35th Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on April 8, 2019

Evaluating Commercial Contributions to Space Domain Mission Assurance

James Doggett
HawkEye 360, james@he360.com

Chris DeMay
HawkEye 360, chris@he360.com
Rob Rainhart
HawkEye 360, rob@he360.com

ABSTRACT

The 2015 Space Mission Assurance Taxonomy[1] defines the OSD Policy perspective on Space Domain Mission Assurance (SDMA) for critical national security space (NSS) assets. The document classifies three approaches to Mission Assurance for NSS systems: Defensive Operations, Reconstitution, and Resilience, which is further separated into six sub-elements. Since its publication, the Taxonomy has gained wide acceptance as a framework for evaluating the ability of NSS missions to continue to operate in the face of an increasingly capable threat environment. What is less well understood is the contribution of commercial space systems, and in particular small satellite or “Space 2.0” constellations, to the mission assurance of the overall US space enterprise. Often the conversation around commercial systems will begin and end with a nod towards Disaggregation, a term which is sometimes misapplied to cover other effects. In fact, commercial space systems contribute to each aspect of the Mission Assurance Taxonomy, and understanding their impacts is crucial to formulating an overall strategy for the US and its operations in a competitive, contested, and congested space environment. This paper presents a qualitative assessment of the impact of commercial space systems to each element of SDMA and recommends a path forward for a quantitative follow-on study.

INTRODUCTION

The US military, and the full national security establishment more broadly, employ space assets every day in order to perform their mission. National Security Space (NSS) systems provide force enhancement to ground operations, as well as command, control, and communications (C3) between national leadership and operational units. Individual satellite architectures such as the Global Positioning System (GPS) and the Advanced Extremely High Frequency (AEHF) constellation combine to form the full NSS Enterprise, each with a unique mission. Typically, these systems consist of a space segment (the satellites themselves), a user segment, and a control segment.

Many of the NSS systems in use today were originally designed, developed, and fielded at a time when potential threats to space systems were not widely available, understood, or considered to be a threat. That perception was dependent upon the linked assumptions that an attack on NSS systems is unlikely to be ordered by an adversary, and that such an attack would be too difficult or impossible to carry out if it were ordered. The first assumption rests on the traditional link between a nation’s space systems and its nuclear capabilities; an attack on NSS assets was thought to be an opening move in a nuclear offensive, and so traditional deterrence theory held that such an attack would be extremely unlikely, and potentially disastrous to the aggressor due to the assumed response from the US. Additionally, the technology and weapon systems needed to carry out such an attack were complex and challenging not only to develop, but to employ. This second assumption has been challenged in recent years by advances in space technology across all sectors, which have significantly increased counterspace capabilities; this was demonstrated most notably in 2007, with the destruction of the Fengyun-1C2￼3￼

In response to this understanding that spacecraft are now critical to operations across the spectrum of conflict, from Phase 0 to nuclear, it has become increasingly common to consider ways to deny this overwhelming advantage to the US military. An attack on a satellite may no longer be equivalent to a declaration of nuclear war, but instead may be an attempt to deny a tactical unit knowledge of its geographic location and communications with its commanding element. Furthermore, attacks on the mission of satellites have already been demonstrated; one example among many is the jamming of GPS during NATO exercises observed by the Norwegian Intelligence Service in 2018.[4]

The 2015 Space Mission Assurance Taxonomy (referred to for the rest of this paper as the Taxonomy) defines the OSD Policy perspective on Space Domain Mission Assurance (SDMA) for critical national security space assets. The document classifies three approaches to Mission Assurance for NSS systems: Defensive Operations, Reconstitution, and Resilience, which is further separated into six sub-elements (Disaggregation, Distribution, Diversification, Protection, Proliferation, and Deception).

