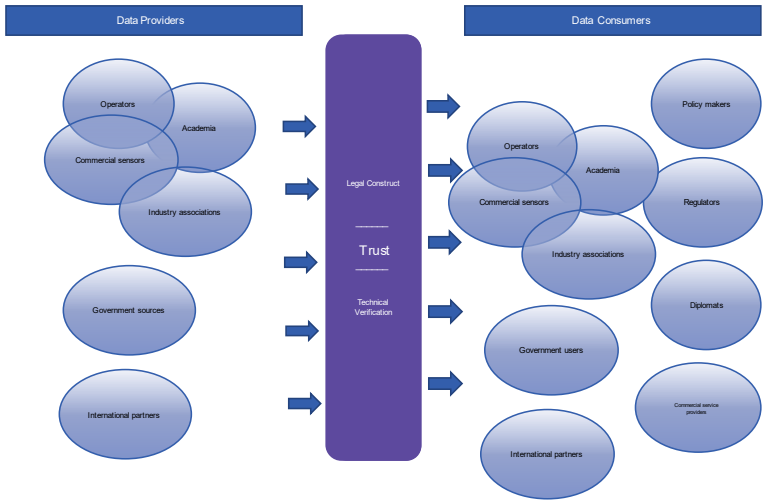

Figure 3: Symmetric Information Sharing

Symmetric space information does not imply that all information is shared with all participants. On the contrary, an effective decentralized information-sharing model asks international participants to share information necessary to achieve a common goal. The space community must agree on what information is needed to be universally shared to achieve an accepted goal, like the long term sustainability of the space domain to ensure continued use and availability for the benefit of all humankind. These foundational principles are already agreed upon in the Outer Space Treaty and in the COPUOS Guidelines for the Long Term Sustainability of Outer Space Activities. Information sharing is recognized as a critical tool to move that goal from aspirational to operational. The Space Safety Coalition (SSC), in developing best practices, identified information sharing as a foundational principle, stating:

> *In developing the following best practices, it was recognized that future efforts may be warranted to:*
> *Adopt an existing forum or establish new forum(s) to create conditions favorable to the sharing of relevant space information and operator-to-operator coordination of space activities [4].*

Industry consortia, like the Space Data Association (based in the US) providing services to members in the global community and the EU SST (the corporation formed under the European Space Surveillance and Tracking Framework) providing services to EU members, recognize the need to share information on space operations that goes beyond sensor derived data. These voluntary consortia demonstrate the value of increased information sharing. While this mechanism creates trust among participants within each consortium, there remains a need for a mechanism to exchange operational space information from entities that are not within a specific consortium or between independent consortia.

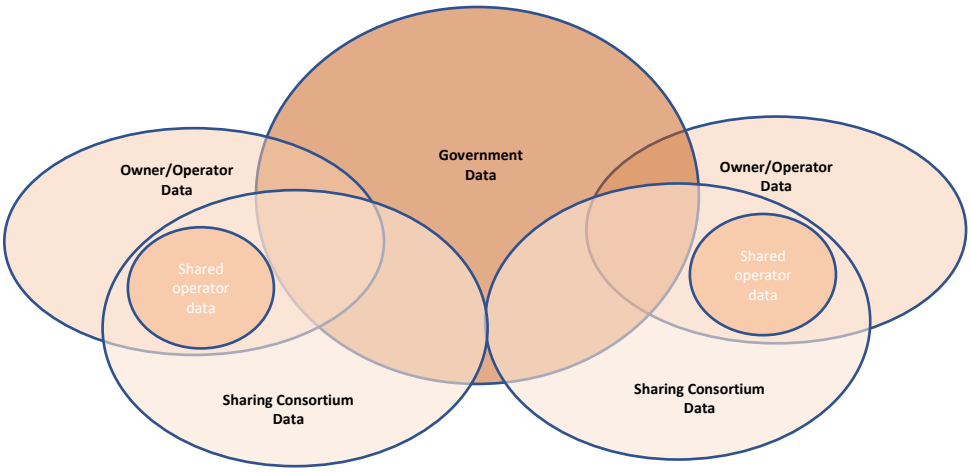

Figure 4: Data sharing with consortia

It is essential to acknowledge that while the space community has adopted certain high-level goals, significant barriers to information sharing remain within the space community. For the long term sustainability of space, it is necessary to enable trusted information sharing that shares information between parties that do not trust one another.

2. TRUST AND TRACEABILITY

The space community continues to work toward increased information sharing, as demonstrated by the proliferation of bilateral arrangements and the emergence of data sharing consortia. There is increasing recognition among governments and satellite operators that actionable shared information is needed to achieve the goal of sustainable space. To be actionable, shared information must be trusted. Trusted means that the information is attributed, has integrity with resilience and tamper-evident properties, assuring the data is not maliciously edited. Achieving this trust requires the information to be traceable across stakeholders to its origin.

Data can be shared using a variety of models, including centralized databases, distributed ledger technology, and blockchain [5]. The primary difference between the data sharing models is the centrality of data - where the data is stored and under whose control. For example, a centralized database stores data centrally, under the control of one organization. Distributed ledger distributes the storage, adding resilience against accident but retains central organizational control. In contrast, blockchain distributes redundant copies of data via blockchain nodes, where control can be decentralized across various stakeholders who own and operate nodes.

The thesis of this paper is that decentralized information sharing is required for the international domain to enable global participation. This guards against a single party retaining control over the information storage and flows since even though many parties may consider the information to be trusted, the ownership of the data itself creates a trust barrier with some and perhaps key participants. Across the literature on space situational awareness, space governance, and space traffic management, a common thread emerges; that global norms of behavior in space need to be established. However, efforts to achieve that goal are frequently sidelined by geopolitical rivalries and a lack of trust between the parties. For example, the Artemis Accords, proposed by the United States in 2019 and adopted in October of 2020, did not diverge from the existing principles agreed to in the Outer Space Treaties: their stated purpose is to "provide for operational implementation of important obligations contained in the Outer Space Treaty and other instruments" [6]. Criticism generally focused not on the content of the Accords but rather that it is too focused on U.S. interpretation and favors U.S. commercial interests, and it was not immune to perceptions regarding the US commitment to international partnerships [7]. This highlights perception barriers to global agreement on norms when the information-sharing mechanism is controlled by one state or region. Decentralized information sharing provides the means to ameliorate this friction.

3. STAKEHOLDER DRIVERS

The international nature of space precludes the application of sovereign hierarchical governance structures as the sole method of governing the space domain, including space safety. While individual states bear international responsibility for governmental and non-governmental national activities in outer space (under the provisions of Article VI of the Outer Space Treaty), there are no provisions for a state to exercise authority over the activities of another state. As we have learned from other international domains, agile polycentric governance can be structured to maintain safe operations in a shared domain. This focus on safety, and a willingness to identify the specific types of data where sharing can enhance safety in shared orbits, can serve as a foundational principle for building trusted systems.

Common shared information is foundational for effective space safety policies. Over the last decade, the ninety-eight members of the United Nations Committee on the Peaceful Uses of Outer Space have agreed to 21 guidelines for the long term sustainability of space [8]. More recently, the United Nations General Assembly has launched another initiative aimed at developing norms of responsible behavior for space to address security concerns [9]. While laudable, implementation of these and other political efforts depends upon stakeholder collaboration and transparency.

Trusted data is required to ensure that the establishment and use of norms are based on measurable behaviors giving stakeholders the opportunity to monitor one another in the shared domain. Without a trusted mechanism to observe or track behaviors, norms are merely aspirations for which we may mistakenly believe others have adopted and with which they comply. Sociology is rife with examples of norms in one culture that conflict with norms in another, and space is not immune from this risk. For example, in 2019, Mission Shakti was celebrated by India as their successful demonstration of an anti-satellite weapon and argued that it was done at a sufficiently low altitude to ensure debris would deorbit quickly. However, some countries were critical of the approach and claimed that there is persistent debris resulting from the mission. Mission Shakti was modeled after the 2008 US destruction of USA193 and illustrated the need for agreed-upon information sharing standards to ensure that the safety discussions do not devolve into political posturing and escalating conflict.

A sustainable space environment benefits all stakeholders. However, there are other motivators in the space community that must be considered. In addition to the shared community value of preserving the space domain, users may also seek to maximize operational freedom, to self-synchronize, to minimize the frequency of conjunction risk where a maneuver is required, and to avoid external regulation. The Satellite Industry Association documented specific industry concerns in a white paper in 2020, including concerns with timeliness, orbital accuracies, tracking and space situational awareness analytics, and availability of information. The paper offers this unambiguous industry view:

> *Currently, space operators rely on SSA services and conjunction messages to characterize the space environment and anticipate and avoid collision. While these SSA services are important and useful today, they fall short of the actionability required to establish space safety and sustainability of the space environment [10].*

3.1. EVOLUTION AND CODIFICATION OF NORMS

The desire to reach information-sharing agreements has created a proliferation of bilateral arrangements that, while necessary for the short-term, may impede progress on the long term global scale. The decentralized information-sharing approach provides an infrastructure that does not presume norms of behavior or standards to be imposed but rather provides a trusted means to store and share data to support international decision-making and meet the shared goal of the preservation of the space domain.

In recent US congressional testimony regarding norms of behavior for space use, phrases were used like "we need enforceable norms" for the use of space. While norms can eventually become laws that may be enforced, norms themselves are not enforceable and cannot be imposed.[*] It is useful to review elements of the evolution and use of norms and their lifecycle. Patterns of norms evolution are described in numerous studies, as cited by Martha Finnemore in her seminal work. In short, norm influence has a three-stage process: norm emergence, norm acceptance, and norm cascade. The tipping point exists at the first two stages, where a critical mass of relevant state actors adopt the norm [11].

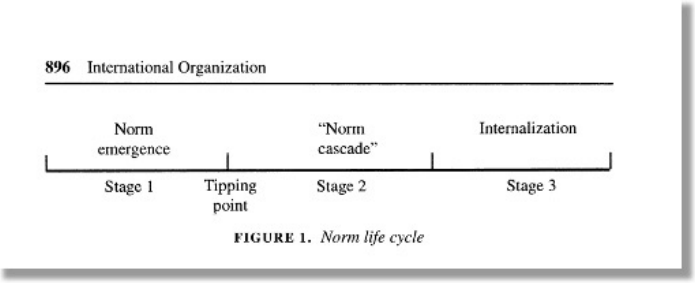

Figure 5: Norms Life Cycle

> *NORM ENTREPRENEURS.* Norms do not appear out of thin air; they are actively built by agents having strong notions about appropriate or desirable behavior in their community. Prevailing norms that medical personnel and those wounded in war be treated as neutrals and noncombatants are clearly traceable to the efforts of one man, a Genevese Swiss banker named Henry Dunant. Dunant had a transformative personal experience at the battle of Solferino in 1859 and helped found an organization to promote this cause (what became the International Committee of the Red Cross) through an international treaty (the first Geneva Convention). Norm entrepreneurs attempt to influence states (norm leaders) to embrace new norms.

