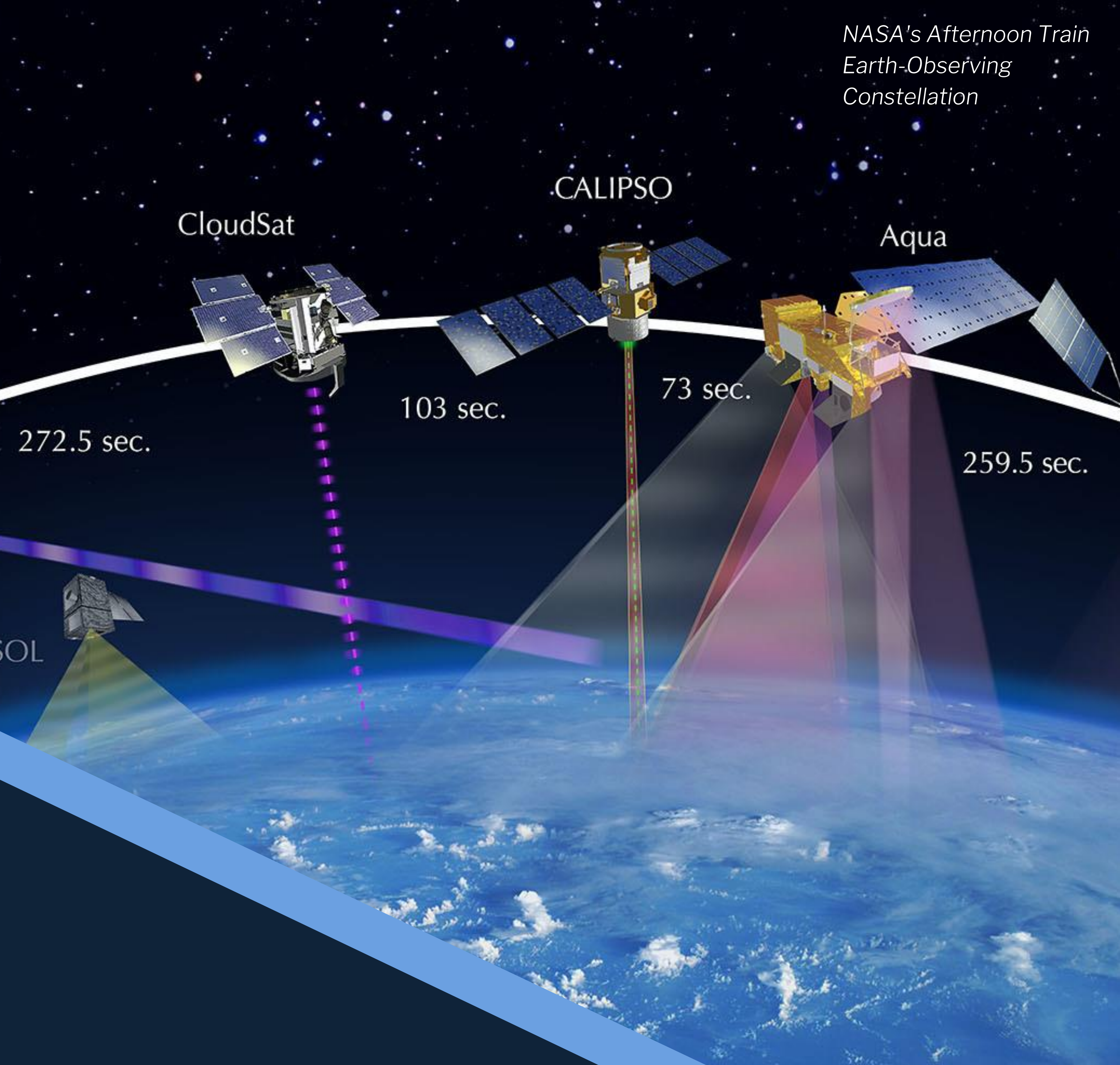


NASA's Afternoon Train Earth-Observing Constellation

Architecture for Advantage

Recommendations for Procuring and Integrating Commercial ISR Data Services

Hallie Griffiths

Applied Policy Project 2021-2022
Prepared on behalf of U.S. Space Command

Acronyms and Abbreviations

AOR	Area of Responsibility
AFRL	Air Force Research Laboratory
C2	Command and Control
C3PAO	CMMC Third Party Assessment Organization
C4	Command, Control, Communications, Computers
C5	Command, Control, Communications, Computers, Cyber-Defense
C6	Command, Control, Communications, Computers, Cyber-Defense, Combat Systems
CCMD	Combatant Command
CFSCC	Combined Force Space Component Command
CIC	Commercial Integration Cell
CMMC	Cybersecurity Maturity Model Certifications
COCO	Commercially Owned/Commercially Operated
COGO	Commercially Owned/Government Operated
COTS	Commercial-off-the-Shelf
CRADA	Cooperative Research and Development Agreement
DaaS	Data as a Service
DoD	Department of Defense
GOGO	Government Owned/Government Operated
HLIF	High-Level Information Fusion
I/PaaS	Infrastructure/Platform as a Service
ISR	Intelligence, Surveillance, and Reconnaissance
JADC2	Joint All-Domain Command and Control
JTF-SD	Joint Task Force-Space Defense
NASA	National Aeronautics and Space Administration
NOAA	National Oceanographic and Atmospheric Administration
SaaS	Software as a Service
SDA	Space Domain Awareness
SOA	Service-Oriented Architecture
SPD	Space Policy Directive
SSA	Space Situational Awareness
USG	United States Government

Introduction

The United States space defense community recently redefined its paradigm for its information collection and analysis from space situational awareness (SSA)—which focuses on day-to-day developments in the space domain, to space domain awareness (SDA)—emphasizing norms and patterns to assess actor's intentions and plans. This internal paradigm from SSA to SDA has created urgency within the United States Space Command's initiative to develop high-speed and high-capacity data processing systems to support its Commander's Strategic Mission. Simultaneously, the diffusion of remote sensing and space surveillance technology and activity across the private sector has complicated the ability of USSPACECOM to define and measure its goal of maintaining a competitive advantage in outer space.

Specifically, the technology that USSPACECOM requires to maintain a competitive advantage lives primarily in the private sector, which operates under distinct norms, standards of security, and motivations that complicate potential security applications. Before the mid-2010s, maintaining a competitive advantage in outer space was largely a function of having the means to access exquisite space data, in terms of satellites and sensing technology. With reference to these two major endogenous and exogenous shifts, this report analyzes the tradeoffs USSPACECOM should develop an acquisitions strategy that prioritizes procurement of commercial ISR DaaS over the existing model of ownership of assets and processing systems. Further, the genesis and early development of the space program in the United States arose from national security aims, and the growth since of what is now understood to be "traditional space" has been directly intertwined with U.S. defense institutions.

This analysis focuses on commercial ISR data service offerings because it is the category of dual-use technology most salient to contemporary national security concerns regarding information advantage and security. Moreover, the simultaneous challenges and opportunities that arise from the various applications of ISR technology and data in terms of investment potential, civilian utility, federal regulation, and military necessity are a microcosm for the challenges associated with the space domain at large. This problem has not been solved because how the problem realizes itself is continually evolving. As a combatant command, USSPACECOM is situated in a place where it has great responsibility in terms of effectively operationalizing U.S. military space components but faces constraints in the amount of control it exercises in directly impacting the guidance it receives from both the Executive and Legislative branches. As a result, what this problem calls for is not one single technical, regulatory, or contracting solution, but rather a way of thinking about commercial offerings that effectively mitigates internal and external tensions.