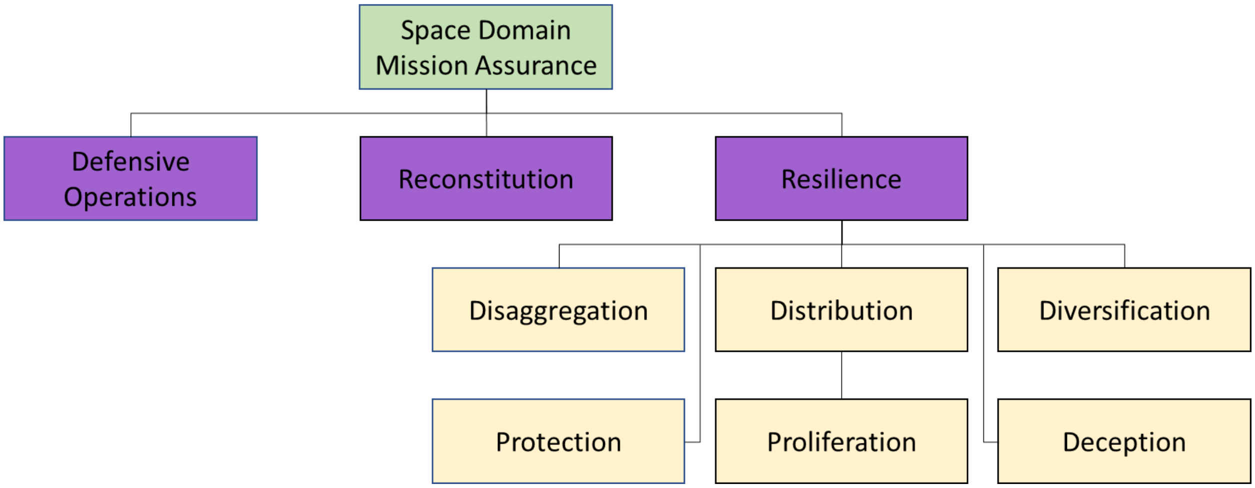

Exhibit 1: The Mission Assurance Taxonomy (adapted from [1])

The Taxonomy does not represent a comprehensive strategy for implementing any one aspect of SDMA; more recent documents such as the 2017 National Security Strategy have addressed specific strategies. Since its publication, the Taxonomy has gained wide acceptance as a framework for describing and evaluating the ability of NSS missions to continue to operate in the face of an increasingly capable threat environment (discussed in greater detail in the next section). More importantly, the Taxonomy seeks to ground this framework in the concept of Warfighting Mission Assurance, rather than the resilience of a particular NSS asset (or indeed of the enterprise). The distinction is in prioritizing the capability delivered to those who rely on NSS assets – warfighters, analysts, policymakers – above any inherent survivability of the assets themselves.

While most of the conversation around SDMA is focused directly on NSS systems and their response to this threat environment, the growing commercial space sector is also critically important to addressing counterspace challenges. Commercial entities have been active in space since the 1960s, with a steadily increasing pace of activity and development as traditional government missions have been adopted by non-governmental organizations. While "commercial space" is a flexible term, for the purposes of this paper it will be used to mean any space actor whose primary motive is earning revenue for a private entity, rather than directly supporting a government mission. In particular, this paper will focus on the wave of commercial entities that are broadly captured under the labels "NewSpace" or "Space 2.0". These companies may have novel or emerging missions, may make use of technologies or concepts that are in the early stages of commercial (vice governmental) use, and tend to use smaller satellites in lower orbits for their space segments, as opposed to large and expensive geostationary satellites. An additional distinction between these emerging companies, and more traditional commercial space providers, is in their business models. While traditional commercial partners may design components, platforms, or even full architectures that are fielded and then operated for a government customer, NewSpace companies are more likely to own and operate their own assets and to interface with the government as a provider of data or analytics.