A dynamic of imitation characterizes the second stage as the norm leaders socialize other states to become norm followers. The stage where norms "cascade" through the rest of the population (in this case, of the international space community) out of a mixture of pressure for conformity, legitimation, or self-esteem. "At the far end of the norm cascade, norm internalization occurs; norms acquire a taken-for-granted quality and are no longer a matter of broad public debate [11]."

Principles and norms that apply to the space domain flow two ways and should tie back to space policy criteria. Incorporating values and organizational culture, norms for space use can drive technology innovation and engineering models that define how systems function. In turn, this can influence acceptable manners in which space faring and space-related organizations go about fulfilling their mission or business. Sound architectural principles may be designed to encapsulate the general intent of space-related activity and serve to facilitate the norm cascade process sufficiently and clearly. Architectural data dictionaries should serve as acceptable vocabulary around which all stakeholders can rally to improve specificity. Norm entrepreneurs call attention to or "create" issues by using language that names, interprets, and dramatizes them in what social movement theorists call "framing" [12]. Such cognitive frames are important for norm entrepreneurs because they help resonate with broader public understanding and subsequently become adopted as new ways of talking about and understanding issues [11].

In all cases, establishment, promulgation, and widespread use of norms require a means of trusted and decentralized information sharing to assure all stakeholders that norms are expressed consistently, and measurement of related activity is expressed without malicious editing or deletion.

[*] In developing norms, it is important to recognize and build on other efforts ongoing in the space community, reports like Robin Dickey's *Building Normentum: A Framework for Space Norm Development,* published by the Aerospace Corporation provide useful definitions and strategic decision points that can be used to focus the efforts of the space community. https://aerospace.org/paper/building-normentum-framework-space-norm-development

Accordingly, architecture disciplines can help to harness technology innovation and frame the vocabulary necessary to influence the normative lifecycle for the responsible use of space by imbuing policy formulation with consistency, clarity, and communicative discourse. At the core of responsible use of space are mutual interest and the principles of spaceflight safety. By extension, this includes the ability for space operators to have an intersubjective understanding of each other's intent regarding certain activities, especially those susceptible to 'dual use' misinterpretations. Due regard, harmful interference, and unimpeded access are some of the commonly discussed ideas requiring improved clarity of understanding, as they are mentioned in the core treaties governing outer space activities yet are not well defined in operational or legal practice.

Recognizing that signatory States act at their discretion with respect to international guidelines for safety and security in outer space, provisions of Article IX of the Outer Space Treaty prescribe a requirement to avoid potentially harmful interference with the space activities of other States. The architectural codification of behavioral norms, ethics, and standards of practice, in conjunction with a universal vocabulary, and policy and technical models, is an approach that enables objectively measuring harmful interference by comparing observed behavior (via SSA capabilities) with prior stated intent (codified shared agreements, norms, and/or declared national policies).

Establishment and use of clearly understood behavioral norms may result in:

- Conditions of stability in outer space.
- Common characterization for actions of self-defense in outer space to minimize problems of ensuring the safety of space operations.
- Objective criterion for what constitutes "harmful interference."
- Criterion for the notion of harm and under what circumstances it should be ascertained.
- Clear understanding of the modalities of resorting to self-defense in outer space.
- Classification of conflict and near-conflict situations in outer space.

Regarding codifying shared agreements for space, there are two basic forms of ethical standards; those that judge based upon the nature of the action being good or bad, and those that judge the goodness of consequences of actions. Such potentially rule/act-based theories of moral obligation are generally classified as deontological and teleological, respectively, in the field of applied ethics. Over the next few years, it may become a topic of discussion among the international community to determine the appropriate mix of rules that guide behavior and specify act-based theories that are flexible enough to deal with conflict and exceptions. Balanced well together, these two approaches for applied ethics in judging space behavior help to avoid the two equal problems of too-many-exceptions vs. too much rigidity in applied ethics. Both families of ethical standards rely on a foundation of trusted shared information.

3.2. MINIMUM VIABLE ECOSYSTEM

Stakeholders form a group and remain together based on a common need to make rational risk-based decisions and evolve shared norms to coordinate activities. The concept of Minimum Viable Ecosystem (MVE) is useful here to describe such groups of stakeholders [13]. There needs to be a critical mass of interested participants to share enough information to warrant the effort expended. Identifying the smallest subset of data needed to share to create value in an ecosystem is as important as the number of participants. This MVE concept is seen in emerging forming ecosystems such as the manufacturing supply chain domain, where actors have a mutual interest to share traceability information (e.g., Mediledger https://www.mediledger.com/dscsa-fda-pilot-project). Decentralized information sharing is emerging as a useful means to exchange risk-based and coordination information in a symmetric and trusted manner and thus can connect stakeholders who are distant from each other.

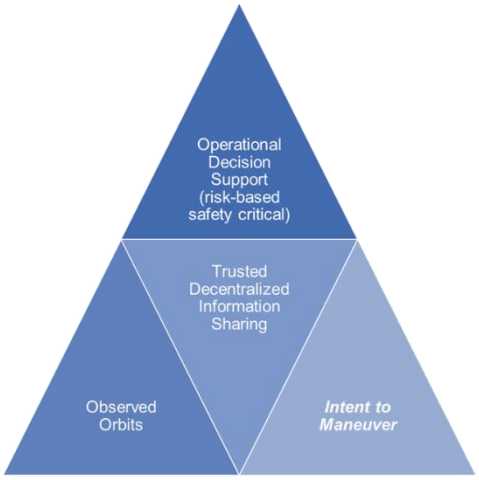

Figure 6: Decision Support Hierarchy

Based on prior calls to share safety-critical operational information and reinforced by space domain SMEs who collaborated in this effort, both orbital position information and intent to maneuver are required as the minimal set of information which must be shared or otherwise made available to all space participants. This information must be shared in a symmetric manner where everyone sees the same shared information and a trusted manner with provable attribution, data integrity, and resilience to attack. The relationship between orbital and intent to maneuver information trusted decentralized information sharing and decision support is shown in Fig. 6.

Starting with the universal set of orbital position information, risk-based decisions also require intent to maneuver. Without universal sharing of both orbits and intents, the terrestrial analogy is road traffic without the use of turn signals. While operations are possible, they are less safe and less efficient than an environment where the intent is signaled as well. Trusted decentralized information sharing is applicable to both stated intent and observed behavior. The combination of intent to maneuver and orbital position can be considered the starting set of information for an initial MVE which includes all space participants.

This research focuses mostly on the universal subset (all space participants) but recognizes that additional subset ecosystems with specific interests (e.g., decommissioning and disposal) will also form. Further, these specialized affinity group ecosystems can grow and operate independently but will depend on the universal subset for orbital and intent information. Such an approach for sharing information promotes norms that enable a consistent understanding of conformant and anomalous operational behavior. These norms and information sharing make it possible to bridge/amend differences of perception in the interest of universal clarity of operational intent. This may result in avoiding unintended effects, surprise, and escalation. The trusted decentralized information-sharing bridges between historical events and behavior stated intents about future events and decision support.

In interviews with industry subject matter experts, the issue brought up repeatedly and across stakeholder types was the need to share information regarding the intent to maneuver a spacecraft, as discussed above. These SME findings reinforce the hypothesis that orbital and intent information forms the basis for the MVE for the universal set of space participants. Despite the ubiquity of the ideal as expressed by SMEs, it is worth noting that while satellite operators stress information sharing, few have been willing to do so outside voluntary participation consortia. Notable exceptions are the members of the SSC who have voluntarily agreed to share information about planned maneuvers as part of their best practices. The SSC practices state:

> ***1. Spacecraft owners, operators, and stakeholders should exchange information relevant to safety-of-flight and collision avoidance.***
>
> *a. Such information should include, at a minimum, operator points-of-contact, ephemerides, ability to maneuver, and maneuver plans [4]*

This is an important step forward in that the Coalition clearly identifies this information is relevant to safety-of-flight and collision avoidance but is too often missing in existing information-sharing regimes. It is necessary for accurate forward-looking space situational awareness at every stage, from planning through decommissioning, and for those tasked with oversight or continuing supervision of space operations. This is significant, not only in that it transitions from the current reflexive system that bases prediction of a space object's future position solely on existing reports of orbital position (which may be a day or more old) or prior behavior, but in that it is a piece of information that is only available from the operator responsible for the satellite. While the position or trajectory of a space object can be provided by the operator and observed by sensors or astronomers, available through both public and private sources, the information for intended future maneuvers can only be provided by that satellite operator. While this information may be currently shared in bi-lateral or selective multi-lateral information sharing through voluntary consortia like the Space Data Association (SDA), that approach falls short of the need for accessible and accurate information for space sustainability. As one government respondent noted, "our needs are not one vendor or the black-box approach of some providers; it needs to be open."

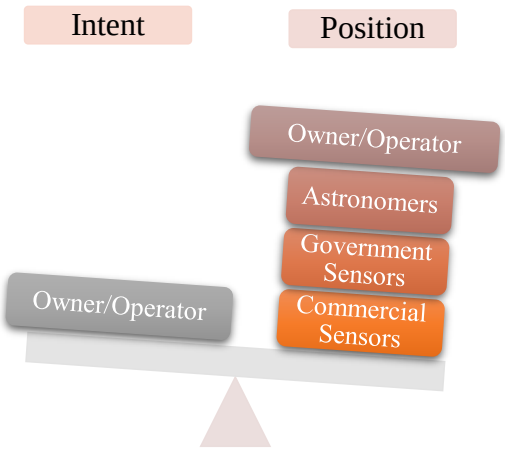

Figure 7: Sources of Information

Sharing information on intent to maneuver in space is like a turn signal on the road; it doesn't change the behavior or options available to the operator; it simply increases the awareness of the planned activity for the other operators in the vicinity. It does not imbue the maneuvering vehicle with an inherent priority or force action by another, nor is it a request for approval for the action. It is simply sharing information about a planned maneuver that is visible to other operators without interrogation. Importantly, this is information that will eventually be known by all participants once SSA systems observe the maneuver into a new orbit.

3.3. INCREASED CAPACITY/SAFETY

Capacity and safety are not divorced partners. As any domain reaches the point of capacity saturation, safety becomes the prevailing concern. However, capacity is not a static metric. The carrying capacity of a specific orbital regime is limited by the ability to mitigate risk while operating in it. That ability increases with the availability of trusted symmetric information shared across system participants. Increasing the quantity, reliability, and quality of information shared reduces the likelihood of unnecessary maneuvers, creates greater access, and allows users to coordinate and self-synchronize their activities.

Although the intent to maneuver is just one type of data that could be shared in a decentralized information sharing regime, it clearly illustrates the limitations of our present partial sharing approach embodied in bilateral sharing agreements and industry consortia. Falling short of a global, resilient, extensible, autonomous, trusted approach, the space community cannot achieve the goal of increasing the carrying capacity needed for a sustainable domain. This is a lesson that has been learned across many shared domains, where capacity is limited by the least able user.

