Research Report

YOOL KIM, GEORGE NACOUZI, DWIGHT PHILLIPS, KRISTA ROMITA GROCHOLSKI, IGOR M. BRIN, BRIAN DOLAN, JONATHAN FUJIWARA, JOHN HOEHN, KOTRYNA JUKNEVICIUTE, GWEN MAZZOTTA, JORDAN WILLCOX, JONATHAN P. WONG, BARBARA BICKSLER

Operational and Policy Implications of Integrating Commercial Space Services into U.S. Department of Defense Operations

For more information on this publication, visit **www.rand.org/t/RRA2562-2**.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-1487-8

Cover: Courtesy photo by U.S. Space Force, viktoria_ngm/Adobe Stock, Lance Cpl. Tanner Lambert/U.S. Marine Corps, Bryce Bennett/U.S. Air Force.

About This Report

In the National Defense Authorization Act for Fiscal Year 2022, Congress directed a federally funded research and development center to conduct an assessment of "(1) the extent of commercial support of, and integration into, the space operations of the Armed Forces; and (2) measures to ensure that such operations, particularly operations that are mission critical, continue to be carried out in the most effective manner possible during a time of conflict."[1] In response to this direction, the Department of the Air Force asked RAND Project AIR FORCE to conduct an independent assessment, which was carried out between January 1, 2023, and September 22, 2023. This time frame provides important context for the assessment contained in this report because the space industry is rapidly evolving with continual changes to markets, companies, and their offerings—market dynamics that influence U.S. Department of Defense (DoD) decisions about the use of commercial space services.

Overall, the military services and DoD agencies rely extensively on commercial space services—although the degree of use differs depending on the mission. Without a doubt, the use of commercial space services will continue to increase in the next decade as technological advances make these services increasingly capable of supporting DoD needs and providing valuable augmentation to the department's own systems and capabilities. Implications for these increasing demands and other congressional concerns about the integration of commercial space services into military operations are explored in this report.

The research reported here was commissioned by the Assistant Secretary of the Air Force for Space Acquisition and Integration and conducted within the Resource Management Program of RAND Project AIR FORCE as part of a fiscal year 2023 project, "Assessment of Commercial Systems Integration into and Support of Armed Forces Space Operations."

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Resource Management; and Workforce, Development, and Health. The research reported here was prepared under contract FA7014-22-D-0001.

[1] Public Law 117-81, National Defense Authorization Act for Fiscal Year 2022, Section 1607, December 27, 2021.

Additional information about PAF is available on our website:
www.rand.org/paf/

This report documents work originally shared with the DAF on October 12, 2023. The draft report, dated September 2023, was reviewed by formal peer reviewers and DAF subject-matter experts.

Acknowledgments

We would like to thank the sponsor of this research, Frank Calvelli, the Assistant Secretary of the Air Force for Space Acquisition and Integration. We also thank his staff for their support throughout the research, including Lt Col Justin Spring, the action officer, for his valuable insights and feedback during the final months of the research and Erin Carper for her intellectual contributions and assistance during the initial execution of the project. Likewise, CDR James Crowe and Lt Col Landon Bastow provided us additional perspective and support throughout the research.

We thank the many subject-matter experts from the U.S. Space Force, the U.S. Space Command, the U.S. Air Force, National Reconnaissance Office, National Geospatial-Intelligence Agency, the Air Force Secretariat, the Office of the Secretary of Defense, U.S. Army, U.S. Marine Corps, and U.S. Special Operations Command, along with many others from the commercial space industry who provided valuable insights for this research. All participants spoke on a not-for-attribution basis. Although we cannot mention them by name, we are grateful for their inputs.

We thank our RAND colleagues, Gary McLeod and Krista Langeland, as formal peer reviewers who helped improve the quality of this report through their comments and suggestions. Our summer associate, Avishai Melamed, also provided useful inputs during the research process that helped inform the analysis. Lastly, we thank Stephanie Young (director) and Anna Jean Wirth (associate director) of the PAF Resource Management Program for their leadership and feedback.

Summary

Issue

The U.S. Department of Defense (DoD) relies on a wide variety of space capabilities to carry out its critical missions. Although DoD has traditionally developed and operated its own satellite systems, its use of commercial space services has increased as the industry has expanded, and it is expected that DoD's use of these services will continue to grow. Despite the benefits these commercial services can bring, DoD must consider vulnerability of these commercial space services to adversary attack when determining how much to rely on them and what missions they should support.

Growing congressional interest in this topic led to a requirement, specified in the National Defense Authorization Act for Fiscal Year 2022, for a study that assesses "(1) the extent of commercial support of, and integration into, the space operations of the Armed Forces; and (2) measures to ensure that such operations, particularly operations that are mission critical, continue to be carried out in the most effective manner possible during a time of conflict."[2]

Approach

The Assistant Secretary of the Air Force for Space Acquisition and Integration asked RAND Project AIR FORCE to conduct an independent study to fulfill the congressional requirement and to cover ten topics detailed in the Senate's legislative proposal.[3] Our key findings are organized according to these ten topics. The scope of this research was focused on how commercial space services or data derived from commercial space systems support U.S. armed forces operations. We explored six commercial space markets—satellite communications (SATCOM); space domain awareness (SDA); remote sensing; environmental monitoring; positioning, navigation, and timing; and space logistics—and focused on the first two in more depth to better address the sponsor's top priorities.

Our research synthesized information collected from a variety of sources, including relevant policy, literature, and other open-source information on the commercial space industry, and discussions with more than 70 government and industry subject-matter experts.

Key Findings

- **Current usage:** Commercial space services make considerable contributions to DoD missions. Commercial SATCOM is a significant contributor and a critical enabler to several high-value

[2] Public Law 117-81, National Defense Authorization Act for Fiscal Year 2022, December 27, 2021.

[3] U.S. Senate, National Defense Authorization Act for Fiscal Year 2022, Bill 2792, Section 1513, Study on Commercial Systems Integration into, and Support of, Armed Forces Space Operations, September 22, 2021.

missions. Although their use varies, all military services use some level of commercial SATCOM in their daily operations. For SDA, DoD relies mostly on its own capabilities to support its missions, augmented by commercial capabilities. The U.S. Space Force and U.S. Space Command are the principal DoD users and providers of SDA services considered in this report. DoD use of commercial services is limited for the remaining space missions that we considered.

- **Anticipated usage:** The degree to which DoD will use commercial services in the future will depend, in part, on how much DoD signals its intentions for future use and projected future needs. Companies will use those demand signals to decide on future investments that will potentially expand capabilities of interest to DoD, thus increasing the use of these services. Our analyses suggest that DoD is likely to increase its use of commercial services in many markets, including many emerging markets as they mature.
- **Operational impact:** It is unlikely that DoD will lose access to all commercially operated space systems because of the inherent resilience of individual company services and DoD access to multiple, independent providers. This is true for both SATCOM and commercial SDA services. Should a loss of access occur, however, the impact will depend on the criticality of the mission and any contingency plans the user has in place, with possible outcomes ranging from degradation in the ability to execute the mission to a mission abort.
- **Mitigation measures:** DoD can mitigate the operational impact of losing commercial services by diversifying its space architectures, including government, international partner, and commercial space capabilities. DoD should consider the criticality of the missions and ensure that its mission architecture can support the minimum essential functions to enable continuity of operations when commercial services are not available. Additionally, DoD can mitigate the risk of losing commercial services by, for example, performing due diligence (such as examining physical and cybersecurity considerations) of individual companies prior to awarding contracts, providing timely threat information, conducting assessments of company viability, and considering countermeasures to possible foreign influence. The department can also diversify its service providers and rely on multiple technological approaches, proliferated commercial networks, and distributed basing.
- **Resiliency:** Commercial space services, if appropriately implemented, can significantly increase the resiliency of DoD space architectures. Commercial services improve many of the resiliency characteristics of DoD space architectures, including disaggregation, distribution, diversification, and proliferation. Commercial SATCOM is one of the key elements in DoD's hybrid SATCOM architecture to increase resiliency. Although we posit that the commercial SDA services leveraged by the Joint Task Force-Space Defense Commercial Operations increase the resiliency of the SDA enterprise, it is not clear to what extent DoD plans to leverage commercial SDA as an additional capability to increase its SDA mission resiliency.
- **Interference activities:** Intentional third-party interference with commercial services that support DoD operations has been limited over the past decade—a period in which the United States did not experience direct armed conflicts with a capable adversary. But in the Ukraine war, Russia has demonstrated its will and capability to interfere with commercial SATCOM

services—a potential warning of what the United States should expect in a future conflict environment.

- **Governance:** The Outer Space Treaty regime represents the strongest set of *hard law* mechanisms that govern the behavior of commercial and government operators in space, but enforcement mechanisms are weak.[4] Moreover, the Outer Space Treaty is dated, and international governing efforts today focus on developing and propagating norms of behavior that are voluntary. Another key set of regulations promulgated by the International Telecommunications Union coordinates and assigns frequencies for the global radio network and designates orbit slots for satellites in geosynchronous earth orbit.
- **Commercial as a military target:** The consensus among policy, legal, and military experts is that a commercial satellite supporting military operations is a legitimate military target under international law. However, questions remain about what constitutes a necessary and proportional military attack against a satellite and what types of attacks might be considered a violation by the international community.
- **Awareness:** Commercial satellite operators supporting DoD are acutely aware that they face threats from U.S. adversaries and would like to have more access to threat information. There are different layers of threat warnings and notifications that range from near-real-time to longer-term general awareness to which commercial operators have various levels of access.
- **Insurance:** Most commercial satellite insurance policies exclude losses occurring from acts of war and cyberattacks, and the insurance industry views cyberattacks as a growing threat. Owners and operators of satellites that support military operations can obtain a variety of types of insurance to cover activities throughout the life cycle of a satellite. About 40 percent of satellites in geosynchronous earth orbit are insured compared with about 1 percent of satellites in low earth orbit.

Conclusions

Commercial space services offer DoD an opportunity to meet its evolving mission requirements more responsively and increase resiliency of DoD's space architectures. As the department moves in the direction of increasing its use and integration of commercial space services and data, it must navigate many operational and policy considerations. Much work remains for DoD to operationalize integration of commercial space into its space architectures—even for commercial SATCOM, an area in which DoD has the most experience working with the commercial sector. And the reality that commercial satellites may be targeted by U.S. adversaries is further complicating the matter.

The policy arena needs to evolve and mature to guide and synchronize a wide variety of activities across multiple U.S. government and DoD components so that commercial space capabilities can be effectively used to meet national security objectives and to protect the vitality of the commercial space industry.

---

[4] *Hard law* can be described as "an instrument that has a binding legal effect" that typically includes "mechanisms for interpretation, monitoring, enforcement, and dispute resolution and increases the damage or cost to state credibility for reneging or violating it" (Bruce McClintock, Katie Feistel, Douglas C. Ligor, and Kathryn O'Connor, *Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity*, RAND Corporation, PE-A887-2, April 2021, pp. 11–12).

Contents

Figures and Tables

Figures

Tables

Chapter 1

Introduction

Space capabilities, such as satellite communications (SATCOM); positioning, navigation, and timing (PNT); remote sensing; and missile warning, are essential elements to protecting national security and enhancing the civilian way of life. The U.S. Department of Defense (DoD) relies on these capabilities to carry out its critical missions and has traditionally developed and operated its own exquisite satellite systems to do so.[1] It also leverages space capabilities developed and operated by other U.S. government agencies, such as the National Oceanic and Atmospheric Administration (NOAA) and the National Reconnaissance Office (NRO).

However, the commercial space industry has expanded significantly over the past several years, offering new opportunities for DoD. Traditional commercial space markets, such as the SATCOM and remote sensing markets, are growing in capacity and diversifying with new entrants that offer differentiated capabilities. New commercial markets are also emerging in areas, such as PNT, environmental monitoring, and space domain awareness (SDA), that have traditionally been served by government agencies.[2] In some cases, the commercial space industry is developing capabilities that the government does not yet have, such as on-orbit satellite servicing to provide space logistics services, an emerging mission for DoD.[3]

To take advantage of the capacity and capabilities in the commercial space sector, DoD is shifting toward increasing its use of commercial space capabilities to integrate into the DoD infrastructure and support armed forces operations to meet mission requirements where it makes sense.[4]

As the commercial space industry continues to support DoD missions and DoD aims to increase use and integration of commercial space, there are also concerns about potential vulnerabilities that commercial space services may introduce. The space environment is becoming increasingly contested, congested, and competitive with adversaries aiming to deny, degrade, or destroy critical space capabilities that DoD relies on. Recognizing that commercial space systems have an increasingly

---

[1] Examples of DoD satellite systems include Global Positioning System (GPS) for PNT; Advanced Extremely High Frequency (AEHF), Wideband Global SATCOM (WGS), and Mobile User Objective System (MUOS) for SATCOM; Space Based Infrared System for missile warning; and Defense Meteorological Satellite Program for weather.

[2] Jonathan P. Wong, Yool Kim, Krista Langeland, George Nacouzi, Krista Romita Grocholski, Jonathan Balk, Karishma V. Patel, and Barbara Bicksler, *Leveraging Commercial Space Services: Opportunities and Risks for the Department of the Air Force*, RAND Corporation, RR-A1724-1, 2023.

[3] For additional information on these and other commercial space markets, see Emmi Yonekura, Brian Dolan, Moon Kim, Krista Romita Grocholski, Raza Khan, and Yool Kim, *Commercial Space Capabilities and Market Overview: The Relationship Between Commercial Space Developments and the U.S. Department of Defense,* RAND Corporation, RR-A578-2, 2022.

[4] NOAA and NRO are also increasing their use of commercial space services to support their missions. Chapter 5 contains more details on their use of these services.

important role in supporting military missions, there are growing concerns about commercial space systems being targeted by U.S. adversaries.[5]

In light of the growth of the commercial space industry and the increasing benefits it may offer to meet DoD's mission requirements and enhance DoD's space capabilities, the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022 directed the Assistant Secretary of the Air Force for Space Acquisition and Integration (SAF/SQ) to determine whether "existing or planned commercially available capabilities could meet all or a portion of the requirements for [a] proposed program [of record]."[6] At the same time, the NDAA prohibits DoD from relying "solely on the use of commercial satellite services and associated systems to carry out operational requirements, including command and control (C2) requirements, targeting requirements, or other requirements that are necessary to execute strategic and tactical operations" unless DoD has mitigation measures in place to account for such vulnerabilities.[7]

In the context of this congressional direction, the NDAA further directed a study that assesses "(1) the extent of commercial support of, and integration into, the space operations of the Armed Forces; and (2) measures to ensure that such operations, particularly operations that are mission critical, continue to be carried out in the most effective manner possible during a time of conflict."[8]

Research Objective and Scope

SAF/SQ tasked RAND Project AIR FORCE to conduct an independent study to fulfill this congressional requirement and, more specifically, to address ten topics detailed in the Senate's legislative proposal. We grouped these ten topics into operational and policy topics (see Table 1.1) to document our findings.

According to literature and discussions with various stakeholders, we observed that the definition of commercial space may differ depending on the context. For this research, we adopt the definition offered in the U.S. National Space Policy:[9]

> The term "commercial," for the purposes of this policy, refers to goods, services, or activities provided by private sector enterprises that bear a reasonable portion of the investment risk and responsibility for the activity, operate in accordance with typical market-based incentives for controlling cost and optimizing return on investment, and have the legal capacity to offer those goods or services to existing or potential non-governmental customers.

[5] See Chapter 7 for further discussion on commercial satellite systems being targeted.

[6] Public Law (Pub. L.) 117-81, National Defense Authorization Act for Fiscal Year 2022, December 27, 2021, Section 1607(a).

[7] Pub. L. 117-81, 2021, Section 1607(b).

[8] Pub. L. 117-81, 2021, Section 1607(d).

[9] Office of the President, *National Space Policy of the United States of America*, December 9, 2020, p. 20.

Table 1.1. Congressional Topics Addressed in This Assessment

Operational Topic	Current usage	The extent to which DoD uses commercial satellites to support armed forces operations
	Anticipated usage	The anticipated increase in such use during the subsequent 10-year period
	Operational impact	In the event that the armed forces lose access to commercially operated space systems and data provided by such systems, the impact on armed forces operations
	Mitigation measures	Steps the department might take to mitigate the risk of loss of such access
	Resiliency	As the department develops plans to increase the resiliency of its space architectures, the anticipated role of commercial systems in such plans
	Interference activities	The frequency with which third parties have interfered with commercially operated satellites that support armed forces operations during the past decade
Policy Topic	Governance	The international agreements and organizations that govern the manner in which commercial entities operate systems in outer space
	Commercial as a military target	Whether, under current international law, a commercial satellite used to support military operations is considered a legitimate military target
	Awareness	The extent to which owners of commercial satellites are aware that such satellites may be targeted by a foreign power
	Insurance	The current insurance coverage scheme for commercial satellites that support armed forces operations.

SOURCE: Features information from U.S. Senate, National Defense Authorization Act for Fiscal Year 2022, Bill 2792, Section 1513, Study on Commercial Systems Integration into, and Support of, Armed Forces Space Operations, September 22, 2021.

DoD can leverage commercial space capabilities in numerous ways, such as buying commercial space services or data (as is), hosting DoD payloads on commercial satellites, buying commercial-off-the-shelf products (e.g., commodity satellite buses), or acquiring commercially developed technologies to be modified to meet military requirements.[10] Additionally, the commercial space industry comprises a wide variety of capabilities that can be categorized into different space mission areas or markets. Each commercial space market has unique attributes in terms of market maturity, commercial viability, and applicability to DoD missions.

Given the breadth of the types of commercial space capabilities and the ways that DoD can leverage them, we determined the scope and focus of the research in consultation with the sponsor. This research examines how commercial space services or data derived from commercial space systems support U.S. armed forces operations, which we judge to be aligned with the intent of the NDAA. We examined six commercial space markets that generally correspond to DoD's space mission areas: SATCOM, SDA, remote sensing, environmental monitoring, PNT, and space logistics—each described in subsequent chapters. Note that commercial remote sensing supports NRO's space-based

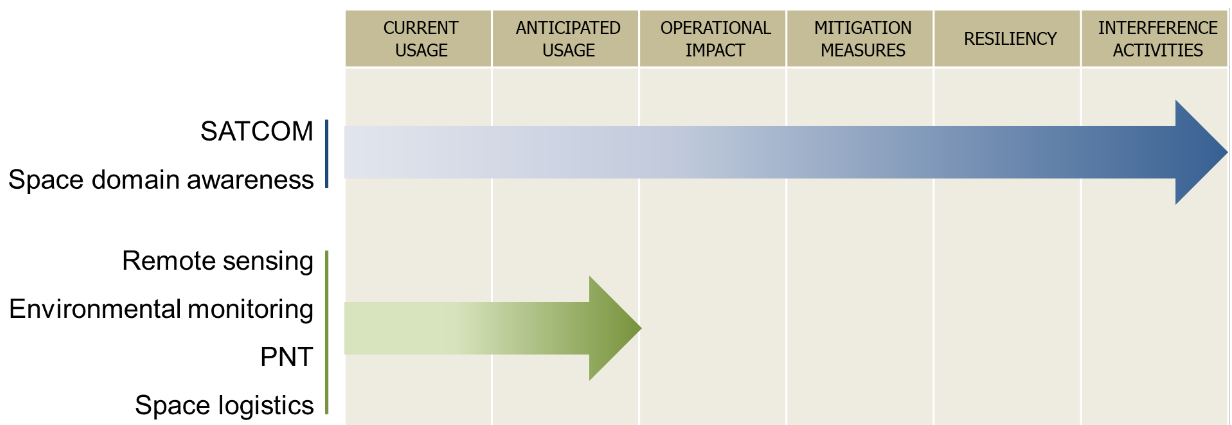
[10] In general, a commercial company is not obligated to sell its services to DoD unless the Defense Production Act is evoked.

intelligence, surveillance, and reconnaissance (ISR) mission and could potentially support DoD's tactical space-based ISR mission, which is an emerging area.

Because the NDAA focuses on commercially operated satellite systems, our research excluded launch services and ground stations as a service.[11] That said, we included SDA even though the commercial SDA providers that are currently supporting DoD do not operate satellites and, instead, use ground-based sensors. However, new SDA entrants with proposed on-orbit capabilities are emerging, and some current remote sensing companies that provide space-based ISR capabilities are also providing non-Earth imaging services in support of SDA as a secondary mission.

Our research delved into two missions that are of high interest to the Department of the Air Force—SATCOM and SDA—and, for these missions, we examined all six operational topics of interest to Congress (see Figure 1.1). For the other four mission areas, we primarily assessed current and future DoD use of commercial space services or data. Furthermore, our research scope was limited to assessing operations conducted by the U.S. Air Force (USAF), U.S. Army, U.S. Marine Corps, U.S. Navy, the USSF, and special forces in support of the joint force. We did not examine how commercial space services or data support U.S. Coast Guard operations because of the timeline and resources available for this project.

Figure 1.1. Research Scope



Research Approach

We used various research and analysis methods to address each of the topics listed in Figure 1.1. For our independent assessment of the operational topics, we collected and synthesized information from various DoD stakeholders on (1) how commercial satellite services or data are being or planned to be used or integrated to support armed forces operations, (2) characteristics of the missions that

[11] DoD relies on commercial space launch providers for all its spacelift requirements and does not own and operate organic space launch vehicles. The U.S. Space Force's (USSF's) Space Based Space Surveillance satellite uses a commercial ground station and a network of ground stations under an experimental program. It has supported telemetry, tracking, and command of DoD research and development satellites and the Navy's Mobile User Objective System satellites. For more details on the space launch and ground as a service markets and DoD's use of these services, see Yonekura et al., 2022.

commercial satellite services or data support, and (3) the role of commercial satellite services or data in future space architecture or future operating concepts. We also collected information from 18 commercial entities in the SATCOM and SDA markets about their capabilities and how they currently support DoD or might support DoD in the future to assess their contribution to enhancing DoD's space capabilities and resilience. We conducted a high-level analysis of the commercial space industry to assess the market outlook for the six space mission areas and potential demand for commercial space services in those areas.

For our assessment of policy topics, we reviewed relevant policy and literature and held discussions with government and industry subject-matter experts to elicit information on the state of the commercial space industry and the policy landscape surrounding the commercial space sector, relationships between government and commercial space industry, and commercial space industry's key concerns and challenges.

In addition to leveraging discussions with and documents provided by government and industry experts, we used such open sources as company financial reports, commercial space industry news articles, and DoD policy documents, as appropriate, to further supplement our analysis for both the operational and policy topics. We also met with more than 70 subject-matter experts from 53 U.S. government organizations, commercial space companies, and federally funded research and development centers (FFRDCs) to support our data collection and analysis.[12] A summary of these organizations follows:

- CIC members in Combined Space Operations Center (nine commercial SATCOM providers)
- Commercial SDA providers (eight companies)
- Other commercial entities (remote sensing provider, space insurance company)
- USSF (Space Systems Command, Space Operations Command, Space Warfighting Analysis Center)
- USSPACECOM (operations, intelligence, capability development, strategy, and policy communities)
- U.S. Army (SATCOM user community)
- USAF (SATCOM user community)
- U.S. Marine Corps (SATCOM user community)
- U.S. Special Operations Command (SATCOM user community)
- the General Counsel of the Department of the Air Force (legal community)
- SAF/SQ (acquisition and architecture community)
- NRO Commercial Systems Program Office (commercial space acquisition community)

[12] We identified subject-matter experts in government organizations and FFRDCs based on their functional expertise and experience in operations, capability development, acquisition, intelligence, policy, strategy, and international law as they relate to DoD's use of commercial space. We met with commercial providers for the two missions for which we conducted an in-depth analysis. We selected major commercial SATCOM companies that are providing services to DoD as determined by their membership in the Commercial Integration Cell (CIC). We met with all SDA companies that are providing services to U.S. Space Command (USSPACECOM) and a few emerging SDA providers that do not yet have operational capabilities. As a result, our results may not fully represent perspectives of start-up space companies or remote sensing companies on how they might support and contribute to DoD missions in the future.