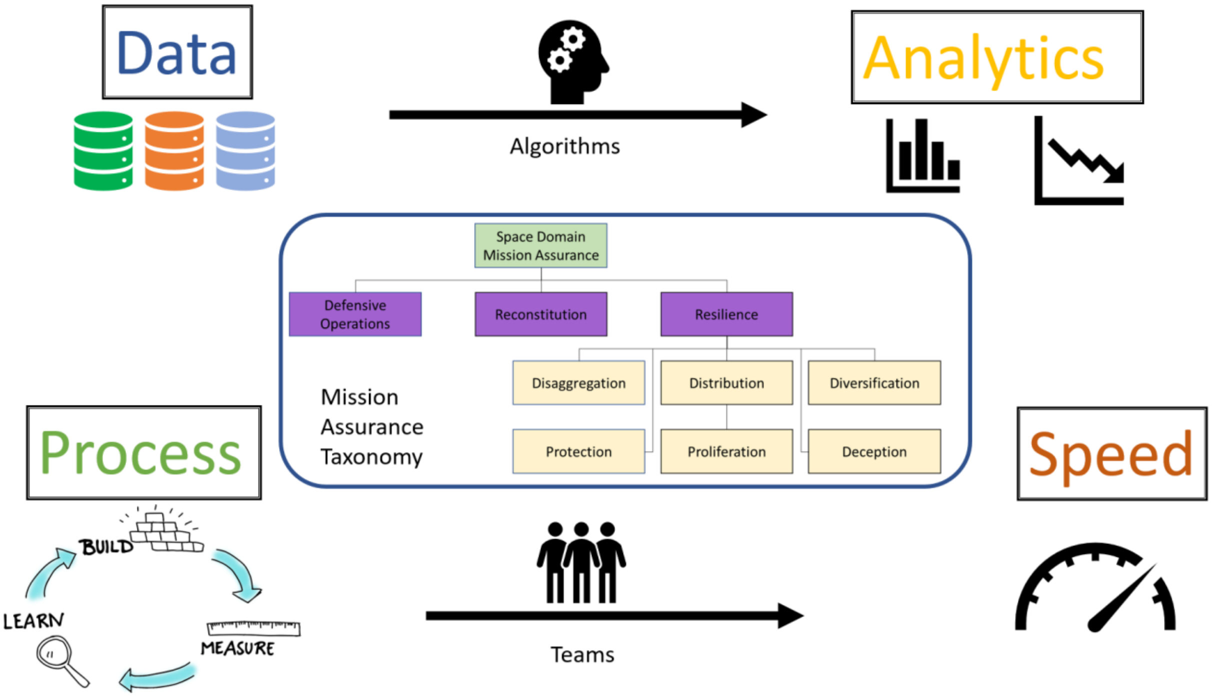

Exhibit 2: Commercial partners have the potential to improve mission assurance through data, analytics, process, and speed

However, in assessing the mission assurance of the full NSS enterprise, it is critical to consider the role played by commercial space systems, as their impact on NSS mission assurance is not neutral. Responsible behavior by commercial actors has the potential to augment and improve the ability of NSS enterprise to respond to threats; irresponsible behavior, or simply actions that are not aligned with an enterprise-level approach to challenges, could degrade this critical ability.

There are four primary vectors through which this variety of commercial partners can improve SDMA. By providing **data** to NSS assets and missions, commercial partners can offload less-critical missions and perform the role of a traditional vendor. **Analytics** represent the next level of sophistication in this model, in which commercial partners are more deeply enmeshed with the problem sets of USG missions and are able to provide insights, rather than just raw data. By bringing a more agile **process** to the development and fielding of space systems, commercial partners can help increase the **speed** at which the NSS innovates, improving the ability of the enterprise to outpace the threat.

THE COUNTERSPACE THREAT ENVIRONMENT

There is growing consensus in the NSS community that the space domain is no longer a sanctuary, if indeed it ever was. Multiple unclassified reports have recently been published by US Government and non-governmental entities describing the growing threats to US space systems. The methods for categorizing these threats varies, but in general the same catalog of threats emerges. The Defense Intelligence Agency (DIA) describes a "counterspace continuum" of threats in terms of their effects, ranging from reversible to irreversible[5], while the Center for Strategic and International Studies (CSIS) categorizes threats according to the mode of their interaction with target systems, from kinetic to non-kinetic. [6]

A reversible threat is one that disrupts the intended operation of one or more NSS systems in a way that is not necessarily permanent (although it may be); by contrast, once a nonreversible threat has successfully been employed against a system, there is permanent impact to the mission that system is intended to perform. The key distinction is in the permanence of the effect to mission. Examples of reversible effects range include electronic warfare (jamming or spoofing) carried out against space, ground, or user segments of an NSS mission; cyber-attacks which temporarily deny service from the effected mission; or directed energy weapons (DEW) which can blind an imaging satellite during its time over a target area.

A nonreversible threat is one which permanently denies service from an NSS mission after its use. The most commonly-used example of a nonreversible threat is an antisatellite (ASAT) missile fired from the ground, such as the one employed by the Chinese in their 2007 destruction of a defunct satellite in low earth orbit (LEO). ASAT missiles can also be launched from non-terrestrial platforms such as aircraft or other satellites.