Client Background: United States Space Command

Originally established in 1985 and consolidated within US Strategic Command in 2002, U.S. Space Command (USSPACECOM) was again stood up as a unified combatant command on August 29, 2019. The eleven regional and functional combatant commands under the Joint Chiefs of Staff are responsible for operationalizing designated personnel and equipment provided by the military services. As the combatant command whose physical area of responsibility (AOR) is 100km above mean sea level, Space Command is responsible for operationalizing U.S. defense capabilities relative to space. As articulated by Joint Publication 3-14, Joint Space Operations:

Further defining the mission of the Command, the Commander's Strategic Vision, Never a Day

> "CDRUSSPACECOM leads DOD space operations planning and ensures planning supports and is synchronized with CCMD plans. CDRUSSPACECOM ensures space plans support national policy and strategy objectives. CDRUSSPACECOM plans for the defense of the space AOR and the creation of space effects. CFSCC support plans translate CDRUSSPACECOM numbered plans into executable OPLANs" (Office of the Chairman of the Joint Chiefs of Staff, 2020).

Without Space, highlights six major tasks to cultivate superiority in space and realize the Command's mission:

1. "Understanding our competition
2. Building the Command to compete and win
3. Maintaining key relationships
4. Maintaining digital superiority
5. Integrating commercial and interagency organizations"

The vision statement emphasizes the centrality of space as the "ultimate high ground," concretizing the importance of ISR collection and analysis capabilities to the Command's mission and situating USSPACECOM at the center of the tension between maintaining secure systems and promoting commercial expansion. Further, the paradigm shift within U.S. defense space strategy at large—shifting priorities from SSA to SDA—has transformed both how Space Command designs and implements its strategies and vision. Emphasizing knowledge over observation, SDA prioritizes a more nuanced, data-driven understanding of normative elements of space developments and actor behavior.

Problem Statement

Without a comprehensive framework to evaluate commercial -as-a-Service offerings for collecting, analyzing, and storing ISR data, the United States Space Command (USSPACECOM) cannot effectively define or achieve its central goal of competitive advantage.

Problem Background

The following section offers additional insight into critical facets motivating the problem outlined above by defining key terms and outlining the exogeneous domain and endogenous institutional pressures demanding attention from USSPACECOM.

Defining Terms

Space Situational and Domain Awareness

Space Domain Awareness (SDA) is a more recent framing of a related concept, Space Situational Awareness (SSA). Specifically, SDA builds on SSA: while situational awareness speaks to an understanding of how many objects are in space, who owns and operates those objects, where are they in orbit, etc, domain awareness compiles SSA to gather a concrete, evidence-driven understanding of the intent of the actors launching and operating these objects (Erwin, 2019). Because of the increasing availability of advanced sensing equipment and surveillance data, advantage is less a sole function of access to information and technology outright, but of the ability to synthesize situational information to sense and act upon developments in space as they arise. Effectively, SSA is an input to SDA, and improvements to domain awareness outputs are connected to improvements to situational awareness. Harnessing commercial innovations from the private sector will provide defense agencies the processing capabilities that are necessary for their operational goals. The aim underlying the SDA shift is that understanding intent of space actors will allow SPACECOM to maximize its ability to deter potential conflicts. Whether these conflicts are precipitated by unintentional incidents—such as the collision of two objects—or potentially maligned behavior—such as jamming the signal from an adversary's satellite to interrupt communication channels—transforming existing SSA into SDA will heighten SPACECOM's capacity to preempt and mitigate issues as necessary. The shift from SSA to SDA highlights a novel emphasis on developing the data management systems in light of this diffusion of surveillance technology.

Interoperability

USSPACECOM has been proactive in establishing data-sharing relationships with commercial actors and nations with space surveillance equipment, signing its 100th partnership in July of 2021. However, the structure of information sharing is unclear and there is a significant gap regarding how this data will actually be managed once received. Interoperability generally refers to the relative ease with which two agencies can connect their systems, personnel, and equipment, and in terms of Space Command specifically can involve other domestic defense agencies, allies' ministries of defense, or commercial actors (Leonard, 2021; National Space Council, 2020). As outlined in the 2018 National Defense Strategy, the Department of Defense has prioritized interoperability—aligning operational concepts, information sharing, training, technology and hardware, and communications—to ensure seamless coordination among and transitions between various AORs can be efficient and seamless. Beyond internal interoperability of U.S. defense agencies and capabilities, the initiative aims to ensure effective interoperations with commercial partners and allies.

Joint All-Domain Command and Control

Joint All Domain Command and Control (JADC2) is a concrete demonstration of interoperability in alignment with Department of Defense objectives. Command and Control (C2) refers to the authority with and process through which designated command authorities direct missions to realize a tactical or strategic objective. Ancillary conceptions of C2 loop in communications and computers, cyber-defense, and combat-systems, as well as intelligence, surveillance, and reconnaissance functions (C4ISR, C5ISR, and C6ISR, respectively) (Daniel, 2020). Recognizing that existing command and control systems are insufficient to provide the degree of efficiency and synchronization needed to make decisions at the rate demanded by the current operating environment, the DoD has initiated JADC2 to connect Army, Navy, Air Force, and Space Force sensors and weapons systems. The goal is to create a cloud environment such that all available information gathered within each service and other component agencies can be accessed in real time by joint force leadership.

Exogeneous Pressures from the Space Domain

Acceleration of Commercial Space Expansion

Within the past decade, the global commercial space market has demonstrated explosive growth. Over 97% of satellites launched since 2020 are registered to commercial operator/owners, a massive increase in both relative and absolute terms from the roughly 60% share of satellites launched between 2010-2020 owned and operated by firms in the private sector (Handberg, 2007). In 2020, the global space economy generated $371 billion in revenues and is projected to grow to $1 trillion by 2040.

The Remote Sensing Market

Although valued at only $2.6 billion in 2020, a mere .7% of the global space market, the commercial remote sensing equipment and services market is projected to double its revenues by 2026, as compound annual growth rates top out at nearly 10% (BryceTech, 2021). Remote sensing satellites use various active and passive sensors that employ optical, multispectral, and infrared imaging, as well as imaging and non-imaging radar technology to gather information about both Earth and other areas of space (Scott et al., 2020). Organizations and industries use satellite sensing technology to monitor climate patterns such as deforestation, inform natural disaster warning systems, survey urban and rural land use, map soil types and crop conditions to support agriculture, optimize the placement of telecom infrastructure, or locate mineral deposits in the Earth's crust, among myriad other uses (GISGeography, 2014). Although used for expressly commercial or civil purposes, these systems rely on the same equipment and data that facilitates military intelligence, surveillance, and reconnaissance (ISR) operations. This rapid proliferation of dual use sensing technology and data has been the driving force for the redefining of defense surveillance programs (Handberg, 2007). Consequently, competitive advantage with respect to space is no longer a function of simply having access to satellite remote sensing equipment, it now depends on the speed, accuracy, and nuance with which insights can be gathered and applied in augmenting or revising existing aspects of domain awareness.