For example, numerous studies indicate that self-driving cars could triple highway capacity, but the benefit is dependent on high percentages of participation and is non-linear. In these models, vehicles are in communication with one another, information sharing. A 2012 Columbia University study found "…if all vehicles on the road are equipped with both adaptive cruise sensors and communication, capacity can be increased by a factor of 3.7. And this increase is without any infrastructure modification: it's purely from making our cars smarter with technology that is commercially available today [14]." Sensors alone do not achieve significant capacity enhancement; it is not until the vehicles are sharing information with each other that the capacity benefits are realized.

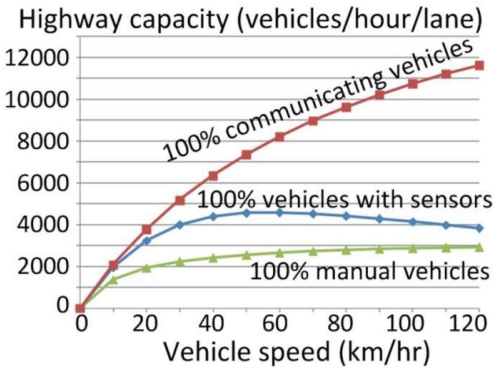

Figure 8: Increased highway capacity with autonomous vehicles (Source av-future.com)

The benefit of increased carrying capacity also requires high participation rates to be realized. The aviation community has experienced the same challenge when implementing capacity-increasing technologies; low levels of user participation did not deliver benefits, creating a challenge in incentivizing first movers. In the national airspace model, enhancements to ground-based functions that did not require equipment onboard the aircraft delivered significant capacity enhancement as they had lower barriers to adoption. Rather than equipping thousands of diverse aircraft, the systems approach focused on improvements to the infrastructure to support ground-based decision-making. The addition of decision support tools and automating routine actions in air traffic control systems, benefiting from the fact that the systems were limited in number and controlled by a central authority, allowed for dramatic increases in airspace capacity.

On the safety side of the equation, the construct where information is collected into a common pool and made available to all systems users has delivered measurable benefits. Aviation provides a clear example of enhancing safety through the provision of shared symmetric information. Airlines and high-performance aircraft operators have access to air traffic and weather surveillance data, often from onboard systems. However, lower-performance aircraft, particularly those operating outside of air traffic control, did not have access to this data until the implementation of the onboard information-sharing program ADS-B In. Under this program, data collected by the FAA from multiple sources is transmitted to systems onboard an aircraft. The Aircraft Owners and Pilots Association reported, "A study that examined the effect of Automatic Dependent Surveillance-Broadcast (ADS-B) In on general aviation and air taxi accident rates found a significant reduction in the likelihood of an accident, which decreased by 53 percent, for aircraft equipped with ADS-B In. It also found that the likelihood of a fatal accident decreased by 89 percent for aircraft using ADS-B In [15]."

Decision support tools ingest shared information to facilitate self-synchronization in a shared environment. Access to information is a critical element in increasing capacity and efficiency where users with diverse interests compete for limited resources. "Smart Cities" use information sharing ecosystems to improve the quality of life for citizens for everything from reducing traffic congestion to fighting crime to delivering a cleaner, sustainable environment. The space industry, perceived as one of the most innovative in the world, is falling behind parking apps when it comes to using available technology to increase capacity.

The challenge of determining what information should be shared is a challenge in every type of activity. It is critical that these decisions are made by the affected community, who will decide what is shared and with whom. For example, certain information, like space surveillance information, should be widely available to all interested

parties. As a proof point, ASTRIAGraph (http://astria.tacc.utexas.edu/AstriaGraph/) has demonstrated the low-risk, high-value benefits of making crowdsourced space situational awareness info publicly available.

But all information does not need to be available to all users, particularly at the initial stage of creating a Minimum Viable Ecosystem. The work to identify the information needed by the various participants has already begun through the process of bilateral arrangements. But rather than multiple iterations of agreements between pairs of system participants, a globalization of the information sharing will increase efficiency and transparency in the space domain. This approach will also allow the engagement of lessor-resourced users who may not have the capacity to participate in multiple bilateral activities while ensuring data records are maintained with forensic veracity.

The incident in Spring of 2021 of a close approach between a Starlink and OneWeb satellite highlights the shortcomings of the current system for space. A OneWeb satellite, launched in March 2021 with 35 others, was raising its orbit up to operational altitude when it was predicted by the U.S. military to have a close approach with a Starlink satellite that had been launched in September 2020. After a back and forth exchange between the two companies, OneWeb requested that SpaceX turn off the automated collision avoidance system on the Starlink satellite so OneWeb could do its own manually planned collision avoidance maneuver. The two satellites passed each other without incident. After the event, the two companies started sparring over the incident, with OneWeb claiming Starlink had a "gung-ho approach" to safety and SpaceX claiming it was not even a serious incident [16]. In the final analysis, a OneWeb representative stated, "the opacity was the problem."

A short paper on SpaceX's Federal Communications Commission (FCC) incident highlights how disagreement and disparity over data exasperated this incident. SpaceX provided a comparison of conjunction probability based on positional data from four different sources – SpaceX, OneWeb, the U.S. Space Force's 18th Space Control Squadron, and LeoLabs (a commercial SSA data provider) – that showed wide-ranging probabilities of collision and miss distances from all four sources that changed in the days leading up to the event [17]. This disagreement in the available data and predictions, combined with different risk and internal processes approaches between the two companies, helped complicate what should have been a routine incident.

Information sharing as a tool to increase the carrying capacity and the safety of the orbital domain faces the same challenge as driverless cars and advanced avionics; most benefits occur only after high levels of participation are achieved. The fragmented system of bilateral agreements, state-based systems, and voluntary consortia can provide an on-ramp to a decentralized information-sharing regime. This is a natural progression of the current state.

It is important to recognize that observers of the space domain are not purely passive. When a mission to protect national assets (and those of one's allies) in space is recognized, certain civil activities may demonstrate behaviors that appear indistinguishable from hostile action. For example, without knowing that an operator has contracted for an on-orbit service when observed by a third party, it may appear that a hostile act is occurring for which a defensive posture is appropriate. It is in everyone's interest to reduce the risk of unintentional escalation of tensions. The inverse is also true; we cannot know what is unauthorized unless we have visibility into what is authorized. This issue was raised in another SME interview that there is a considerable lag, often measured in years, between the time of launch and the registration of space objects. This indicates that some actors may be unaware of the obligation, and a launching state may not recognize an urgency in sharing this information.

3.4. SCALABILITY

Throughout stakeholder interviews conducted as part of this research, concerns emerged that the existing systems are not scalable to meet the needs of a growing space sector. One government expert expressed the concern as, "we are not where we need to be; machine learning, artificial intelligence, and blockchain are not just 'nice to have' but are necessary for scalability." The use of manual systems for the evaluation and interpretation of conjunction alerts is not only resource-intensive but has the effect of limiting the carrying capacity of the space domain. The European Space Agency describes the current state; "a typical satellite in low Earth orbit will receive hundreds of alerts a week, and on average two per satellite, per week, will require detailed review including hours of analysis of the distance between the two objects, likely positions in the future and uncertainties in observations [18]." The reliance on manual processes limits the carrying capacity of the domain and limits the scalability of the systems and their

ability to maintain the current safety standard when faced with exponential growth in the number of operational space objects in certain orbits. These manual processes are further limited by the lack of information on intent to maneuver.

In addition to manual processes contributing to scalability challenges, the lack of symmetric information also inhibits scalability. Key to the lack of symmetric information sharing is the proliferation of bilateral information-sharing agreements (opacity) and lack of agreed ontologies (completeness of the information and shared understanding of information). There is considerable value to codifying agreements for machine-readable formats to allow a system to ingest agreements and identify commonalities, conflicts, and anomalies. This activity could yield useful information on the organic development of norms for both behaviors in space and information sharing that could advance ongoing efforts across the space community. These efforts include those like the SSC, who, in addition to the point mentioned before, their Best Practices for the Sustainability of Space Operations document, state:

> ***Spacecraft owners, operators, and stakeholders should exchange information relevant to safety-of-flight and collision avoidance.***
>
> *a. Such information should include, at a minimum, operator points-of-contact, ephemerides, ability to maneuver, and maneuver plans.*
>
> *b. Typical interfaces include direct operator-to-operator coordination and use of Space Situational Awareness and/or Space Traffic Management entities.*
>
> *c. Such exchanges should respect owner/operator intellectual property and proprietary information.*
>
> *d. Space industry stakeholders should be protected from legal liability associated with the good faith sharing of information relevant to safety-of-flight*
>
> *e. Such exchanges should be in accordance with each operator's country export regulations [4].*

While there is a documented interest in the space community to share information, the currently available processes to do so are not scalable to meet the burgeoning demand. These best practices capture important principles of information sharing but fall short of a symmetric and trusted practical approach. The reliance on operator-to-operator manual coordination and the use of SSA or STM entities limits the reach of the shared information. If, as an alternative, stakeholders had access to share and read this information using decentralized information sharing, we would move closer to a common, symmetric, actionable information for all stakeholder types.

The role of automation in scalable systems is to reduce the workload needed to accomplish a task. The growth in conjunction alerts will ultimately lead to a state where the alerts themselves exceed the capacity of operators to evaluate them. As ESA points out, at the current rate, a typical satellite is the subject of hundreds of alerts a week, an average of two of which will require hours of analysis to determine if a maneuver is needed. The remaining "hundreds of alerts" risk being treated as nuisance alerts, a critical human factors concern across safety systems.

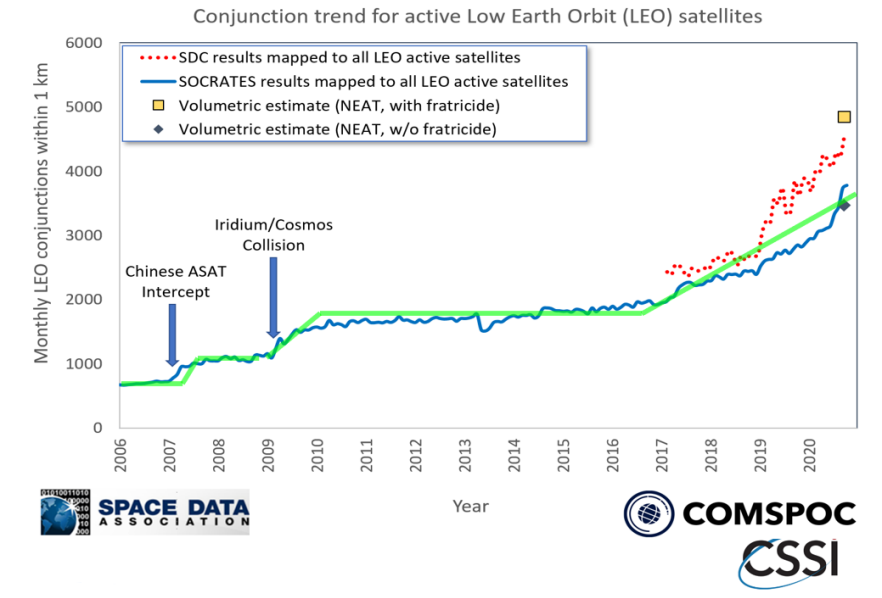

Figure 9: Monthly LEO conjunction warnings (Data Source AGI/Space Data Center)

Research has shown that the number of daily conjunction alerts for spacecraft in LEO is growing at an accelerated rate. Data collected by Analytical Graphics, Inc. Space Data Center shows that spacecraft in LEO are receiving warnings of close approaches within one kilometer twice as often in 2020 as in 2017, from approximately 2,000 to 4,000 per month (Fig. 9) [19]. Simulations that take into account projected future launches of large satellite constellations and an increase in satellite catalog to 200,000 objects suggest that the rate of close approach warnings within one kilometer will go up by an order of magnitude for most satellite operators in LEO within ten years. At the same time, the estimated annual collision rate between an active satellite and a piece of debris at 775 kilometers is predicted to jump from 0.04 to 5.2 per year [20].