- National Geospatial-Intelligence Agency (NGA) (commercial space acquisition community)
- Office of the Secretary of Defense, Space Policy
- FFRDCs.

The research in this report builds on several years of the RAND Corporation's prior research on the commercial space industry, assessing the benefits, risks, and challenges that the industry offers to DoD. Many of these research reports are cited throughout this report. The findings presented in the chapters that follow reflect a synthesis of information collected from all research sources, unless otherwise indicated.

The research team sought stakeholder interviews, including interviews with representatives from each military service, as one input among a broad range of qualitative and quantitative data inputs to inform the analysis. The team was unable to interview a representative from the U.S. Navy, so the analysis does not benefit from that perspective. Although the overall analysis benefited from expertise of stakeholders engaged, this report represents the research team's independent analysis of a broad evidence base, and it does not represent the authoritative position of any stakeholder.

Organization of the Report

Before turning to the congressional topics of interest, in Chapter 2, we provide an overview of the threat environment as context for our assessment. The remainder of our research is documented in three parts. Part I contains three chapters in which we present the results of our assessment of the six operational topics as they relate to DoD use of commercial space services. Chapter 3 and Chapter 4 present our in-depth assessments for commercial SATCOM and commercial SDA, respectively. Chapter 5 contains our assessment of DoD's current and anticipated use of commercial remote sensing, environmental monitoring, PNT, and space logistics services. In Part II of the report, we address our findings for the four policy topics. We cover the issues of governance for commercial space activities (Chapter 6), commercial space systems as military targets (Chapter 7), commercial awareness of being potential targets (Chapter 8), and insurance coverage schemes for commercial space systems (Chapter 8). In Part III, we summarize our assessments (Chapter 9). The appendix contains an overview of commercial SATCOM and SDA companies.

Chapter 2

Evolving Threat Landscape for Commercial Space Operators

As the threat environment for U.S. space-based capabilities continues to evolve and expand, it is driving changes in the role of commercial space operators in supporting DoD missions and their relationships with DoD. The evolving threat landscape is also influencing the policy discourse, factoring into discussions about governance and information-sharing with industry, among others.

Commercial space services face threats that are similar to those faced by government space systems. Commercial space services could face a higher risk of attack if an opponent perceives those systems as an easier target and the consequences for their actions less severe than attacking a government or military system because it may be perceived as less escalatory. The types of antisatellite weapons that can be used against commercial providers range from non-kinetic attacks, such as jamming and cyberattacks, to kinetic attacks, including interceptors. However, the latter form may have an insignificant direct effect against highly proliferated low earth orbit (LEO) constellations, such as SpaceX's Starlink, unless a large number of interceptors are used.[13] The various types of counterspace weapons causing reversible to nonreversible damage are shown in Figure 2.1.[14] Commercial space providers could be targeted by almost any of the weapons shown in the figure. However, a nuclear detonation in space would indiscriminately affect a large number of satellites so would likely not be used for a targeted attack against a commercial provider.

These counterspace threats can disrupt, degrade, or deny commercial space services or even destroy commercial space assets, which would be detrimental to the commercial entities' business and introduce risks to DoD missions that depend on such services or assets. Commercial space companies could also face other types of threats, such as financial or regulatory actions that U.S. adversaries could take to influence or restrict the company's operations.[15]

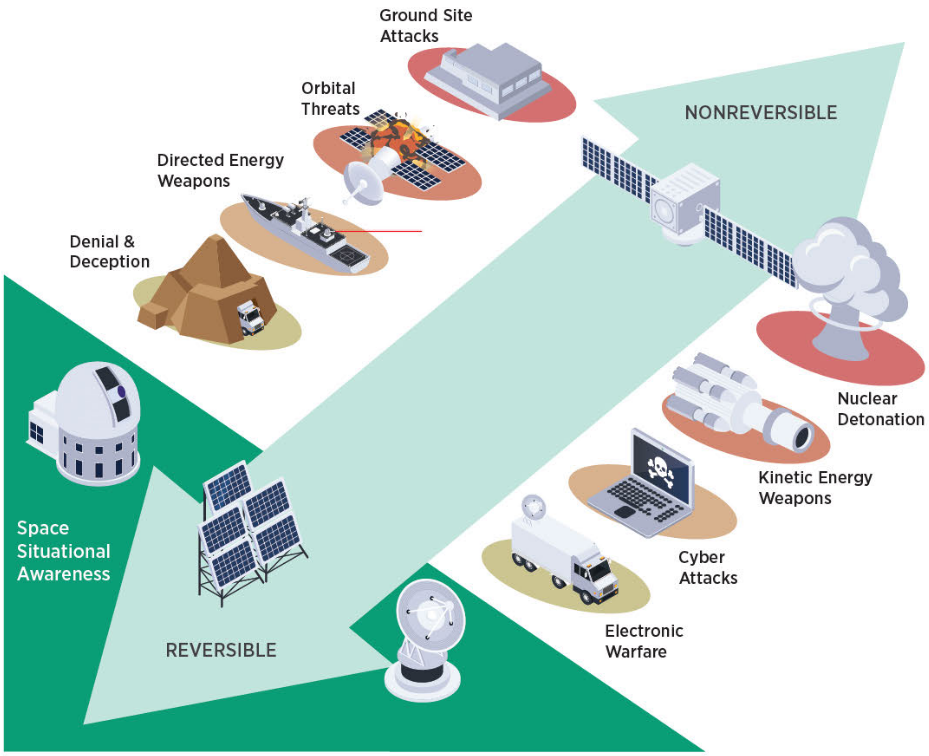
---

[13] Indirect effects, such as collision with the debris generated from an impact, can affect other satellites in nearby orbits. If sufficient debris is generated, a worst-case cascading effect (known as Kessler Syndrome) can cause a runaway chain reaction of collisions. See Heather Riley, "Micrometeoroids and Orbital Debris (MMOD)," National Aeronautics and Space Administration, June 14, 2016.

[14] Defense Intelligence Agency, *2022 Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion*, 2022.

[15] Yool Kim, George Nacouzi, Mary Lee, Brian Dolan, Krista Romita Grocholski, Emmi Yonekura, Moon Kim, Thomas Light, and Raza Khan, *Leveraging Commercial Space Capabilities to Enhance the Space Architecture of the U.S. Department of Defense*, RAND Corporation, RR-A578-1, 2022, Not available to the general public.

Figure 2.1. Counterspace Threat Continuum



SOURCE: Reproduced from Defense Intelligence Agency, 2022.

PART I. ASSESSMENT OF OPERATIONAL TOPICS

Chapter 3

Commercial SATCOM Support of and Integration into Armed Forces Operations

DoD has leveraged commercial SATCOM to augment its military SATCOM capacity for decades and continues to do so. As the military forces' demand for more capacity, resilience, and higher performance in SATCOM increases, the growing capacity, diversity, and innovations in the commercial SATCOM industry have the potential to meet many of DoD's needs.[16] To that end, DoD is moving toward increasing integration of commercial SATCOM into its future SATCOM architecture.[17]

With this anticipated increasing role of commercial SATCOM in supporting military operations, there are concerns that loss of access to commercial SATCOM (especially in times of conflict) could have a detrimental impact on DoD missions. As a result, Congress inquired about mitigation measures that should be in place to address such risks. This policy problem is embodied in the six operational topics outlined in Chapter 1 (see Table 1.1).

Current and Anticipated DoD Use of Commercial SATCOM

The USSF operates military SATCOM satellites to enable the exchange of voice, data, or video for C2 and other information exchange needs to support military forces, the President, Secretary of Defense, Joint Chiefs of Staff, and international partners. The current military SATCOM architecture comprises protected SATCOM (Milstar, its follow-on AEHF constellations, and hosted payloads that are in polar orbits as adjunct to AEHF-Interim Polar System and its follow-on Enhanced Polar System), wideband SATCOM (Defense Satellite Communications System and its follow-on WGS, hosted payload Global Broadcast Service), and narrowband SATCOM (Ultra High Frequency [UHF] Follow-On and its follow-on MUOS) to support a diverse set of missions and users with different SATCOM performance needs.[18] Protected SATCOM systems support strategic users for nuclear command, control, and communications (C3) and a limited number of tactical users who

[16] For more details on the emerging capabilities and trends in the commercial SATCOM industry, see Wong et al., 2023, and Yonekura et al., 2022.

[17] Jay Raymond, *United States Space Force Vision for Satellite Communications (SATCOM)*, January 20, 2020; Theresa Hitchens, "Space Force Wraps Initial Plan for Building 'Hybrid' Commercial/Military 'Outernet,'" *Breaking Defense*, April 26, 2023.

[18] Global Broadcast Service is a transmission-only wideband system, hosted on DoD and commercial satellites. See USSF, "Global Broadcast Service," fact sheet, October 2020.

require capabilities with high jam resistance and low probably of detection or intercept. Wideband SATCOM users are primarily those who have high capacity and high data rate needs, and narrowband SATCOM users are highly mobile users with lower capacity or data rate needs.[19]

Current DoD Use of Commercial SATCOM

Commercial SATCOM systems do not have the capabilities that protected military SATCOM systems offer (e.g., low probability of detection or intercept, survivable communications), and there is no commercial market for such military-unique capabilities. Rather, commercial SATCOM services largely support DoD's wideband and narrowband SATCOM applications. DoD users turn to commercial SATCOM for several reasons. First, because there are more DoD SATCOM capacity needs than the current military SATCOM architecture can provide, commercial SATCOM is used to augment DoD SATCOM capacity. Second, commercial SATCOM may be the only option for DoD users who do not have the priority to gain access to military SATCOM capacity for their missions or for those users operating in regions where military SATCOM is not available (e.g., polar regions). Third, our discussions with DoD stakeholders highlighted that access to military SATCOM is not always responsive or reliable, whereas procurement of commercial SATCOM can provide assured access to SATCOM when needed. Lastly, DoD users may prefer commercial SATCOM for its easier setup and use characteristics (e.g., simpler terminal setup and flexible and responsive user management and bandwidth allocations) and better performance (e.g., higher data rate) than those of current military SATCOM systems.

Commercial SATCOM supports a diverse array of DoD missions and users worldwide. These mission categories include airborne ISR; logistics; C2; special operations; morale, welfare, and recreation; and training.[20] In addition to supporting USAF, Army, Marine Corps, Navy, and Special Operations Command users, commercial SATCOM supports the Coast Guard, various combatant commands, and a host of DoD and other U.S. government agencies.[21] Although the USSF procures commercial SATCOM for all DoD users, it is not yet a user of commercial SATCOM itself.

The SATCOM industry primarily serves commercial customers, and DoD represents a small fraction of the overall SATCOM customer base. However, DoD is the largest single customer to many major SATCOM operators. Although there are more than 50 operators in the commercial SATCOM industry, the market share is concentrated in a smaller number of global operators. Major operators include Inmarsat (which merged with Viasat in 2023), Iridium, Eutelsat, SES, Viasat, and

[19] Commercial SATCOM systems that support wideband applications operate in C-, X-, Ku-, or Ka-bands. Wideband military SATCOM systems operate in X- and Ka-bands. Commercial SATCOM systems that support narrowband applications operate in L-band and S-band (upper range of the UHF band). Narrowband military SATCOM systems operate in the lower range of the UHF band.

[20] Space Systems Command, Commercial Satellite Communications Office (CSCO), *Fiscal Year 22 Commercial Satellite Communications Expenditures and Usage Report*, August 2023, Not available to the general public.

[21] The North Atlantic Treaty Organization (NATO) also procures commercial SATCOM services, and such services may support U.S. defense missions.

Intelsat, to name a few.[22] Going forward, operators of proliferated LEO (pLEO) constellations, such as SpaceX and OneWeb (which merged with Eutelsat in 2023), are likely to be part of this mix of operators that serves DoD.[23]

The mix of use between commercial and military SATCOM varies depending on a particular user community, and it is likely to change in the future as advanced commercial SATCOM systems come online with significantly higher capacity (e.g., high throughput satellites and pLEO constellations) and as DoD users exploit such capabilities for higher data rates and lower latency applications.

Anticipated DoD Use of Commercial SATCOM

The use of commercial SATCOM to support armed forces operations is likely to grow substantially, based on our review of DoD's potential demand for SATCOM in the future and the commercial SATCOM market outlook, which we discuss in this section. However, how much it will grow and at what rate remain uncertain because of many variables, such as the extent of commercial SATCOM's role in future operating concepts and DoD's implementation of its future SATCOM force design, including the modernization of the ground infrastructure (e.g., hybrid terminals, enterprise SATCOM management and control capability).

DoD's demand for wideband SATCOM capacity is expected to grow substantially in the future.[24] Many factors are driving the anticipated growth in demand for SATCOM. Various future warfighting scenarios and associated operating concepts require vast amounts of information exchange among a large number of operational elements and, increasingly, at the tactical level. DoD is also increasing use of technologies that require high bandwidth across long ranges (e.g., near-real-time video feeds from sensing platforms; capabilities enabled by cloud computing, such as artificial intelligence and machine learning, at the tactical edge). For instance, DoD's Joint All Domain Command and Control (JADC2) concept is aimed at connecting a large network of sensors to command centers and to shooters to enable the joint force to act inside an adversary's decision cycle. The USAF, Army, and Navy are all pursuing their own implementation of JADC2 as it relates to their missions and functions. Implementation of JADC2 will require rapid delivery of high-volume data, use of artificial intelligence technologies, and resilient networks. Thus, SATCOM is a key enabler of JADC2. Future concepts, such as JADC2, will drive increasing demand for high bandwidth, low latency, and jamming-resistant SATCOM capabilities.

---

[22] DoD also works with integrators who combine capabilities from multiple operators (including regional operators) to provide a commercial SATCOM solution that meets the user's specific requirements. Global operators also partner with fellow global operators or regional operators to provide a solution for a DoD customer.

[23] CSCO awarded 16 companies not-to-exceed indefinite delivery, indefinite quantity contracts in July 2023 for pLEO satellite-based services with a total cumulative value of $900 million. The contracts were awarded to pLEO constellation operators and integrators who provide satellite services in a variety of space mission areas in addition to SATCOM. The first task order in the indefinite delivery, indefinite quantity contract was awarded on September 1, 2023, to SpaceX for Starshield service, SpaceX's service for national security customers. See Sandra Erwin, "Space Force Selects Vendors for Low Earth Orbit Satellite Services," *SpaceNews*, July 25, 2023c; and Sandra Erwin, "SpaceX Providing Starlink Services to DoD Under 'Unique Terms and Conditions,'" *SpaceNews*, October 3, 2023e.

[24] Space Warfighting Analysis Center staff, discussion with authors on space data transport force design, March 27, 2023, Not available to the general public.

Many DoD user communities are planning on turning to commercial SATCOM to meet their growing SATCOM needs. Consistent with this expectation, the Space Warfighting Analysis Center's recent space data transport force design includes commercial SATCOM as one of the key elements.[25] The force design does not prescribe how much commercial SATCOM would be part of the SATCOM architecture, but it does indicate that the majority of DoD's wideband SATCOM needs could be met by commercial SATCOM capabilities, assuming an appropriate security framework is in place.[26]

The commercial SATCOM industry is well-postured to meet DoD's anticipated high demand for wideband SATCOM capacity and other capabilities, such as low-latency needs. The global SATCOM market is mature and is expected to grow steadily over the next ten years, offering a diversified portfolio of capabilities.[27] In particular, capacity in the wideband commercial SATCOM market is expected to grow significantly with introduction of geosynchronous earth orbit (GEO) high-throughput satellites and pLEO constellations in Ku- and Ka-bands. Many emerging SATCOM technologies (e.g., beam steering, nulling) and architectural approaches (pLEO, multi-orbit) will provide improved and differentiated offerings that could further add to increasing resilience against a variety of threats.[28] However, the market segment that provides narrowband SATCOM capabilities is much smaller and less diverse than the segment that provides wideband SATCOM capabilities. Thus, DoD incurs risks if there is insufficient coverage or capacity on the market that can provide legacy UHF capabilities (i.e., support legacy UHF radios).

Role of Commercial SATCOM in DoD's Plans to Increase Resiliency of Its SATCOM Architecture

The USSF's force design for space data transport is guiding SATCOM capability development decisions for DoD. The force design lays out a hybrid architecture in which military SATCOM is integrated with commercial and allied SATCOM capabilities.[29] Resilience is one of the key assessment criteria in developing a force design for space, in addition to cost and performance. The USSF's hybrid SATCOM architecture reflects many attributes of resilience as outlined in DoD's space capability resiliency taxonomy in Joint Publication 3-14: proliferation, diversification, protection, disaggregation, and distribution.[30] Commercial SATCOM primarily contributes to proliferation and diversification;

---

[25] Hitchens, 2023.

[26] Space Warfighting Analysis Center staff, discussion with authors on space data transport force design, March 27, 2023, Not available to the general public. It is unclear at this time whether commercial SATCOM will have a significant role in meeting the narrowband SATCOM needs. The narrowband analysis of alternatives was ongoing at the time of this research.

[27] Satellite Industry Association, *State of the Satellite Industry Report*, 2022.

[28] For additional details on the current and emerging capabilities that commercial SATCOM offers and the general market landscape, refer to Wong et al., 2023, and Yonekura et al., 2022.

[29] DoD has mutual military SATCOM exchange agreements with certain allies, which enables it to access capacity on these allies' miliary SATCOM systems (and for these allies to access DoD's military SATCOM systems) as a contingency plan. Switching between DoD and allied military SATCOM systems is generally easy because they operate in the same frequencies, and terminals may be interoperable.

[30] Joint Publication 3-14, *Space Operations*, Joint Chiefs of Staff, August 23, 2023.

the commercial SATCOM industry comprises a large number of operators whose constellations may span from 20 satellites in medium earth orbit (MEO) to about 50 satellites in GEO to thousands of satellites in LEO, operating in various frequency bands with different technologies.[31] Thus, the intent of the hybrid SATCOM architecture is to leverage multiple orbits, multiple frequency bands, and multiple vendors. Leveraging multiple vendors would also increase resiliency on the ground segment (e.g., proliferated gateways) via proliferation.

Ultimately, the resiliency effects envisioned in the force design would only be realized if the commercial SATCOM capabilities are integrated with military SATCOM capabilities across the doctrine, organizations, training, materiel (the equipment), leadership and education, personnel, facilities, and policy (DOTmLPF-P) dimensions. That is, there are other elements besides the space segment (i.e., satellites) that need to be implemented for SATCOM users to roam seamlessly across all the different networks and maintain connectivity through all operating conditions as if they were on a single communications network. Such an end state would require DoD to (1) modernize its SATCOM ground architecture and the terminal enterprise and (2) evolve its approach to acquisition and operational management of commercial SATCOM.

For instance, many current user terminals lack the flexibility to operate across military SATCOM and commercial SATCOM, multiple frequency bands, multiple orbits, or multiple commercial SATCOM vendors.[32] DoD's current approach to acquiring commercial SATCOM does not enable sharing of commercial SATCOM resources across the enterprise. Each user organization has its own one-on-one contract with a provider. As a result, there is no flexibility for one user organization to access capabilities that another user organization may have acquired from a different or even the same provider, unless explicitly specified in the terms of contract. Furthermore, each user organization operationally manages its own commercial SATCOM resources working with their provider. There is no single DoD operational element that has an enterprise-level situational awareness of commercial SATCOM operations, which would make it extremely difficult to manage the operations of an integrated architecture.

Multiple stakeholders are developing and investing in various enablers, such as hybrid terminals (e.g., the Army's Next Generation Tactical Terminal, the USAF's Global Lightning program), for accessing multi-orbit, multi-band, and multi-vendor capabilities and enterprise SATCOM management capabilities (USSF's SATCOM Enterprise Management and Control program) to manage the hybrid network.[33] However, synchronization and implementation of all of these efforts could take several years or longer.[34] Further work needs to be done to improve the acquisition strategy

---

[31] See the appendix for information on capabilities of major SATCOM operators. For additional insights on how commercial SATCOM capabilities can increase resilience, refer to Wong et al., 2023.

[32] For example, users may have terminals that can access both military and commercial SATCOM in GEO orbits, but only with a single vendor because of the vendor's proprietary waveform. Other users may have access to multiple commercial SATCOM vendors by acquiring multiple vendor proprietary terminals.

[33] U.S. Army, Program Executive Office Command Control Communications-Tactical, "Satellite Communications: FOT," webpage, undated; L3Harris, "L3Harris Awarded $81 Million Contract to Connect Multi-Orbit Satellite Constellations," press release, June 6, 2023; DoD Chief Information Officer, *Department of Defense Enterprise SATCOM Management and Control (ESC-MC) Implementation Plan*, October 20, 2022.

[34] For instance, integration of a hybrid terminal to a platform such as an aircraft may require adding new antennas or other modifications. Testing and certification for airworthiness (or for electromagnetic compatibility for ships) would also add many more years.

for commercial SATCOM and mature an operating concept for managing an integrated SATCOM enterprise. Although user communities generally share the vision of integrating commercial with military SATCOM, some users are skeptical of full implementation of the hybrid architecture and have expressed concerns about losing operational control of their own commercial SATCOM services under the construct of enterprise management (as is done with military SATCOM today).[35] Depending on whether these enablers of a hybrid architecture come to fruition and overcome potential cultural challenges, the role of commercial SATCOM in DoD's plans to increase resiliency of its SATCOM architecture could be delayed or diminished.

Third-Party Interference Activities with Commercial SATCOM Systems

According to our discussions with commercial SATCOM providers and DoD experts, no commercial SATCOM satellites have experienced a kinetic attack. However, electromagnetic interference is common. The assumption is that this interference is usually accidental and happens as part of normal operations, such as when satellites are being relocated. Although companies experience interference and can report it, they cannot ascribe intent or officially attribute the sources of the intentional interference.

USSPACECOM has been able to determine that some of the interference experienced in recent years by commercial companies that serve DoD customers has been intentional and that there has been a substantial increase in purposeful electromagnetic interference activities since 2020.[36] However, SATCOM operators indicated that no electromagnetic interference has been significant enough to impair commercial SATCOM operations, although the operational impact to the users may have varied.

Cyber interference and attacks are a constant for commercial SATCOM providers. These attacks are primarily aimed at the ground segment, and there has been no indication that the space segment has been interfered with via cyber means. The providers have invested significantly in increasing their cyber defenses and adopting best practices for hardening their systems and have not reported significant intrusions or impacts to their operations, with the exception of Viasat, which experienced a major cyberattack in 2022 during the Russia-Ukraine conflict.[37]

The Russian invasion of Ukraine has changed the tenor of the conversation about interference with commercial satellite systems. Russia has used both electromagnetic jamming and cyber weapons to target commercial SATCOM providers during the war.[38] Companies observed an increase in the

---

[35] Wong et al., 2023.