Within the remote sensing segment, there is a relatively small, but growing, sector that focuses specifically on space surveillance equipment and services. This market has been dominated by customers in the public sector: 80% of the $24 million in global Space Situational Awareness market value in 2019 was generated by government clients (Commercial Space Surveillance and Tracking, 2020). This market value is projected to quintuple by 2035 to over $125 million and see sizeable expansion in its private sector customer base (Commercial Space Surveillance and Tracking, 2020). While the SSA market is the segment that aligns most closely with military surveillance, the remote sensing market as a whole is significant in terms of the paradigm shift it has brought about in the availability of surveillance data. Further, the SSA sector has and will continue to provide readily available avenues for commercial integration important to the daily functioning of USSPACECOM.

Development of the Dual-Use Paradigm

The expectation guiding the development of the space program at its inception was that it will exist under the oversight and guidance of the military. Space science began as an ecosystem to support defense efforts in space, and early commercial technological initiatives arose in partnerships with the Department of Defense (Handberg, 2007). Under this paradigm, space surveillance has been a function lead by the U.S. military, beginning in the 1950s as a Cold War missile warning and satellite monitoring system. The DoD developed its early monitoring capacities into its modern Space Surveillance Network (SSN), integrating the space-related agencies that have formed within the DoD since the beginning of the military space age (Weeden, 2019). Under the direction of SPD-3, official responsibility for SSA and STM have been relocated to the Department of Commerce, in large part due to the growing predominance of the space private sector.

The civil and commercial utility of Earth- and space-sensing technology, coupled with the diffusion of ownership of sensing data and hardware across all sectors introduces additional complexity into the dual-use debate. Roger Handberg explains the implications of dual-use remote sensing for national security (Handberg, 2007):

> "Over time, the global spread of space technologies has eliminated U.S. capacity to determine to whom and for what uses the technologies will be available. That raises some interesting implications for the broader question of U.S. security policy. As a general policy concept, dual use embodies several implications, the most significant of which is keeping the United States secure from its enemies by denying them improved militarily useful technology. What has slipped out of U.S. hands is the ability to control dissemination due to the multiplicity of players."

The dual-use paradigm and the genesis of new space activities are concurrent phenomena--on the whole, commercial space has taken on a life of its own. In the traditional space environment, the need for the investments that came with public-private partnerships offered the U.S. Government natural avenues for leverage over the private sector. As the "new space" market begins to diverge from the traditional defense primes, there are currents among policy experts that ask whether public sector agencies will even maintain relevance in guiding the development of the space domain (Lal, 2018). While a complete sidelining of federal influence is unlikely, as the scope and pace of the space private sector's expansion picks up, the reasons for and means by which the DoD connects to this increasingly multifaceted commercial sector are in flux.

Endogenous Pressures from within United States Government

The opportunities and challenges arising from the shifting realities of the space domain itself evolve alongside simultaneous pressures from within the Department of Defense, and the federal government at large. Scoping the analysis of this project requires situating USSPACECOM within the network of these interrelated dynamics. This section identifies the role of USG stakeholders outside of the Department of Defense, as well as relevant institutional trends within the DoD that inform and direct USSPACECOM's position.

Remote Sensing Regulatory Trends

The Department of Commerce and Congress are the other two primary federal bodies with influence in regulating the commercial remote sensing market directly, as well as how defense agencies interface with commercial technology and data providers. Various regulatory tactics have been employed to maintain oversight in the resolution of, frequency at which, and customer base for which the remote sensing industry can produce and sell images of earth and other objects in space. Currently, all U.S.-owned/operated imaging satellites must be registered by the National Oceanic and Atmospheric Administration (NOAA), a division of the Department of Commerce that approves and oversees remote sensing satellite operations (Bailey, 2020). The longstanding strategy for managing growing transparency is to limit the image quality and number of times commercial satellites are able to pass over and capture images or other information from an area—known as the revisit rate.

This regulatory strategy was successful during the early stages of remote sensing; but, as other nations have invested in indigenous remote sensing hardware and the remote sensing market has expanded to include global providers and customers, the status quo of the space domain has overtaken the efficacy of this regulatory strategy. In 2020, the Department of Commerce enacted new regulations for remote sensing providers: effectively, if the technology employed by the private firm is "capable of only producing unenhanced data substantially the same as unenhanced data available from sources not regulated by Commerce, such as foreign sources," the conditions placed on its operations are minimal (Hitchens, 2020). The intent of this change is to not handicap U.S. providers in the global market. Technologies that provide unenhanced data of quality comparable to other domestic providers, public and private, are subject to stricter regulations to protect the data derived from superior technology indigenous to the U.S. private sector.

Institutional Friction Regarding Commercial Acquisitions

Two obstacles complicate defense public-private partnerships: first, commercial innovators generally do not design their products at the level of security demanded by a national security application (Taverny, 2020; Denker 1998). Ensuring rigorous security standards is costly, especially for contractors outside of the traditional defense ecosystem, and this mismatch in incentives adds complexity to tech acquisition. Second, the defense contracting process is complex and time-consuming, which limits the pool of private sector innovators—especially those that are smaller, newer, or operate on a start-up model—that are readily disposed to partner with defense agencies (Flagg & Corrigan, 2021). The technology that is required of an innovative space data processing system—applied artificial intelligence, machine learning, and big data analytic platforms—are especially popular among those start-ups and young companies whose organizational design is often starkly oppositional to that of the DoD. While there are cells and offices that support defense innovation, these initiatives are removed from mainstream Department operations due to the complexity and rigidity of commercial defense contracting.

Another related issue is that the Department of Defense is not a monolith, and there are different perspectives towards innovation and commercial integration operating at various levels among the complex bureaucracies of the Departments (Myers, 2021). Defense institutions as a rule are risk averse, and the rate at which they process change is constrained by bureaucratic complexity. Consequently, the sourcing of critical data from vendors or the filtering of sensitive information through non-proprietary systems has given defense leaders pause. However, research in the development commercial-off-the-shelf (COTS) model for purchasing space equipment produced in the early 2000s offers a useful corollary for evaluating the viability of acquiring space surveillance services from the private sector (Baron, 2004). Baron's study analyzes of the production process, quality, cost, and timeframe of two similar satellite ground control systems—one, DELTA, produced under the tradition public-private model of private sector development of an entirely novel product under the supervision of the DoD, and the other, GAMMA, manufactured with COTS inputs. GAMMA was produced at a cost 1/40th of that of DELTA, was ready in 2 years sooner, and employed operating software requiring significantly less training (Baron, 2004).

Architects of the GAMMA program interviewed by Baron reported significant pushback from colleagues within the Department of Defense, even as the program proved highly successful in terms of the speed and cost-effectiveness of manufacture of a virtually identical product (Baron, 2004). While the concerns of leaders in the Department of Defense regarding the viability of contracting data processing services from the commercial space sector are well-founded and merit investigation, they must be tempered with the evidence from the immediate predecessor of commercial software services procurement: commercial-off-the-shelf hardware, which has quickly cemented itself as a central model of defense tech acquisition. Representing a growing movement for increasing institutional risk tolerance, a recent address by General Hyten, the Vice Chairman of the Joint Chiefs of Staff emphasized that the overly secretive, highly-risk averse culture of the DoD is counterintuitively working against the attainment of its goals (Myers, 2021). In a domain that requires the degree of agility and creativity as is demanded by space strategy, this tension among the DoD's structure, predominant culture, and strategic aims is especially stark.

