Showing Our Hand: The Case for Open SSA Data

P.J. Blount[*]

1. Introduction

A fundamental challenge for any proposed space traffic management (STM) system is the underlying data and whether that data can be trusted. The technical and legal aspects of STM both rely on the quality and trustworthiness of the underlying data. Currently, space situational awareness (SSA) data that is publicly available is incomplete as a result of both technological gaps in monitoring and policy decisions that keep parts of these data sets classified due to military sensitivities. This data gap will be an issue for STM going forward as stakeholder trust, and therefore buy-in, in an STM system will begin with the data.

This paper will make a case for why states with SSA data should make that data open. Specifically, it will argue that the security interests of the main actors in space will be maximized through an open data system, despite the risks in releasing full data sets. An open data model is integral to the effectiveness of STM, because transparency will be a key value needed to build a system that users trust.

This paper, which functions more as a position paper than a research article, will proceed by first arguing that the choice of open data has a significant impact on the evolution of the legal framework of a potential STM system. This argument will focus on the role of stakeholder trust in the system through the lens of transparency. Next, this paper will argue that, as a matter of policy, open data better protects the contemporary space security environment than secrecy, in particular among the major space actors. Finally, this paper will make the case that the achievement of a global STM system will require open data as a threshold building block. This section will emphasize that open SSA data, as a global public good, will better support the goals of international peace and security as set out in the UN Charter. It should be noted that this paper is lightly cited as it is meant to be aa position paper rather than a research paper.

[*] University of Luxembourg.

2. Openness

As a general rule, entities trust processes that they can see and understand. As a result, openness and transparency have been critical to the modern project of establishing legitimacy in the rule of law. When rules and procedures are made visible, then the governed are able to understand and verify that the system that strikes the balance between them and the sovereign power is working fairly and justly. It also gives them a foundation upon which they can build trust in the system, as transparency serves as a tool to prevent and expose corruption and injustice. Openness serves as a tool that fosters trust in decision making and bolsters the legitimacy of legal restraint upon the populace. It also facilitates public debate and discourse as to how the governance system should evolve into the future.

This need for openness is not limited to formal government and legal systems. It has been useful in all types of governance systems including private and public organizations. One of the best examples might be the Internet Engineering Task Force (IETF), which adopts the standards that are at the heart of network technology. The IETF is not really an organization in that it lacks legal personhood. Instead, the IETF is a procedure that facilitates interested parties in contributing to the technical specifications of the core Internet protocols that govern how Cyberspace functions. The IETF functions via an "open process" with the goal of creating "open standards for Internet functionality (and thereby governance.[1] While the IETF serves as an extreme example due to its lack of legal personhood, the resulting global network of networks that functions using protocols for interoperability displays the power of openness to help overcome collective action problems.

The power of openness as a security stabilizer can also be seen in the area of remote sensing. In the 1970's LANDSAT set a trend for openness in civilian remote sensing products with its policy of nondiscriminatory access.[2] Since then civilian remote sensing satellite programs globally have trended towards openness. For example, the European Union's Copernicus system has implemented an "open data policy" in the underlying regulation.[3]

It is submitted that openness and transparency are critical to developing a space traffic management system at a global scale. This is because trust by stakeholders in the system is needed to bridge across state borders and ensure the system's efficacy in coordinating space activities. Mistrust is what characterizes the current STM system (to the extent that it can be characterized as a system). At present, STM is handled on an ad hoc basis with the United States Air Force being the single most important player. The USAF, through its Combined Space Operations Center (CSpOC) collects

[1] "Tao of the IETF," https://www.ietf.org/about/participate/tao/.

[2] 51 U.S. Code § 60111(c)(3).

[3] Regulation (EU) No 377/2014 at para 36.

space situational awareness (SSA) data and processes this data. The main goal of this operation is to protect US national security interests and also to protect US civil and commercial assets that are in orbit. If CSpOC, when processing the data finds that there may be a chance of an on orbit conjunction, they notify the responsible operators of the conjunction. At this point it is the operators that make a decision on what course of action to take. CSpOC also maintains bilateral agreements with partner countries and at least one NGO for bilateral sharing of SSA data.

The central critique of this system is that there is a lack of transparency. While CSpOC, under its statutory authority, makes some SSA data openly available, it maintains its high accuracy data as classified and only shares it on the basis of bilateral agreements. States that the United States considers to be adversaries would be unlikely to reach such a bilateral agreement. Thus from other state's points of view, CSpOC data is not trustable, because it is meant to serve US interests rather than the public good. So, while CSpOC has been a relatively responsible actor when it comes to SSA sharing (and is indeed contributing data than can be considered a public good), as long as the bulk of the data and processing are hidden behind a classification system, users will have a difficult time having sufficient trust in the system. This is exacerbated by the fact that we lack information on the modelling algorithms that make determinations as to when a conjunction is likely. Of course, this is not intended to criticize the United States, as other state collectors of SSA data do not openly share their data or processing either. The lack of sharing on behalf of all of these states is based on a lack of political trust. In other words, highly detailed data on military satellites, makes them much easier to target using anti-satellite (ASAT) technology, therefore states do not want to expose themselves to such interference.