[36] Combined Space Operations Center/SATCOM Integrated Operations Division, "SATCOM Electromagnetic Interference (EMI), Trending Report: CY 2013-2022," undated, Not available to the general public. We reviewed the historical data on purposeful electromagnetic interference activities on commercial SATCOM systems that support armed forces operations over 2013–2022 and assessed that the increase in interference activities is most likely correlated with geopolitical environment and may not be indicative of a general trend of increasing frequency of purposeful EMI activities.

[37] Katrina Manson, "The Russian Hack Everyone Is Finally Talking About," *Bloomberg Businessweek*, March 6, 2023.

[38] Manson, 2023; Kate Duffy, "Elon Musk Says Russia Has Stepped Up Efforts to Jam SpaceX's Starlink in Ukraine," *Business Insider*, May 11, 2022.

sophistication of purposeful electromagnetic interference techniques and cyberattacks by a third party and shared with us that these attacks have been more front of mind than before.

Operational Impact of Losing Access to Commercial SATCOM and Mitigation Measures

Given the pervasiveness of commercial SATCOM in supporting armed forces operations, losing access to these services would likely have an adverse effect on the operational effectiveness of the supported missions. However, there are numerous military applications of commercial SATCOM, as discussed earlier, and the operational impacts associated with each of those applications is highly context dependent. To examine a variety of potential operational impact of losing commercial SATCOM, we examined each service's major commercial SATCOM applications that epitomize the current and future ways commercial SATCOM will be used to support their missions.[39] We selected the following applications based on the mission categories that provide direct support to combat operations and discussions with DoD user communities:[40]

- airborne ISR (USAF)
- operational C2 (USAF)
- C3, logistics, and Blue force tracking (Army)
- maritime C2 (Navy)
- multi-missions (Marine Corps)
- anti-ship fires (Marine Corps).

To assess the potential operational impact through these case studies, we examined how dependent these applications are on commercial SATCOM, how critical the mission is that is being supported, and whether there are ways to mitigate the impact of loss of service.

Airborne ISR (Air Force)

Airborne ISR is a critical joint mission supporting combatant commands by characterizing enemy forces, monitoring activities and movement, identifying and tracking potential targets, providing threat warning, and assessing battle damage, among fulfilling other information needs. It is a joint mission that potentially supports all friendly forces but is primarily fulfilled by the USAF and has long been identified as one of five USAF core missions.[41] Combatant commands have often relied on airborne ISR more than other sources of intelligence in supporting current operations because they have direct

[39] We recognize that these use cases do not comprehensively capture all military use cases of commercial SATCOM. However, these commercial SATCOM applications represent various ways that armed forces are using commercial SATCOM services in terms of dependency, criticality of supported mission, and mitigation measures in place.

[40] We discussed these topics with operational users and reviewed such documents as concepts of operations, storyboards, operational views, after action reviews, and other artifacts to supplement those discussions.

[41] USAF, *Global Vigilance, Global Reach, Global Power for America*, 2013. Other services also operate airborne ISR platforms that use commercial SATCOM (e.g., the Navy's EP-3 and MQ-4, the Army's Gray Eagle).

C2 authority. The commands are not competing for airborne ISR resources and access to the diverse capabilities on airborne ISR platforms. In some theaters, there are typically multiple airborne ISR sorties daily.

Airborne ISR is a critical and high-tempo mission that is extensively dependent on SATCOM to maintain C2 and sensor datalinks across large and often remote geographic regions. Because sensor data such as video feeds and high-resolution images require much higher communications bandwidth than many types of tactical data, airborne ISR platforms often require high data rates and make up a significant share of SATCOM use. Both crewed and remotely piloted airborne ISR platforms use commercial SATCOM extensively, and the impact of losing commercial SATCOM for the airborne ISR mission would depend on

- the importance of the airborne ISR mission to supported military missions
- whether commercial SATCOM is being used for C2 links, sensor data, or both
- the presence (or lack) of redundant communications
- whether the airborne ISR is remotely piloted (or not).

Losing commercial SATCOM on a temporary or permanent basis could have drastic effects on the level of situational awareness available to military leaders and the ability for tactical units to execute kill chains. To mitigate such consequences of losing commercial SATCOM to airborne ISR missions, DoD could consider either actions to restore communications through alternative means or alternative collectors to reduce the impact. Potential options include restoring communications to airborne ISR platforms (e.g., enhancing airborne or terrestrial relays or fielding hybrid communications systems) or using alternative collectors (e.g., space-based collectors or nontraditional ISR systems).

Operational C2 (Air Force)

Almost all USAF C2 functions regularly use commercial SATCOM to help meet their communications bandwidth needs and constitute one option within a multi-path C2 communications architecture.[42] A mix of long-haul communications (typically SATCOM and undersea cables) and short-haul communications (such as terrestrial fiber and line-of-sight datalinks) connect C2 nodes together and are used to control air operations.[43] This section focuses on operational-level C2.[44]

The USAF leads a joint air tasking cycle that compiles current and anticipatory intelligence, information on Blue forces and weapons, direction from the joint force commander, and weather predictions, among other information, to produce an air battle plan. Centralized control and decentralized execution have been part of the foundation of USAF doctrine throughout the service's

[42] USAF experts in warfighting communications and air operations center operations, discussions with authors, July 14, 2023, and August 11, 2023, Not available to the general public.

[43] Miranda Priebe, Alan J. Vick, Jacob L. Heim, and Meagan L. Smith, *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation*, RAND Corporation, RR-2959-AF, 2019.

[44] Operational-level C2 bridges the gap between tactical execution and the strategic goals of a combatant commander or higher authority. For air forces, operational-level command authority has traditionally been vested in the Joint Force Air Component Commander, who provides centralized control of joint air forces from the air operations center within their area of responsibility.

history; however, today's typical manifestation of this C2 philosophy results in highly prescriptive direction from centralized C2 nodes to tactical units, including detailed weaponeering and resource allocations—leaving little flexibility for forward commanders to plan tactical details.[45] A disruption of communications between operational-level C2 nodes and forward units would leave forward forces with greatly reduced ability to plan, execute, and assess air operations.[46]

Current Department of the Air Force practices and systems often assume reliable communications, including long-haul reachback to the continental United States via underseas cables and SATCOM.[47] Air operations centers, the primary operational-level C2 nodes for the air domain and senior C2 element of the theater air control system, have such high data capacity demands that terrestrial data paths and commercial and military SATCOM are all regularly used to meet those demands.[48] Especially for overseas locations where terrestrial fiber may not be reliable, commercial SATCOM is a well-integrated communications capability that adds data bandwidth and resiliency by contributing to disaggregated and diverse communications paths.

Losing commercial SATCOM would affect operations by reducing available bandwidth at operations planning nodes, making some centralized planning operations slower or less efficient (by forcing some C2 functions to use more burdensome or less reliable communication methods) and degrading communications resiliency. Losing commercial SATCOM alone, even permanently, will not result in a total failure to control air forces. But receiving, using, and distributing information is the core task of the C2 mission, and removing the ability to do so can be a severe blow. Nascent concepts of operations, such as Agile Combat Employment,[49] increase the need for communications between distributed tactical units and centralized C2 nodes to improve the ability for those units to continue operations through a degraded communications environment.[50]

The USAF is advancing concepts to better operate through contested and degraded communications environments to mitigate the loss of C2 communications, including commercial SATCOM. The service is considering enhancing options for alternative communications pathways (e.g., high frequency systems or use of Global Broadcast Service) but more fundamentally is going through major shifts to make the USAF better prepared for truly distributed operations and control when required (e.g., mission command; decentralized planning, control, and execution).

---

[45] Miranda Priebe, Laurinda L. Rohn, Alyssa Demus, Bruce McClintock, Derek Eaton, Sarah Harting, and Maria McCollester, *Promoting Joint Warfighting Proficiency: The Role of Doctrine in Preparing Airmen for Joint Operations*, RAND Corporation, RR-2472-AF, 2018, pp. 18–20; Air Force Doctrine Publication 1-1, *Mission Command*, U.S. Air Force, August 14, 2023.

[46] Priebe et al., 2019.

[47] Mary Lee, Brien Alkire, Jim Dimarogonas, Jeff Hagen, Christian Johnson, Moon Kim, Abbie Tingstad, Kristin Warren, and Michael Wilson, *Reliable Communications in a Contested Environment:* Vol. 1-*Policy Findings*, RAND Corporation, 2022, Not available to the general public.

[48] USAF warfighting communication subject-matter experts, discussion with the authors, July 14, 2023, Not available to the general public.

[49] *Agile Combat Employment* is an emerging USAF concept of operations focused on maneuver of air forces between operating locations "within threat timelines to increase survivability while generating combat power" against advanced threats (see Air Force Doctrine Note 1-21, *Agile Combat Employment*, U.S. Air Force, August 23, 2022, p. 1).

[50] Lee et al., 2022.

C3, Logistics, and Blue Force Tracking (Army)

The Army primarily uses a variety of military SATCOM systems, including AEHF, WGS, and MUOS, for general C3 purposes. Commercial SATCOM is a force multiplier that supplies some units with additional communications capacity. The Army has traditionally employed commercial SATCOM via a family of military-owned, general-purpose terminals that can communicate with either military or commercial satellite networks in multiple frequency bands (e.g., such as the Warfighter Information Network-Tactical [WIN-T] and Phoenix terminals).[51] These hybrid terminals provide operational flexibility by enabling communications path diversity, should access to commercial SATCOM be lost. As a result, the Army has limited dependency on commercial SATCOM for C3 and has the capacity to maintain its essential C3 operations if commercial SATCOM is lost.

Although commercial SATCOM is not essential to current overall Army C3 operations, Army commanders are aware of the limitations of military SATCOM, and consider the improved throughput, low latency, and especially the autonomy offered by commercial SATCOM's consistent availability without prior coordination to be critical to future Army operations. Depending on U.S. Army leadership decisions, the Army's dependence on commercial SATCOM could grow sharply through 2030.[52]

Unlike general C3 applications, the Army is heavily dependent on commercial SATCOM for Blue force tracking and logistics operations for transmitting critical data at longer ranges. In both cases, there are no reliable alternatives to Army use of commercial SATCOM, other than (possibly) attempts to manually communicate equivalent information over the Army's already saturated and scarce military SATCOM channels.[53]

The Army exclusively relies on commercial SATCOM in its Joint Battle Command-Platform system to aggregate and transmit PLI of Army units to higher command.[54] The Army has 100,000 L-band SATCOM transceivers, developed by Inmarsat, on various Army platforms.[55] Vehicles and aviation platforms typically transmit their PLI to their units' Network Operations Center over Viasat's (formerly Inmarsat's) L-band satellites, where these data are aggregated before being rebroadcast back to the Defense Information Systems Network via military SATCOM and then distributed globally. The final step is when broader PLI, now aggregated across DoD, is pushed back

---

[51] Phoenix terminals operate on X- and military Ka-bands to access WGS and C- and Ku-bands to access commercial SATCOM. WIN-T is also used to access WGS and Ku-band on commercial SATCOM. See Ryan Schradin, "The Role of COMSATCOM in Army Communications and the WIN-T Increment 2," *Government Satellite Report*, October 18, 2016.

[52] U.S. Army, Indo-Pacific Command personnel, discussion with authors, July 27, 2023, Not available to the general public.

[53] Another possible alternative is to arrange Army formations spatially such that line-of-sight communications platforms are sufficient to create communications paths back to higher echelons. Both the Army's position and location information (PLI) and logistics SATCOM systems have alternate line-of-sight communications systems fielded to work with the commercial SATCOM; and the Army's non-SATCOM alternative high bandwidth communications systems often have limited range. However, this posture could deeply constrain Army operations or even cause mission failure.

[54] PLI consists of geospatial coordinates of minimal message size. The Joint Battle Command-Platform is one of several discrete Army systems, consisting of computing hardware, software applications, or both, that participate in the PLI data collection, aggregation, and distribution process.

[55] Viasat, "Blue Force Tracking with Viasat L-Band Terminals," webpage, undated.

down to U.S. commanders, allowing them to maintain near-real-time information on the positions of their forces at the vehicle level.[56]

Loss of L-band commercial SATCOM for Blue force tracking would result in loss of easily representable and timely PLI, which would reduce commanders' situational awareness and adversely affect their ability to command their forces. Should Viasat's L-band satellites become inaccessible (per any threat means discussed in Chapter 2), there are limited L-band satellites in the commercial SATCOM market.[57] To mitigate the operational impact, combat units could use tactical communications equipment to manually aggregate unit PLI and send it via radio-net and military SATCOM channels. Sending the PLI over military SATCOM, however, could introduce other challenges given that military SATCOM bandwidth and terminals are already oversubscribed. This could jeopardize the success of some unit missions.

Commercial SATCOM is also the most common means by which logistics personnel report maintenance, supply, and readiness information from military units to enterprise data distribution and tracking systems. Army units deployed to locations distant from a home installation require ongoing resupply and the performance of regular vehicular and equipment maintenance to maintain combat effectiveness. The average brigade combat team's unit supply consumption and transport capabilities, as designed, allow the team to operate for about three days of combat before requiring resupply.[58] In current operations, logistics units very frequently pass data on their requirements, activities, and the equipment and supply consumption of their parent units to the central servers of the Global Command and Control System-Army (GCCS-A)—the Army's strategic, theater, and tactical C3 system, in the continental United States.[59] These data exchanges are enabled by Combat Service Support Very Small Aperture Terminal (CSS VSAT) SATCOM terminals, owned and operated almost exclusively by logistics units, to access a network of Ku-band commercial SATCOM satellites.

Loss of commercial SATCOM would limit the logistics units' ability to share supply, maintenance, and transportation resource information and would likely inflict critical disruption on Army logistics operations depending on the nature of disruption in commercial SATCOM services. If commercial SATCOM services were disrupted because of electromagnetic interference activities on one of the satellites handling CSS-VSAT traffic, logistics operations would unlikely be critically disrupted, unless adversaries were successful in recognizing and responding to mitigation measures that operators and specialists would take in response to this interference.[60] In the event of loss of access to all commercial SATCOM satellites, logistics personnel would be forced to return to

---

[56] K. R. Chevli, P. Y. Kim, A. A. Kagel, D. W. Moy, R. S. Pattay, R. A. Nichols, and A. D. Goldfinger, "Blue Force Tracking Network Modeling and Simulation," *MILCOM 2006: 2006 IEEE Military Communications Conference*, 2006.

[57] From authors' analysis based on a systematic, global review of commercial SATCOM satellite specifications performed during production of unpublished research on employing commercial satellites to help improve military SATCOM by Timothy Bonds, Scott Grossman, Jordan Willcox, James Bonomo, Daniel Gonzales, and Frank Camm.

[58] Matthew Cox, "Future Army Brigades Will Fight for a Week Without Resupply, General Says," Military.com, November 6, 2018. Three days serve as a planning factor and operational requirement for unit design rather than a reliable outcome. Unit supply consumption will vary according to circumstances, while supply storage and transportation capacity is of limited flexibility.

[59] All of the following are documented in GCCS-A: each instance of a supply unit's transfer of ammunition or consumables to a combat unit; each request for a spare part or resupply from warehouses; and each act of vehicle maintenance, the assignment of trucks or transport to distribute supplies, the approvals of equipment transfer or maintenance requests, and medical and aviation resupply.

[60] U.S. Army acquisition source, discussion with authors, August 10, 2023, Not available to the general public.

manually telecommunicated requests for supplies and maintenance work approval. Unit supply and maintenance personnel face significant time and availability constraints in current operations, and the need for manual communications and tracking of each supply and maintenance operation would both delay resupply and maintenance, degrading combat effectiveness of the force.[61] The future development of a disconnected mode for GCCS-A operators will mitigate but not eliminate this risk.

Maritime C2 (Navy)

The nature of afloat maritime operations requires the use of SATCOM for nearly all beyond line-of-sight communications. The other method available to Navy ships for beyond line-of-sight communications is high frequency radio communications, which is not optimal or sufficient to support the volume of Internet Protocol–based communications required by afloat units. To understand the Navy's use of SATCOM while afloat, we looked at the communications capabilities and C2 requirements for a carrier strike group.

A carrier strike group generally consists of an aircraft carrier, several destroyers, a cruiser, and an air wing. The commander and the commander's staff are the central point of C2 for the carrier strike group and are located onboard the aircraft carrier. This command element needs to be able to communicate with higher headquarters often located at ashore bases or afloat command ships in the case of the 6th and 7th Fleets. The command element also needs to be able to communicate with subordinate forces that are collocated on the aircraft carrier or dispersed across the accompanying ships. In addition, there is a need to communicate with other joint services, other Navy operational forces, and partner nations.

The aircraft carrier, destroyers, and cruiser utilize protected, wideband, and narrowband military SATCOM and commercial wideband SATCOM provided by the Commercial Broadband Satellite Program.[62] The services from this program provide a significant amount of bandwidth to the carrier strike group that enables access to the Non-classified Internet Protocol Router (NIPR); Secret Internet Protocol Router (SIPR); secure telephones; video teleconferencing; telemedicine; intelligence database and imagery; and morale, welfare, and recreation. The air wing utilizes the network and SATCOM provided by the aircraft carrier while not airborne and only on narrowband military SATCOM—specifically, MUOS while airborne.[63]

---

[61] For a similar conclusion and summary of the value of the CSS VSAT and GCCS-A on Army operations, see Diana Maurer, *Defense Logistics: Army Should Ensure New System Operates in All Situations and Soldiers Complete Training*, U.S. Government Accountability Office, GAO-21-313, April 2021.

[62] The Commercial Broadband Satellite Program contract was awarded to Inmarsat (now Viasat) in 2022. Under this contract, Viasat provides managed SATCOM services worldwide to crewed and uncrewed maritime, airborne, and ground platforms operating in C, X, Ku, and Ka frequency bands. Viasat is providing this service as an integrator using its own satellite fleet and capabilities from other operators. See Inmarsat, "U.S. Navy Commercial Broadband Satellite Program Services Contract Worth up to $980m Awarded to Inmarsat Government," October 11, 2022. There is a growing interest among DoD users to leverage such managed services as the Commercial Broadband Satellite Program contract to shift the burden of integration and network management to the commercial provider. Using managed services or an integrator could address some of the DOTmLPF-P challenges discussed earlier in the chapter, but further analysis would be needed to understand the feasibility as it applies to a hybrid architecture.

[63] When the air wing is airborne and in line of sight, there are several datalinks, including Link-16 and Cooperative Engagement Capability, and secure UHF and very high frequency voice communications used to communicate with the rest of the carrier strike group.

Commercial SATCOM is primarily used to augment bandwidth and is not a single source communications path.[64] Although the carrier strike group will utilize all available bandwidth during non-conflict operations, the Navy has recognized the possibility that commercial SATCOM may not be available in contested operations during conflict. Because of this expectation, tactics, techniques, and procedures (TTP) have been developed to prioritize critical bandwidth needs and to enable operation on military SATCOM alone. Part of these tactics, TTP addresses utilization of the limited bandwidth for prioritized data and prioritized personnel. Often the prioritized personnel are not leaders or decisionmakers but the sailors who are responsible for staffing the carrier strike group operations.

Another aspect that enables the Navy to operate in a contested environment is the ability to operate on mission type orders. The nature of maritime operations better enables the use of mission type orders because of the distributed C2 structure of a Navy fleet. There is also less need for bandwidth within the carrier strike group due to the geographically consolidated nature of the composite warfare commander structure, which allows the carrier strike group commands and units to physically communicate or use low bandwidth line-of-sight communications (radio frequency, sending printed documents via helicopter, or semaphore). These TTP enable the carrier strike group to continue critical operations if access to commercial SATCOM may be lost.

Multi-Missions (Marine Corps)

The Marine Corps is undergoing significant organizational changes that will have implications for how it uses commercial SATCOM. Although it uses commercial SATCOM for a variety of applications today, it is more useful to examine its new commercial SATCOM initiatives in support of its Force Design 2030 organizational changes.[65] These changes provide insight into the future demand for commercial SATCOM not only in the Marine Corps but also across the other services pursuing similar efforts.

Force Design 2030 is a broad effort to address adversary adaptations to U.S. operational strengths demonstrated over the past 30 years.[66] One prominent feature of this initiative is Expeditionary Advanced Base Operations, which calls for disaggregated units to provide sensing, fires, and forward arming and refueling nodes in support of Navy surface and subsurface operations.[67] This concept results in higher demand for connectivity to compensate for the dilution of combat power because of units being disaggregated across the battlefield.[68] Our analysis of the Expeditionary Advanced Base Operations concept suggests that these expeditionary advanced bases will be small (most will be

---

[64] The Navy utilizes Consolidated Afloat Network and Enterprise Service as the program of record for afloat NIPR, SIRP, and SCI networks. The Consolidated Afloat Network and Enterprise Service connects to Automated Digital Network System, which automatically determines how to best utilize the available SATCOM to transport data on and off the ship. Because the Automated Digital Network System can automatically adjust the transport of dataflow between military and commercial SATCOM, there is a near-seamless transition between the two.

[65] Space Systems Command, CSCO, 2023, p. 41.

[66] U.S. Marine Corps, *Force Design 2030 Annual Update*, June 2023, p. 1.

[67] U.S. Marine Corps, *Tentative Manual for Expeditionary Advanced Base Operations*, 2nd ed., May 2023.

[68] I Marine Expeditionary Force, discussions with authors, June 26, 2023.

platoon-sized or smaller) and dispersed beyond their ability to provide mutual support to each other and that they will need more communications capabilities than would usually be the case for small units. The distances between expeditionary advanced bases necessitate either high frequency or SATCOM; because of the volume of data that these bases intend to pass through, SATCOM is the only viable choice.[69]

The Marine Corps anticipates that it will be largely dependent on commercial SATCOM and plans to integrate more commercial SATCOM into almost every mission that requires communications.[70] These missions range from enabling C2 using Command and Control Personal Computer, controlling fires using the Advanced Field Artillery Tactical Data System (AFATDS), and more.[71] Because of the diversity of missions and supporting applications, we judge that commercial SATCOM generally will be critical for enabling Marine Corps operations.

This dependency requires the Marine Corps to consider the possibility of commercial SATCOM being disrupted or lost. The Marine Corps has taken two approaches to mitigating the impact of such an outcome. The first is a robust communications architecture achieved through a diversity of commercial providers, frequency bands, and orbits to ensure some level of service during operations (see Table 3.1).[72]

Table 3.1. U.S. Marine Corps PACE Plan

Plan Element	Contributors	Band
Primary	Fiber	N/A
	Transponded military	Ka
	Commercial GEO very high throughput satellite	Ka
	Commercial LEO	Ka, Ku
Alternate	MEO very high throughput satellite	Ka, Ku
	Travelling wave tube	X
Contingency	Transponded military	X
	Transponded commercial	Ku

[69] I Marine Expeditionary Force, discussion with authors, July 14, 2023.