Problem Consequences

As the organization responsible for effectively operationalizing its military components relative to space, USSPACECOM is in the unique position of having to absorb the competing exogeneous pressures from the space domain and the endogenous pressures from within the DoD and U.S. Government broadly.

Never a Day Without Space

Ultimately, this problem necessitates a framework for evaluating commercial offerings within the context of US Space Command's goals and strategic priorities. "Never a Day Without Space," the enunciation of Commander Dickinson's strategy, signifies the centrality that space maintains in all aspects of life on Earth and the urgency that underscores securing vital assets in space. The vision carries a dual message: the first, an observation, emphasizes the ever-growing global dependence on space assets. From GPS navigation, communication, broadband internet, and meteorology, each rely on secure, uninterrupted access to satellites as well as communication channels between those satellites and infrastructure on Earth. Should crucial satellites become damaged, or the signal between ground and orbit tech infrastructure be interrupted, there is significant potential for the ramifications—social and economic—to be widespread. The second meaning is a call to action, establishing the Command's role in securing U.S. public and private access to and assets within the space domain. Maintaining comprehensive domain awareness translates directly into the reliability of USSPACECOM's deterrence against intentional or unintentional threats to these applications that have become critical for functioning on Earth.

GEOINT Singularity: Remote sensing's implications for security

The growth of the remote sensing industry necessarily creates challenges for security agencies to define and maintain a competitive advantage. Information asymmetry—both knowing more outright and being able to know more through superior capabilities—is one of the central hallmarks driving national security strategy (Kaspar, 2001). As the pace of public and private innovation increases rapidly, analysts have described the possibility of GEOINT Singularity: the convergence of imagery, communications, and artificial intelligence technology such that the general public could access images of any point on Earth or in near-Earth orbit at any time (Koller, 2019). While this singularity is still a hypothetical in terms of democratized public availability of exquisite remote sensing data, the implications of this theory convey both the inevitability and the magnitude of this challenge. Specifically, from the perspective of a national security agency, the proliferation of ISR capabilities and data demands a rethinking of how superiority is defined. Defense officials have begun this reconceptualizing: recent strategy documents emphasize the centrality of knowledge, especially as a capacity to "outthink" adversaries (Leonard, 2021). SDA itself is a manifestation of this shift, focusing on cultivating an ability to preempt that hinges on a comprehensive understanding of domain norms and dynamics in real time.

Moreover, the ways in which this singularity has already begun to come to life in regard to the perennial challenge of massive data inflows illustrates that its impacts transcend realization of total observational singularity. Although it creates tensions, the growth of the space private sector is understood to be a good thing by leaders at USSPACECOM, as well as the defense community broadly—it fits within the overarching national priorities of promoting economic growth and prosperity (White House, 2021; Commander's Strategic Vision, 2020; Myers, 2021). Moreover, the military has a history of partnering with and leveraging technologies developed by the private sector in all domains, as evidenced by the success of companies such as IBM, Boeing, Northrop-Grumman as a few key examples. Where the problem arises is in the intricate network of tensions among issues of security and issues of prosperity in U.S. space activity. While the volume and variety of actors in space does create security strain, it also introduces significant opportunity for USSPACECOM to harness technologies and processes from the commercial sector that heighten SDA and optimize internal operations (Thompson, 2020). Even so, ISR data collection capabilities only stand to increase in quality and availability, and the private sector firms driving this proliferation cannot—nor should not—simply be regulated away. Increased investment in small sat SAR, artificial intelligence for pattern recognition an anomaly identification,

As it rounds out its third year since it was stood up as a unified combatant command, how U.S. Space Command navigates its relationship with commercial providers will set enormous precedent for its success in realizing its strategic vision in the near-to-medium term. The Command, as well as the DoD at large are in a unique moment to redesign its conception of security and its relation to the private sector, alongside the investments it makes in updating and integrating its legacy data collection and processing systems. Relatedly, the relative novelty of USSPACECOM offers it an opportunity to implement lessons learned in commercial procurement and data management from other corners of the Department of Defense (Hale et. al., 2021). The ongoing process of defining and solidifying the Command's operations create a unique window for optimization, unencumbered by particularities and institutional complexities, as are longer-standing agencies, due directly to the fact that those particularities have not yet cemented.

Defining Avenues For Solutions

The following section reviews relevant literature in commercial procurement models and navigating misalignments in security standards across public and private sector users.

Procuring versus Owning: Overarching Contract Models

Within the past two decades, spending on commercial services has occupied a growing share of the DoD's budget—increasing from $93 billion in FY02 to just under $202 billion in FY20. However, comprehensive strategy for effectively incorporating commercial service offerings within the DoD lags behind the spending trends—likely due to a combination of institutional friction, as well as the sheer variety encapsulated under the "services" umbrella. As with early adaptors of COTS capabilities, although the utility of commercial data collection and integration has begun to be embraced in pockets of the DoD, there remains a critical need for a framework that comprehensively addresses the unique requirements and tradeoffs of commercial service procurements.

To address this gap, Morin and Wilson (2020) propose a framework that evaluates acquisition models for commercial space capabilities by their proximity to weapons and relative integration within the kill chain. Acquisition models are defined along three categories: traditional contracting of a tailored product, commercial-off-the-shelf procurement, and procurement of services. Further, the report offers a spectrum from least to most tied to violence with the rule of thumb that if it's a weapon, the DoD should own it. In other words, the risks of outsourcing ownership and operations of "innocuous" capabilities, such as weather monitoring or PNT, are minimal relative to the potential benefits of procuring these assets as services from commercial providers. However, as the spectrum of capabilities moves closer to weapons, practical considerations demand adherence to a traditional model of in-house production with ancillary contractor support and sole operation by the contracting agency (Morin & Wilson, 2020).

The model proposed by Morin and Wilson is useful in offering an applications-based approach for differentiating between the tradeoffs of various acquisition models. Further, the centrality of a hybrid model of owning and procuring capabilities has become increasingly self-evident in terms of recent developments in DoD procurement. However, extrapolating their framework for data collection and analysis requires a revising of the distinctions drawn between the three acquisition models that motivate their analysis. In particular, the debate about contracting commercial ISR data services hinge upon the additional element of *who operates* the technology in question, implied but not directly addressed in the framework proposed by Morin & Wilson. Whereas Morin and Wilson treat ISR capabilities as a singular category that falls within the broader spectrum they define, the implications of the availability of ISR technology for data collection and processing unto itself demands further attention.

Likewise, especially in terms of software for analysis and integration of ISR data, the avenues for flexibility in customization, access, and oversight muddy the sharp lines Morin and Wilson draw between COTS and procurement of services. Because the connection between the vendor and customer is ongoing in -as-a-service model, the question of "who made this?" underlying the COTS mode is insufficient for evaluating tradeoffs within various models of owning and operating. A more recent framework by Harrison & Stromeyer classifies contracted products and services along three categories: government owned/government operated (GOGO), in which capabilities are custom-made for and operated by the contracting agency; commercially owned/government operated (COGO), in which capabilities are contracted from a provider and operated by a government agency, but the provider maintains ownership over the capability; commercially owned/commercially operated (COCO), in which the provider maintains oversight over both the capability and its operation (Harrison & Strohmeyer, 2022).