In describing a threat as reversible or nonreversible, it is important to consider the effect on the system beyond the method in which it is delivered. A kinetic weapon such as an ASAT may have a reversible effect if, for example, it does not deliver its intended effect but does have an impact on mission. Certain threats may be intended to operate in either capacity or to provide an adversary with a scalable approach to escalating a space-based conflict. A spacecraft capable of performing a satellite servicing mission, for example, could be used to either “hold” an NSS system in an orientation which prevents it from accomplishing its mission (by shielding solar panels from sunlight, for example) or to permanently damage a critical component.

While reversible threats are often considered lower on the spectrum of severity than nonreversible threats due to perceived impact, they have just as much potential to cause harm as nonreversible threats. Physically destroying a single GPS satellite out of the full constellation is certainly irreversible; but it will likely have less impact than a jamming attack that denies access to the full AEHF constellation.

“Kinetic Physical” is the term used by CSIS to describe counterspace weapons that are used to physically damage or destroy a satellite. This type of weapon system must be able to detect and track its targets in the final stages of flight.

OVERVIEW OF COMMERCIAL CONTRIBUTIONS TO MISSION ASSURANCE

This section provides a brief description of each element of the Taxonomy, and a qualitative overview of the potential contribution of commercial actors to that element. This survey provides a starting point for a more formal quantitative assessment of the relative mission assurance provided by alternative future architectures that incorporate commercial systems.

Defensive Operations

The Taxonomy defines Defensive Operations as “Activities or operations undertaken to interrupt an adversary kill chain or provide warning or insight to the targeted mission system in support of defensive actions.” Commercial entities do not directly interrupt adversary systems through intentional, direct action targeted at those systems. However, commercial systems may directly support Defensive Operations carried out by the US government in a number of ways.

A critical contribution from commercial sources can be indications and warnings (I&W) of adversary activity on a timescale that enables a defensive response. The US Government maintains several systems dedicated to Space Situational Awareness (SSA) in recognition of the fact that a prerequisite of taking preventative action against an attack is understanding that the attack is occurring, or immanent, in the first place. These systems are exquisitely capable, but they are not omniscient, and monitoring of the space environment by trusted commercial partners can augment capabilities that are already fielded. By tracking objects in space and maintaining a catalog of their standard activities, commercial partners can contribute to pattern-of-life analysis that makes it easier to identify activity out of the ordinary. Rather than allocating scarce resources and attention on benign objects, the NSS enterprise can focus on potentially threatening actions.

I&W regarding counterspace threats extends beyond SSA, as most threats to space systems are not space-based. Commercial data providers also play a role in monitoring the earth for human activity that serves as an indicator of threatening behavior, from ballistic missile tests to potential ASAT launches. By providing earlier warning of these activities, commercial actors can increase the range of available options to support defensive operations.

Commercial actors can also contribute to post-engagement activities, such as Battle Damage Assessment (BDA), providing important context to a situation and allowing US leaders to control escalation. Positive attribution of an attack is essential to preventing and deterring future incidents, and integration of commercial sources can increase the amount and variety of information available to policymakers.

Reconstitution

Reconstitution is defined as "Plans or operations to bring new assets on line…in order to replenish lost or diminished functions to an acceptable level for a particular mission, operation, or contingency after an attack or catastrophic event." Conceptually, Reconstitution covers the range of options for replacing mission capability that an adversary has successfully attacked and, thereby, denied to users who rely on it. This can include replacing the exact asset that was destroyed through responsive launch, maintaining a hot- or cold-spare that can be rapidly fielded, or restoring (in whole or in part) the lost capability through the use of different assets.