The problem is that, other operators suffer from this lack of trust among states collecting and disseminating SSA data. Many operators have turned to private solutions for SSA data, and may take the risk that they will be notified by the relevant authority in case of risk. The problem is that any single data set is often insufficient at predicting a conjunction, as can be seen in the Iridium Cosmos collision of 2009. Further, while private actors may currently be able to coordinate among themselves, if the population of space objects continues to rise according to projections, such coordination, in the absence of authority, will be in danger of collapsing if defection from established yet nonbinding norms occur. And the risk of this happening will likely increase as long as "disruptive" is held as a positive value in innovation.

3. Openness and Security

National Security is the core reason that states have adopted secrecy with relation to their SSA data. The justification is simple, if an adversary has detailed information on a spacecraft that spacecraft will be easy to target. This is akin to troop positions in the battlefield, because troops are made vulnerable when their locations are known by the enemy. But satellites are not troops in the battlefield and treating them as such may actually increase vulnerability across the space domain. In all likelihood, the states that pose a credible threat of actually crippling the US military with destructive attacks on space objects likely have good data on these assets. While some states may pose a threat to a few satellites, actually disrupting US global command and control for a significant amount of time would be quite difficult.

There is no dearth of scholarship pointing out the need for debris mitigation and STM to ensure that space operations are safe and sustainable. Critical to safety and sustainability is the avoidance of conjunctions and collisions in orbit, and the ability to avoid such incidents is driven by SSA data. The need to avoid collisions is shared by all operators: military, civil, and commercial. Military operators that hold better information sets are not insulated from the risks that result from other actors. Two commercial actors experiencing an on-orbit collision resulting in debris, contributes directly to insecurity for national security assets. Military actors therefore have a salient interest in ensuring that non-military actors are behaving in a responsible manner. Open systems support decision making that reduces risk across the spectrum of space activities.

A second reason that this increases security, is that space is inherently transparent. Military satellites cannot be hidden from view from hobbyist sky watchers, much less other states. Indeed, this is why the 2001 Rumsfeld Report used the phrase “a space pearl harbor,” because despite the secrecy there was already inherent transparency and thus inherent vulnerability. This transparency means that while there may not be a high accuracy data set publicly available, there is general knowledge of military space assets and their locations. The lack of high accuracy data might protect these assets from precision attacks such as a direct ascent ASAT, but it does not protect them from less precise attack methods such as co-orbital explosions.

4. Foundations

Openness in data and processing will be foundational to any international system, because the data and processing will be critical to decision-making. Openness gives decision making legitimacy by instilling trust by stakeholders in the system. This is important in light of current geopolitics, which are in general resistant to new international legal texts dealing with space activities.

While most space actors agree that some form of STM is needed, there has been little to no formal movement at the international level towards developing such a regime. Indeed, most action has taken place at the national level or within the private sector. At the international level, international space law making is frozen. But domestic regimes alone do not solve the collective action problem of ensuring responsible behavior on orbit, because not all actors are from the same state. Similarly, not all actors would be a member of private consortiums working on these issues. A true STM system needs to function globally, and as such needs to have the authority of states backing it.

Openness presents a distinct tool for beginning to build the inter-state trust needed to establish an international system. It should be accepted that an international STM regime will not be adopted immediately or easily, but it is argued that unilateral openness from a major player and its allies could lay a foundation on which an international regime could be built. Such unilateral action could be coupled with diplomatic encouragement of other space actors to contribute to the data set, which could function like a transparency and confidence building measure. This type of cooperation could be instrumental in opening a path to negotiations on how STM could be established in a multilateral context. If the data set is strong enough there will be evidence on which to base rule formation through space operator practice. It is feasible that a formal coordination mechanism could be built on those practices and that data set. Such a mechanism could range from an international technical committee similar to the IADC to an ITU type structure with rulemaking ability.

Further open data furthers much of the purpose of the Outer Space Treaty. A core theme in the treaty and in international space law in general is the sharing of information about activities in space. The treaty system includes numerous provisions that open up opportunities for states to communicate with each other in order to build trust and confidence during the Cold War. This underlying value is still quite relevant, but in a more multilateral world in which the cost of engaging in space activities is plummeting, information sharing needs to be more formalized and adapted to innovations in the industry. In order to build trust in space operations, all operators should be able to understand where other operators are and how their operations might interfere with another's operations. Open data can facilitate proper risk assessment for all operators in space.

5. Conclusion

There is a general agreement in the discourse on STM that any system likely to emerge will come from the bottom up, meaning that it is likely to originate at the domestic level rather than at the international level. Open Data is a likely path to globalizing a national system by giving a public good to others than ones allies. From there open modeling can be developed which can lead to trust. Trust is the foundation of an effective governance system.