Ensuring alignment in security standards

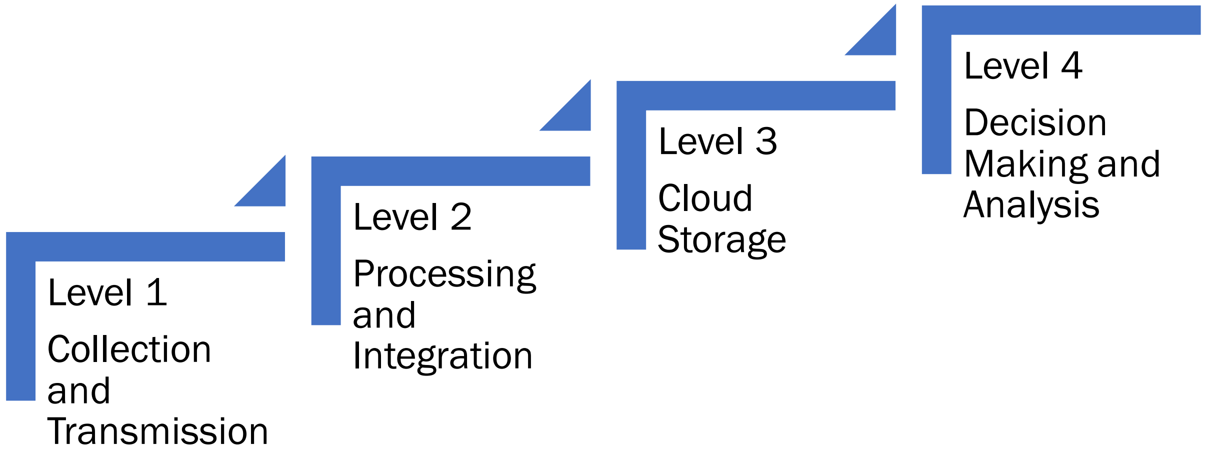
High standards for cybersecurity are increasingly a non-negotiable for defense partnerships given the centrality of cyber to defense operations, coupled with the challenges the U.S. has faced in ensuring its government and commercial networks are protected from incursions (Schradin, 2018). Notably, there have been initiatives from within the private sector to adapt to the security standards of the Department of the Defense to preempt complications associated with finding and establishing contracts with defense agencies (Vaughn, 2021). Cyber networks are the medium through which data relevant to both situational and domain awareness are transmitted, processed, and stored. Vulnerabilities in the cyber supply chain threaten both national security as it relates to space, as well as all civil and commercial uses of technology. To ensure reliability in its cyber supply chain, the DoD uses a tiered assessment, known as Cybersecurity Maturity Model Certifications (CMMCs) to evaluate its potential contractors (Padilla, 2021). Further, the DoD authorizes other commercial organizations to assess and advise other companies as they prepare to seek DoD accreditation. These firms, known as C3PAOs

(CMCC Third Party Assessment Organizations) help commercial contractors seeking to join the defense industrial base meet the standards for the CMMC assessment (Padilla, 2021).

Overview of Alternatives

Evaluating the viability of ownership versus procurement of as-a-Service offerings of technologies that support ISR data delivery, processing, integration, and decision-making is not a question that can be neatly sectioned into a conventional list of alternatives. To reconcile this ambiguity with the necessary discussion of tradeoffs, I've structured this section in terms of each level of ownership of throughput from collection of remote sensing data to its storage and application in a decision analysis program. This model reflects the argument furthered in Morin and Wilson's analysis: although delineated in a different way, the model proposed here is reflective of their argument for evaluating the need for ownership of space capabilities based on the capability itself, as well as the utility of developing a hybrid architecture of owning and procuring (Morin & Wilson, 2020; Kennedy et al., 2020). Alternatives here are structured as "levels"—relevant steps from data collection to its potential applications, as seen in Figure 1—and are discussed broadly, as specific capabilities, commercial offerings, and relevant case studies will be added during the evaluation of findings phase. The levels approach is partially referential to work by analysts at the Air Force Research Lab, describing the ontology of high-level data fusion as a series of levels outlining information management processes and requirements (Blasch et al., 2012).

Figure 1: Levels of ISR data service offerings


Level 1
Collection and Transmission
Level 2
Processing and Integration
Level 3
Cloud Storage
Level 4
Decision Making and Analysis

Level 1: Data Collection and Delivery: Data as a Service (DaaS)

The foundational level describes the collection and delivery of raw data inputs. In terms of collection, USSPACECOM has already initiated a significant effort to establish data sharing partnerships from a variety of actors—including space programs in other countries, commercial firms, and NGOs or other research organizations (Atkins, 2018). Reliability is critical at this level, as the quality of inputs into the ISR intelligence cycle determine the quality of domain awareness that can be provided.

The convergence of military and commercial satellite communication technologies offers a valuable case study in the utility of commercial infrastructure. Specifically, ongoing public-private partnerships regarding satellite communications demonstrate the effectiveness of a hybrid model of GOGO and COGO capabilities, especially in terms of the DoD's leasing of bandwidth and utilizing of network linkages from commercial satellites. A limitation on the extent to which this case matches with the considerations required in evaluating ISR data services is the distinction in how results are conceived in each use case. In other words, SATCOM focuses on throughput and crosslinks to support the outcome of stable, rapid communication (Wilcoxson, 2013; Lober, 2017). On the other hand, ISR collection services are measured on the viability of downlinks as well as the actual imagery outputs (Lal, 2018). Despite the noted constraints, ongoing partnerships with commercial satellite providers offer significant evidence for the viability of procurement of commercially owned and operated capabilities and services overall (Comparetto, 1993; Wilcoxson, 2013; Lober, 2017).

Level 2: Data Processing and Integration: Integration/Software as a Service (I/SaaS)

As the second level, processing and integration involve an additional layer of complexity in terms of either channeling raw data inputs into a useable form or combining inputs from various sources or of distinct types. The output here is information, still relatively concrete given its direct derivation from raw data inputs. Case studies and commercial vendor use cases indicate that acquiring commercial SaaS applications meet the criteria for effectiveness. Specifically, in the cases of both CANES and Vantage, the system is able to compartmentalize data and access based on user classification (Cui & Rao, 2021; Vantage Fact Sheet FINAL, 2022; Porche, 2014; Riposo & Rand Corporation, 2012). Furthermore, multi-tenancy is technically feasible in the Vantage application, therefore ensuring classification of information or systems via exclusivity is dependent upon the terms of the contract, rather than on features of the software itself (Strout, 2021).

Level 3: Data Storage Platforms: Database Management Systems (DBMS) and Platform as a Service (PaaS)

This level pertains to the storage of data and information from levels one and two. It involves additional complexity because of the sheer volume of data involved relative to processing and integration; however, data storage does not produce an informational output, which sets it apart from the other levels within the framework. Significant precedent from the Intelligence Community offers insight into opportunities and risks associated with contracting cloud infrastructure from commercial vendors.