Reconstitution is intrinsically tied to responsive space launch, which is currently a priority of DARPA and several other USG organizations. Historically, launch vehicles have been designed with large spacecraft as the primary customer. Launch providers such as United Launch Alliance (ULA) and ArianeSpace can carry approximately 20,000 kg to LEO at once. Newer players, like SpaceX and Blue Origin, are competing with the established launch base, still targeting payloads of 45,000 kg or more. Opportunities have existed for small satellites to be put in orbit, as rideshares on these "heavy" vehicles, leveraging excess capacity as secondary payloads. To that end, smaller spacecraft have been at the mercy of larger spacecraft for launch timing and orbital targets. Over the last decade, however, with the increased investment in -- and development of -- small satellites, the demand for scaled and dedicated launch has grown proportionally. The result has been a seemingly disproportionate growth in the number of launch providers, currently in various stages of business development. By some counts, there are over 100 companies competing for the business of the developing small satellite constellations. While it is almost-certain that all 100+ companies succeed, each is attempting to demonstrate differentiation through technology and/or business models. The competition will ultimately produce an industrial base subsector that is right-sized for actual demand, which will be shaped over the next 3-5 years, as new constellations come online. In order to compete and succeed, surviving small and medium launch class vehicles will posture themselves for responsive launch. Characteristics of responsive launch include (a) on-orbit delivery of small satellites, (b) with orbital parameters specified by the small satellite customer, (c1) on a timeline that is reasonably flexible for spacecraft manufacturing delays, (c2) on a schedule that is consistently repeated and met by the launch provider, (e) provides for interchangeability between vehicles for late changes to the schedule, and (f) demonstrates a success rate consistent with the risk postures reflected by venture-backed commercial companies. The ability to reconstitute critical assets is dependent upon all of these launch criteria.

Responsive launch is only an effective means of reconstitution if there is something to launch, and so maintaining spare assets on the ground is another key component of reconstitution. The use of small satellite bus technology for developing an inventory of on-the-ground spare units can take advantage of the economies of scale already in play for satellite constellation development. Privately funded satellite constellations depend on near-commoditization of bus technologies with significant repeatability and optimized testing approaches to ensure reliability while maintaining affordability as the non-recurring engineering bus design work is amortized over the constellation. As small satellite buses are built more affordably and at scale, spare assets become comparatively low cost, and inventory can be rotated into commercial constellation replenishment planning to ensure that spare buses are fresh. Similarly, as mission payloads are developed as part of a commercial constellation capability, spares can be developed and put into a similar replenishment rotation. By designing payload interface flexibility, payloads can be either pre-integrated or integrated on-demand. Moreover, collections of mission capabilities, across multiple missions and companies, should be evaluated for bundled launch planning in an effort to minimize expense or delay for reconstitution. As an alternative consideration to launching a 1-for-1 replacement of a destroyed asset, the lost mission capability could instead be reconstituted through a nontraditional asset.

As space actors develop and mature new commercial technologies, which are increasingly persistent and of higher quality, they also reflect capabilities that historically had been monopolized by governments. As such, government should consider the benefits of leveraging those commercial capabilities as both an augmentation of national systems as well as temporary mission "backfill" in a time when the NSS has been diminished or destroyed. While commercial companies make no claim of replacing exquisite national systems, commercial solutions do offer capabilities that are venture capital-backed, available on-demand, and carry little technical or financial risk. Even in peacetime, there is benefit to integrating commercial space solutions as a service, such that the capability can augment national systems, as needed, as a service.

Resilience

As defined in DoDD 3100.10, Resilience is "The ability of an architecture to support the functions necessary for mission success with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats, in spite of hostile action or adverse conditions." The Taxonomy distinguishes Resilience as an element that is intrinsic to the NSS system itself, as opposed to Defensive Operations (offboard effects) or reconstitution (system replacement). Because NSS assets are complex, expensive, and highly-capable technological systems, there is certainly high incentive to design them to be inherently survivable instead of relying solely on defense or replacement. Resilience is further subdivided into six sub-elements, each of which is described in greater detail below.

Because Resilience is conceptualized as being inherent to the system being described, to analyze the commercial contributions to Resilience, the system is considered to be the overall NSS enterprise, rather than a specific asset. There are commercial contributions to the resiliency of military spacecraft, for example, in the hardening of components against attack by vendors; but, for the purposes of this discussion, the contribution will be of wholly-commercial systems to the NSS enterprise.

Disaggregation

Disaggregation is the segregation of separate functions or capabilities into separate platforms or payloads. The standard example is the separation of Strategic and Tactical support functions into separate satellite platforms, vice the current architecture of large, aggregated systems. This idea has been challenged as "painting a target" on tactical systems, by implying that it is more acceptable for an adversary to attack them than strategic platforms. If disaggregation is framed as simply doubling a small number of large, expensive satellites that are easy to track using existing SSA technology, then this criticism has some validity. All that would be gained is an increased number of targets, which would fail to deplete an adversary's magazine depth, while removing the perceived deterrence-related "shield" conferred by a strategic mission.

Integration of commercial space-based data sources into the NSS enterprise further complicates this picture by forcing the question of how the USG would respond to an attack on a US commercial entity in space. Engagement with Allies and potential adversaries, and a whole-of-government approach to messaging norms for responsible behavior in space, will help to provide clarity and stability in orbit.