3.5. LIMITATION OF BILATERAL ARRANGEMENTS

A comprehensive analysis of the organic development of a polycentric governance model evolving from existing bilateral agreements may discover commonalities and norms that can help drive a global information-sharing model. However, the process of identifying emerging norms is a manual process for which there is no standard framework or ontology. Evaluating the information that stakeholders have voluntarily agreed to share with one another can provide important insight into what information may be shareable with the space community and the applicable nascent norms. Nonetheless, the reliance on bilateral arrangements limits the utility of the shared information. Concerns about intellectual property, data rights, and propriety information inhibit sharing information outside the bilateral agreement structure. In addition, a party with a number of discrete bilateral agreements may find themselves in a position of possessing critical safety information but restricted by confidentiality provisions from sharing it with a party that needs it because those parties may not have agreements with each other. Respondents in an information-sharing exercise as part of MITRE's ongoing work in this area indicated that the unwillingness to

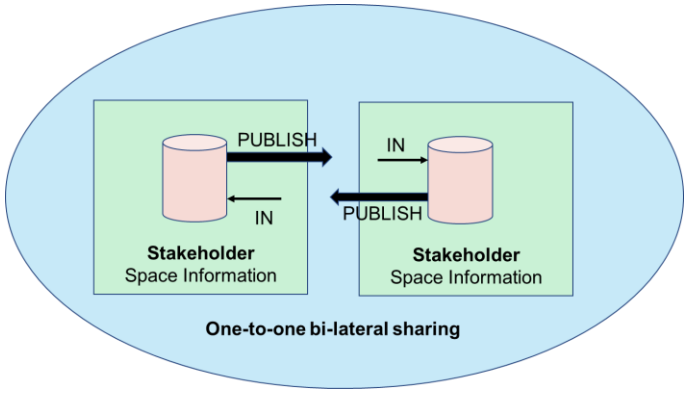

Figure 10: Bilateral information sharing

share certain information related to other contractual relationships, including non-disclosure agreements, as well as concerns about legal restrictions like ITAR (International Traffic in Arms Regulations) when they did not have knowledge about who may have access to the data. The result was a risk-averse decision not to share in the face of uncertainty of whether agreements or regulations applied in the situation.

The proliferation of bilateral arrangements in space is not a new concern, but it is rapidly increasing. In July 2021, U.S. Space Command (USSPACECOM) signed the 100th Commercial Space Situational Awareness Data Sharing Agreement in its history. While this is to be expected, as USSPACECOM provides global SSA services, this represents a small subset of the bilateral arrangements across the space sector. A study from Laval University has identified an "explosion" in bilateral agreements since 2010. Remarkably, most of the 931 agreements they have so far identified do not include a party, either public or private, from the US [21]. The rapid expansion of space actors is seen in both the state and private spheres. In the decade between 2008 and 2018, the number of countries with a satellite in orbit increased from 50 to 82, while the infusion of private capital has created an investment ecosystem where private actors are playing a more prominent role and whose goal is to operate in space independently from sovereign governments. By 2020, the number of bilateral arrangements exceeded 900 and was growing, with the rate of increase in arrangements far outpacing the number of new actors in space [21].

The emergence of a de facto model of governance through bilateral agreements has significant limitations and reinforces the premise that a stakeholder-driven decentralized model is necessary. Thus, if the goal is the preservation of space, then multiple actors must independently make decisions based on symmetric and trusted information. The preservation of space will then be an emergent effect of independent decisions based on symmetric and trusted information.

Nature is rife with examples of simple elements self-organizing into complex systems without a central organizing entity. As scientists study them more, they discover the ways in which information is shared between the elements to enable emergence to occur.

The value of bilateral agreements is necessary to move the space community to where we are today, but now we must ask: Is the proliferation of bilateral arrangements a reflection of their long term utility – or do they persist and grow because a more effective means to share is not yet available? Like the Space Data Association and EU SST, participation in data sharing consortia indicates a desire for multilateral and perhaps decentralized access to two-way information.

3.5.1. MOVING FROM BILATERAL TO DECENTRALIZED

The thesis for this research is that a decentralized, stakeholder governed approach for sharing critical operational information (e.g., ecosystem, MVE) enables a resilient, international means for independent space actor decision making, which results in an emergent effect of preserving the space domain. In contrast, a multi-lateral approach or capability that is owned and controlled by a single state (see Fig. 11) will not achieve the level of voluntary participation on a global scale that includes all space-faring states. This is true because not every stakeholder will agree that the stakeholder owning the sharing capability is trustworthy. Conversely, if a single owner multi-lateral model of information sharing across all stakeholders is viable, we would already have one.

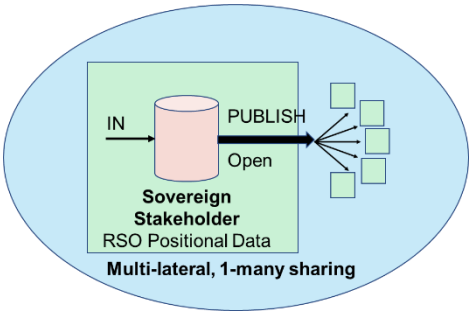

Figure 11: Centralized multilateral information sharing

The alternative to bi-lateral and multi-lateral information sharing is whole ecosystem information sharing. It is symmetric and trusted information sharing, enabled by decentralized data technology, used by an ecosystem of participants who write and read data, resulting in sharing among all participants in that ecosystem, as shown below in Fig 12.

If that ecosystem is universal (all space participants), such as for sharing orbit, intent to maneuver, and related safety-critical data, then the ecosystem is for all participants. If the ecosystem concerns a specialized topic, then that ecosystem has participants who are a subset of space participants interested in that topic. Using the example of decommissioning within the ecosystem for decommissioning participants, the participants will employ whole ecosystem sharing using their own permissioned blockchain. This decommissioning ecosystem can and should be distinct (implementation, governance, specialized data) from the universal safety-critical ecosystem. The result is that each space participant can then join the ecosystems that are applicable to their endeavors. The ecosystems can form and grow and interact depending upon need and without imposing undue dependencies on each other.

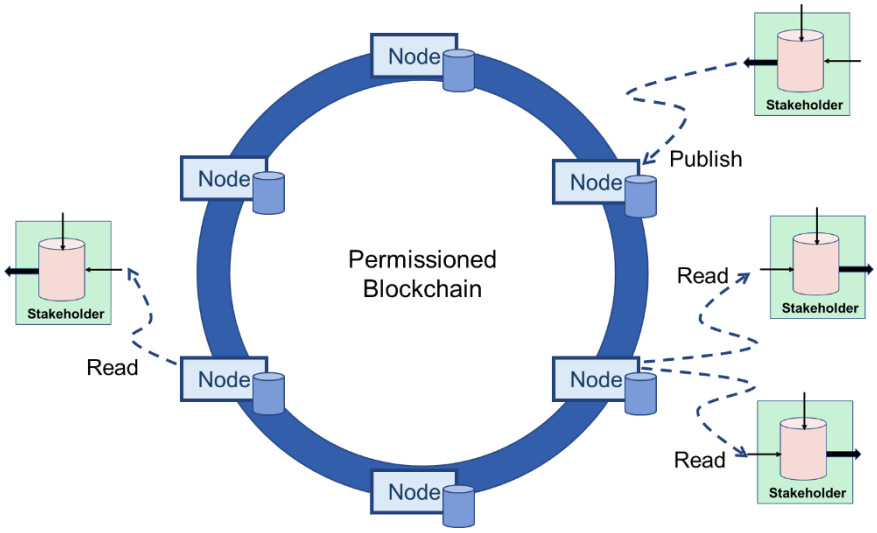

Figure 12: Example Information Sharing with Permissioned Blockchain

The critical shift in cultural perspective required for this model is embracing the approach of incrementally growing ecosystems of sharing information versus constructing a pre-defined system that is owned and operated by a single stakeholder. The difference is as follows:

- A pre-defined system must know all requirements up front, and the requirements must be held static for the duration of construction of the system, which may take years. In the end, the system is owned by one stakeholder, which may prove to be a trust issue with one or more potential users/participants.
- An incrementally grown ecosystem, in contrast, starts with a Minimal Viable Ecosystem (MVE), discussed below, which is not intended to be the "final" capability because the requirements of what the ecosystem needs must be discovered not declared. The ecosystem then grows incrementally, adding functionality and infrastructure, from MVE to full-fledged ecosystem, based on actual demand signal, not projected requirements. Further, the nature of decentralized data technology lends itself to incremental development, test, and rollout. Finally, decentralized data technology can add participants without needing updates so that the incremental growth of participants can be relatively independent of the growth of functional capability.

Three steps toward establishing an MVE:

1. Establish the minimal set of relevant data to share; needs to have sufficient value to motivate stakeholders to participate.
2. Establish an initial set of decentralized sharing principles; assure symmetrically and trusted information sharing for all ecosystem participants, and governance to assure the principles are not usurped.
3. Establish an initial decentralized information sharing capability; it needs to be constructed, tested, and operated in the open with transparency.

Once established, the MVE uses decentralized principles and decentralized information sharing to demonstrate to the space community that the MVE is operational. Further, the MVE must also track findings and challenges which need to be addressed in subsequent iterations of governance and capability. This establishes a pattern of continual improvement while also recruiting and onboarding additional stakeholders.

Decentralized information sharing enables polycentric space governance necessary in a shared international domain. Polycentric governance or polycentricity is "a governance system in which multiple governing bodies interact to make and enforce rules within a specific policy arena or location, is considered to be one of the best ways to achieve collective action in the face of disturbance or change [22]." The emergence of a polycentric governance model could serve to break the logjam in applying traditional legal models to space governance. Polycentric governance allows action by partially overlapping, non-hierarchical regimes that are multilevel, multipurpose, multi-type, and multisectoral and offers certain advantages over the top-down governance approach [23]. Polycentric governance models are not exclusive to international frameworks and can work across multiple levels and combine both binding and non-binding elements into a larger framework.