[70] Marine Corps C2 experts, discussions with the authors, June 22, 2023. The I Marine Expeditionary Force represents one-third of the Marine Corps' operating forces and is intimately involved in concept experimentation; we judged their perspective to be the most useful for this research. The Marine Corps judges that it will often have low priority for military SATCOM and may not have reliable access to military SATCOM when needed.

[71] Collaborative services are a suite of capabilities and applications common across the entire DoD, such as NIPR or SIPR access, Microsoft Office 365, and others. Core services are specific to the Marine Corps (or are not common across DoD). Core emergency services include common operating picture (Joint Tactical Common Operational Picture Workstation), internet relay chat, AFATDS, Joint Range Extension Applications Protocol (JREAP) versions A and C. See 9th Communication Battalion, "I MEF Agile and Assured C5ISRT Overview," U.S. Marine Corps, May 1, 2023, p. 12.

[72] At the time of this writing, it appears that the Marine Corps is in the process of initiating a variety of contracts that contribute to its intended PACE plan (along with hybrid terminals to use the range of systems), but it is not yet clear whether it has met its goal yet. See Johannes Schmidt, "The Corps' Newest SATCOM Terminal Adds Lethality Through Speed," Marine Corps Systems Command Office of Public Affairs and Communications, January 26, 2023; and "OneWeb Technologies Demos Seamless LEO and GEO Multi-Orbit Services for the U.S.M.C.," *SatNews*, July 28, 2023.

Plan Element	Contributors	Band
Emergency	Mobile User Objective System	UHF
	AN/PRC-150	High frequency/very high frequency

SOURCE: Features information from 9th Communication Battalion, 2023.
NOTE: PACE = primary, alternate, contingency, and emergency.

The Marine Corps' second approach to mitigating its dependency on commercial SATCOM is the use of deception and signature management TTP to improve unit survivability and enable mission accomplishment. This is instantiated in its emissions control levels, which range from a permissive level to a zero-emissions level.[73] Each level has best practices (for the permissive level) and directed restrictions. For instance, power management and emissions levels are restricted as the threat increases. Migration to Ka-band to reduce vulnerability to jamming and other offensive electronic warfare is also encouraged. However, it is unclear how widely these plans are integrated into operational planning and how faithfully they are executed.

Anti-Ship Fires (Marine Corps)

To better contextualize our analysis of Marine Corps usage of commercial SATCOM, we turn our attention to one specific mission: anti-ship fires. The mission is enabled by the Navy Marine Corps Expeditionary Ship Interdiction System (NMESIS), which pairs a medium range Naval Strike Missile with an autonomous firing platform. The firing platform and launcher are controlled by a weapon control system that receives both J- and K-series messages that are the most common means of relaying targeting information.[74] The weapon control system can utilize terrestrial line-of-sight and SATCOM to relay targeting information.

According to the Marine Corps' emerging Expeditionary Advanced Base Operations concept, anti-ship fires help the Navy's surface combatants, naval aviation, and amphibious forces gain freedom of maneuver (particularly in the face of the People's Liberation Army Navy threat in the Indo-Pacific), particularly in the early phases of a conflict when land-based fires may be in the best position to attrit People's Liberation Army Navy forces. This mission is often cited by joint force leaders in the Indo-Pacific as a particularly critical one.[75]

It appears that the Marine Corps is reliant on commercial SATCOM broadly for primary communications between different parts of the kill chain.[76] AFATDS is a service that is enabled by

[73] 9th Communication Battalion, 2023, p. 10.

[74] The Link-16 communications system employed by aircraft to communicate targeting data uses J-series messages, while AFATDS, commonly used in ground-based fires systems, uses K-series messages. See Ridge R. Flick, "Winning the Counterland Battle By Enabling Sensor-to-Shooter Automation," *960th Cyberspace Wing*, October 6, 2021; and Headquarters Marine Corps, Combat Development and Integration, *Navy Marine Corps Expeditionary Ship Interdiction System (NMESIS) Concept of Employment*, August 5, 2021, Not available to the general public, p. 6.

[75] Philip Davidson, "Advance Policy Questions for Admiral Philip Davidson, USN Expected Nominee for Commander, U.S. Pacific Command," Senate Armed Services Committee, April 18, 2018.

[76] The *kill chain* is a conceptual framework of the tasks required to effectively engage a target: find, fix, track, target, engage, and assess (F2T2EA). See Joint Publication 3-09, *Joint Fire Support*, Joint Chiefs of Staff, April 10, 2019, p. IV-13.

nine different communications pathways across the Marine Corps PACE plan.[77] Four of the pathways are commercial; there is provision for emergency communications using MUOS point-to-point network, but the available bandwidth and competing users are likely to make continuity of operations difficult. Other applications (e.g., Android Team Awareness Kit, internet relay chat, JREAP-C, and Theater Battle Management Core Systems especially) may also contribute to closing the kill chain for NMESIS. This conceptually provides more redundancy, but how this may be instantiated is unclear. Applications like JREAP-C and internet relay chat are available through emergency communications pathways.

The severity of the loss of commercial SATCOM to support this mission depends on the character of the loss. Assuming the Marine Corps can secure the diversity of commercial SATCOM contracts that it has articulated in its PACE plan, the degradation or loss of commercial SATCOM generally can be mitigated by migrating firing message traffic to military SATCOM alternate, contingency, or emergency systems.

Summary Assessment

Our assessments of commercial SATCOM usage across the military services reveal three overarching trends. First, DoD's need for commercial SATCOM is increasing for many uses, including for missions that are critical to joint warfighting. The need for SATCOM broadly is driven (1) by a growing demand for reliable connectivity at increased ranges as the military services develop concepts and doctrine that rely on disaggregating units and capabilities to increase survivability in the face of peer threats and (2) by bandwidth-intensive applications to leverage advanced technologies. At the same time, the supply of military SATCOM has not substantially increased and is unlikely to do so in the near future. These factors leave commercial SATCOM as an attractive alternative, which is well-postured to meet this increasing demand as capacity in the global SATCOM market is expected to grow with the introduction of high-throughput satellites and pLEO constellations.

Second, some missions are incurring more risk by becoming substantially reliant on commercial SATCOM. The demand for commercial SATCOM has reached a point where some missions have become largely reliant on commercial SATCOM.

Finally, efforts to mitigate vulnerabilities attendant to increased reliance on commercial SATCOM are nascent and sporadic. Examples of mitigation measures under consideration include incorporating diversity of commercial SATCOM providers, integration into PACE plan, or employment of TTP that enable continuity of operations in bandwidth-limited environments (e.g., operating on mission type orders). Use of military SATCOM, international partners' SATCOM, or other means of communication (e.g., tactical radios) could also serve as mitigation measures. However, additional analysis would be needed to understand the feasibility and effectiveness of each of these mitigation measures for specific commercial SATCOM applications.

Implementing some of these mitigation measures and operationalizing a hybrid SATCOM architecture to enable users to roam seamlessly between military and commercial SATCOM networks (or between different commercial networks) would require fielding such enablers as hybrid terminals

[77] 9th Communications Battalion, 2023, p. 10.

and an enterprise SATCOM management and control system. Without such enablers and an operating concept for managing an integrated SATCOM enterprise, continued reliance on commercial SATCOM will place many DoD missions at risk.

Chapter 4

Commercial Space Contribution to SDA Mission

SDA is an essential capability needed to support the safety and sustainability of space operations and is critical to the USSF's protect and defend mission.[78] The SDA designation occurred in 2019, as an enhancement to space situational awareness (SSA), to emphasize a new military posture in space needed to protect U.S. and other friendly space systems.[79] SSA is now a subset of SDA that focuses on the orbital segment to provide knowledge and characterization of space objects.[80] This shift in posture occurred as DoD considered space to be a new warfighting domain given adversaries' development of capable antisatellite weapons. The contested and increasingly congested space environment requires DoD to better identify, locate, and track potential threats to space systems.

The large volume of space, the increasing number of active satellites, the increasing sophistication of both friendly and adversary satellites (e.g., smaller size and signature), the use of larger satellites deploying smaller satellites, the increasing maneuverability of satellites, and the ability to perform close-proximity operations with both cooperative and uncooperative space systems are all challenging and will continue to further stress SDA capabilities. The DoD SDA mission supports the following four principal activities:

- launch and human flight safety
- catalog maintenance (i.e., maintaining accurate tracking information on all trackable resident space objects)
- conjunction assessment (i.e., project possible collision between resident space objects—two satellites or a satellite and space debris—and provide warning to affected space operators)
- protect and defend mission (i.e., protect U.S. and friendly orbiting satellites).

Although commercial companies can support several of these four activities, the USSF and USSPACECOM use commercial SDA services mostly to support the protect and defend mission, which involves similar tasks as the other three SSA activities listed above, including the following:

- **Detect, track, and identify space objects in all orbits:** Commercial companies have different sensors, including passive radio frequency, electro-optical/infrared (EO/IR), and radar, which they use to support this task. Currently, these sensors are mostly ground based and distributed

[78] *SDA* is defined as "the identification, characterization and understanding of any factor associated with the space domain that could affect space operations and thereby impact the security, safety, economy, or environment of our Nation" (USSF, *Spacepower: Doctrine for Space Forces*, Space Capstone Publication, June 2020).

[79] Sandra Erwin, "Air Force: SSA Is No More; It's 'Space Domain Awareness,'" *SpaceNews*, November 14, 2019.

[80] Joint Publication 3-14, 2023.

throughout the globe. Limited space-based non-Earth imaging capabilities are being explored by established space-based terrestrial ISR companies, and start-ups are planning to deploy space-based SDA capabilities.

- **Develop threat warning and assessment:** Information and data from commercial SDA providers have been used to develop threat warnings about possible hostile actions in space. The USSF has leveraged the provided data, but commercial companies have also developed analytics capabilities to analyze and identify potential threats.
- **Characterization of space objects:** Data from commercial companies can support the characterization of space objects (e.g., use photometric curves to identify microdynamics).
- **Data integration and exploitation:** Commercial companies are also acquiring and integrating data from different providers. These companies can augment government data integration and exploitation capabilities.

Although commercial SDA–derived data are not (as of the writing of this report) supporting the catalog maintenance activities, the USSF is experimenting with leveraging commercial SDA services to support catalog maintenance activities by integrating commercial SDA data with DoD's information. This initial effort involves a handful of sensors; however, the intent is to leverage a much larger number by the end of 2024.[81] In this report, we did not consider hosted government payloads as a commercial SDA service but included the leasing of commercial sensors or platforms.[82]

Commercial SDA Capabilities

The U.S. military has historically executed its SDA mission using its Space Surveillance Network (SSN), which is a network of ground-based radars and sensors, optical telescopes, and on-orbit capabilities that span several sites around the world. The SSN allows the U.S. military to detect, identify, track, and catalog artificial objects observed in Earth's orbit.[83]

Current and Evolving SDA Capabilities

Current commercial SDA capabilities are well established. Prior RAND research has aptly described the SDA market and has provided an overview of the leading commercial SDA companies

[81] USSF personnel, discussion with authors, February 23, 2023.

[82] USSPACECOM has SSA sharing agreements with a large number of commercial satellite operators worldwide. Under the agreements, USSPACECOM provides advanced SSA services, such as collision avoidance support, in addition to other basic spaceflight safety support that it provides to all operators. The participants of the agreement share ephemeris data of their satellites and information on other space activities (e.g., maneuver plans) that bear on spaceflight safety. Such data are used to contribute to DoD's space catalog maintenance. However, our research focused on commercial entities that collect and sell SDA data.

[83] The sensors within the SSN are generally categorized as three types: dedicated, collateral, or auxiliary. As these categories suggest, the first type is dedicated to the SDA mission, the collateral sensors support the mission but have a different primary mission (missile warning/missile tracking), while the auxiliary sensors can collect data for the SSN on an as-available basis. The C2 of the SSN is executed by the 18th Space Defense Squadron of USSPACECOM (see Joint Task Force-Space Defense [JTF-SD], "18th Space Defense Squadron," fact sheet, May 2, 2022).

and their respective capabilities.[84] However, the market continues to evolve, and companies are also making plans to evolve their capabilities. The appendix presents a comprehensive list of commercial SDA providers along with a short description of their capabilities.

Today, some of the commercial SDA companies are well established and continue to evolve while new entrants are developing innovative systems, including space-based SDA and rendezvous and proximity operations (RPO) capabilities. Current providers cover the LEO, highly elliptical orbit (HEO), MEO, and GEO regimes, with growing interest in beyond GEO. Companies provide a mix of services for consumers, including collecting observational data using ground-based telescopes, radars, and passive radio frequency sensors; analyzing the collected data; and providing data analytics services. Each phenomenology is better suited for specific observations compared with others. For example, ground-based radar sensors are better at observing objects in LEO compared with ground-based optical telescopes, which are better at observing objects in higher orbits (e.g., GEO). Active and passive radio frequency sensors are good at observing at all times of day, including through clouds, although passive radio frequency sensors require an object to emit a signal to detect it. Whether by individual companies or the entire industry, data collected via multiple phenomenologies contribute to a more resilient architecture.

Another evolving SDA service involves space-based terrestrial ISR providers imaging on-orbit satellites. This service can provide valuable information to help with anomaly resolution (e.g., imaging a damaged solar panel) or support space object characterization. The NRO Electro-Optical Commercial Layer (EOCL) contract—awarded to three commercial vendors, Maxar, Planet, and BlackSky—has a provision for non-Earth imaging to support SDA.[85] Leveraging these companies sensors for non-Earth imaging can provide DoD with high-resolution satellite images not easily obtainable with ground sensors.[86] According to our discussions about this capability with BlackSky representatives, the company expects to support on-orbit satellite imaging services in the near future. BlackSky also plans to leverage its terrestrial observations with non-Earth imaging capability to support an integrated observation of terrestrial and space operations when possible—for example, provide indications of a rocket launch preparation and, if possible, observe the payload at various stages of its operations. This potential custody throughout the phases of a launch can provide valuable information to DoD.[87]

Benefits of Leveraging Commercial SDA Capabilities

Commercial SDA services provide a wide variety of space surveillance and reconnaissance capabilities that can be of beneficial value to DoD. These services augment DoD capabilities and improve the SDA architecture resiliency. The valuable attributes related to commercial SDA include the following:

---

[84] Yonekura et al., 2022.

[85] Theresa Hitchens, "NRO Keeps 3 Vendors for Commercial Imagery with New 10-Year Contracts," *Breaking Defense*, May 25, 2022a.

[86] The resolution will depend on several parameters, including the observing satellite telescope's properties (e.g., aperture, range to the satellite being imaged, lighting conditions).

[87] BlackSky representatives, discussions with authors, August 2, 2023.

- innovativeness, responsiveness, flexibility, and rapid deployment inherent with many commercial companies, especially smaller high-tech ones
- globally distributed proliferated sensor networks that can improve resiliency and increase capacity, surge, and coverage capabilities—especially in the Southern Hemisphere (commercial SDA providers operate about 700 sensors over 75 sites, while the SSN has more than 30 sensors across a couple of dozen sites)[88]
- access to advanced commercially developed analytics
- smaller to no upfront DoD investments for new technologies and capabilities
- multiple phenomenologies and approaches across the different providers (e.g., EO/IR, radar, passive radio frequency, open-source data and information) can help improve overall detection and characterization of targets
- quicker access to state-of-the-art technology, such as daytime EO/IR observation capability, other innovative technologies, and analytics
- easier access to international sensor deployment sites versus DoD (i.e., access does not involve potentially lengthy government-to-government negotiations and agreements)
- deterrence support by attributing hostile or aggressive space activities publicly (due to the unclassified, releasable nature of commercial data)
- flexible response options (e.g., ability to quickly assign assets to support a task).

The extent and effectiveness with which DoD can leverage commercial SDA data are highly dependent on the level to which the commercial SDA services are operationally integrated and linked with DoD systems; the development and institutionalization of concepts of operations for the use of commercial services; and the implementation of appropriate supporting acquisition processes that encourage, support, and enhance the development of commercial space services by U.S. companies. All the elements of DOTmLPF-P[89] need to be considered to fully leverage the value of commercial SDA services. We also note that U.S. policy encourages the use of commercial space services by DoD whenever possible.[90]

Current DoD Use of Commercial SDA

The use of commercial SDA services by DoD is developing from a relatively nascent stage and will likely progress as commercial providers continue to advance and DoD is better able to leverage these services. It appears that DoD has been taking a slow approach in incorporating commercial SDA within its SDA architecture; a handful of providers are fairly mature, having been established more than 15 years ago. This slow approach is understandable given the criticality of the mission, the potential consequences of failure, and the limited budget allocated to commercial SDA services. The

[88] Jon Ludwigson and Alissa H. Czyz, *Space Situational Awareness: DoD Should Evaluate How It Can Use Commercial Data,* U.S. Government Accountability Office, GAO-23-105565, April 2023.

[89] DOTmLPF-P represent the nonmateriel needs to effectively support a weapon system. The materiel segment in the acronym usually includes the supporting elements (e.g., ground systems and software) needed to operate the weapon system.

[90] Office of the President, 2020, p. 20.

USSF requested funding for commercial SDA services for the first time in FY 2022 and in FY 2023, with $20 million budgeted for FY 2023 and about $110 million allocated for FY 2023 through FY 2027.[91] This request is a small fraction of the total SDA budget, which was estimated to be $1 billion a year from 2015 to 2020.[92]

DoD uses two principal venues to acquire commercial SDA services: (1) the Joint Task Force-Space Defense Commercial Operations (JCO) through the marketplace or unified data library and (2) a direct agreement with the provider (bypassing the marketplace).[93]

JTF-SD Commercial Operations

The JCO is a commercial SDA cell stood up to support the JTF-SD protect and defend mission. Although, as of FY 2023, JCO operates in a limited mode, it has successfully demonstrated how DoD can effectively leverage commercial services using a wide variety of U.S. and foreign commercial services and allied capabilities. Mission operations examples include the following:[94]

- surveillance tracking in LEO, MEO, and GEO
- maneuver detection and anomaly notifications
- data and information collection to support patterns of life development
- launch and early orbit tracking of new foreign launch
- publications of Notice to Space Operator, including RPO and other anomalous behavior notifications
- improved capabilities to quickly find lost resident space objects.

The JCO operates exclusively at the non-classified level[95] and provides data and information to the national space defense center and commercial space operators, including to allies and partner nations. The JCO acquires sensor data from various providers using a short-term (approximately one month), renewable contract, through the unified data library. Although the JCO buys some analytic services, it uses in-house tools (e.g., Army Dragon) to integrate and analyze the acquired data. The in-house analytic capabilities help alleviate some potential operational security concerns resulting from the use of commercial data. A high-level architecture of the JCO is depicted in Figure 4.1. As the figure shows, the JCO leverages commercial and partner SDA sensors.

---

[91] Sandra Erwin, "Report: Space Force Could Benefit from Commercial Data to Monitor Satellites and Debris," *SpaceNews*, April 2023a.

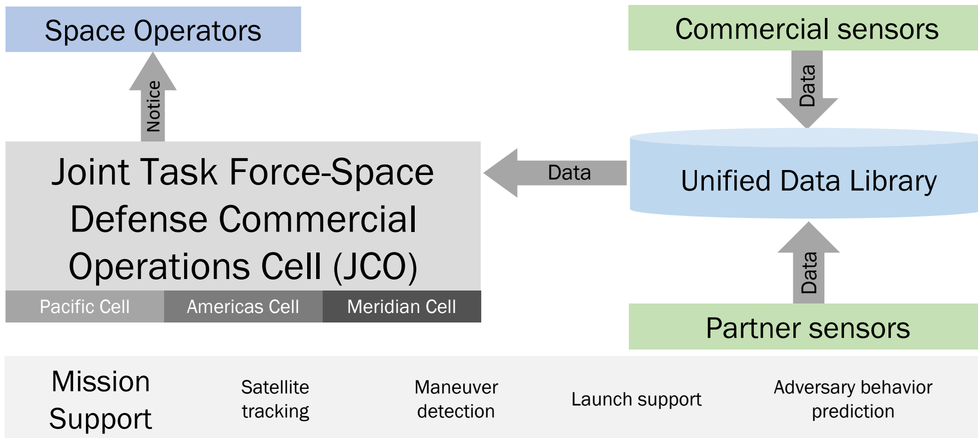
[92] The $1 billion estimate is based on the SDA expenditures for DoD, National Aeronautics and Space Administration (NASA), and NOAA as provided by the U.S. Government Accountability Office. See Cristina T. Chaplain, *Space Situational Awareness Efforts and Planned Budgets*, U.S. Government Accountability Office, GAO-16-6R, October 2015.

[93] Jennifer Thibault, "JTF-SD Awards Space Domain Awareness Contract via Marketplace," Joint Task Force-Space Defense Public Affairs, undated; Sandra Erwin, "Bluestaq Wins $280 Million Space Force Contract to Expand Space Data Catalog," *SpaceNews*, March 23, 2021.

[94] "JTF-SD Commercial Ops (JCO)," briefing presented by Joe Gerber, KBR, Inc., March 2023; supplemented by authors' discussions with commercial providers.

[95] The JCO uses the term *non-classified* instead of *unclassified* to highlight its use of commercial, nongovernment data that are typically available to the public.

Figure 4.1. JTF-SD Commercial Cell Construct



SOURCE: Derived from "JTF-SD Commercial Ops (JCO)," 2023; supplemented by authors' discussions with commercial providers.

We also considered the operational value that commercial SDA services can provide DoD, which include supplementing the coverage volume and improving the revisit rate to selected objects, improving the resiliency of the SDA mission, providing analytics to help alleviate government workload, and supporting dynamic tasking to improve the responsiveness and flexibility of the SDA mission. These operational values are summarized in Table 4.1.

Table 4.1. Commercial SDA Characteristics and Contribution to DoD

Characteristic	Primary SDA Task Support	Contribution to DoD
Coverage and revisit	• Detect, track, and identify • Threat warning and assessment	Fills coverage gaps, timelier indications and warning, improved search of lost objects and improved characterization
Resiliency	• Detect, track, and identify • Threat warning and assessment • Characterization of space objects • Data integration and exploitation	Substantial improvement to ecosystem resiliency
Analytics	• Threat warning and assessment • Characterization of space objects	Alleviate related government requirements and improve threat warning and assessment
Dynamic tasking	• Threat warning and assessment • Characterization of space objects	High responsiveness, flexibility
Capacity	• Detect, track, and identify	Responsiveness to task requests
Availability and data security	• User trust level	Requires additional C2, government analytics

One example of the operational value that these services provide to DoD is the detailed, high-tempo observation and analysis provided in December 2021 by ExoAnalytic of the Shijian 21 activities, including high delta-V maneuvers and docking. Another notable example is the JCO's development of an integrated intelligence product of the Russian direct ascent antisatellite test in November 2021, starting from left of launch to post-event observations. The JCO developed indications and warning of the Russian test (based on information from the public satellite research analyses team), identified COSMOS 1408 as a likely target using KBR software, and provided subsequent detection and tracking of debris resulting from the impact using Slingshot's electro-optical telescopes.[96]

Direct Agreements with Commercial Providers

Although the majority of DoD's acquisition of commercial SDA occurs through the JCO, one commercial provider indicated during our discussions that the provider has small supporting contracts with other DoD organizations.[97] These other government organizations leveraged more commercially provided analytics capabilities and provided longer-term contracts than the JCO.

[96] "JTF-SD Commercial Ops (JCO)," 2023.