Level 4: AI-Enabled Decision-Making Applications

Recently, security officials in both defense and intelligence agencies have turned significant attention to artificial intelligence and its potential military applications (Blackburn, 2018). In terms of space, the greatest opportunity exists in applying AI data processing capabilities to increase the rate and degree of nuance with which the continual streams of surveillance data can be synthesized (Mori, 2018). In July 2021, the 11 combatant commands convened for the third iteration of a wargame exercise headed by the Northern Command to pilot AI decision technology. This exercise successfully demonstrated the capacity for artificial intelligence to take in and synthesize data from a variety of sources across the Department of Defense in real time—highlighting the potential in automating data inputs to thoroughly inform human decisionmakers (USNORTHCOM Public Affairs, 2021). The results of this wargame align with ongoing efforts to heighten interoperability: in the immediate term, applying AI would facilitate internal integration along the many facets of the DoD. Beyond internal applications, the level of integration provides encouraging evidence for the attainability of similar partnerships with commercial partners.

Framework for Evaluation

Figure 2 offers an overview of the evaluative criteria and their definitions as they are used in this analysis. [1]

Figure 2: Summary of Criteria

Effectiveness	Exclusivity of information	Would a partnership allow classification of information or systems?
	Novelty and nuance of insights	Would this service improve the quality, complexity, or speed of analysis?
Reliability	Physical assets and software	Is the relevant network supply chain secure?
		Does the capability meet requirements?
	Accuracy of information	Can the outputs (data or information) be verified?
Feasibility	Alignment with JADC2 and interoperability objectives	Does this service comport with existing models for interoperability?

Effectiveness

Effectiveness in this case is defined in terms of the degree to which the capability supports comprehensive SDA, especially as it pertains to General Dickinson's Strategic Vision and the Five Tenets of Responsible Behavior in Space set forth by Secretary Austin. A major aspect of the depth of SDA is the automating of SSA—in other words, the degree to which policymakers and strategists within USSPACECOM can dedicate attention to the "Why?" and "How?" of developments in space, rather than gathering intel regarding "Who?", "What?", or "Where?" considerations. Effectiveness relative to SDA will be measured in terms of the speed and reliability with which the service operates as well as the extent to which commercial data and information inputs and outputs could be given exclusivity. Although definitions of effectiveness vary, each definition contains similar undertones: effective applications bring about higher quality products and minimize time to transport data (Kennedy et al., 2020). Information fusion literature defines effectiveness along three dimensions: information gain, quality, and robustness (the extent to which an application produces replicable results) (Blasch et. al, 2012).

[1] *An earlier version of this framework included cost as an individual criterion. Given that the guiding assumption (re: Harrison and Stromeyer, 2022) underlying procurement of commercial services is an expectation of cost-sharing (in terms of application sustainment costs, as well as figurative costs in the form of risks), this analysis assumes that the short-term contracting costs are less than the cost of developing a similar proprietary function within USSPACECOM.*

Reliability

Reliability refers to the relative risk involved in contracting the service: from veracity of data and analysis outputs, as well as the resilience of the capability itself. An important distinction needs to be drawn between reliability and dependence. Specifically, a primary concern in contracting commercial services is the extent to which incorporating that service would create dependence on a vendor or product the DoD cannot directly control. Reliability requires that the offering itself demonstrate clear adherence to established security standards for vendors and managers of technologies (DoD Cloud Strategy, 2020). Articulating this distinction is significant because it concretizes the need for a definitive yet broadly applicable framework for evaluating the utility of various service offerings. This clarification reflects the distinction put forward by Blasch of the AFRL between information fusion and resource management in the HLIF technology: in essence, resource management deals directly with the human element in terms of mission and application management strategy, while information fusion explicitly considers the tech itself (Blasch et. al., 2012). Further, important to note is that reliability contains within it economic costs and risks to the procurement opportunities.

Feasibility

Feasibility in this case evaluates the extent to which the the capability can be viably implemented within the confines of Space Command's mission and DoD Tenets of Responsible Behavior. Specifically, feasibility in terms of promoting interoperability by reducing (or at least not contributing to) the partitioning of various processing and integration applications—allowing the user to plug-in different streams of data inputs.

Findings

Figure 3 summarizes the use cases analyzed to motivate a recommendation based on the given alternatives.

Figure 3: Overview of Case Studies and Use Cases Used to Evaluate Alternatives

Name	Agency/Vendor	Source Type	Level
MILSATCOM public-private partnerships	DoD/Inmarsat, ViaSat	Case Study	1
Consolidated Afloat Networks and Enterprise Services (CANES)	U.S. Navy	Case Study	2
Vantage	U.S. Army	Case Study	2
Blackjack	DARPA, SDA	Case Study	1,2
USGovCloud	Intelligence Community	Case Study	3
Global Information Dominance Experiments (GIDE)	USNORTHCOM	Case Study	4
Foundry	Palantir	Commercial Offering	2
Red Wing	Maxar Technologies/US AFRL	Commercial Offering	2
Cloud Computing Security Requirements Guide	DoD	Requirements Context	3

Defense Acquisition Guidebook	DoD	Requirements Context	1-4
DoD Data Strategy	DoD	Requirements Context	1-4

Recommendation

Rather than propose one specific level of data technology on which to invest or a specific model for contracting commercial services, this analysis was designed to offer a framework for how to prioritize relevant considerations at each level. To the extent that SDA hinges on pattern recognition and overarching insight, this analysis emphasizes the utility of bringing a similar paradigm to understanding shifts and developments in the commercial ISR and software markets. In the same way that hybrid data fusion literature centers on a services-oriented architecture, U.S. Space Command must build a comprehensive architecture for its IT and data management needs. The intuition behind SOAs is the ease of integration, system agility, and minimization of dependency provided by connecting each discrete function to a larger platform integrator. In other words, rather than cultivate an ad-hoc model for procuring commercial capabilities and services, the strategy USSPACECOM articulates for its development versus outsourcing decision will act as the "integrator" (Sayler & Hoadley, 2020; *Commercial Integration Cell Fact Sheet*, 2021; Morgan et al., 2020; Slingerland & Perry, 2021).

Elements of this strategy include specifying organizational functions and goals that can be articulating acceptable versus unacceptable risks, pinpointing areas of potential dependency, and prioritizing the extent to which potential acquisitions align with established system operations. As articulated, the strategic goal of ensuring interoperability fuels competitive advantage by integrating information collection, sharing, and storage systems. Consequently, all operations and acquisitions strategies cannot be effective unless they further this priority—interoperability itself offering an abstract integrator that can then be matched with a technical component. The key to this model is its reflexivity—the technical means by which ends can be achieved can be augmented and revised, whereas an operating concept that has been conceived of piecemeal via ad-hoc development of its technical component lacks reflexivity. The massive undertakings in both the Army and the Navy to overhaul its legacy systems and connect its sensors demonstrate the challenges of implementing an OPCON after the fact. Overcoming the noise in endogenous and exogeneous domain pressures is a function of clearly and explicitly defining competitive advantage and Command requirements (Lal et al., 2018; National Space Council, 2020).