The purpose of polycentric governance is to accommodate multiple centers of semi-autonomous decision-making. Under this model, where one stakeholder "owns" the information sharing for the entire set of stakeholders, we lack both the resilience and trust needed to serve the entire space community.

The decentralized model allows each node to hold the same data and can be verified against each other (Fig. 12). This polycentric model can not only serve to overcome geopolitical barriers and expand the availability of shared data but can also provide a design that is more resilient than existing systems.

3.6. PERMISSIONED BLOCKCHAIN AS A KEY ENABLER

Permissioned blockchain has demonstrated utility across a variety of domains, including finance, supply chain, and logistics. It safely stores data in a secure, immutable, distributed manner that facilitates stakeholder self-synchronization and coordination. Permissioned blockchain is well suited for use in contexts outside of a single govt or commercial entity's enterprise security and computing/storage boundaries (external collaboration from the perspective of an individual stakeholder). Note that permissioned blockchain is distinct from cryptocurrencies that use public blockchains. Public blockchains use computing energy as part of their security approach. However, permissioned blockchains rely on agreed governance to constrain participation to well-known stakeholders via onboarding and vetting governance processes. This enables sovereign nations, commercial and non-profit organizations to share critical space safety-related and other information while also providing protection of intellectual property and privacy.

Thus, permissioned blockchain can serve as a trusted, symmetric information-sharing foundation for diverse space stakeholders across governments, corporations, NGOs, academia, and operators to notify, coordinate, and cooperate in a highly interdependent space domain [24]. From this point forward in this paper, the term blockchain is understood to mean permissioned blockchain.

3.7. PROBLEM SUMMARY

Current information sharing practices constrain the carrying capacity of space and limit the ability to scale space safety functions to meet demand. The reliance on bilateral arrangements satisfies an immediate need and is enabled by existing legal, contractual, and information technology structures. A sustainable orbital domain will be realized through distributed control, with access to trusted and symmetric space community safety-critical information to inform individual operator actions. The emergent effect will be a robust, sustainable space environment with the flexibility to accommodate innovative services and needs while preserving this shared resource for the economic and security benefit of all.

4. DECENTRALIZED INFORMATION SHARING INFRASTRUCTURE

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 but rather through the trusted data integrity created by the decentralized information sharing infrastructure. Coupled with governance and norms to encourage consistent sharing of critical safety-related information, the emergent effect is symmetrically sharing trusted space information.

4.1. PRINCIPLES

Blockchain helps implement a decentralized information sharing infrastructure based on the following principles:

- Access - equal for all stakeholders
- Symmetric – all stakeholders are encouraged to share certain types of information, and all stakeholders have access to this information
- Trusted – Shared information is provably attributed, available, has known provenance and pedigree, and cannot be altered
- Decentralized – Data is replicated across nodes where the nodes are not all controlled by any single stakeholder or subset group of stakeholders

These decentralized principles are necessary for a blockchain-enabled trust framework. However, they are not sufficient. Principled consideration must also be given to building upon, not replacing, legacy capabilities. 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, new decentralized information sharing capabilities can be used by existing legacy systems to coordinate and share information.

4.2. BENEFITS OF DECENTRALIZED INFORMATION SHARING APPROACH

A decentralized approach to sharing information provides equal access to governments, operators, academia, and international or industry organizations. International partnerships benefit from the ability to coordinate and collaborate, combining expertise across sovereign and commercial boundaries. Such a decentralized information sharing capability is constructed, tested, and operated in the open by multiple entities and not constrained by the politics, budgets, or stability of a single host entity.

Trusted information sharing makes stakeholder information useable beyond those who created it and between users that do not presently have a bilateral or multi-lateral relationship. Crucially, in a shared domain, it is unlikely that the effects of operational decisions by an individual stakeholder will impact only those with whom they have a bilateral agreement at any moment in time. As the space economy expands, the categories of actors requiring access to the same space situational awareness information will grow, including operators, policy makers, licensing authorities, planners, regulators, and the diplomatic community.

4.3. AUTONOMY AS A KEY DRIVER

The goal of a decentralized information sharing capability is to allow operators to act autonomously in a shared environment while ensuring the safety of the operation for themselves and others. Disparate actors, safely operating in a shared environment while under the continuing supervision of independent sovereign states as structured under the Outer Space Treaty, require trusted symmetric information to decide and act independently. Since there is no central authority to approve or restrict activities in space, these operators must act in a decentralized manner. Decentralized information sharing is a key enabler for independent decentralized decision-making and operational actions. In contrast, a centralized model for information sharing empowers the stakeholder who controls access to information to have de facto authority over the domain, a concept specifically precluded in the international treaty structures for space activity.

Compatible with the model of polycentric governance, the concept of autonomy is the stakeholder's ability to operate on their own values and interests. For example, this concept allows operators to self-determine whether they will deploy automated systems on satellites or utilize ground-based determinations for conjunction avoidance through the utilization of symmetric information about the space domain.

4.4. DECISION SUPPORT AFFINITY ECOSYSTEMS

The discussion above focused on sharing safety-critical space information, including intent to maneuver. The hypothesis is that if such information is shared in a trusted and symmetric manner, then independent safety-related decision-making will improve, creating an emergent effect of improving space safety and preserving the space domain. All space participants are interested in such information. The combination of decentralized information sharing capability, plus orbital, intent to maneuver, and other critical safety-related information, forms a space safety affinity ecosystem used by all participants.

Other decision-type affinity ecosystems naturally arise. For example, affinity ecosystems for major lifecycle phases like decommissioning can enable operators to share best practice info and share decommissioning information and proof of parking for their space object. Each of these ecosystems can similarly use a decentralized information sharing capability and share well-defined data sets with well-known participants.

There are also affinity groups that may be highly specialized with only a small set of participants. One example is Sensor Network Autonomous Resilient Extensible (SNARE) which is a set of autonomous agents which decide how to task the Space Sensor Network sensors to make observations [25]. This affinity group runs continuously and shares trusted symmetric data regarding observations and whether the maneuver was detected. If so, the SNARE ecosystem can immediately react to try and confirm and follow the maneuver. As an emergent effect, SNARE can generate TLEs (orbital descriptors) near real-time versus the present once-a-day update on TLEs using SP Tasker centrally controlled algorithms. SNARE is presently in the operational prototype phase with Space Force. SNARE is envisioned to replace the current tasking regimen to produce TLEs and related positional data (for the safety-related affinity ecosystem) and discussed next.

4.5. DECENTRALIZATION EXAMPLE: SENSOR NETWORK AUTONOMOUS RESILIENT EXTENSIBLE (SNARE)

This section describes a recently initiated Space Force operational prototype that uses decentralized decision-making to task space sensors as an alternative to the present once-per-day SP Tasker generated centralized tasking for the Space Sensor Network (SSN) [25].

Problem Statement

The SSN currently utilizes a network of over 30 ground-based radars and optical telescopes in addition to on-orbit telescopes to gather information on over 20,000 RSOs. Managing a high quantity of objects given limited resources is a challenging problem that scales poorly as the catalog of objects increments. To maintain SDA, each object in the catalog requires a degree of certainty in which they must be positionally accounted for. While some objects are easily tracked by the network, others might be largely outside of coverage zones. While some objects are high-valued assets, others are debris from other missions. While some objects are known to be “friendly,” others are subject to scrutiny, and sometimes the intent or origin of an object is unknown or unclear. Each of these qualifiers leads to differences in both trackability and desired positional awareness, and these factors, among many others, make SDA very challenging to achieve, let alone sustain.

Current Centralized Tasking of Sensors

Today, there is no fully automated system in place for the SSN to do network-wide sensor tasking to help obtain certainty in the state of the catalog. The closest system utilized today by the SSN is the SP Tasker. The SP Tasker has been in use by the Space Defense Operations Center (SPADOC) since late 2005 as a replacement to the “greedy”

tasker that was in place previously, which was so preferential to high-priority objects that it often disregarded objects of low priority when it sent out tasks. SPADOC determines priority levels for each object based on interest, desired positional accuracy levels, and other qualifiers. Although there is no ranking system that uniquely orders the importance of each object in the catalog, there is a system in place which assigns each object a Category (CAT) of 1-5 (which represents object priority) and Suffix of A-Z (which indicates collection requirements). An object that is a CAT 1A/2A is highly important and demands a strict collection of information to satisfy requirements, whereas a CAT 3, 4, 5 with various suffixes will be of lesser priority which is tasked less often. Each combination of categories has different tasking requirements. Clearly, a CAT 1 or 2 will take tasking precedence and will usually require as much information collection as possible from the network. The suffixes generally indicate how many tracks are required throughout the day, and that often varies depending on the type of sensor that will end up making the collection [26].

Information collection on an RSO comes in the form of a track of metric observations. Each observation in this track is the sensor measurement of the RSO (e.g., azimuth, elevation, range, and range rate) at a specific time. Correlated tracks are used to update the orbital state as specified in TLE updates. When tracks do not correlate to a known RSO, then a new catalog entry is often made, and additional information must be gathered to improve confidence in its orbital state.

TLEs degrade in usefulness over time and hence must be refreshed periodically to maintain positional awareness among the catalog; this is the functional intent of the SP Tasker. TLEs are refreshed based on daily observation collections, priorities of objects' ebb and flow based on the measurements of recent collections, and the SP Tasker utilizes that information (among other relevant information about the catalog and the sensor network) to generate the Consolidated Task List (CTL) for the next day, attempting to maximize information gain between a dynamic sensor network with limited sensing capacities. In other words, the SP Tasker is trying to allocate work to a resource-limited network to satisfy the tasking requirements of the catalog with minimal loss of positional awareness [27].

The CTL that the SP Tasker generates is intentionally vague from a scheduling perspective. Essentially, each sensor is given a list of RSOs to collect on, where an expectation is set for how many observations and tracks should be achieved. At a coarse level, this is a daily schedule, although it lacks the specificity in the timing of a more traditional scheduling problem. This is mainly due to the assumption that each sensor has some local process that can determine its own schedule to satisfy the tasks at hand. Part of what the SP Tasker attempts to encapsulate in the CTL is historical data on a sensor-by-sensor basis to determine which sensors can collect on which objects successfully and approximately how many tracks a sensor can get per day based on empirical data

Limitation of Centralized Tasking

Even if it were the case that the SP Tasker or another algorithm could design an effective, optimized, rigid schedule, there are some assumptions that cannot be ignored. A traditional schedule is meant to be "fixed" to achieve optimality. In other words, every item on the schedule must occur precisely as scheduled to accomplish whatever objective is at play. When an item on the schedule falls through, takes longer than accounted for, or occurs in a way otherwise not planned for, the schedule itself may break down in validity. Further, it is impossible to account for unplanned events. What if a sensor experiences a temporary outage? What if an RSO starts maneuvering? What if something launches unexpectedly? Presumably, the calculus of what is important to collect information on rapid changes in these situations. The SP Tasker is set up to run once per day, in which case these types of events are typically handled by manual schedule adjustments (by humans) throughout the day.