[97] Commercial provider, discussion with authors, 2023 (details withheld for non-attribution reasons).

Anticipated Increase in DoD Use of Commercial SDA

On the basis of anticipated DoD demand for commercial SDA services and data and the SDA market outlook, DoD will need to continue leveraging commercial SDA and will likely increase its use.[98] As demand expands and DoD increases its use of commercial SDA, DoD will need to address potential challenges in integrating commercial SDA into its SDA enterprise.

Continued Growth in DoD Demand

The demands on SDA will continue to grow, requiring more timely data for a larger number of objects, for more maneuvering RSOs, and from an expanded volume of space (beyond GEO). DoD systems will likely continue to be challenged to meet these demands.[99] DoD is also increasing its investments, albeit relatively small in magnitude, to leverage commercial SDA more effectively (e.g., expanding the JCO operations to 24/7). This trend will enable, and possibly motivate, DoD to increase its use of value-added commercial SDA services.

Future SDA Capabilities and Market

As the number of space objects continues to increase, commercial SDA products and services will likely continue to grow to support SDA and space traffic management for all operators. Many providers plan to develop and enhance their current offerings through the deployment of additional sensors, increased on-orbit capabilities, and building out their products for users. We expect DoD to increase its use of commercial SDA as these capabilities increase. The JCO model will enable this increased use by relying on as many qualified commercial SDA providers as possible to complement DoD capabilities. The newly established commercial services office dedicated to buying commercial space services expects an increase in the purchase of value-added commercial SDA services.[100]

A five-year outlook of the market is difficult to predict. Companies have their own plans for growing capabilities and business, including opening new sites and increasing sensor diversity. Companies talked about investing in software capabilities,[101] and leveraging artificial intelligence, machine learning,[102] or other software developments. Future services will likely also include space-based commercial SDA services. A new start-up, True Anomaly, is planning to provide on-orbit imaging and close-proximity operations in support of the USSF's protect and defend mission.[103] Information regarding the planned capabilities is limited given that company's nascent stage.

---

[98] None of the government subject-matter experts with whom we spoke were able to specify how much more commercial SDA will be used in the future.

[99] As the number of objects in orbit increases, satellites will need to perform more collision avoidance maneuvers. Additionally, many future DoD satellites will likely be more maneuverable to increase their resiliency and mission flexibility.

[100] Sandra Erwin, "New Space Force Procurement Shop Subscribes to the Space-as-a-Service Model," *SpaceNews*, November 21, 2022c.

[101] U.S. commercial SDA provider, discussion with authors, June 1, 2023.

[102] U.S. commercial SDA provider, discussion with authors, May 31, 2023.

[103] True Anomaly, homepage, undated.

Additionally, commercial satellite owners and operators may in the future rely more on commercial SDA services for exquisite capabilities to support future advanced commercial space missions, such as refueling. Exquisite SDA capabilities can also help with anomaly resolution by, for example, providing high resolution images of satellites. However, given the scarcity of relevant data and information, we were not able to assess the commercial SDA market needs that satellite owners and operators may generate.

One government expert in SDA shared that the growth in the commercial SDA market would likely depend on the U.S. Department of Commerce's use of commercial SDA data for commercial space traffic management and on the interest of international partners and allies in commercial SDA capabilities.[104] A U.S. commercial SDA provider shared a similar view, noting that they expect the most growth in their business to come from international governments.[105] However, another government expert indicated that there is an ongoing effort to leverage commercial data in support of the catalog maintenance task. This effort involves developing a capability to automatically ingest and integrate commercial sensor data into the public catalog.[106]

Ultimately, the growth of the market will be tied to the expansions of all these activities, including DoD's use. The department's use of commercial SDA capabilities that are of highest value to its mission (e.g., RPO activities characterization) will likely have a significant effect on the viability of the companies providing these services. Our hypothesis is that if, in the future, DoD represents a small demand signal for unique commercial SDA services, the commercial industry would likely invest more in the higher demand services to satisfy larger customers. Although we did not perform a future market analysis of commercial SDA needs because of the large uncertainties and lack of information regarding future use, such an analysis should be performed, when possible, to provide DoD visibility into the future commercial SDA market conditions.

We are not able to determine what level of dependence commercial space operators will have on commercial SDA providers, because future basic SSA information will continue to be provided publicly and for free by the Department of Commerce.[107] Adding value to the free offering of information will be necessary for customers of commercial SDA. We heard government and commercial users discuss the importance of such factors as the fidelity, timeliness, and integration of commercial SDA data with government SDA data. In some cases, commercial SDA providers can exceed DoD's capabilities, such as through the timeliness of the collection of data, location, proliferation of sensor sites in areas where government sites are sparse, and software capabilities that utilize the data to provide a more user-friendly product to operators. However, DoD is continuing to develop highly capable systems to improve its SDA capabilities.[108]

---

[104] U.S. government SDA subject-matter expert, discussion with authors, March 9, 2023.

[105] U.S. commercial SDA provider, discussion with authors, May 24, 2023.

[106] USSF SDA subject-matter expert, discussion with authors, June 5, 2023.

[107] Christine Joseph and Sandy Magnus, "Overview of NOAA's Office of Space Commerce: A Presentation to the NOAA Science Advisory Board," briefing, April 27, 2023.

[108] Ludwigson and Czyz, 2023.

Challenges and Limitations of Commercial SDA

Leveraging commercial SDA in an effective and efficient manner also involves technical, operational and security, and acquisition-related challenges. Although the JCO has addressed some of these concerns, additional improvements are likely needed to better operationalize the SDA capabilities at scale. Although most, if not all, of the difficulties articulated here can be solved, a concerted and planned effort by the government will be required to do so.

Technical Challenges

Technical challenges the government can face when leveraging commercial SDA include the following:

- SDA observations can be perishable and need to be disseminated in a timely manner to be valuable; appropriate communications lines between DoD and commercial providers are needed to ensure timely request and receipt of the data.
- Data provided by vendors come in various formats and are based on different references. They need to be standardized to be usable by DoD systems.
- Automated data ingestion and integration from different sensors are needed to enable various DoD organizations to better leverage these data. Obtaining and using data stored in the unified data library can be cumbersome; improvements in how data from the unified data library can be ingested will likely be needed as the size of this depository increases.[109]

Although the first two challenges listed appear to have been addressed by the JCO, further improvements to the process may be needed to address future, more-challenging scenarios in which larger amounts and types of near-real-time data and information may be needed to support the protect and defend mission, especially if the reliance on commercial SDA services continues to grow. The last concern listed appears to be an ongoing issue; however, an effort is underway to address it.[110]

Operational and Security Challenges

Operational and security challenges include the following:

- Efficient and effective mechanisms are needed to ensure that DoD can request the needed observations from the commercial providers in a timely manner throughout the different phases of competition while maintaining operational security.
- Security (including cyber and physical) challenges need to be considered.
- Assuring the pedigree of the commercial data (e.g., not corrupted through intentional or unintentional means, especially for automated data ingestion) is needed.

The first two challenges listed appear to have been addressed by the JCO; however, it is not clear how much these processes can be scaled up.

---

[109] Massachusetts Institute of Technology Lincoln Laboratory SDA subject-matter expert, discussion with authors, July 28, 2023, Not available to the general public.

[110] USSF personnel, discussion with authors, February 23, 2023.

Acquisition Challenge

One acquisition concern among industry and government experts we met with is the short duration contracts being issued by the JCO. The JCO has been successful in rapidly issuing short-term contracts (approximately 30 days) to commercial SDA providers. Although this model has been successful in maintaining the best capabilities and motivating the contractors to perform their best, it also has longer-term risks that should be considered. For example, the short-term contract model does not support future capabilities development because of the high uncertainty of these contracts.[111] Although this approach is intended to motivate these companies to continually upgrade their capabilities and be responsive to JCO's needs to remain competitive, it may not be as effective in the long run.

Depending on future commercial SDA market demands, companies may prioritize competing for other longer-term contracts (including with international customers) over the shorter-term JCO contracts. Another short-term contract concern among government SDA experts with whom we met was that they could rely on a given commercial SDA provider being on contract only for a short time. Consequently, one government team was reluctant to spend resources developing tools that would improve the exploitation of data from any specific commercial provider.[112] There may be other approaches to address this issue (e.g., common data format and standards across contractors). However, we did not have the opportunity to further investigate this possibility.

Longer-term, yearly contracts would alleviate these concerns—however, further analysis by JCO staff would be needed to assess the impact on JCO's operating model. Longer contracts may require a larger budget allocation to the JCO to support its operations and maintain the flexibility to issue short-term contracts when needed.

This issue could manifest itself in the future if commercial SDA demands approach or exceed the available capacity, resulting in companies prioritizing longer and possibly larger contract opportunities.

Frequency of Interference Activities

Overall, interference activities against commercial SDA providers appear to have been relatively limited and manageable. Companies that we talked to have experienced disruptions that were mostly caused by natural events, such as weather. These providers experienced either no indications of cyber intrusion or some limited possible cyberattacks, such as power outages.[113] None of the attacks were confirmed, but the companies are acutely aware of the threats and report having robust measures in place to address cyber intrusions into their systems.[114] New start-up companies we met with indicated possible cyber monitoring by foreign entities and attempts to infiltrate company networks, which

[111] In our discussions with commercial SDA providers, they noted that they have to write a proposal every 30 days (i.e., be awarded 12 contracts for a year's support).

[112] USSF personnel, discussion with authors, February 23, 2023.

[113] Commercial SDA provider, discussion with authors, May 24, 2023.

[114] Commercial SDA provider, discussion with authors, May 26, 2023.

would provide the intruders with access to technical data. These companies also were aware of these activities and reported taking proper precautions to deny access.[115]

The interference events noted to date have occurred during a period with no armed conflict with peer adversaries. The level of interference during an armed conflict, or just prior to one, would likely be different.

Operational Impact from Loss of Service

From an operational perspective, the JCO model appears to provide a valuable and effective means of leveraging commercial SDA companies. The approach entails using as many commercial SDA providers as possible and ensuring some redundancy exists for all the services being provided by these companies (i.e., backup capabilities from independent companies). The JCO is also planning to improve its C2 resiliency by leveraging the services of a reliable and secure cloud provider, such as Amazon Web Services. If properly implemented, this approach should significantly complicate any attacker's attempts to affect the JCO C2 operations.

The combination of the large number of providers, which when combined have access to over 700 ground-based sensors (passive and active), and the expected robust C2 construct make the JCO services resilient to an opponent's attack. An opponent would need to affect dozens or more sensors from different, independently operated companies, and/or penetrate and affect a robust, protected, and networked cloud architecture, such as Amazon Web Services, to affect the JCO C2 network. Nevertheless, the current commercial SDA data are used to augment the DoD SDA capabilities. Although a loss of all these services would affect the DoD SDA mission, it would not have a catastrophic impact. Some opponents' space activities would likely take longer to detect, anomaly investigations would also be affected because less data and information would be available, and public attribution would be significantly affected because unclassified publicly releasable SDA-related data originating from DoD systems are scarce.

In the future, as DoD relies more on commercial SDA services, a complete loss of these services would likely have a greater impact. However, we also expect that the DoD systems used to leverage commercial SDA and the overall commercial SDA capabilities will be more resilient than they are today. Given the criticality of SDA, we also suggest that DoD maintain the critical capabilities needed to execute the protect and defend mission at an acceptable level of effectiveness. We are not suggesting that DoD should not rely on commercial SDA services but that DoD should be judicious in its decisions about how much and which missions should heavily rely on commercial SDA.

One potential criterion could be to consider the degraded performance of the government mission when losing commercial SDA and develop sufficient organic capabilities to ensure the minimum or threshold performance level can be met without commercial support. In other words, although complementary commercial services would enable achieving the full objective level, the complete loss of these services would not degrade the mission performance below a minimal value. This approach would need to be balanced against available budget, and DoD would need to balance the risk of losing critical commercial SDA services with the value they provide if funded at a higher level.

[115] Commercial SDA provider, discussion with authors, May 24, 2023.

Measures to Mitigate Risk of Loss of Access

One of the concerns associated with DoD reliance on commercial SDA is how to ensure access to commercial data and services through the competition continuum—an environment that includes cooperation, competition below armed conflict, and armed conflict.[116] There is risk associated with using commercial SDA and with relying too heavily on it without properly considering the potential for loss of access. This loss of access could be the result of many scenarios, including business decisions, business failure, adversary or natural interference, severe weather events, cyberattacks on networks, and many more. Although government systems also deal with some of these risks, they may be more pronounced for commercial providers because their systems are likely not as hardened as government-owned systems; they need to remain profitable to operate; and they are subject to business activities, such as acquisition, bankruptcy, and influence by stakeholders.

The government can take several measures to mitigate the risk from using commercial SDA, but the extent of these measures would depend on such factors as mission type, contract parameters (i.e., size and length), level of dependency, or criticality of provided service. These factors help determine the types and level of mitigation needed. For example, a 30-day contract may not require assessing the business viability of a company; however, an analytics services provider may require a more in-depth review of the company because it can more directly affect government decisionmaking. Mitigation measures that can be used include the following:

1. Performing due diligence prior to contract award, and possibly on a regular basis, to ensure that the providers meet minimum standards related to
   - business viability
   - operational security (including cyber)
   - foreign influence.
2. Developing a resilient, multilayer commercial SDA enterprise that provides the USSF with multiple options (including phenomenologies) and sources from which to obtain the commercial services.
3. Limiting the use of commercial SDA to less than critical, non-time-sensitive tasks that would minimize the impact of loss. However, we recognize that commercial SDA can provide valuable time-sensitive information (e.g., indications and warning), and the USSF could task several providers to mitigate the impact of an individual company failing to execute.
4. Maintaining essential (and sufficient) USSF capabilities to execute the SDA mission (albeit with reduced capacity), as discussed in the previous section.
5. Developing a flexible, scalable, and resilient USSF command center to task, integrate, analyze, and exploit commercial SDA capabilities.

These five measures are intended to help mitigate the impact of losing individual providers and, from a commercial SDA architecture perspective, would alleviate some of the risks associated with using commercial SDA. The JCO construct implements some of these measures—numbers 2 and 5 and, to some extent, number 1.

[116] Joint Doctrine Note 1-19, *Competition Continuum*, Joint Chiefs of Staff, June 3, 2019, p. v.

Commercial Contribution to DoD Resiliency Plans

Joint Publication 3-14 defines *resilience* as

> 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, despite hostile action or adverse conditions.[117]

The SDA architecture we consider here is a hybrid one that combines USSF and commercial SDA systems.[118] Although the primary purpose of the JCO is to augment the DoD SDA capability, the diverse and proliferated characteristics of the hybrid commercial SDA enterprise supports many of the resiliency characteristics listed in Joint Publication 3-14, including disaggregation, distribution, diversification, and proliferation.[119]

Although we posit that the commercial SDA services leveraged by the JCO increase the resilience of the SDA enterprise, it is not clear to what extent DoD considers commercial SDA as an additional factor in increasing its SDA mission resiliency. This judgment is solely based on the lack of documentation from DoD stating that commercial SDA is a contributor to resiliency.

Summary Assessment

Overall, commercial SDA companies benefit DoD in several ways. They provide some support to the USSF's protect and defend mission, increase the resilience of the SDA enterprise, provide surge and coverage capability to the USSF when needed, augment the DoD SDA capability, and can help improve its performance by possibly alleviating the task load of more-exquisite government sensors. Although some of the commercial SDA companies have been operating for more than ten years, the overall industry is relatively nascent, and DoD has only recently started to systematically leverage commercial SDA services through the JCO.

Although commercial SDA providers currently augment DoD capabilities, our qualitative assessment is that a total loss of commercial SDA services would not be catastrophic to the DoD SDA mission; however, such a loss would affect the overall performance of the government SDA enterprise by lowering its capacity, timeliness, and resilience. Identifying a scenario in which a total loss of commercial SDA services occurs is difficult given the number of providers and sensors and the multitude of possible links through which DoD could receive data. For example, DoD could obtain data directly from providers without going through the unified data library, although it would be much less efficient. As the USSF becomes more reliant on commercial SDA in the future, it should consider the implications of losing commercial services and develop appropriate mitigation plans, including resiliency measures to ensure that essential SDA capabilities remain available.

The commercial market for SDA services may also grow as users further develop space capabilities, including pLEO constellations, space logistics, and other missions requiring more-

---

[117] Joint Publication 3-14, 2023, p. III-4.

[118] Although the JCO includes some allied systems, we focus on commercial providers for the purposes of this report.

[119] Joint Publication 3-14, 2023.

exquisite SDA data than provided free of charge by the USSF and/or the Department of Commerce. This evolving market along with interest by other government agencies (e.g., the Department of Commerce and others) and international governments (i.e., allies and partners) will help the commercial SDA market. However, the future size of the commercial SDA market remains to be seen, so it is not yet clear how many commercial providers it can support. Nevertheless, commercial SDA companies continue to grow, and start-ups are betting on a growing market.

The future growth of the commercial SDA enterprise will depend on the overall marketplace and will likely be strongly influenced by the actions of DoD with respect to the use of commercial SDA. A continued evolution of the JCO to include a larger budget and some longer-term contracts will benefit the industry and motivate continued growth. Clearer messaging on the needs of DoD and the possible future roles of commercial SDA providers would also help more targeted growth by the companies to support DoD. Technical, operational, and acquisition challenges remain, as discussed in this chapter, and they need to be addressed to enable DoD to better leverage potentially valuable capabilities to help DoD execute its SDA mission.

On the other hand, ignoring the needs of the commercial SDA providers, limiting the budget allocated to their services, and not addressing the main challenges involved in leveraging their capabilities would likely reduce the growth of the industry or at least reduce the development of capabilities and the focus of these companies to support DoD missions.

Chapter 5

DoD's Use of Commercial Remote Sensing, Environmental Monitoring, PNT, and Space Logistics Services

With advances in small satellite technologies, lower cost of access to space, and other technological advancements, new entrants to the commercial space industry have significantly changed the makeup of the industry over the past several years. New commercial space markets emerged as perceived needs for new services spurred companies to make investments in such services as environmental monitoring, PNT, and space logistics. New entrants to such traditional markets as remote sensing are also diversifying the types of service offerings with innovative technologies and business models.

DoD is monitoring many of the emerging markets, such as PNT and environmental monitoring, to evaluate the utility of new commercial space capabilities in meeting DoD's space mission requirements or increasing resiliency. Changes in DoD missions and requirements in response to evolving threats are also motivating DoD's increased interest in the ongoing innovation in commercial space markets—such as in the potential use of commercial remote sensing capabilities to meet tactical space-based ISR needs or USSF's interest in enhancing space maneuverability with commercial on-orbit refueling.

This chapter addresses DoD's current and anticipated use of commercial capabilities to support armed forces operations in the following four space mission areas: remote sensing, environmental monitoring, PNT, and space logistics. The missions are presented in order of the maturity of respective commercial space markets.

Remote Sensing

DoD integrates military operations and intelligence activities under the missions known as ISR that "synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations."[120] ISR supports the U.S. armed forces in fulfilling intelligence missions, including strategic intelligence, anticipatory intelligence, and support to current operations.[121] Commercial remote sensing capabilities could play a role in all of these intelligence missions.

[120] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, February 2022, p. 118.

[121] For definitions and discussion of the foundational intelligence missions, see Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America*, 2019.

Strategic intelligence spans many high-level topics, including national political, economic, and security trends, and such transnational issues as terrorism. The military relies on anticipatory intelligence to track developments in adversary military capabilities and plan for emerging opportunities or threats. ISR provides critical support to current operations by informing planning and decisionmaking through characterizing enemy forces, monitoring adversary activities and movements, identifying and tracking potential targets, providing threat warning, and assessing battle damage, among fulfilling other information needs.

DoD leverages a variety of ISR sensors and platforms in all domains to fulfill its intelligence missions. However, DoD does not operate its own space-based ISR systems, but rather shares national space-based systems that the NRO develops, fields, and operates for DoD and the intelligence community (IC). DoD is one of many organizations that generates ISR collection requirements for national systems. Additionally, the NRO assumed the role of lead acquirer of space-based commercial imagery in 2017, and thus, most commercial remote sensing data that DoD exploits is acquired by the NRO and processed in part by the NGA before it reaches DoD users.[122]

Current DoD Use of Commercial Remote Sensing Capabilities

Commercial companies have been supporting DoD with space-based remote sensing services for decades.[123] However, in recent years, the pace of change in the technology on offer and economic conditions have greatly accelerated.[124] As technology has progressed, commercial space-based ISR has advanced to increasingly provide time-sensitive operational and tactical support to the joint force.[125] Commercial sensor data and analytics can add capacity in addition to government-owned systems, improve exploitation capabilities, improve revisit rates, increase the shareability of data with allies and partners, and improve space architecture resiliency.

Given these benefits, NRO is heavily investing in commercial EO/IR observation data, using the services of several companies (e.g., Maxar, Planet, and BlackSky) to build the EOCL capability.[126] The EOCL contract increases the number of remote sensing satellites that DoD and IC users have access to and increases space-based ISR capacity. For instance, the EOCL providers delivered about

---

[122] Cristina T. Chaplain, *Defense Space Acquisitions: Too Early to Determine If Recent Changes Will Resolve Persistent Fragmentation in Management and Oversight*, U.S. Government Accountability Office, GAO-16-592R, July 27, 2016. As a 2022 Government Accountability Office report noted, DoD and the IC have not formally defined the roles and responsibilities for acquiring commercial imagery, and, in recent years, DoD has acquired space-based imagery in limited ways. However, the vast majority of space-based ISR data are collected by the IC and support multiple interests, including the military's. There are ongoing debates about the future of overhead ISR responsibilities. See Brian Manzanec, *National Security Space: Actions Needed to Better Use Commercial Satellite Imagery and Analytics*, U.S. Government Accountability Office, GAO-22-106106, September 2022.

[123] Yonekura et al., 2022.

[124] Yonekura et al., 2022; Todd Harrison and Matthew Strohmeyer, *Commercial Space Remote Sensing and Its Role in National Security*, Center for Strategic and International Studies, February 2, 2022.

[125] Thomas Taverney, "The Evolution of Space-Based ISR," *Air & Space Forces Magazine*, August 10, 2022.

[126] The NRO awarded EOCL contracts to these three providers in 2022 that are worth about $4 billion over ten years (NRO, "NRO Announces Largest Award of Commercial Imagery Contracts," press release, May 25, 2022; NRO, email correspondence with authors on EOCL, September 12, 2023, Not available to the general public).

3.6 million images of new commercial imagery between June 2022 to June 2023.[127] The majority of commercial imagery acquired under the EOCL contract (about 94 percent of EOCL imagery) is used for NGA's foundational geospatial intelligence mission, which includes maritime and aeronautical safety of navigation, mapping, charting, and geodesy.[128] The increased commercial capacity to satisfy a larger number of customer requirements, including the armed forces requirements, allows national space-based ISR systems to focus on the most challenging and sensitive missions.[129]

Because of the increased capacity and access to commercial imagery, combatant commands are using the imagery to support their missions. Additionally, because commercial data are unclassified and NRO commercial data provider contracts are specifically designed with end user agreements to facilitate broad sharing of the data across the U.S. government and with U.S. allies and partners, combatant commands have been able to share such data easily with their foreign partners.[130]

Anticipated DoD Use of Commercial Remote Sensing Capabilities

DoD use of commercial remote sensing is highly likely to continue growing. How much, how fast, and in what sectors will be determined by DoD's demand for space-based sensing, market conditions, IC investment strategy, and policy decisions on the future responsibilities and force structure for tactical ISR.