Due to their heavy use of small satellites, which are necessarily limited in size, weight, and power (SWAP), NewSpace actors tend to operate disaggregated platforms by default; there are simply not enough on-orbit resources to combine multiple functions on a single small satellite. Many commercial small satellites are intended to perform a single mission, or at most a small number of related functions. Although small satellites are inexpensive compared to exquisite satellites, they still represent a large capital expenditure to small venture-backed startup companies, and so there are strong incentives to maximize the opportunity for success by remaining focused on the primary mission of the company.

By incorporating commercial systems, the NSS enterprise will become more disaggregated by nature as different functions are carried out by different platforms. Critical missions will always be performed by exquisite USG-owned and operated spacecraft, but there is significant potential to offload lower-priority missions to commercial operators.

Distribution

The canonical example of Distribution, defined as a number of nodes working in concert to perform a single mission, is the GPS system. No single GPS satellite is essential to the operation of the system, and the resilience of the PNT mission provided by the NSS enterprise is therefore enhanced by this distribution. While performance will begin to degrade as nodes are lost, the delivered mission capability can persist in the face of some losses. A non-distributed system, by contrast, is either monolithic in nature (there is only one node) or contains one or more single points of failure (nodes whose loss would render the system incapable of operating).

Many NewSpace companies operate architectures that are distributed by their very nature. Advances in small satellite components, manufacturing methods, and communications are enabling companies to launch larger numbers of spacecraft. This results in distributed constellations that are tolerant to the loss of a single node.

The upcoming generation of commercial communications architectures will begin to shift the paradigm for satellite communications from monolithic GEO-based platforms to a distributed LEO-based architecture. These constellations, consisting of hundreds of individual satellites, will be inherently tolerant to the loss of any individual node.

Beyond these commercial mega-constellations, the trend for NewSpace companies in general is towards multi-plane, distributed constellations. These constellations can improve the resilience of the NSS enterprise by forcing adversaries to maintain custody of a wider variety of space platforms, complicating targeting decisions. Furthermore, by utilizing these constellations for communications where permissible, the enterprise gains a distributed architecture in the face of potential threats.

Diversification

Diversification is defined as contributions to a mission coming from multiple vectors including different platforms, orbits, systems, and even ownership models, such as government owned, commercially operated (GOCO).

Commercial space partners increase the diversity of the NSS architecture along each of these vectors, providing a low-cost way to increase resiliency. By diversifying data sources, the NSS enterprise can increase its resiliency to a threat to any individual source. By diversifying its processes, the enterprise can increase its resiliency to emerging and unanticipated threats, by fielding new capabilities with increased speed.

Protection

Traditionally, protection has been focused on the security of the data and the networks. As nefarious actors are thwarted by advanced cyber protections, there is an incentive to turn their focus to manipulation of data used to inform decision makers. Injection of malicious data anywhere in the production cycle can have catastrophic consequences. Instead of a large-scale data breach, hackers can make small changes in data and analytic processing that are less likely to be detected yet result in significant impact.

Satellite operators must adopt end-to-end protection strategies to ensure data that is feeding the NSS enterprise is accurate, reliable, and auditable. The space enterprise is, perhaps, one of the most complex environments to protect holistically. Data collection and processing traverse multiple transports and processing platforms, and bad actors are constantly assessing vulnerabilities at the "seams" of these distributed systems. Adoption of commercial encryption technologies by the Federal Government are allowing end-to-end encryption, even with commercial platforms. Due to size, weight, and power restrictions, even government funded smallsat programs have struggled to implement Type 1 encryption. AES 256 and other commercial encryption can provide some level of protection, but challenges in key management and known exploits limit their efficacy.

In order to implement an end-to-end protection architecture that is extensible beyond government systems, the architecture must be comprised of commercial technologies. An all software solution would allow even microsats to use this encryption architecture. The architecture could implement a dual-AES256 encryption technique, like NSA's Commercial Solution for Classified (CSfC), at a landing zone established at the boundary, e.g. mission ground station or commercial ground station, to terminate the primary encryption tunnel. The payload tunnel could securely connect the enterprise to the space asset through the primary tunnel. This dual tunnel approach eliminates the transition "seams" for both the uplink and downlink. Commercial cloud providers are beginning to offer landing zone services which will further protect data delivery directly into customer containers.