Decentralized Tasking of Sensors (SNARE)

SNARE network is composed of a set of sensors (referred to as sensing nodes), each of which communicates directly with interfacing nodes (i.e., a node that is paired with a sensing node). Interfacing nodes have access to the catalog of TLEs (in SNARE Data Store), which are provided to the sensors to make collections (in the form of observations) as needed and as possible, per SNARE's logic driver. Objects that have not been tracked recently or are suspect to require additional collections are given priority. Each sensor acts independently and autonomously according to the same set of rules as every other sensor. Inevitably, an interfacing node will select appropriate work for the sensor (independent

decentralized tasking). Once a process receives validation from the validating nodes, the work is attempted. If the collection results in observations, they are sent to the validating nodes to be checked for feasibility and are eventually processed using astrodynamics tools which update the state of the object(s) collected in the form of a TLE. These TLEs, once validated, are then published for use by the network.

Looking Forward

SNARE holds the promise of using decentralized tasking of sensors to improve tactical relevance of SDA by providing near real-time positional state of objects in the space domain that is timely, accurate, and actionable. SNARE has been transferred from MITRE to USSF, and the SNARE operational prototype phase is underway. Future papers will describe subsequent improvements and results.

4.6. TRUST ALIGNMENT ACROSS DECISION SUPPORT AFFINITY ECOSYSTEMS

This research is agnostic to the type or nature of an affinity ecosystem, although the space safety-related data affinity ecosystem has been used as an example the most and is an obvious starting point. Each ecosystem owns its data, processes, conventions, and norms, including governance. Each ecosystem consumes certain types of information and provides certain types of information. This creates an interlinked web of ecosystems over time. For example, the SNARE ecosystem (owned and operated by one country) generates TLEs consumed by the space safety ecosystem (all participants).

Data is maintained within each affinity ecosystem by consistently applied participant practices and the decentralized information sharing capability, which assures trusted data integrity and symmetric access. However, when sending data from one ecosystem to another (as in the SNARE ecosystem to Space Safety ecosystem example), maintaining trust requires basic practices to be aligned across ecosystems. For example, if two ecosystems refer to the same RSO, the means to identify the RSO, and relevant activities and participants regarding the RSO, should be consistent or have a known mapping between the ecosystems.

In manufacturing supply chains, traceability (pedigree and provenance of goods and services) is obfuscated by bilateral information-sharing arrangements, prevalent in legacy systems. As a result, ecosystems are self-organizing to share traceability information within affinity ecosystems (e.g., MediLedger). Further, some of these ecosystems will likely intersect soon, begging foundational alignment to enable traceability to cross ecosystems[†]. This is a close, but not exact, analogy to the space domain, both in the formation of ecosystems and in need for ecosystem-to-ecosystem interaction. This similarity is clear when sharing information is considered part of a larger "information supply chain."

Having independently evolving affinity ecosystems is beneficial because existing federated information sharing approaches can evolve into trusted and symmetric affinity ecosystems. However, in addition to forming such ecosystems, the interconnection between ecosystems must also be considered. For example, pedigree and provenance (traceability) should be understandable, or at least mappable, across ecosystems.

4.6.1. PEDIGREE AND PROVENANCE

One possible affinity ecosystem could be GEO Disposal Compliance and Monitoring and could implement and operate their own blockchain. As they onboard information from their sources, one of the fundamental activities is to record the pedigree and provenance for each source of information. If a GEO Disposal ecosystem needs to send information to a Space Sustainability ecosystem, then the pedigree and provenance of that information in GEO need to be conveyed to Sustainability and in a manner that Sustainability can understand it. This is critical because if

[†] NIST / NCCoE has started exploration of the impact of using decentralized information sharing to improve traceability of goods and products in manufacturing supply chains. This effort is analyzing several case studies from industry and is presently producing a White Paper summarizing their findings, which includes formation of information sharing ecosystems.

GEO also performs compliance activities, the authenticity of information must be preserved and usable in legal and diplomatic activities.

4.6.2. ATTRIBUTION AND VERIFICATION

Continuing with the GEO example, if an RSO or organization, or individual needs to be identified, the means of identification must be understandable across ecosystems. Attribution takes the identity and encodes it in the applicable data records. Assuming decentralized data technology is used, the attribution is provable, enabling associated data records to be used in legal and diplomatic activities.

4.6.3. ANOMALIES

Some information recorded in the affinity ecosystems will be planning, or intention and some information will be observed behavior. One example could be a stated intention to operate with certain frequencies or in a certain orbit and the actual behavior (frequency and orbit). Using affinity ecosystems, information can be compared (intent vs. observation), enabling anomaly detection and adjudication since the information to support these claims will have forensic qualities (e.g., provable pedigree and provenance, attribution, etc.).

4.6.4. AUTOMATION

Trusted symmetric data with forensic qualities supports high-quality decision-making and may enable further workflow automation. In turn, increased automation is a key component of increasing the carrying capacity of space. One potential opportunity is to use trusted symmetric information about intent to maneuver (safety ecosystem) to reduce manual workload in processing conjunctions.

Judicious use of automation, supported by blockchain (trusted and symmetric information), is being explored in another global safety-critical international domain, nuclear non-proliferation. In this case, the SLAFKA prototype project was developed to explore reducing the manual accounting of uranium hexafluoride (UF6) containers between sovereign nations. Presently, a central authority International Atomic Energy Agency (IAEA), helps track the outflow and inflow of UF6 containers between sovereign nations, discovers anomalies, and adjudicates anomalies.

This process is challenged by intense manual methods to track and report inflow/outflow, etc., and SLAFKA is seen as an exemplar of the type of coordination and reporting possible when using blockchain (trusted and symmetric information). Similar to present-day SSA, nuclear material accounting records are based on electronic documents that have inefficiencies in data integrity and correctness. In contrast, SLAFKA "(1) validates and improves the management of safeguards data and (2) enhances permissioned information sharing between operator and regulators on nuclear material transactions (movements and processing). SLAFKA tests DLT as a novel method to track nuclear material, detect diversion, and monitor treaty compliance [28]."

5. USE CASES

To illustrate the use of a decentralized information-sharing approach, initial use cases are identified.

5.1. USE CASE: INTENT TO MANEUVER

The intent to maneuver information has widespread value added to multiple stakeholders. Without operator-provided intent information, other stakeholders are basing decisions on incomplete data. This carries both business and physical risks. By sharing information that a maneuver is planned, a maneuver is being executed, and a maneuver is complete, projections of the future position of a space object becomes more reliable and precise. This facilitates conjunction alerting, compliance monitoring to meet a state obligation for continuing supervision, and other functions dependent upon awareness of the space domain. It facilitates decision-making for orbital insertion

and planning and academic research and analysis. It is widely accepted in the space community that intent to maneuver information would add value to existing systems and is included in the industry best practices document of the Space Safety Coalition. Space-track.org encourages the submission of maneuver information and provides detailed instruction on how to do so.

5.1.1. NARRATIVE

A maneuver is defined as: To intentionally steer or manipulate (via either propulsive effects or induced perturbations) a spacecraft's subsequent position. Surveillance-based SSA can detect that a maneuver has occurred but, by its observational nature, is a backward-looking tool. Astrodynamicists can project a future position based on the characteristics and movement of a space object to provide a forecast, but that forecast is nullified if the operator executes an unexpected maneuver. It is important to note that the conjunction assessment screening process is an iterative one, requiring repeated re-evaluation as updated information and observations are received.

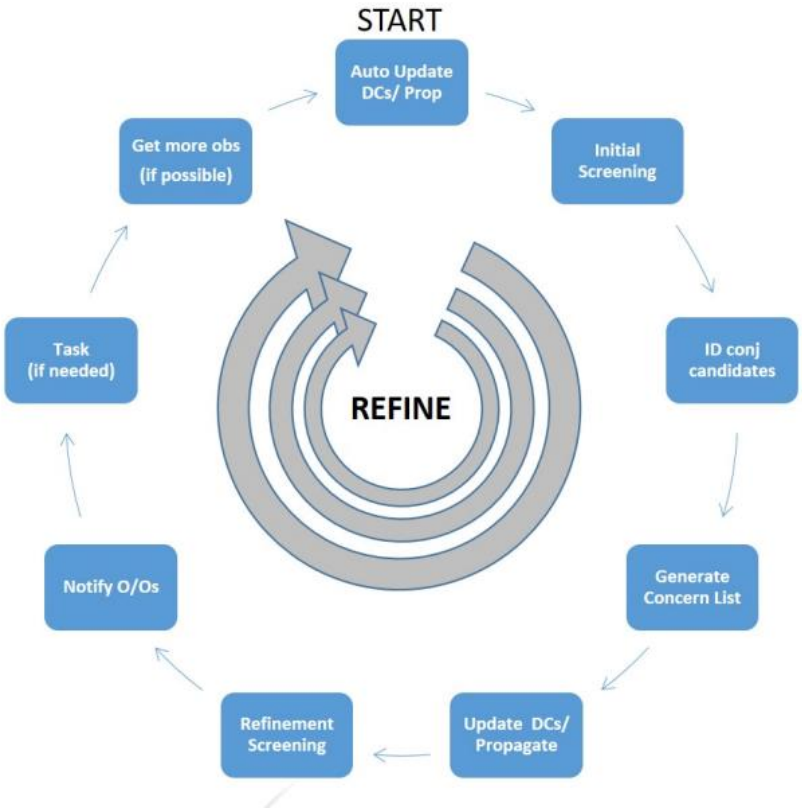

Figure 13: Conjunction Assessment Screening Process (source: 18th Space Control Squadron)

While there is clear value in sharing maneuver information to the conjunction assessment screening process, access to this information is asymmetric. Many operators participate in consortia, like the Space Data Association, where the information may be shared with other members of the consortium. Like bilateral agreements, this approach addresses the immediate needs, increases the safety of the domain, and should continue to do so. However, while information is shared among the trusted partners within defined groups, access to information both from and to entities outside the consortium remains limited. These structures add considerable value and should be integrated into the broader information-sharing regime. Like other safety information-sharing networks, the self-organized substructures are effective tools to overcome barriers and provide access to critical information between entities that

do not trust one another. In this way, the consortium provides credibility to the data without the need for each participant to make a value judgment on the legitimacy of the data from every other participant.

Proposals to require operators to share intent information do not seek to use this information for the purpose of approving or denying the maneuver; is it to ensure completeness of information in creating space situational awareness. This is an important distinction. While governance models benefit from more accurate information, including intent to maneuver, the information-sharing model itself is not governance, regulation, or an approval mechanism. It is a decision support tool, not a decision-making one.