Key drivers of demand include increasing demand for sensing capacity and sensor diversity (i.e., different sensing phenomenology) and a growing need for shareability with U.S. allies and partners.[131] The armed forces continue to require more ISR capacity than is available. As U.S. adversaries employ mobility and various denial and deception techniques as a countermeasure to space-based ISR collections, frequent revisit, persistent monitoring, and diversity of sensing phenomenologies are becoming increasingly important attributes that DoD seeks in a space-based ISR architecture.[132] Military missions typically do not require very high resolution to identify objects or events, but change detection, pattern of life analysis, and target tracking require frequent revisit or persistent monitoring. By increasing the use of commercial space-based sensing, more military ISR priorities can be serviced, and persistent monitoring tactics can be applied more broadly.

Recently, the NRO has been increasingly experimenting with other space-based sensor phenomenologies offered by commercial remote sensing providers, including synthetic aperture radar and radio frequency sensing, to evaluate their utility, which over time could expand the use of

---

[127] NRO, email correspondence with authors on EOCL, September 12, 2023, Not available to the general public.

[128] NRO, email correspondence with authors on EOCL, September 12, 2023, Not available to the general public.

[129] Taverney, 2022.

[130] NRO, email correspondence with authors on EOCL, September 12, 2023, Not available to the general public.

[131] We focus here on drivers that do not span across all space missions and are characteristic of (though not necessarily unique to) the ISR mission set. For example, cost savings through economies of scale, increased resiliency through system disaggregation and diversification, or increased frequency of technology refresh are potential benefits across the space missions that are not listed here.

[132] Synthetic aperture radar can be used during both day and night and through many types of weather—including clouds that obscure other forms of imagery. Passive radio frequency sensing can provide characteristics of the emitter and allows geolocation of many simultaneous collection targets. Hyperspectral imaging can identify materials being imaged, aiding in the identification and characterization of terrain and objects.

commercial sensors by both the IC and DoD. Although these contracts are relatively limited in time frame and dollar value, NRO's plan is to "buy what we can" and, like the recent growth and operationalization of commercial EO/IR services, hope that some of these experiments will lead to operational capabilities.[133]

Although DoD's current direct procurement and use of commercial remote sensing data and services have been limited to date, we anticipate that this trend will change. There is a growing interest within DoD to pursue its own space-based ISR capabilities to support tactical military users.[134] As part of that effort, DoD is exploring acquisition of its own space-based ISR systems and leveraging commercial remote sensing services to meet military-unique requirements. If the military invests in space-based tactical ISR sensing services in addition to NRO-provided capabilities, then the level of funding for commercial remote sensing services may grow.

However, there are several risks or constraints that may impede future growth of DoD use of commercial remote sensing.[135] The commercial remote sensing market has been changing rapidly in recent years.[136] Because of this rapid change, the future size of the remote sensing market and financial viability of emerging providers or systems are uncertain. Additionally, investments in ground infrastructure associated with processing, exploitation, and dissemination may be needed to fully leverage the volume of data offered by commercial remote sensing services on an operationally relevant timeline.

For instance, intelligence exploitation has historically been a highly time-consuming manual process. Although the IC is working to automate and augment its workflows through software,[137] commercial remote sensing satellites generate huge amounts of data.[138] To justify investment in commercial data providers, the IC will likely need to improve its processing, exploitation, and dissemination infrastructure, such as by increasing software-based analytic capabilities into its workflows (including commercial analytics within the IC processes and capabilities). Lastly, if policy decisions are made that constrain the military's ability to invest directly in space-based remote sensing, that might impede the growth of DoD's use of those services. There is an ongoing debate about the future roles and responsibilities for space-based ISR between DoD and NRO, which has traditionally executed this mission.[139] How this debate plays out may also influence DoD's demand for commercial remote sensing services.

---

[133] C. Todd Lopez, "Allies, Partners Central to U.S. Integrated Deterrence Effort," *DOD News*, March 1, 2023.

[134] A debate about the future roles and responsibilities of space-based ISR is ongoing.

[135] Like the positive drivers, we focus here on risks and constraints that do not span all space mission sets. For example, limited funds need to be balanced between government and commercial investment for all space missions, which may constrain commercial growth.

[136] Yonekura et al., 2022; Harrison and Strohmeyer, 2022.

[137] Josef S. Koller, *The Future of Ubiquitous, Realtime Intelligence: A GEOINT Singularity*, The Aerospace Corporation, August 2019.

[138] In 2017, the then–NGA director estimated that, in roughly five years, the agency would be dealing with a million times more geospatial data. See Robert Cardillo, transcript of remarks at the 2017 GEOINT Symposium, National Geospatial-Intelligence Agency, June 5, 2017.

[139] Peter Suciu, "How the Space Force Is Planning to Use Commercial Satellites," *National Interest*, February 19, 2022; Theresa Hitchens, "First Joint Pentagon-Intel Community Space ISR Needs Assessment Nears Completion," *Breaking Defense*, June 3, 2022b.

Environmental Monitoring

Joint Publication 3-14 uses the term *environmental monitoring* to summarize tasks that space assets and operations are required to perform to collect information on weather phenomena, both within and beyond Earth's atmosphere.[140] Weather affects DoD operations in ways too numerous to review or summarize, and information on weather effects can change the outcome of military operations.[141] Precursors to DoD have been collecting information on weather operations in support of U.S. military efforts for more than 200 years.[142] Our discussion here, and the requirements underpinning our analysis, are limited to terrestrial and space weather data collection performed from space and may not capture the full scope of DoD requirements for terrestrial and space weather data from all sources.[143] Similarly, we do not discuss the overall commercial market for weather data collection, forecasting services, or analysis in detail; we limit our discussion to the commercial market for terrestrial and space weather data derived from space-based sensors.

Current DoD Use of Commercial SBEM

DoD collects terrestrial and space weather data from a family of civil, military, and international space assets, totaling nearly 50 orbital platforms that host a wide variety of sensors.[144] DoD makes limited use of commercial space-based environmental monitoring (SBEM) capabilities, although U.S. government needs and service requirements appear to dominate the commercial market. Instead, DoD has largely allowed civil U.S. government agencies to take the lead in incorporation of commercial services. This may be changing, however, because the USSF recently awarded a $17 million Small Business Innovation Research contract to a Boston-based start-up in support of a planned constellation of 32 mini-fridge-sized, radar-equipped satellites tasked to collect weather data.[145]

---

[140] Joint Publication 3-14, 2023.

[141] Weather can affect DoD operations in ways ranging from simple and at scale—such as the effects of heat and cold on soldier performance—to those that are specific and technical, such as the effect of precipitation on the dispersal and dilution of chemical weapon effects. A common and prominent class of effects includes limitations created by water vapor and particulate matter on sensor effectiveness, with implications for various weapon systems. See Richard A. Radvanyi, *Operations Eagle Claw—Lessons Learned*, United States Marine Corps Command and Staff College, AY 2000-01, 2002.

[142] Neal L. Triplett, *Evolution of Air Weather Service with Emphasis on Enlisted Participation*, research paper, Air University, August 1991.

[143] The term *terrestrial weather data* refers to meteorological and oceanographic data, and the term *space weather data* refers to data that characterize the conditions of the space environment (e.g., charged particles, radiation) around the Earth, resulting from solar activity (e.g., solar flares) and their effects on the Earth's atmosphere (Descriptions are based on subject-matter expertise and JP-3-14, 2023, p. IV-4).

[144] Government satellite assets available to DoD include those owned by the USSF (i.e., the EWS-G1 satellite [1] and the Defense Meteorological Satellite Program [12] satellite constellation); those owned by U.S. government civil agencies (i.e., the Windsat [1] and SNPP satellites [1] and the GOES [3] and EOS constellations [10]); those owned by international partners (i.e., the MSG series [Europe, 4], the Himawari-8 satellite [Japan, 1], and the MetOp satellites [Europe, 2]); and joint and coalition assets (i.e., the COSMIC constellation, [12]). See Michael Farrar and Adam DeMarco, "Air Force Space-Based Environmental Monitoring (SBEM) Update," briefing, Headquarters, U.S. Air Force, Directorate of Weather, February 28, 2020.

[145] Debra Werner, "Tomorrow.io Wins Air Force Funding for Weather Satellite Constellation," *SpaceNews*, October 1, 2021b.

NOAA and NASA have taken the lead in encouraging the development of a commercial SBEM market, primarily focused on space weather data. Both NASA and NOAA have cited legislation passed in 2017 and 2020 as impetus for their outreach to commercial service providers. The 2020 PROSWIFT Act's purpose is to encourage space weather monitoring and assigns prominent roles to NASA and NOAA for this task.[146]

NOAA's first pilot program for space-based commercial weather services began as a fairly small program, with a contract award of $1 million to two companies in 2016, and grew to a modestly sized program awarding an indefinite-delivery, indefinite-quantity contract valued at $23 million by 2020 (and again in 2023) to two companies.[147] A second pilot program began in 2022, offering contracts to companies that succeeded in prior pilots. Although the new pilot program's press release specifies "near-real time radio occultation measurements," the headline describes the data requested as "space weather data" for the first time, implying an expansion of the services performed by radio occultation data.[148] Meanwhile, NASA, which had previously supported SBEM companies with small contracts,[149] has released a request for proposal for commercial Earth observation data; the annual ceiling approaches $100 million. This effort could mark a significant increase in investment in commercial SBEM.[150]

Anticipated DoD Use of Commercial SBEM

The commercial market for SBEM is currently dependent on the U.S. government. The three companies that have successfully signed contracts with U.S. government agencies, especially the NOAA pilot and follow-on programs, are the primary players in the commercial SBEM market. These companies are GeoOptics, Spire Global, and PlanetIQ. GeoOptics' capabilities are based on its Community Initiative for Cellular Earth Remote Observation constellation, with second-generation satellites that began launching in 2022.[151] The constellation provides radio occultation data derived from GNSS signals in LEO that measure weather, atmospheric, surface, and oceanic conditions.[152]

Spire Global maintains a growing constellation of more than 100 multi-sensor nanosatellites capable of optical, multispectral, hyperspectral, and infrared imaging. The company's LEMUR constellation performs thousands of daily radio occultation measurements and atmospheric and

[146] Pub. L. 116-181, Promoting Research and Observations of Space Weather to Improve the Forecasting of Tomorrow Act, October 21, 2020.

[147] NOAA, Office of Space Commerce, "Commercial Data Program (CDP)," webpage, undated.

[148] Global Navigation Satellite System (GNSS) Radio Occultation (GNSS-RO) is a measurement method obtained by sending a signal from a GNSS satellite in high orbit to a LEO satellite at low orbit. The signal bends, or *occults*, because of the interference from refraction, influenced by temperature, humidity, and electron density. It seems that a potentially wide variety of measurements may be obtainable from GNSS-RO data. See Global Geodetic Observing System, "GNSS Radio Occultation," webpage, undated.

[149] Debra Werner, "GeoOptics Wins NASA Commercial SmallSat Data Contract," *SpaceNews*, November 15, 2022.

[150] Jane Edwards, "NASA Releases Solicitation for $476M Commercial SmallSat Data Acquisition Vehicle," *GovConWire*, March 22, 2023.

[151] Stephen Clark, "Live Coverage: SpaceX Launches Rideshare Mission, Lands Another Falcon Booster," *Spaceflight Now*, May 25, 2022.

[152] Jeff Foust, "GeoOptics to Launch Next-Generation Earth Science Constellation," SpaceNews.com, July 29, 2021.

oceanographic analyses.[153] PlanetIQ is in the process of launching the 20-satellite constellation of GNSS Navigation and Occultation Measurement Satellites (GNOMES), which utilizes GNSS-RO sensors and intends to provide terrestrial and space weather data. Three GNOMES are operational, and subsequent launches plan to incorporate a broader variety of environmental monitoring sensors.[154]

These three companies are the only ones to win any of the aforementioned NOAA contracts. These types of contracts tend to be relatively modest, with awards in the low millions of dollars payable over multiple FYs. In addition, GeoOptics and Spire Global have received the only prior NASA contracts for radio occultation data.[155]

Although these companies are industry leaders, they are not the only firms active in the SBEM market. Tomorrow.io and Orbital Micro Systems have received small contracts from the USSF and USAF, respectively.[156] Muon Space also received a contract from the Air Force Life Cycle Management Center and Defense Innovation Unit for atmospheric conditions and ionosphere measurements.[157] There may be additional private sector activity in this space, but little publicly verifiable information is available.

At the time of writing of this report, the SBEM market and its participants did not have capabilities that can fully meet DoD's validated requirements, shown in Table 5.1, further limiting the potential of commercial SBEM. DoD plans to support these requirements largely through its government-owned satellites and those of international partners. However, whether this approach will fully satisfy DoD's requirements given past challenges with acquiring SBEM satellites remains to be seen.[158]

Table 5.1. DoD Validated SBEM Requirements

Gap Priority	Description
1	Cloud Characterization
2	Theater Weather Imagery
3	Ocean Surface Vector Winds
4	Ionospheric Density
5	Snow Depth
6	Soil Moisture
7	Equatorial Ionospheric Scintillation
8	Tropical Cyclone Intensity

[153] European Science Center, "About Spire," webpage, undated.

[154] "PlanetIQ's GNSS Navigation and Occultation Measurement Satellite's (GNOMES) Successful Launch," Satnews.com, webpage, May 2, 2022.

[155] Werner, 2022; and NASA, "NASA Extends Contract with Spire Global for Satellite Data," NASA Earth Data, July 1, 2021.

[156] Debra Werner, "Orbital Micro Systems and Thomas Keating Forge Weather Data Pact," *SpaceNews*, October 5, 2021c.

[157] Muon Space, "Muon Space Awarded Additional Funding for Space Weather Data Collection," press release, July 11, 2023.

[158] Sandra Erwin, "A Race Against Time to Replace Aging Military Weather Satellites," *SpaceNews*, May 24, 2021.

Gap Priority	Description
9	Sea Ice Characterization
10	Auroral Characterization
11	LEO Energetic Charged Particle Characterization
12	Electric Field

SOURCE: Features information from USAF, *Department of Defense Plan to Meet Joint Requirements Oversight Council Meteorological and Oceanographic Collection Requirements*, report to congressional committees, August 2016.

The USSF has expressed strong interest in supporting its SBEM needs via commercial partners. The radio occultation data so far provided by the industry were initially viewed as a potential solution to Ionospheric Density (Gap 4) but may ultimately be used to fulfill other space weather data needs. It remains an open question whether remote sensing and earth observation satellite companies could or wish to provide the millimeter-wave and EO/IR sensing required for other requirements shown in the table. Given the general growth in the remote sensing industry, it seems plausible that, with sufficient upfront DoD incentives, the private sector could develop solutions to DoD's SBEM needs. However, the USSF must decide if this approach represents the most economically efficient, or otherwise preferrable, solution.

DoD's current use of commercial SBEM capabilities is minimal and primarily consists of GNSS-RO data. Despite this increased interest from NOAA and NASA, the commercial SBEM market remains a small portion of the overall remote sensing market. Furthermore, the data collected by commercial SBEM companies do not necessarily match up well with DoD's requirements for weather data (Table 5.1). Although it is possible that this could change over time, the small size and immaturity of the commercial SBEM market, and the competition that firms face from free data services, makes it unlikely that significant private sector–driven growth will occur without extensive DoD or U.S. government investment.

PNT

DoD has increasingly relied on PNT since its introduction in the late 1980s. DoD's PNT solution, GPS, is used for a myriad of military tasks, from tracking friendly forces as they maneuver to synchronizing frequency-hopping radios to providing guidance for precision guided munitions, and more.[159] The broad utility of PNT and GPS in particular is difficult to understate; it is a fundamental enabling capability that supports a wide variety of combat, combat support, and combat service support tasks across the joint force.

Despite ongoing investments to modernize and increase the resilience of GPS, however, DoD leaders believe that an alternative PNT solution that is independent of GPS is necessary to increase

[159] Karen Howard and Jon Ludwigson, *Defense Navigation Capabilities: DOD is Developing Positioning, Navigation, and Timing Technologies to Complement GPS*, U.S. Government Accountability Office, GAO-21-320SP, May 10, 2021b, p. 3.

the resilience of the capability overall.[160] Improved resilience is especially needed as peer competitors begin to understand the importance of GPS and other space-based capabilities to U.S. military operations and begin prioritizing them for disruption, denial, or outright destruction.[161]

At the same time, DoD is increasingly seeing the value of enhanced PNT capabilities that GPS cannot provide given limits of its underlying technology and architecture. Advanced technical capabilities, such as increased accuracy (down to less than 10 centimeters), faster time to first fix, and stronger signals that can penetrate dense urban or underground terrain, can improve and enhance PNT's utility across the joint force. These enhanced capabilities can also contribute to efforts to mitigate adversary efforts to target U.S. PNT capabilities.[162]

The confluence of these trends is driving DoD to examine a variety of alternative PNT solutions to complement GPS. Efforts such as improvements in inertial navigation systems are terrestrial in nature. Our research, however, focused on examining space-based capabilities.

Current DoD Use of Commercial PNT

DoD relies mostly on GPS for its space-based PNT needs. Commercial capabilities are limited and make up a minor fraction of the total DoD PNT use. Only Satelles is providing commercial space-based PNT capabilities. It uses the existing iridium commercial SATCOM constellation, which consists of 66 satellites in LEO. Satelles has been offering its satellite time and location services to DoD and other customers since 2016.[163] The Army has a limited partnership with Satelles, but this effort is largely focused on technology demonstration and conceptual development.

Anticipated DoD Use of Commercial PNT

In addition to Satelles, two U.S. firms are in the process of building their own constellations to provide GPS-independent PNT solutions in LEO: Xona Space Systems and TrustPoint. Xona Space Systems is planning a constellation of about 300 cubesats in LEO with a 2027 target for final operational capability.[164] It launched its first satellite in May 2022 and has completed a successful demonstration, via simulation, of its planned positional accuracy of less than 10 centimeters.[165] Less information is available about TrustPoint's planned constellation of microsatellites, but it did have its first successful launch in April 2023.[166] Although these capabilities aim to provide position and timing

---

[160] Howard and Ludwigson, 2021, p. 8.

[161] Howard and Ludwigson, 2021, p. 3.

[162] Wong et al., 2023, pp. 13–15.

[163] Satelles, "Global Coverage," webpage, undated.

[164] Matteo Luccio, "PNT by Other Means: Xona Space Systems," *GPS World*, July 5, 2023.

[165] Rachel Jewett, "Xona Broadcasts Demo PNT Signals, Certifies Constellation Simulator with Spirent," *Satellite Today*, May 31, 2023.

[166] Debra Werner, "TrustPoint Launches First PNT Cubesat," *SpaceNews*, April 15, 2023.

information independently of GPS, the two firms plan on initially providing GNSS augmentation services as they build out their full constellations.[167]

Adding a potential complication to the commercial PNT market, research has shown that it is possible to use signals from pLEO commercial SATCOM satellites as a source of GPS-independent position information.[168] This indicates that it is theoretically possible to use other pLEO commercial SATCOM constellations as an alternative to GPS. This is a potential additional service and source of income for pLEO companies and may have implications for the commercial space-based PNT market. This solution may also be of interest to DoD as it could mitigate the user equipment challenge that commercial PNT presents.[169]

Using our examination of the commercial space-based PNT landscape in this and prior research,[170] we conclude that there are limited prospects for stand-alone commercial PNT services to increase the overall capability and resilience of DoD's PNT capability. Thus, DoD will not substantially increase its use of space-based commercial PNT over the next few years. Better alternatives to commercial space-based PNT exist, and substantial policy and technological barriers will make it difficult to offer an alternative in the next decade. One potential exception would be if existing or in-progress LEO commercial SATCOM constellations are ultimately leveraged to provide commercial space-based PNT. The relative stability of the commercial SATCOM market makes it more likely that these services could be available to DoD in the near future.

Space Logistics

Space logistics has historically had a broad definition. According to the American Institute of Aeronautics and Astronautics, it is defined as "the theory and practice of driving space system design for operability and supportability, and of managing the flow of materiel, services, and information needed throughout a space system lifecycle." In the context of the commercial space industry, the space logistics market encompasses on-orbit services that support satellite operations from deployment to end of life.[171] On-orbit servicing capabilities, such as satellite refueling, inspection, and maintenance, fall into this market, as well as orbital change capabilities and the required infrastructure to support such activities.[172] This is a burgeoning area within the space industry. Commercial companies are working toward being able to provide these capabilities to support operations by commercial, civil, and military users in, from, and to the space domain, including those that would

---

[167] Debra Werner, "Startups Map Out Strategies to Augment or Backup GPS," *SpaceNews*, August 4, 2021a.

[168] Mark L. Psiaki, "Navigation Using Carrier Doppler Shift from a LEO Constellation: TRANSIT on Steroids," *NAVIGATION: Journal of the Institute of Navigation*, September 2021, Vol. 68, No. 3; Zaher (Zak) M. Kassas, "Navigation from Low-Earth Orbit: Part 2: Models, Implementation, and Performance," *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, Vol. 2, 1st ed., Wiley-IEEE Press, 2020.

[169] For further discussion of this challenge, see Wong et al., 2023.

[170] Wong et al., 2023.

[171] American Institute of Aeronautics and Astronautics, "AIAA Space Logistics Technical Committee," webpage, undated.

[172] Space logistics is also supported by many elements, including common design standards for valves and docking adaptors, grappling arms, and other technical widgets. However, though these elements are needed to enable a larger, robust, space logistics market, they do not constitute a robust market by themselves and are not included in the discussion of the space logistics market.

extend spacecraft life (e.g., through refueling, attachment of additional thrusters on-orbit, or hardware maintenance).

Current DoD Use of Commercial Space Logistics Services

DoD is not leveraging commercial space logistics services because of the nascent nature of this industry sector and the limited operational capabilities currently available. However, DoD is keenly interested in this capability and is planning demonstrations in the next five years, which we discuss in the next section.

Anticipated DoD Use of Commercial Space Logistics Services

The USSF leadership has indicated that space logistics is a priority. According to the Vice Chief of Space Operations, the service has been observing the commercial industry's growth in this area and views space logistics operations, such as in-orbit servicing and refueling as a "core capabilities" and a "strategic advantage."[173] The USSF is preparing today to use commercial capabilities in space logistics when they are available. It added a Space Access, Mobility and Logistics program under Space System Command's Assured Access to Space directorate in early 2023.

Today, the commercial space logistics market is technologically immature. Both the commercial sector and the U.S. government are in an experimental phase, working to develop technologies to support the array of space mobility and logistics activities (inspection, refueling, maintenance, orbit change, and others). Assuming that commercial space logistics capabilities continue to evolve and mature, DoD will likely expand its use of these services. The extent of the use will depend on the value of the services to DoD.