Level-Specific Recommendations:

In order to appropriately manage the complexity at hand, the recommendation identifies the non-negotiable criterion for each level. In other words, this is the "do not pass GO point"—if this condition is not satisfied, the investment at hand is moot. Rather than offer an outright ranking of each criteria in terms of priority, this approach imposes metrics for potential commercial service acquisitions while allowing for flex in defining criteria in a way relevant to each level.

Level 1: Given reliability in terms of the veracity of data inputs, would procurement offer exclusivity or classification of data or improve insight?

Level 2: Given effectiveness in terms of improved insight, is this application secure and interoperable?

Level 3: Given reliability in terms of platform security, is the cloud platform interoperable among various users or applications?

Level 4: Given reliability in terms of veracity of output and platform security, does this application improve insight?

Conclusion

The diffusion of technology with dual purpose applications in military intelligence, sensing, and reconnaissance throughout the commercial sector has created a unique network of domain realities that place U.S. Space Command's aims to build a network of resilient capabilities that with the agility that is required of the rate at which space activity is growing. Historically, the Department of Defense has been the catalyst for technological innovation, mediating commercial-side involvement through calls for proposals, funding contracts, and ongoing partnerships. Now, as the commercial sector is increasingly the force through which the space domain will be defined and mediated, the institutional design and organizational thought with regard to risk and experimentation within the DoD reflects a state of affairs that does not exist as it once did. Recently re-established and with leadership that seeks out innovative solutions, the Command is uniquely disposed to address these challenges by informing its conceptions of advantage and security with these internal and external facets in mind. Further, the ability for USSPACECOM to actionably define and realize its strategic aims are directly tied to its ability to articulate a clear, comprehensive strategy for commercial technology integration.

I. References

Atkins, S. (2018). Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace. *Air & Space Power Journal*, 26–44.

Bailey, B. (2020). *Establishing Space Cybersecurity Policy, Standards, And Risk Management PracticeS* (p. 15). Aerospace Corporation. https://aerospace.org/sites/default/files/2020-10/Bailey%20SPD5_20201010%20V2_formatted.pdf

Baron, S. J. F. (2004). Keeping Pace: Organizational Barriers To Commercial Product Use In Dod. *Journal of Public Procurement*, *4*(2), 182–209.

Blackburn, R. A. (2018). *Summary of the 2018 Department of Defense Artificial Intelligence Strategy* (p. 17). https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI- STRATEGY.PDF

Blank, S. (2018, February 12). *The National Defense Strategy: A Compelling Call for Defense Innovation—War on the Rocks*. https://warontherocks.com/2018/02/national-defense-strategy-compelling-call-defense-innovation/

Blasch, E. P., Lambert, D. A., Valin, P., Kokar, M. M., Llinas, J., Das, S., Chong, C., & Shahbazian, E. (2012). High Level Information Fusion (HLIF): Survey of models, issues, and grand challenges. IEEE Aerospace and Electronic Systems Magazine, 27(9), 4–20. https://doi.org/10.1109/MAES.2012.6366088

Blasch, E., Pugh, M., Sheaff, C., Raquepas, J., & Rocci, P. (2017). Big data for space situation awareness (K. D. Pham & G. Chen, Eds.; p. 1019607). https://doi.org/10.1117/12.2264684

Blasch, E., Shen, D., Jia, B., Wang, Z., Chen, G., Chen, Y., & Pham, K. (2019). Autonomy in use for space situation awareness. In K. D. Pham & G. Chen (Eds.), Sensors and Systems for Space Applications XII (p. 7). SPIE. https://doi.org/10.1117/12.2519212

BryceTech. (2021). *State of the Satellite Industry Report*. Satellite Industry Association. https://brycetech.com/reports/report-documents/SIA_SSIR_2021.pdf

Commander’s Strategic Vision. (2020). https://www.spacecom.mil/Mission/Commanders-Strategic-Vision/

Commercial Space Surveillance and Tracking (Future Markets Research: Commercial Space Surveillance and Tracking Final Report). (2020). UK Space Agency. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/917912/Euroconsult_-_Commercial_SST_Market_-_for_publication.pdf

Commercial Integration Cell Fact Sheet. (2021). https://www.vandenberg.spaceforce.mil/Portals/18/documents/CFSCC/CIC-FactSheet-Feb21.pdf?ver=ch0p0vC3F2c1CUBVlT9E7A%3D%3D

Comparetto, G. (1993). On the Use of Intelsat and Inmarsat to Support DoD Communications Requirements. *Proceedings of MILCOM ’93 - IEEE Military Communications Conference*, *1*, 6–13 vol.1. https://doi.org/10.1109/MILCOM.1993.408555

Department of Defense. (2021, July 7). *Tenets of responsible behavior in space* [Memorandum]. https://media.defense.gov/2021/Jul/23/2002809598/-1/-1/0/TENETS-OF-RESPONSIBLE- BEHAVIOR-IN-SPACE.PDF___

Cui, J., & Rao, S. (2021). US Army Big Data Military Applications and Reflections. *2021 3rd International Conference on Big-Data Service and Intelligent Computation*, 92–96. https://doi.org/10.1145/3502300.3502312

Denker, S. T. (n.d.). *“TRUST ME—I’LL DELIVER” :ACQUISITION APPROACHES TO GUARANTEE COMMERCIAL COMPANIES DELIVER CRITICAL SPACE PRODUCTS IN TIME OF CRISIS*. 71.

Drezner, J., Schmid, J., Grana, J., McKernan, M., & Ashby, M. (2020). *Benchmarking Data Use and Analytics in Large, Complex Private-Sector Organizations: Implications for Department of Defense Acquisition*. RAND Corporation. https://doi.org/10.7249/RRA225-1

Erwin, S. (2019, November 14). *Air Force: SSA is no more; it’s ’Space Domain Awareness’*. SpaceNews. https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/

Flagg, M., & Corrigan. (2021, July). Ending Innovation Tourism. *Center for Security and Emerging Technology*. https://cset.georgetown.edu/publication/ending- innovation-ourism/

Giannetti, W. (2021). Cloud Conundrum. *Air & Space Power Journal*, *35*, 33–40.

GISGeography. (2014, October 22). *100 Earth Shattering Remote Sensing Applications & Uses*. GIS Geography. https://gisgeography.com/remote-sensing-applications/

Global Counterspace Capabilities: An Open-Source Assessment. (2019). Secure World Foundation. https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf

Hale, L., Last, J. C., De Namur-Paul, J. L., & Barber, R. (August 2021). *Partnering Not Bossing: Better Leveraging International Capabilities for Space Domain Awareness*. Aerospace Corporation. Retrieved October 15, 2021, from https://aerospace.org/paper/partnering-not-bossing-better-leveraging-international-capabilities-space-domain-awareness

Handberg, R. (2007). Dual-Use as Unintended Policy Driver: The American Bubble. In S. Dick & R. Launius (Eds.), *Societal Impact of Spaceflight* (pp. 353–368). NASA. sp4801-chapter18.pdf

Harrison, T., & Strohmeyer, M. (2022). *Commercial Space Remote Sensing and Its Role in National Security*. Center for Strategic & International Studies.https://www.csis.org/analysis/commercial-space-remote-sensing-and- its-role-national-security

Harding. (2021). *From Data to Insight: Making Sense out of Data Collected in the Gray Zone*. Retrieved February 16, 2022, from https://www.csis.org/analysis/data-insight-making-sense-out-data-collected- gray-zone

Hitchens, T. (2021, July 13). HAC Excoriates DoD Failure To Reform Space Acquisition. *Breaking Defense*. https://breakingdefense.sites.breakingmedia.com/2021/07/hac-excoriates-dod-failure-to-reform-space-acquisition/

Hoehn, J. R. (2021). *Joint All-Domain Command and Control: Background and Issues for Congress* (No. R46725; p. 25). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R46725/2

Kaspar, Beth M. (2001). *The End of Secrecy? Military Competitiveness in the Age of Transparency*. Occasional Papers. Center for Strategy and Technology: Air War College. https://sgp.fas.org/eprint/kaspar.pdf.