Example: It is important to note that this is a simplified example to illustrate the consequences of this gap in knowledge. It is not a comprehensive illustration of the conjunction assessment processes.

For the purposes of this illustration, we will consider a satellite subject to the NASA Conjunction Assessment and Risk Analysis (CARA) program. The CARA process is illustrated in Fig. 15.

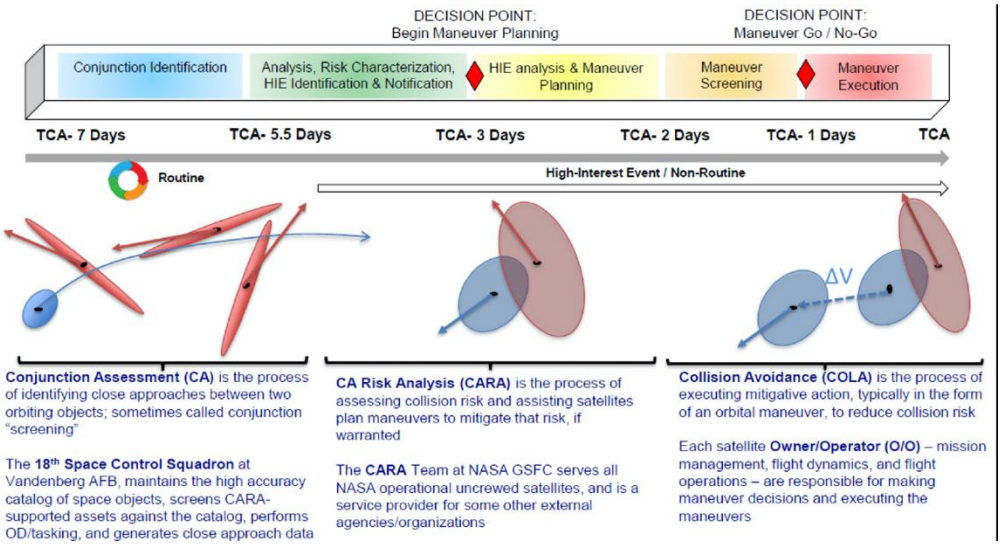

Figure 14: Overview of the NASA CARA Process (source: NASA)

The 18th Space Control Squadron screening process for Earth-orbiting objects is forward-looking. The 18th SPCS maintains a catalog of space objects that is updated every eight hours with data collected from a global network of telescopes and radars. Using that catalog:

- 18th SPCS predicts the trajectories of cataloged objects 7 days into the future and compares them to look for potential close approaches between two space objects
- 18th SPCS screens CARA supported assets against the high accuracy catalog and generates close approach data
- Concern lists are generated for follow on screening
- Concern lists evaluated by the Conjunction Assessment Team
- If a close approach is validated with an active satellite, the owner/operator of that satellite is notified
- O/O considers whether a collision avoidance maneuver is warranted

- O/O notifies the Space Command and provide predictive ephemeris for screening against the high accuracy catalog
- O/O may provide 18th SPCS with ephemeris on potential maneuvers to see if it may generate additional close approaches
- The process repeats with new information

This process is currently manpower intensive as it may involve multiple iterations and data exchanges back and forth between the 18th SPCS and the satellite owner/operator as new observations are collected, and the maneuver planning is refined, the requirement to evaluate and predict close approach based on current information when one party knows that information will not be valid at the time of closest approach illustrates the challenge of asymmetric data. Like NASA, each operator has a process for evaluating conjunction alerts, many of which are opaque to external actors.

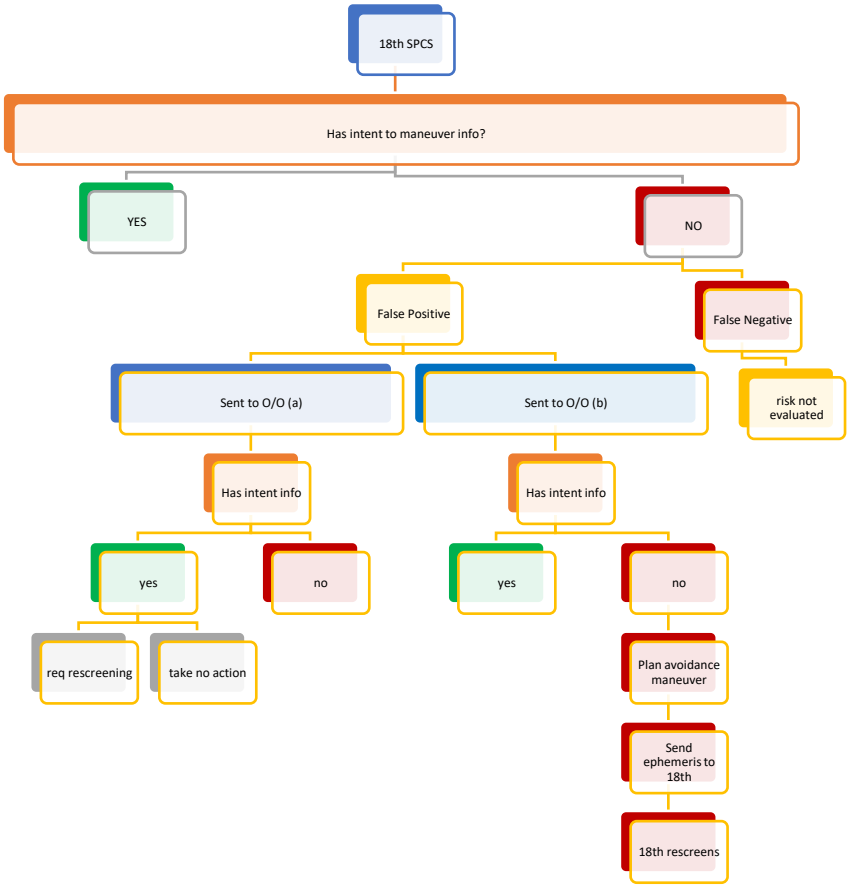

Figure 15: Simplified activity diagram with asymmetric information

5.1.2. FINDING

The lack of information about the planned maneuver causes resources to be expended unnecessarily. In this example, both the 18th SPCS and the NASA CARA resources were expended as though the information would be relevant at the predicted time of the closest approach. It is only the owner/operator in this

example that has complete information to determine early in the process that action was not needed. As a result, one space actor imposed costs on other space actors. While that may not have been the intent, the result is the same. In more extreme examples, operators have executed maneuvers as a precaution because information about the intent of another operator was not available. This can result in expended fuel and potentially reduce the service life of the satellite. In addition, considering the high volume of alerts, this example could illustrate the diversion of resources needed to analyze other events. Finally, the post-event analysis may perceive this event as a nuisance alert, degrading confidence in the system.

5.2. USE CASE: DIPLOMACY

5.2.1. NARRATIVE

The diplomatic uses of the decentralized space information sharing system are innumerable. Spacefaring and non-space-faring nations alike scan the skies for points of concern. The foundational basis of the Outer Space Treaty was not to create commercial markets; it was and remained to ensure the peaceful use of space for all humankind. However, as States have explored the space domain's applications, this noble expression has been narrowly interpreted to prevent the deployment of weapons in space. Satellites are routinely used for reconnaissance, battlefield communications, and other activities that support military action. Still, the weaponization of space remains a concern, and it is in our interest to avoid any unintentional escalation of hostilities. This requires an understanding of not just the position and location of objects in space, but to avoid misinterpretation, it is vital to share pertinent mission information. Simply put, how do you know what is unauthorized if you don't know what is authorized?

5.2.2. EXAMPLE

- Country R launches a satellite described as a “space apparatus inspector.”
- Unidentified satellite behaves erratically in proximity to a commercial satellite launched from Country S
- The behavior of satellite raises concerns of Country S diplomat who characterizes it as a potential space weapon
- State Department spokesperson from Country S describes Country R satellite as “behavior on-orbit was inconsistent with anything seen before.”
- Country R has stated publicly that it is developing new anti-satellite capabilities.
- Country R responds that accusations by Country S are “the same unfounded, slanderous accusations based on suspicions, on suppositions and so on."
- Country S announces it is considering sanctions if the suspicious satellite continues to operate in close proximity to the US space object.
- Commercial satellite operator advises that it had contracted for on-orbit servicing, and proximity operation was planned and routine.
- Due to escalation interactions, the resulting unplanned fuel expenditure to maneuver country S satellite effectively reduced its operational life, which affects expected ROI for this commercial venture.
- Country R rhetoric on legitimacy: “Well, Country S conducts similar activities, so why can’t we?”

This scenario represents escalation or spiral theory, often referred to as a security dilemma. International relations and diplomacy scholars study the security dilemma which has caused many conflicts throughout history, including the First World War. A security dilemma – or spiral theory, refers to a situation in which actions by one nation intended to strengthen its security measures can cause other states to respond with similar measures. This spiral of action and reaction can produce unintended tensions and subsequent conflict. According to Robert Jarvis, when offensive and defensive behavior are not distinguishable, and the offense has an advantage, the security dilemma can be "very intense,” and the situation is "doubly dangerous" [28]. In this case, even states that tend to be status-quo are likely to behave in an aggressive manner, and an arms race may arise. Cooperation between states in these conditions is unlikely.

Hence, analyzing satellites and their dual-use nature through the lens of the security dilemma perspective offers insights into how satellites influence world politics. In policy, recognizing how satellites and their dual-use nature prompt insecurity and fear in states provide insights on what measures states and the world community could adopt to mitigate such destabilizing factors. Since the security dilemma has a caused many wars, identifying satellites' problems is essential to prevent future conflict stemming from space use [29]. The dual-use nature of satellites creates functional ambiguities that blur perceptions of offensive and defensive behavior. Studying the dual-use nature of satellites through concepts of international relations studies and theory sheds new light on determining the impact of satellites on international systems. Examining how satellites impact the emergence of a security dilemma is a crucial example of this impact.

Lubojemski discussed three essential ways in which satellites, through their dual-use characteristics, influence the security dilemma [30]. This influence is rooted in the theoretical basis that states cannot recognize if a satellite is offensive or defensive, therefore not knowing if it is a threat to their security. As a result, states start to build up their security, creating a possible security spiral, a security dilemma. There are no natural interceptors between states and satellites. As such, states are incapable of determining if satellites could be offensive weapons. Second, because satellites inherently possess dual capabilities, civilian and military, states cannot readily recognize the real satellite intent. Because of the dual-use nature, it is impossible to establish a clear definition of a space weapon in international law, hence damaging trust-building in politics, forestalling the creation of norms and laws, halting the development of an arms race in space. Recognizing the existence of a security dilemma before it escalates into a conflict is essential for conflict prevention. Since satellites impact the security dilemma, measures and mechanisms are needed to address this development. There remains a window of opportunity for such action as operational deployments of space weapons and fighting a war in space are yet to take place. On the other hand, a failure to act will likely be detrimental to international stability and order due to the world's dependence on satellites and satellite systems [30].