Both traditional contractors (e.g., Northrop Grumman through its SpaceLogistics subsidiary)[174] and start-ups (e.g., Orbit Fab, Astroscale, Tethers Unlimited, and Starfish Space) are working to develop space logistics capabilities. Several companies are beginning to execute technology demonstrations, with some counted as a success. SpaceLogistics completed two successful dockings of its mission extension vehicles with Intelsat GEO satellites to move them to other locations in February 2020 and April 2021.[175] Orbit Fab, a start-up with financial investment from both Lockheed Martin and Northrop Grumman, among others, has made progress on developing common interfaces and valves, such as its Rapidly Attachable Fluid Transfer Interface to enable the connection of servicing vehicles with satellites in space that can supply propellant to spacecraft in multiple orbits. It also launched a fuel depot in sun-synchronous orbit in 2021.[176] Although Orbit Fab does not yet have

---

[173] Sandra Erwin, "Space Force Eager to Harness Satellite-Servicing Technologies," *SpaceNews*, June 13, 2023b.

[174] Northrop Grumman, "SpaceLogistics," webpage, undated.

[175] A mission extension vehicle can dock to a GEO satellite with fuel near empty, then use its own thrusters to extend the vehicle's lifetime. SpaceLogistics is also developing the Mission Robotic Vehicle, which utilizes a robotic arm for on-orbit servicing activities, and the Mission Extension Pod, which is a smaller but similar version of the mission extension vehicle that would be able to provide satellite orbit control (Northrop Grumman, undated).

[176] Valerie Insinna, "Lockheed, Northrop, Invest in a Startup That Wants to Refuel Satellites in Space," *Defense News*, September 7, 2021.

any successful demonstrations of its technologies, in October 2022, the company received $13.3 million from the USSF to deliver fuel to four GEO military satellites beginning in 2025,[177] and closed a $28.5 million Series A funding round in April 2023. The company is also in partnerships with other companies, including Astroscale, whose orbital servicing satellites it will refuel in GEO.[178] Commercial innovation in areas that are driven by commercial needs (e.g., debris identification, tracking, repair) can be utilized for such DoD needs as mission extension, orbit transfer, RPO, SSA, SDA, and resiliency.[179]

The USSF is also providing clear support of technology development by the space mobility and logistics industry through SpaceWERX's Orbital Prime program. Between June 2022 and September 2022, AFWERX administered the program's 124 Small Business Technology Transfer Phase 1 contracts to 92 companies, including those engaged with 66 research institutions.[180] The 124 contracts come with a five-month term and are valued at $250,000 each. A portion of those companies will be invited to participate in a Small Business Technology Transfer Phase 2, with up to $1.5 million available per award. With such a large number of companies receiving awards in Phase 1, the USSF is actively supporting each of these companies and research institutions while allowing the industry to lead. This quasi-investor type engagement is an effective way to participate in the development of a market and technologies that are largely led by industry, while demonstrating that the USSF has interest in the success of the industry as a likely customer.

Other government agencies, such as the Defense Advanced Research Projects Agency (DARPA) and NASA, have also been developing space logistics capabilities and have planned demonstrations in the near term. DARPA's Robotic Servicing Geosynchronous Satellites vehicle is scheduled to launch for a GEO demonstration in 2024.[181] NASA's On-orbit Servicing, Assembly, and Manufacturing 1 (OSAM-1) spacecraft is scheduled for a polar-LEO demonstration around 2026, when it will service a Landsat 7 satellite and complete activities to perform servicing activity of OSAM by taking apart the satellite and refueling it. Its payload, Space Infrastructure Dexterous Robot, will also complete activities to perform assembly and manufacturing activities of OSAM, by assembling a communications dish and using additive manufacturing (3D printing) to produce a 10-meter beam.[182]

This broad interest from across the U.S. government and commercial sectors is an indication that the nascent space logistics market may continue to emerge over the next decade. Certainly, the space logistics market will continue to be in an experimental phase over the next ten years. Such companies as Astroscale that are planning to conduct debris removal activities for commercial and government customers will need to utilize on-orbit servicing and refueling provided by other space logistics commercial entities.

---

177 Jacqueline Feldscher, "Space Force Will Be One of the First Customers of a New Gas Station in Space," *Fast Company,* October 13, 2022.

178 Aria Almalhodaei, "Orbit Fab Closes $28.5M Series A for On-Orbit Refueling Capabilities," *TechCrunch,* April 17, 2023.

179 SpaceWERX, "Orbital Prime," briefing slides, undated.

180 Brian Holt, "SpaceWERX Awards 124 Orbital Prime Contracts," Air Force Research Laboratory, November 4, 2022.

181 Jane Edwards, "DARPA's Robotic GEO Satellite Servicing Tech on Schedule for 2024 Launch," *ExecutiveGov,* November 9, 2022.

182 Wendy Morgenstern, "Episode 91: OSAM-1," *Small Steps, Giant Leaps,* podcast, August 24, 2022.

However, prior RAND research found that the commercial satellite operators' outlook of space mobility and logistics capabilities is not yet decided. With longer lasting GEO satellites giving way to the proliferation of smaller satellites and satellite constellations, demand for repair and refueling may decline if it becomes cheaper to replace rather than repair or refuel satellites.[183] Because there is not yet a full-fledged market, more time and technology development are needed to determine whether a true space logistics market will develop.

The commercial space logistics market is still largely in development, and any further development that could be of use to DoD in the near term would be valuable in efforts to build up the market and become an early customer. These services, especially on-orbit servicing capabilities, which are developing quickly, would be of value to the USSF if they move beyond early technology demonstrations to be commercially offered services in the future.

Summary Assessment

Commercial remote sensing is the most technically mature market with the most proven value to DoD of the space mission areas discussed in this chapter. However, despite its clear value, how DoD makes use of these capabilities is still emerging. All DoD use of these services occurs through coordination with the IC, and there are uncertainties about relevant policy decisions (e.g., future responsibilities and force structure for tactical ISR). Despite this uncertainty, it is likely that DoD use of commercial remote sensing will grow in the near term, but a lack of significant commercial demand means DoD should consider the trade-offs that come with anchoring this market.

The commercial SBEM, PNT, and space logistics markets are still evolving and still proving whether they can provide consistent value to DoD customers. There is a combination of uncertainty and potential for each of these markets.

The SBEM and PNT markets directly compete with data and services that are provided for free by the U.S. government (NASA, NOAA, and GPS), making the future of these markets the most uncertain. Their fates are dependent on different factors—SBEM on U.S. government investment and PNT on a combination of DoD and the potential for large commercial demand for highly accurate PNT signals (e.g., agriculture or automated vehicles). Space logistics, while not technologically advanced enough to be useful in the immediate and near term, may be incredibly valuable to DoD and commercial entities in the longer term. This market is one to watch and to be accounted for in current architectural and satellite manufacturing decisions and investments.

Overall, we anticipate that DoD will increase its use of the remote sensing and space logistics markets in the near- and long-term future, respectively. Whereas the SBEM and PNT mission areas will experience minimal growth in DoD use in the future. In any case, DoD must be mindful of the dynamics in these emerging commercial space markets and intentional in its decisions; DoD actions may have significant impacts on these emerging markets' growth and direction.[184]

---

[183] Yonekura et al., 2022.

[184] See Wong, 2023, for a more in-depth discussion on potential risks that DoD may face in leveraging immature markets and trade-offs that it should consider when investing in such markets.

PART II. ASSESSMENT OF POLICY TOPICS

Chapter 6

International Agreements and Organizations Governing Commercial Space Activities

When the space age began in the 1960s, the few leading national space actors came together with the international community to establish what became the Outer Space Treaty regime.[185] The Outer Space Treaty outlined rules for the peaceful use of space to which all parties agreed to abide by. Four additional space treaties followed the Outer Space Treaty, addressing the issues such as astronaut rescue and return, liability, space object registration, and activities on the moon and other celestial bodies.[186] However, the space operating environment has changed significantly since the late 1970s when the previous treaty entered into force.

As discussed in Part I of this report, commercial space activities are expected to increase in both new and established markets. Where once there were fewer than a dozen national government space actors, today there are more than 75 government space operators and hundreds of commercial space operators. As actors, on-orbit assets, and types of commercial space capabilities increase, governance plays a critical role in ensuring spaceflight safety and long-term space sustainability. Given this remarkable expansion of space activities that is expected to continue, Congress has expressed interest in governance mechanisms for commercial space activities.

Today, the international space legal environment is framed by the gaps between limited hard law mechanisms for regulating space activities and the pursuit of soft law or norms for space behaviors.[187] Although the space treaties regime represents an initial set of hard law, the focus of international legal efforts since the late 1970s has been on developing and propagating norms of behavior that are voluntarily accepted and that informally guide and influence actor conduct. Development of rules and

---

[185] United Nations, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 610 UNTS 205, January 27, 1967.

[186] United Nations, 1967; United Nations, Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 672 UNTS 119, April 22, 1968; United Nations, Convention on International Liability for Damage Caused by Space Objects, 961 UNTS 187, March 29, 1972; United Nations, Convention on Registration of Objects Launched into Outer Space, 1023 UNTS 15, January 14, 1975; United Nations, Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, 1363 UNTS 3, December 18, 1979.

[187] *Hard law* can be described as "an instrument that has a binding legal effect" that typically includes "mechanisms for interpretation, monitoring, enforcement, and dispute resolution and increases the damage or cost to state credibility for reneging or violating it." The term *soft law* is defined as "instruments that are nonbinding that facilitate state cooperation without the threat of enforcement." A *norm* is "a standard of appropriate behavior for actors with a given identity" and can be distinguished by two types: "regulative norms, which order and constrain behavior" and "constitutive" (see Bruce McClintock, Katie Feistel, Douglas C. Ligor, and Kathryn O'Connor, *Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity*, RAND Corporation, PE-A887-2, April 2021, p. 11).

norms for space, and particularly commercial space entities, is challenged by a fluid space environment that is increasingly "congested, contested, and competitive" because of rapid changes in technology and an explosion of actors.[188] Commercial actors from multiple countries increasingly provide space services to private and public customers from other states, including defense establishments. Even if not serving a military customer, many space services, such as communications, remote sensing, or on-orbit servicing, are dual purpose, if not dual use—serving both military and civilian users. Complicating the issue is that commercial satellites can carry commercial, military, and research payloads on the same satellite platform.

The legal uncertainty regarding commercial space entities is a result of ambiguous or outdated language in the existing treaty regime and weak or nonexistent international enforcement regimes. If a space operator—government or commercial entity—desired to press damage claims, it would face a lack of historical precedents, experiences, and fact patterns in international space law. Although commercial and inter-governmental efforts are underway to resolve this uncertainty, they are generally focused on specific issues, such as space debris, and still lack enforcement or liability mechanisms.[189] The result is that commercial space operators have few recourses for damages caused by parties from other countries.

International Treaties—Space Treaties Regime

When space exploration first became a pursuit of multiple countries in the early 1960s, the few leading space actors and the international community came together to develop a codified set of national responsibilities. This set of treaties between 1967 and 1979 came to be known as the space treaty regime (see Table 6.1). The Outer Space Treaty explicitly states that international law applies to space:

> States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding.[190]

Over 100 states are parties to the Outer Space Treaty; the United States, Russia, and China are parties of each space-related treaty, except for the Moon Treaty.[191]

[188] Douglas C. Ligor and Bruce McClintock, "Nasty, Brutish, and Short—The Future of Space Operations in the Absence of the Rule of Law: Addressing Congestion, Contestation, and Competitiveness in the New Space Era," *NATO Legal Gazette*, No. 42, December 2021, pp. 53–67.

[189] Articles XIV through XX of the Liability Convention provided for the creation of a standing Claims Commission, but the international community has never established it. The Liability Convention is the short name for United Nations, Convention on International Liability for Damage Caused by Space Objects (United Nations, 1972).

[190] United Nations, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 18 UST 2410, January 27, 1967, Art. III.

[191] United Nations, Office for Outer Space Affairs, *Status of International Agreements Relating to Activities in Outer Space*, A/AC.105/C.2/2022/CRP.10, January 1, 2022.

Table 6.1. Outer Space Treaty Regime

Treaty (short name)	Date	Total Parties	Key Elements
Outer Space Treaty	1967	110	• Outer space shall be free for exploration and use by all states • Outer space is not subject to national appropriation • States shall not place nuclear weapons or other weapons of mass destruction in orbit • States shall be responsible for national space activities whether carried out by governmental or nongovernmental entities • States shall be liable for damage caused by their space objects
Rescue and Return Agreement	1968	96	• States shall take all possible steps to rescue, assist, and return astronauts in distress as well as recover and return objects launched into outer space
Liability Convention	1972	95	• A launching state shall be absolutely liable to pay compensation for damage caused by its space objects on the surface of the Earth or in the atmosphere • In space, liability is determined by fault
Registration Convention	1975	67	• States are required to establish national registries for their space objects and provide this information to the United Nations Register
Moon Agreement	1979	18[a]	• Moon and its natural resources are the common heritage of mankind and that an international regime should be established to govern the exploitation of such resources when exploitation becomes feasible

SOURCE: Features information from United Nations, 1968; United Nations, 1972; United Nations, 1975; United Nations, 1979.

[a] United States, Russia, and China are not parties.

Regarding commercial companies, the Outer Space Treaty departs from traditional international legal doctrine by making states responsible for nongovernmental entities in space.[192] When the Outer Space Treaty was developed, commercial space actors were few and predominantly supported government missions. Through Outer Space Treaty Article VI, state parties have a duty to authorize and supervise the activities of commercial entities from their states.[193] Specifically, Article VII of the Outer Space Treaty and Article I of the Liability Convention designate the responsible state parties that can be held internationally liable as the *launching state*. A launching state is a state that launches the space object or procures the launch of a space object, or a state from whose territory the object is launched.[194] Through Article VIII of the Outer Space Treaty, only one of these launching state parties will be the registry state, giving that state party jurisdiction and control over the space object in

[192] Brianna Rauenzahn, Jasmine Wang, Jamison Chung, Peter Jacobs, Aaron Kaufman, and Hannah Pugh, "Regulating Commercial Space Activity," *Regulatory Review*, June 6, 2020.

[193] United Nations, 610 UNTS 205, 1967, Art. VI, VII, VIII.

[194] United Nations, 961 UNTS 187, 1972, Art. 1(c).

space, which is typically the state party that operates the space object in space. That the space governance regime applies only through states was a compromise forced during deliberations by the Soviet Union delegation, who considered corporations a subset of national activities.[195] The result is a legal regime in which member states are responsible for governing the activities of commercial entities in space.

Since the development of the space treaties, the number of commercial space actors and the scope of their activities have grown dramatically as technology and space services evolved. Now populated by a multitude of government agencies (civilian and military), multinational companies, start-ups and universities, space actors and experts have called for revisiting the space treaty governance model.[196] Several nongovernment initiatives have sought to expand and clarify rules governing commercial and military use of space.[197] However, the space treaty regime remains the only existing hard law specifically governing commercial space activities. If a commercial company violates any treaty to which its host nation is a party, that host nation *could* face international repercussions. Many countries with well-developed space programs have created internal systems of regulation and licensing to govern commercial entities and prevent safety hazards.

International space law is insufficiently mature to determine the scope of liability or rules of causation in instances of damage to property in space. The Outer Space Treaty and Liability Convention only allow state governments to press damage claims on behalf of commercial companies against the responsible state. Adding more complexity to the issue of liability, today it is not uncommon for a commercial space object to be launched from one state, registered by another state, operated by a command center residing in a different state, and delivering space services for multiple governments or national domestic markets. Although Article VII of the Outer Space Treaty and the Liability Convention provide a liability framework, the adjudicative processes and procedures to determine fault remains undefined and undeveloped. The Liability Convention clarifies the damage claim process, but essentially limits its practical application given that it articulates principles as opposed to detailed rules and procedures.

Between the Outer Space Treaty and the Liability Convention, there is no established legal entity to resolve disputes or conflicts related to activities in space that result in damage to a space object, and there is no established mechanism for commercial entities to press claims of liability beyond their host nation government officials. If a state party, on behalf of a commercial party, determines that another state or a national entity within that state is liable for damages to its space object, there is no formal way to ensure cooperation and resolution of that claim. Instead, both states must agree on an adjudication through diplomatic negotiation and/or by a Claims Commission, created on a case-by-case basis. Each case would be fact dependent, with potentially multiple states being jointly liable depending on what state launched the object, registered the object, authorized or supervised the object, operated (or controlled) the object, or owned the object. If diplomatic negotiations or a Claims

---

[195] David A. Koplow, "Reverse Distinction: A U.S. Violation of the Law of Armed Conflict in Space," *Harvard National Security Journal*, Vol. 13, January 7, 2022, p. 58.

[196] William Welser IV, "The Democratization of Space," *RAND Blog*, March 28, 2016.

[197] See The Hague Institute for Global Justice, *The Washington Compact on Norms of Behavior for Commercial Space Operations*, July 4, 2022. See also Ram S. Jakhu and Steven Freeland, eds., *McGill Manual on International Law Applicable to Military Uses of Outer Space:* Vol. I*, Rules*, Centre for Research in Air and Space Law, 2022.

Commission finds liability, the state deemed to be liable would be required to pay compensation in the amount determined through those negotiations or a Claims Commission adjudication.

Although the United Nations does not provide mechanisms for space dispute resolution, United Nations bodies have become the primary international forums for discussion of international space laws, nonbinding rules, voluntary guidelines, and norms. The United Nations Committee on Peaceful Uses of Outer Space (COPUOS) is the principal United Nations body that brings together country representatives in regular meetings to discuss international space issues. Working with its members over the past two decades, COPUOS published space debris guidelines (2007) and long-term sustainability guidelines (2019). Additionally, the United Nations General Assembly established the Open-Ended Working Group on Reducing Space Threats to specifically focus on "reducing space threats through norms, rules and principles of responsible behaviors."[198] COPUOS and the Open-Ended Working Group are the principal forum where such states as the United States, China, Russia, and others lodge complaints and make declaratory statements regarding their space policies. Although useful as a forum for signaling country positions, COPUOS and the Open-Ended Working Group have not resolved many of the conflicting interpretations of the space treaties or international norms in space (e.g., debris mitigation, harmful interference, congestion, resource mining).

U.S. Government Role

Because national governments are designated as the sole mediators for commercial entities under existing international space law, how the U.S. government plays this role significantly influences the investment risk profile for commercial entities. Since the space treaties came into effect, the U.S. government has played an increasingly significant legal and policymaking role, beginning with the development of an expanded body of laws, regulations, and national space policy directives.[199] A main theme of U.S. law policy has been to promote and protect the growth of the U.S. space sector.[200] Space Policy Directive-2 (2018) streamlines regulations on the commercial use of space by calling on the executive branch agencies to "review existing regulations and ensure rules are not duplicative while also promoting economic growth, advancing national security and foreign policy goals, and encouraging U.S. space commerce leadership."[201] Space Policy Directive-5 (2020) encourages public-private cooperation by directing government space operations and the commercial space industry to work

198 United Nations, "Reducing Space Threats Through Norms, Rules, and Principles of Responsible Behaviours," A/RES/76/231, adopted December 24, 2021.

199 See, for example, U.S. Code, Title 51, National and Commercial Space Programs; and Code of Federal Regulations, Title 14, Aeronautics and Space. See also Office of the President, 2020.

200 For example, U.S. Code, Title 51, National and Commercial Space Programs; Section 50903, General Authority. According to this section of policy,

> [i]n carrying out this chapter, the Secretary shall—(1) encourage, facilitate, and promote commercial space launches and reentries by the private sector, including those involving space flight participants; and (2) take actions to facilitate private sector involvement in commercial space transportation activity, and to promote public-private partnerships involving the United States Government, State governments, and the private sector to build, expand, modernize, or operate a space launch and reentry infrastructure.

201 White House, "Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space," presidential memorandum, May 24, 2018.

together to protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations.[202]

U.S. government space law, regulation, and policies are implemented through the Federal Aviation Administration, the Department of Commerce, Federal Communications Commission, and DoD. The Federal Aviation Administration regulates launch, reentry, and airworthiness of space objects. The Department of Commerce regulates Earth remote sensing from space, promotion of the U.S. space industry, and export controls on space technology. In 2025, the Department of Commerce, through the NOAA, will assume responsibility from DoD for SSA and space traffic management of civilian space objects. The Federal Communications Commission regulates SATCOM and coordinates with the International Telecommunications Union (ITU) through licensing (discussed further in the following section).[203]

Although DoD is relinquishing some government responsibilities, its role has become more ambiguous and potentially more expansive given its new charge to "protect space assets and their supporting infrastructure."[204] One of the reasons that U.S. space policy remains in a state of flux and uncertainty is because there is no shared government-commercial understanding of the parameters, mechanisms, and limits of U.S. government protections for U.S. commercial space entities, either through international governance or DoD protections.

On the international scene, the U.S. government approach has been to focus on establishing norms that foster a more predictable and stable environment in space rather than pursuing treaties or other customary international law solutions. In theory, norms should help both the U.S. government and U.S. commercial space actors by providing assurances to commercial entities while allowing states to distinguish between hostile behavior and intent more easily. The State Department has pursued norm-building, primarily by announcing a norm that the United States will follow and then encouraging other states to make similar declarations.

The first example of this approach occurred in 2021, when Secretary of Defense Lloyd J. Austin III signed a formal memorandum with five tenets of responsible space behavior for DoD to follow that included limiting generation of long-lasting space debris, avoiding the creation of harmful interference (although neither term was defined), and notifying other parties of hazards.[205] The United States and the United Kingdom expanded on this approach with complementary norm asserting statements at Open-Ended Working Group meetings in 2023.[206] However, norm building can also occur implicitly by nonaction, particularly when the United States and other states fail to respond to a hazardous or undesired behavior. Beyond the issues of international space traffic management and debris

---

202 White House, "Memorandum of Space Policy Directive-5—Cybersecurity Principles for Space Systems," presidential memorandum, September 4, 2020.

203 Daniel Morgan, *Commercial Space: Federal Regulation, Oversight, and Utilization*, Congressional Research Service, R45416, November 29, 2018.

204 White House, 2020.

205 Lloyd J. Austin III, "Tenets of Responsible Behavior in Space," memorandum from the Secretary of Defense to the secretaries of the military departments, July 7, 2021.

206 UK Mission to the WTO, UN and Other International Organisations (Geneva), "Exchange of Views on the Outcome of the First Session and Outlook Towards the Second Session," United Nations, Office of Disarmament Affairs, May 13, 2022; U.S. Mission to International Missions in Geneva, "U.S. Statement to the Open-Ended Working Group on Reducing Space Threats," January 30, 2023.

prevention, increasing debate surrounds norms regarding military targeting of commercial space actors, which the next chapter addresses.

International Cooperation Among Commercial Companies

As commercial and national space activities increased, other entities have attempted to develop norms governing space—usually focused on specific topics over general rules. The most prominent of these efforts is the ITU, which is a specialized United Nations agency and a product of the International Telecommunication Convention. ITU coordinates satellite radio frequency allocations and geosynchronous orbital slots. For commercial space operators who serve civilian and government customers, the ITU is an example of how operators interact with space governance at the international level and the limits of their protections from damage or loss caused by other parties.

ITU

The ITU is made up of members from 193 countries and representatives from more than 700 telecommunications companies. It is an agency branch of the United Nations that oversees coordinating and assigning frequencies for the global radio network and coordinating and designating orbital slots for geo-orbit satellites. The ITU also regulates, controls, and standardizes the development of international internet communications.