Kennedy, S. O., Dunn, A., Cleveland, D., & Aerospace, O. (2020). *Enabling Hybrid Architectures and Mesh Network Topologies to Support the Global Multi-Domain Community*. 15. https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4708&context=smallsat

Kirby, J. (2020). *The Space Review: From SSA to space recon: Setting the conditions to prevail in astrodynamic combat*. https://www.thespacereview.com/article/4013/1

Lal, B., Balakrishnan, A., Caldwell, B. M., Buenconsejo, R. S., & Carioscia, S. A. (2018). *Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM)* (D-9074; p. 153). Institute for Defense Analysis. https://www.ida.org/-/media/feature/publications/g/gl/global-trends-in-space- situational-awareness-ssa-and-space-traffic-management-stm/d-9074.ashx

Lober, R. (2017, February 14). *Commentary | How DoD can harness commercial SATCOM's rapidly changing technology*. SpaceNews. https://spacenews.com/commentary-how-dod-can-harness-commercial-satcoms-rapidly-changing-technology/

Maurer, T., & Hinck, G. (August 2020). *Cloud Security: A Primer for Policymakers*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf

Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR3139-1.html

Mori, S. (2018). US Defense Innovation and Artificial Intelligence. *Asia-Pacific Review*, *25*(2), 16–44. https://doi.org/10.1080/13439006.2018.1545488

Morin, J., & Wilson, R. (2020a, November 16). *Leveraging Commercial Developments for National Security Space Acquisition | The Aerospace Corporation*. Aerospace Corporation. https://aerospace.org/paper/leveraging-commercial-developments-national-security-space-acquisition

Myers, M. (2021, October 28). *Risk aversion and secrecy are costing US its military advantage, No. 2 general says*. Military Times. https://www.militarytimes.com/news/pentagon-congress/2021/10/28/risk-aversion-and-secrecy-are-costing-us-its-military-advantage-no-2-general-says/

National Space Council. (2020). *Recommendations on Trust and Interoperability in Space Situational Awareness Data*. https://www.nasa.gov/sites/default/files/atoms/files/white_paper_on_saa_data_findings_and_recommendations_rev2020-10-22b.pdf

Niu, Y., Ying, L., Yang, J., Bao, M., & Sivaparthipan, C. B. (2021). Organizational business intelligence and decision making using big data analytics. *Information Processing & Management*, *58*(6), 102725. https://doi.org/10.1016/j.ipm.2021.102725

Odell, L. A., Farrar-Foley, B. T., Kinkel, J. R., Moorthy, R. S., & Schultz, J. A. (2012). *Beyond Enterprise Resource Planning (ERP): The Next Generation Enterprise Resource Planning Environment:* Defense Technical Information Center. https://doi.org/10.21236/ADA590682

Office of the Deputy Secretary of Defense. (2020). *DoD Data Strategy*. Department of Defense. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA- STRATEGY.PDF

Padilla, J. (2021, June 30). *Protecting Critical Information, Contracting with DoD and CMMC* (J. Gilroy, Interviewer) [Podcast]. https://www.kratosdefense.com/-/media/k/p/t/constellations-podcast-episode- 105.pdf

Porche, I. (2014). *Data_flood: Helping the Navy address the rising tide of sensor information*. RAND National Defense Research Institute. https://www.rand.org/pubs/research_reports/RR315.html.

Riposo, J. (2012). *CANES contracting strategies for full deployment* (No. 9780833060174). RAND National Defense Research Institute. https://www.rand.org/pubs/technical_reports/TR993.html.

Sayler, K. M., & Hoadley, D. S. (2020). *Artificial Intelligence and National Security*. 43.

Schradin, R. (2018, January 10). *Demystifying the CNSSP-12 with Andrew D'Uva of Providence Access Company*. SES Government Solutions. https://ses-gs.com/govsat/defense-intelligence/demystifying-cnssp-12/

Slingerland, P., & Perry, L. (2021). *A Framework for Developing Trust in Artificial Intelligence | The Aerospace Corporation*. Aerospace Corporation. https://aerospace.org/paper/framework-developing-trust-artificial-intelligence

Space-Track. (2021). Current catalog files: Low earth orbit (LEO). https://www.space-rack.org/#recent

Strout, N. (2021). *Palantir: With Joint All-Domain Command and Control, the Pentagon is finally catching up*. https://www.c4isrnet.com/industry/2021/08/12/palantir-with-joint-all-domain-command-and-control-the-pentagon-is-finally-catching-up/

Taverny, T. (2020, December). Commercial Solutions Answer Space Force's Call. *Air Force Magazine*. https://www.airforcemag.com/article/commercial-solutions-answer-space-forces-call/

Thompson, C. (2020). *Why U.S. National Security Requires a Robust, Innovative Technology Sector*. The Lexington Institute. https://www.lexingtoninstitute.org/why-u-s-national-security-requires-a-robust-innovative-technology-sector/

Tingley, B. (2021, July 30). *Joint Chiefs Seek A New Warfighting Paradigm After Devastating Losses In Classified Wargames*. The Drive. https://www.thedrive.com/the-war-zone/41712/joint-chiefs-seek-a-new-warfighting-paradigm-after-devastating-losses-in-classified-wargames

U.S. Space Command Public Affairs Office. (July 2021). USSPACECOM signs 100th commercial agreement to share space data, service. *USSPACECOM*. https://www.spacecom.mil/#/

USNORTHCOM Public Affairs. (2021, July 21). *NORAD and U.S. Northern Command lead the third Global Information Dominance Experiment (GI*. U.S. Northern Command. https://www.northcom.mil/Newsroom/News/Article/Article/2702954/norad-and-us-northern-command-lead-the-third-global-information-dominance-exper/

Vantage Fact Sheet FINAL (14 Jan 22).pdf. (n.d.). Retrieved March 22, 2022, from https://www.eis.army.mil/sites/default/files/2022-01/Vantage%20Fact%20Sheet%20FINAL%20%2814%20Jan%2022%29.pdf

Vedda, J. A. (2021). *THE FUTURE OF CIVIL AND COMMERCIAL SPACE AUTHORIZATION AND OVERSIGHT*. 12.

Wilcoxson, D. (2013). Advantages of Mobile Broadband Communications Services for Military Applications. *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 266–272. https://doi.org/10.1109/MILCOM.2013.53

Wilson, S., & Stover, C. (2020, September 17). *Defense Space Partnerships: A Strategic Priority | The Aerospace Corporation*. Aerospace Corporation. https://aerospace.org/paper/defense-space-partnerships-strategic-priority