Developing a method with which to document and blueprint a shared understanding of the normative landscape for space use, coupled with an information-sharing construct such as this paper presents, makes it possible to define and objectively measure the harmful nature of interference and may decisively promote relevant agreed understanding. Therefore, vocabulary is essential in any architectural effort for international space use. Data dictionaries are a fundamental architectural tool that may be leveraged in conjunction with distributed information systems that share pertinent mission information. As put by Radcliffe Brown in his seminal work on Methods in Social Anthropology, "The fundamental principle and supreme rule of all scientific terminology is that terms must be constructed and appropriated so as to be fitted to enunciate simply and clearly true general proposition" [31].

5.2.3. FINDING

Delays in registration, gaps in SSA, and lack of coordination could result in misinterpretation of actions, resulting in an unnecessary escalation of tensions. Understanding the space domain requires more information than the position and trajectory of space objects.

6. CONCLUSION

Space preservation can be strengthened by empowering individual space actors to share trusted and symmetric space information via a web of affinity ecosystems. At least one affinity ecosystem exists that includes all space actors (critical space safety), while other affinity ecosystems are specialized (GEO decommissioning and SNARE). Affinity ecosystems can start as a Minimum Viable Ecosystem and evolve from that point. Within each affinity ecosystem, decentralized information-sharing tools can assure all participants can share space information in a trusted and symmetric manner. Existing bilateral and multilateral information-sharing agreements are a natural starting point to build MVEs. The fact that the space community has organically moved to a polycentric governance model through the proliferation of bilateral arrangements indicates that a decentralized approach is appropriate and building an MVE for critical space safety information is the first step. Space preservation is rooted in independent space actor

decision making, and the affinity ecosystems will assure that each space actor has the most trusted and complete information on which to base their decisions.

Overcoming key challenges to affinity ecosystems, such as willingness to share information, requires confidence in the approach itself. The key to trust in this approach is building trust in a decentralized information sharing capability, which includes trust in the construction, testing, governance, and operation of the capability. Future increments of this research will explore a decentralized approach to construction, testing, governance, and operation. There are examples in use today, such as the Sovrin network for decentralized identity, where independent stakeholders own and operate test and production nodes for the Sovrin blockchain [32].

The benefits of affinity ecosystems to individual stakeholders (consumers of data, producers of data, or both) are significant. More complete and actionable data aids in planning, but that is one of many benefits. For example, the critical space safety ecosystem should reduce the volume of conjunction alerts where no action is necessary, allowing operators to focus on the alerts that require further human analysis. Trust and symmetric information will increase the carrying capacity of the space domain itself, as we have seen in other domains. Such sharing can help avoid unnecessary and costly maneuvers and facilitate state compliance with their treaty obligation to provide continuing supervision.

Future research regarding space affinity ecosystems is suggested in broad terms as follows:

- Identity
  - Identity of people, organizations, objects in shared information
- Shared Information Types
  - Intent to Maneuver and other types
- Challenges to Adoption
  - Enable all space actors to participate
- Patterns for MVE
  - Building the MVE requires both stakeholder participation and specific data types to be identified
  - Lessons learned and repeatable patterns to make MVEs easier to establish over time
- Interoperability of Affinity Ecosystems
  - Extend properties of trusted information sharing across affinity ecosystems

7. ACKNOWLEDGEMENTS

The authors would like to thank the numerous subject matter experts from industry, government, and academic institutions who participated in discussions and interviews and contributed their expert opinions to the development of this work.

8. REFERENCES

[1] United States Department of State. *Agreement Among the Government of Canada, Governments of Member States of the European Space Agency, the Government of Japan, the Government of the Russian Federation, and the Government of The United States of America Concerning Cooperation on the Civil International Space Station*. Online: https://www.state.gov/wp-content/uploads/2019/02/12927-Multilateral-Space-Space-Station-1.29.1998.pdf [Accessed August 9, 2021]

[2] H.G. Reed, N. Dailey, R. Carden, and D. Bryson. *Blockchain Enabled Space Traffic Awareness (BESTA): Discover of Anomalous Behavior Supporting Automated Space Traffic Management.* MITRE. November 2020. Online: https://www.mitre.org/publications/technical-papers/blockchain-enabled-space-traffic-awareness-discovery-anomalous-behavior [Accessed July 20, 2021]

[3] U.S. Securities and Exchange Commission. *Economic Analysis: Providing Insight to the Advance the Missions of the SEC and PCAOB.* October 22, 2015. Online: https://www.sec.gov/news/speech/keynote-address-pcaob-missions-of-sec-and-pcaob.html [Accessed August 13, 2021]

[4] Space Safety Coalition. *Best Practices for the Sustainability of Space Operations.* 16 September 2019.

[5] D. Bryson, D. R. Penney, D. C. Goldenberg, and G. J. Serrao. *Blockchain Technology for Government.* MITRE. April 2018. Online: https://www.mitre.org/publications/technical-papers/blockchain-technology-for-government [Accessed August 18, 2021]

[6] National Aeronautics and Space Administration. *The Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes.* Online: https://www.nasa.gov/specials/artemis-accords/img/Artemis-Accords-signed-13Oct2020.pdf [Accessed August 9, 2021]

[7] Christopher Newman. *Artemis Accords: whay many countries are refusing to sign Moon exploration agreement.* The Conversation. October 19 , 2020. Online: https://theconversation.com/artemis-accords-why-many-countries-are-refusing-to-sign-moon-exploration-agreement-148134 [Accessed August 9, 2021]

[8] United Nations Office of Outer Space Affairs. *Long-Term Sustainability of Space Activities.* https://www.unoosa.org/oosa/en/ourwork/topics/long-term-sustainability-of-outer-space-activities.html [Accessed July 12, 2021]

[9] United nations Office for Disarmament Affairs. *Report of the Secretary-General on reducing space threats through norms, rules and principles of responsible behaviors (2021).* https://www.un.org/disarmament/topics/outerspace-sg-report-outer-space-2021/ [Accessed July 11, 2021]

[10] Satellite Industry Association. *White Paper: The Future of Space and Space Traffic Coordination and Management*. Online: https://sia.org/wp-content/uploads/2020/09/REVISED-White-Paper20-STCM-Sept-23rd-V1.0.pdf [accessed June 1, 2021] (Finnemore & Sikkink, 1998, p. 896).

[11] Martha Finnemore and Kathryn Sikkink (1998). International Norm Dynamics and Political Change. International Organization, 52, pp 887-917

[12] Snow, David A., et al. *Frame Alignment Processes, Micromobilization, and Movement Participation.* American Sociological Review, vol. 51, no. 4, 1986, pp. 464–481. www.jstor.org/stable/2095581. [Accessed August 9, 2021.

[13] R. Adner. *The Wide Lens: What Successful Innovators See That Others Miss*. Penguin Group, New York, NY (2012).

[14] E Ackerman. *Intelligent Cars Could Boost Highway Capacity by 273%.* IEEE Spectrum 0 September 2012. Online: https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/intelligent-cars-could-boost-highway-capacity-by-273 [accessed June 5, 2021]

[15] M Collins. *Study Shows Accidents Less Likely With ADS-B In: Data could lead to more ground stations.* AOPA, April 18, 2019. Online: https://www.aopa.org/news-and-media/all-news/2019/april/18/study-shows-accidents-less-likely-with-ads-b-in [accessed June 20, 2021]

[16] Bojan Pancevski. *Elon Musk's Satellite Internet Project Is Too Risky, Rivals Say*. Wall Street Journal, April 19, 2021. https://www.wsj.com/articles/elon-musks-satellite-internet-project-is-too-risky-rivals-say-11618827368 [Accessed July 11, 2021]

[17] SpaceX. *Re: IBFC File No. SAT-MOD-20200417-00037*. April 20, 2021. https://licensing.fcc.gov/myibfs/download.do?attachment_key=6212177 [Accessed July 12, 2021]

[18] European Space Agency. *Automating Collision Avoidance.* (2019) Online: http://www.esa.int/Safety_Security/Space_Debris/Automating_collision_avoidance [accessed June 1, 2021]

[19] D. Werner. *Average monthly conjunction rates surge from 2017 to 2020.* Space News. Online: https://spacenews.com/space-traffic-management-idling-in-first-gear/ [Accessed: August 19, 2021]

[20] Salvatore Alfano, Daniel L. Oltrogge, and Ryan Shepperd. *LEO Constellation Encounter and Collision Rate Estimation: An Update*. IAA-ICSSA-20-0021 (2020).

[21] J.F. Morin. *Introduction to a new space governance dataset v.1.* Online: https://www.youtube.com/watch?v=OEbACdfR9wU&list=PLrZysWZ8u5h3cc2_UxN_I8lJRcDEhVWHF [accessed June 8, 2021]

[22] R. Biggs, M. Schlüter, M. Schoon ed. *Principles for Building Resilience: Sustaining Ecosystem Services in Social-Ecological Systems.* Cambridge University Press. United Kingdom. 2015.

[23] S. Shackelford. *Governing the Final Frontier: A polycentric Approach to Managing Space Weaponization and Debris.* American Business Law Journal, Vol. 51, Issue 2, (429-513). Summer 2014.

[24] P. de Filippi. *Blockchain Technology as an Instrument for Global Governance*, SciencesPo, Paris, 2021

[25] R. Cardin, D. Burchett, H.G. Reed. *SNARE (Sensor Network Autonomous Resilient Extensible): Decentralized Sensor Tasking Improves SDA Tactical Relevance*, AMOS 2021.

[26] J. G. Miller, "A new sensor allocation algorithm for the space surveillance network," 74th MORS Symposium, vol. 5, August 2006.

[27] North American Aerospace Defense Command Cheyenne Mountain Complex Integrated Tactical Warning and Attack Assessment Program Technical Report-Study Services Special Perturbations Tasker Programmer Documentation for the Integrated Space Command and Control (ISC2), Lockheed Martin Information Systems and Global Solutions, 9970 Federal Drive Colorado Springs, CO 80921-3616, July 2014.

[28] C. Vestergaard, G. Green, E. Obbard, E. Yu, G.D. Putra. *SLAFKA: Demonstrating the Potential for Distributed Ledger Technology for Nuclear Safeguards Information Management.* Stimpson. Online: https://www.stimson.org/2020/slafka/ [accessed June 26, 2021

[29] R. Jervis. War and misperception. *The Journal of Interdisciplinary History*, *18*(4), 675-700. (1988). doi:10.7916/D8251VV9/download

[30] Aleksander M. Lubojemski (2019) Satellites and the Security Dilemma, Astropolitics, 17:2, 127-140, DOI: 10.1080/14777622.2019.1641689

[31] A. R. Radcliffe-Brown and M.N. Srinivas. Method in social anthropology. (1960). Retrieved from https://philarchive.org/rec/RADMIS

[32] Sovrin Foundation. *Four Pillars of an SSI Network*. Online: https://sovrin.org/four-pillars-of-an-ssi-network/ [accessed August 30, 2021].