Proliferation

Proliferation means deploying a large number of the same platform to perform a mission. Given the long development timelines involved, traditional NSS systems have been custom-built to each mission, even within multi-satellite constellations. By contrast, many NewSpace companies operate architectures that are by their nature proliferated.

Similar to the discussion of distribution, many Space 2.0 systems are by their nature proliferated. These satellites can be incrementally improved between launches and generations to provide additional capability, but in general will all be performing the same mission. While the hardware platforms may be identical, the increased adoption of software-defined architectures allows for proliferated systems to be regularly updated. While a single generation of small satellites may be launched over the course of five years, they may also receive regular monthly software updates over that same period that provide continuously-increasing capability to a large number of nodes.

Deception

Deception is defined as measures intended to confuse or mislead an adversary with respect to the characteristics of an NSS system. Similar to Defensive Operations, Deception is not a mission that will be directly carried out by commercial actors. However, by increasing the capability of the NSS enterprise to detect and respond to threats, commercial data sources can provide support to resiliency effects.

TOWARDS A QUANTITATIVE APPROACH TO SDMA ASSESSMENT

Both the SDMA Taxonomy and this paper stop short of providing a quantitative analysis of mission assurance for the space domain. In the words of the Taxonomy, "…that is a job for engineers and system developers." However, it is within the scope of this paper to recommend the top-level requirements that any framework for quantitative analysis, and specifically the commercial contribution to it, must satisfy.

Any analysis of alternative future NSS architectures must take as its metric contribution to what the Taxonomy labels "Warfighter Mission Assurance", and what may more generally be referred to as mission delivery. While some space missions exist to produce effects in space, the goal of NSS missions is almost always to impact something on earth: military operations, intelligence analysis, policymaking, or some combination of the above. A quantitative analysis of SDMA must take as a founding assumption the concept that mission impact, rather than impact on an individual space asset, is the primary metric.

Beginning with this assumption, an important corollary is that threats should be evaluated in terms of their impact to mission, rather than the physical characteristics of their interaction with the nodes of the NSS architecture. The same weapon system may be used to produce a reversible or a nonreversible impact on the mission of an individual NSS node, and so there cannot be a blanket model for each threat; effects must be a primary consideration.

In order to express the impact a threat system has on an NSS mission, a quantitative assessment could express the impacted performance level relative to the initial (un-impacted) mission performance; relative to a complete loss of performance; relative to some required threshold of performance; or, relative to some combination of the above. Each approach has benefits and drawbacks, but the shared characteristic is that mission performance is a relative assessment, rather than absolute.

These guidelines provide a high-level, although not exhaustive, set of characteristics that a quantitative assessment of space domain mission assurance should have.

CONCLUSION

The Space Mission Assurance Taxonomy provides a useful framework for evaluating the contribution of disparate elements to the mission assurance of the NSS enterprise as a whole. While private companies have always contributed to NSS missions, the recent wave of “Space 2.0” or “NewSpace” companies are doing so in a different way. Rather than contributing components or spacecraft to a mission that is then owned and operated by the government, these companies are contributing data analytic products, software as a service, and even full architectures as a service.

As these commercial partners increase in size and scope, any analysis of NSS enterprise mission assurance must, by necessity, incorporate the contribution of these systems to a truly a heterogenous architecture. There is a demonstrated need for a follow-on study that proposes a quantitative methodology for evaluating enterprise mission assurance and applies it to the contribution of both traditional NSS and nontraditional commercial assets.

[1] “Space Domain Mission Assurance: A Resilience Taxonomy”. White paper. Office of the Assistant Secretary of Defense for Homeland Defense and Global Security. September, 2015.

[2] “2007 Chinese Anti-Satellite Test Fact Sheet”. Report. Secure World Foundation. November, 2010.

[3] See, among many others, “Survivability Analysis of a Small Satellite Constellation” by Edward Hanlon from the 2018 Space Symposium Technical Track.

[4] “Norway: GPS jamming during NATO drills in 2018 a big concern”. News Report, Associated Press. February, 2019.

[5] “Challenges to Security in Space”. Report. Defense Intelligence Agency. February, 2019.

[6] “Space Threat Assessment 2018”. Report. Center for Strategic & International Studies Aerospace Security Project. April, 2018.