As a regularly meeting international agency with established coordination processes, the ITU provides a forum for cooperation among member states. National regulatory authorities in different states are coordinated and guided by ITU activities. Commercial SATCOM systems must work through their national governments with the ITU to prevent frequency interference with other communications networks. Each state is responsible for ensuring its satellite operators follow rules and conditions outlined in ITU's radio regulations. In the United States, the Federal Communications Commission is the national regulatory authority for ensuring commercial company compliance with ITU regulations. However, in the case of disputes over frequency usage, the ITU has no authority to force a settlement.[207] The ITU Constitution does not address cyberattacks, and it explicitly recognizes that states have freedom of action when their security is threatened. ITU provisions do not apply to member states' national defense or military radio installations, although some states—particularly NATO members—seek to comply.[208]

Commercial and Industry Associations

As hazards, frictions, and threats have grown in an increasingly congested and ungoverned space environment, commercial space operators have found a shared interest in advocating for common best

---

[207] Roscoe M. Moore III, "Business-Driven Negotiations for Satellite System Coordination: Reforming the International Telecommunication Union to Increase Commercially Oriented Negotiations over Scarce Frequency Spectrum," *Journal of Air Law and Commerce*, Vol. 65, No. 1, 1999.

[208] As mentioned in NATO, "NATO Joint Civil/Military Frequency Agreement (NJFA)," Extract for Public Disclosure 2014, February 14, 2017.

practices for space operations. Several commercial consortiums have formed to advocate common standards, policies, and norms of space behavior that support commercial interests, including collision avoidance, space traffic management, RPO, and debris prevention. However, commercial consortiums also frequently lobby against additional regulations. These consortiums often have overlapping membership rosters, with U.S. space companies often playing a leading role. These space industry associations frequently play a role as interlocutor for commercial space companies with the federal government in developing space governance—including SDA, federal regulations, and international norms of behavior. A common theme among these industry associations is the desire for increased collaboration between the U.S. federal government and commercial companies in addressing these issues.

Summary Assessment

The Outer Space Treaty regime represents the strongest set of hard law mechanisms that govern the behavior of commercial and government operators in space. The Outer Space Treaty makes participating host nations responsible for the behavior of their commercial space owners and operators; however, the regime has weak or no international enforcement mechanisms. Additionally, the Outer Space Treaty is dated, and current international governing efforts focus on developing and propagating norms of behavior that are voluntary. Absent clear international norms and guidance, commercial operators are working together to establish their own operational guidelines. During conflict, the existing international space forums are likely to have little impact on restraining aggressor behavior.

Chapter 7

Question of Commercial Satellites as Legitimate Military Targets

Commercial satellites used to support military operations are widely considered to be legitimate military targets. Although international law does not make an explicit declaration regarding commercial satellites, experts from the policy, legal, and military realms have come to this view based on both practicalities and their interpretation of existing international law. The principal adversaries of the United States (Russia and China) generally do not recognize a distinction between commercial and military satellites. Most Russian and Chinese space organizations are a fusion of civil and military activities. Perhaps the more contentious issue—and one about which there is considerable debate—is what would constitute a necessary and proportionate military attack against a commercial space asset and what types of attacks might be considered a violation of international law by the international community.

Lack of common understanding of rules of engagement among the international community became evident in the early phase of the Russia-Ukraine conflict when Russia launched a denial of service cyberattack on Viasat's SATCOM network to disrupt Ukrainian C2 and attempted to jam SpaceX's Starlink SATCOM services used by Ukrainian forces.[209] Addressing policy and legal issues surrounding commercial satellites as legitimate military targets is becoming increasingly important as DoD increases its use of commercial systems for military operations, especially during a time of conflict, which could further increase risks to commercial systems.

Current Debate on Commercial Space Support to Military Operations During Conflict

Existing international *space* law has little to say about the use of commercial satellites supporting military operations. As discussed in Chapter 6, the Outer Space Treaty advocates for "the exploration and use of outer space" for all countries and does not preclude military activities in space. [210] Rather, Article IV commits state parties to "undertake not to place in orbit around the Earth any objects carrying nuclear weapons or other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station weapons in outer space in any other manner" and that the "moon and other

[209] Manson, 2023; Duffy, 2022.

[210] United Nations, 18 UST 2410, 1967, Art. 1.

celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes."[211] Instead, when considering the use of commercial satellites in support of military operations, most space legal analysis draws on the Law of Armed Conflict and Law of Neutrality.

DoD officials have refrained from making public comments about the implications for commercial space operators that support military operations during conflict.[212] But many legal scholars of the topic of mixed-use satellites agree that commercial spacecraft supporting military objectives lose their protected civilian status and can be legally targeted.[213] This entanglement is further complicated by the growing infeasibility of segregating commercial space services from those being used for military applications.[214] In part, this finding rests on acknowledgment that a state's inherent right of self-defense extends to actions against space activities supporting military attacks.

In that context, several legal regimes apply to *military operations in space*: the United Nations Charter, the space treaty regime, the Law of Neutrality, and the Law of Armed Conflict.[215] The United Nations Charter governs the lawfulness of the resort to force between states. Although it prohibits the threat or use of force, and mandates member states to settle their international disputes by peaceful means, it also recognizes the "inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[216] The space treaty regime recognizes the common interest of mankind in the exploration and use of outer space by all nations—a legally binding principle that bears on military activities in space.[217] The Law of Neutrality regulates relations between belligerent states and neutral states in times of armed conflict and serves to mitigate and contain the adverse effects of a conflict.[218] Finally, the Law of Armed Conflict establishes limits on the right of belligerents to choose means and methods of warfare and rules on the conduct of hostilities to protect civilian populations, as well as civilian objects from dangers arising from military operations.[219]

---

[211] United Nations, 18 UST 2410, 1967, Art. 4. The treaty further states regarding celestial bodies:

> The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the moon and other celestial bodies shall also not be prohibited.

[212] Christian Davenport, "Commercial Satellites Test the Rules of War in Russia-Ukraine Conflict," *Washington Post*, March 10, 2022a.

[213] International Committee of the Red Cross, *Constraints Under International Law on Military Operations in, or in Relation to, Outer Space During Armed Conflicts*, May 3, 2022. According to International Committee of the Red Cross (2022, pp. 2, 4): "Many of these civilian satellites, or some of their payloads, may also serve armed forces, and are therefore of a dual-use nature, which may make them military objectives"; the same article noted, "Direct attacks against civilians or civilian objects, including civilian space objects are prohibited. No space object nor any of its constituent parts may be attacked, unless and for such time as they would be military objectives." See also Koplow, 2022, pp. 38, 102–103. See also a discussion of mixed-use and hosted payloads in Koplow, 2022, pp. 79–82.

[214] Cassandra Steer, "Application of International Humanitarian Law/Laws of Armed Conflict in Space: Civilians and Neutral States," 5th Session of the Open-Ended Working Group, United Nations, Office of Disarmament Affairs, May 11, 2022, p. 4.

[215] International Committee of the Red Cross, 2022, p. 3.

[216] United Nations, Charter of the United Nations, 1 UNTS XVI, October 24, 1945, Ch. VII, Art. 5.

[217] United Nations, 18 UST 2410, 1967, Art. 3.

[218] Hague Convention, (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, October 18, 1907.

[219] International Committee of the Red Cross, Convention (IV) Relative to the Protection of Civilian Persons in Time of War, August 12, 1949.

Notwithstanding international law, Russia and China have been forthright about their intent to treat civilian and commercial space assets supporting military operations as military targets. In the United Nations Open-Ended Working Group on Reducing Space Threats, Russia criticized Western use of commercial satellites as an "extremely dangerous trend . . . [and that] quasi-civilian infrastructure may become a legitimate target for retaliation."[220] When discussing commercial companies assisting Ukraine in the conflict with Russia, Chinese officials have publicly indicated that they would target commercial assets if they were used to assist Taiwan in a similar crisis.[221] However, in the Open-Ended Working Group, China tends to take a less aggressive approach, advocating for eliminating any ambiguity regarding the use of commercial assets and protecting the rights of developing countries.[222] Russian and Chinese actions suggest that their governments are preparing to fight a conflict in space.[223] Although arguments based on the Law of Armed Conflict will likely not deter adversaries from military responses in space, they may help the United States forge globally accepted norms that encourage belligerents to avoid attacks that cause widespread hazards for the broader international spacefaring community.

Applicability of Law of Armed Conflict to Space

Even if commercial space assets directly supporting military operations can be legitimately targeted in principle, there are still widely recognized limits grounded in the Law of Armed Conflict on *how* they can be targeted. Three dimensions of this law particularly apply to military operations in space during conflict—distinction, neutrality, and proportionality. When the principles of distinction and proportionality were codified in the Geneva Conventions following World War II, the issue largely concerned aerial bombardment, maritime interdiction, artillery shelling, and ground assaults against military targets intermixed among civilian populations (e.g., combatants fighting inside a city or religious site) or dual-use civilian-military targets (e.g., bridges, power plants, dams, rail networks, fuel

---

[220] See Konstantin Vorontsov, "Statement by Mr. Konstantin Vorontsov, Deputy Head of the Delegation of the Russian Federation, Deputy Director of the Department for Non-Proliferation and Arms Control of the Ministry of Foreign Affairs of the Russian Federation, at the Thematic Discussion on Outer Space (Disarmament Aspects) in the First Committee of the 77th Session of the UN General Assembly," unofficial translation, *Journal of the United Nations*, October 26, 2022. Several news articles discuss escalating Russian rhetoric, including an article about Russia threatening to attack Starlink. See Christian Davenport, "Russia Threatens Commercial Satellites That Pentagon Sees as Its Future," *Washington Post*, October 28, 2022. See also Sandra Erwin, "Russia Escalates Rhetoric on Commercial Satellites, Calls Them 'Legitimate Targets for Retaliation,'" *SpaceNews*, October 27, 2022b. For an article that references Vorontsov's comment, and the White House response that any attack on a commercial U.S. satellite would provoke a response from the United States, see Miriam Kramer, "Commercial Satellites are the Next Front in Space War," Axios, November 1, 2022. Vorontsov's comments originate from the second session of the Open-Ended Working Group, see Vorontsov, 2022. For articles quoting Russia's Konstantin Vorontsov, Deputy Director of Russian Foreign Ministry Department for Non-Proliferation, see Erwin, 2022b; and Davenport, 2022b.

[221] Thomas Novelly, "Citing Growing Threat from China, Space Force Leaders Say They Need More Money," *Military.com*, October 28, 2022.

[222] Permanent Mission of the People's Republic of China to the United Nations Office at Geneva and other International Organizations in Switzerland, "Remarks by H. E. Amb. Li Song on Topic 2 (Earth-to-Space Threats) at the Second Substantive Session of the Open-Ended Working Group on Reducing Space Threats," Open-Ended Working Group, United Nations, Office of Disarmament Affairs, September 14, 2022. China argued that rules are needed to avoid potential misinterpretation and conflict escalation. China also argued that commercial space enterprises should be required to properly use telecom-spectrum and orbital resources so as to not undermine the rights of developing countries to peaceful uses of space.

[223] Defense Intelligence Agency, 2022.

supplies). Although the Law of Armed Conflict is generally seen as extending to outer space, the actual implications of distinction and proportionality are likely to be tested by complicated dual-use arrangements for space launch and space services.[224] Finally, reversibility is a fourth dimension particular to warfare in space, cyberspace, and the electromagnetic spectrum that bears significantly on calculations of proportionality.

Distinction

According to the Law of Armed Conflict, the principle of *distinction*—distinguishing between objects that are clearly nonmilitary—always applies as a limit to the use of force against an entity.[225] If a commercial asset is clearly nonmilitary and can be segregated from military usage, under the Law of Armed Conflict it must not be attacked.[226] However, the issue of distinction is further complicated by the question of whether dual-use space assets should be treated differently from dual-purpose ones. A dual-use space asset is one that could potentially be used for military or civilian purposes, while a dual-purpose space asset is one that is currently being used.[227] By the Law of Armed Conflict, dual-purpose space assets are valid targets during war because the object is concurrently supporting military objectives. An even grayer area is whether dual-use assets are valid targets.[228] The debate about dual-use assets has a temporal element: Is the asset at a potential time of attack supporting or capable of supporting a military objective?[229]

The Law of Armed Conflict defines *military objectives* as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[230] Specific to the space domain, recent international efforts have defined *military space activities* as those "of a military character," which require considering "the actors involved in the

---

[224] Bryan Frederick and David E. Johnson, *The Continued Evolution of U.S. Law of Armed Conflict Implementation*, RAND Corporation, RR-1122-OSD, 2015, pp. 70–75.

[225] "Indiscriminate attacks, namely those of a nature to strike military objectives and civilians or civilian objects without distinction, including civilian space objects, are prohibited" (see International Committee of the Red Cross, 2022, p. 5).

[226] "Distinction is directed at the attacker's intentions and judgments: the only legally-authorized goal is to weaken the enemy's warfighting capabilities" (Koplow, 2022, p. 31).

[227] Almudena Azcarate Ortega, "'Reducing Space Threats Through Norms, Rules, and Principles of Responsible Behaviours,' Topic 3: Current and Future Space-To-Space Threats by States to Space Systems," working paper, Open-Ended Working Group, United Nations, Office of Disarmament Affairs, September 14, 2022, p. 3.

[228] There is an ongoing debate in U.S. policy circles about whether space should be designated as a separate critical infrastructure sector (in addition to the current 16 sectors) and whether such a designation has implications for making the U.S. civilian space architecture a legitimate military target. However, designation as a U.S. critical infrastructure sector would not automatically make that sector a legitimate military target (e.g., agriculture and food; health care and public health). Ultimately, the key question that will remain is whether a dual-use asset is a legitimate military target. For discussion of space as a critical infrastructure sector, see Sarah Fortinsky, "Bipartisan Bill Designates Space as Critical Infrastructure Sector," *The Hill* blog, July 27, 2023.

[229] Koplow (2022, p. 38) states that

> [t]o the extent that a person or object provides an effective contribution to the military action of the other side, it may sacrifice its protected status, but the borderline judgment calls become ineffably controversial.

[230] International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949; and relating to the Protection of Victims of International Armed Conflicts (Protocol I)," June 8, 1977, Art. 52.

activity, the aims of the activity, and the effects of the activity."[231] Conversely, once a mixed-use satellite loses its protected status and becomes a valid military target, then associated ground control and launch facilities might also be considered legitimate military targets.[232] The same principle also applies when commercial space services—including launch services—are used to support military operations.[233]

One reason that DoD is interested in increasing integration of commercial space capabilities into its space architecture is to increase resilience, as discussed in Part I of this report. However, a few legal scholars have argued that the military has a "reverse distinction" legal responsibility to deliberately maintain separation between civilian and military purposes by not promoting commercial integration in its military space architecture.[234] As a principle, reverse distinction is not absolute, but it does require "best efforts to separate military and civilian assets," taking account of feasibility.[235] Critics of commercial-military integration, including the International Committee of the Red Cross, argue that this choice is not excused by considerations such as cost.[236] Although the United States has not signed the Geneva Conventions additional protocol that is the primary codification of reverse distinction (Article 58, Additional Protocol 1), the United States has acknowledged that many of its provisions are now considered custom.[237]

Other scholars contest the feasibility of segregating the entire military space architecture, particularly given the proliferation of dual-use commercial space capabilities. Communications, data transport, and SDA are all uses that make distinction extremely difficult to discern.[238] Furthermore, commercial-military integration of certain space activities is by far the most efficient means to achieve military and commercial objectives and is supported by widespread state practice.[239] Even opponents

[231] Jakhu and Freeland, 2022, Rule 105, p. 9.

[232] Koplow, 2022, p. 102.

[233] Koplow, 2022, pp. 79–83.

[234] According to Koplow, 2022 (p. 38), "To the extent that a person or object provides an effective contribution to the military action of the other side, it may sacrifice its protected status, but the borderline judgment calls become ineffably controversial." See additional discussions in Koplow, 2022 (p. 27), also on labeling the United States as an "offender" (pp. 31–32); discussing genesis of reverse distinction in Additional Protocol I of the 1949 Geneva Conventions (p. 96); contrasting U.S. practice in space to traditional terrestrial adherence to reverse distinction (p. 103); labeling commercial integration an "illegal act" (p. 103); and referring to this practice as "illegal, unwise, or both" (p. 105).

[235] Koplow, 2022, p. 28.

[236] Koplow, 2022, p. 95. See also International Committee of the Red Cross (2022, p. 5):

> All feasible precautions must be taken, notability in the choice of means and methods of warfare, to avoid, and in any event to minimize, incidental civilian casualties and damage to civilian objects . . . an obligation that States must already implement in peacetime . . . and working towards identifying space systems serving specially protected objects like hospitals and objects indispensable to the survival of the civilian population (drinking water, irrigation).

[237] John Goehring, "The Legality of Intermingling Military and Civilian Capabilities in Space," Lieber Institute at West Point, October 17, 2022, p. 3.

[238] Steer, 2022. See Goehring, 2022, p. 3.

[239] Goehring, 2022, pp. 2, 10, 11. Goehring (2022) cites Italy's and South Korea's use of SpaceX to launch military satellites; the United Kingdom's 2022 Defence Space Strategy calling for integration with commercial satellites; Australia's 2022 Defense Space Strategy (which extends to commercial ISR); France's 2019 Space Defence Strategy; and NATO's 2022 space policy, referencing the United States, Canada, and Finland permitting the use of commercial imagery in the war in Ukraine. Goehring (2022, p. 4) quotes the *Department of Defense Law of War Manual* and Article 14 of the Lieber Code in concluding that

of this position recognize that, in some cases, it is not possible for the military to avoid commercial infrastructure.[240] Ultimately, absolute segregation of military and commercial space assets for purposes of maintaining distinction is both impracticable and unverifiable.

Neutrality

The question of neutrality arises regarding space objects that remain under the jurisdiction of a neutral state—either the launching state, registering state, or operating state.[241] Legal reasoning is similar to the question of distinction: Is the neutral party's space object being directly used to serve the military purpose of a belligerent? One perspective is that a spacecraft that is privately owned by a commercial entity of a neutral government becomes a legitimate military target once it begins serving the military purposes of a belligerent, and the sponsoring state may forfeit its status as a neutral.[242] However, a corollary argument is that the attacker should still apply the principle of proportionality by weighing the impact and danger to neutral populations of an attack against this space asset's military value.[243]

Proportionality

Even after a space object is determined to be a legitimate military target, the principle of proportionality still places limits on *how* that space object or system may be attacked. The principle of proportionality flows from weighing the relative military value of an attack against its negative harm.[244] Most legal scholars accept that the rights of self-defense extend to space, but that there are limits to these rights due to unique characteristics of the space environment as a global commons without territorial contiguousness where the creation of hazards often has long-term effects that are very difficult to remedy or mitigate.[245] Interestingly, the Outer Space Treaty prohibits placing nuclear weapons in orbit, installing them on the moon or other celestial bodies, or stationing them in space, but the treaty does not specifically address them as a method of attack.[246] Ultimately, the question of method of attack returns to the principal tests of proportionality:

---

intermingling can be militarily necessary when required "to achieve a creditable and legitimate military requirement" and "achieve broad imperative of winning the conflict as efficiently as possible."

[240] For example, "On the other hand, there are certain important areas in which maintenance of a rigid, sustained separation between national security and civilian assets would surely not be regarded as 'feasible'" (Koplow, 2022, pp. 45–46).

[241] Steer (2022) interprets the provisions of the Outer Space Treaty Article II as precluding principles of neutrality. See also United Nations, 1967, Art. 2, which states: "Outer space . . . is not subject [to] national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."

[242] Koplow (2022, pp. 101–102) uses the example of the U.S. military relying on Swedish, Brazilian, or United Arab Emirates satellites and concludes that the legal neutrality of the sponsoring state may be jeopardized.

[243] Steer, 2022.

[244] International Committee of the Red Cross (2022, p. 5) states, "Disproportionate attacks are prohibited . . . which would be excessive in relation to the concrete and direct military advantage anticipated."

[245] Jakhu and Freeland (2022, p. 22) notes that Reference Rule 152 states that "the physical and legal characteristics of outer space must be taken into account in any exercise of a State's right of self-defence."

[246] United Nations, 1967, Art. 4.

- whether the attack "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated"[247]
- whether the attacker takes "all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[248]

The reality that almost any attack against objects in space involves minimal to no direct danger or loss of life or injury to civilians or even military personnel suggests that many attacks could be justified as a proportional response to military usage of commercial spacecraft. Kinetic attacks that generate debris fields, such as antisatellite missiles or deliberate collisions, must be weighed against the expected harm they create to other nonbelligerent and civilian space assets.[249] Another key question is which elements of the space infrastructure (e.g., elements of space, ground, or user segments and other supporting elements) does the principle of proportionality permit attacks and to what level of impact or destruction? For example, does the military use of a space infrastructure mean supporting ground stations can also be legitimately targeted? Again, the principle of proportionality applies in terms of military value of the attack against the civilian harm that might result.

The principle of proportionality also suggests downstream implications beyond debris that an attacker should consider. Even if space debris can be avoided using a soft attack, attacks on dual-use satellites could cause terrestrial harm to noncombatants, given the growing reliance of civilians on space for safety, commerce, and transportation—including such services as "navigation, communication, aviation, shipping, disaster response, search and rescue, banking and finance, tracking climate change, deforestation, identifying sites of mass atrocity."[250] One question is whether essential space services are legally shielded from being targeted. Similarly, although the International Committee of the Red Cross does not provide a designated list of protected essential services, it does designate objects to avoid damaging or destroying: "medical services, cultural property, hospitals, drinking water installations and supplies, irrigation networks, and other objects "indispensable to the survival of the civilian population."[251] The U.S. government could seek through declaratory policy and/or international forums to carve out international norms of protection for essential services. However, even with these norms, one would face the challenge of how an adversary might determine the distinction and what is appropriate in areas of overlap.

[247] International Committee of the Red Cross, 1977, Art. 51, 5b.

[248] International Committee of the Red Cross, 1977, Art. 57, 2b. Although the U.S. government is not a party to this treaty, commonly known as "Additional Protocol 1 to the Geneva Conventions of 1949," it accepts many provisions while taking issue with many others. The *Department of Defense Law of War Manual* includes an extensive analysis of how U.S. military forces assess proportionality and precautions that incorporate accepted U.S. government interpretations (see DoD, *Law of War Manual*, Office of the General Counsel, 2023, Sections 5.10–5.13).

[249] Steer, 2022.

[250] Steer, 2022, p. 1.

[251] International Committee of the Red Cross, 2022, pp. 5–6.

Reversibility

Considerations of proportionality and the appropriateness of attacking commercial space assets often lead to questions about reversible military space attacks. *Reversible attacks* are defined as those that are "nondestructive and temporary, and the system is able to resume normal operations after the incident."[252] Electronic warfare attacks, such as jamming or spoofing, are reversible. Directed energy weapons and cyberattacks can be reversible or permanent, depending on the severity. At one extreme, legal analysts argue that even reversible attacks are off limits where they affect essential civilian services.[253] Legal scholarship supports the opportunity that reversible attacks offer permissibility as a proportionate response to the use of commercial space objects for military purposes.[254] A further complication is the challenge of attribution. Such attacks as cyberattacks or radio frequency interference may be difficult to pinpoint to the perpetrating actor. The key point is that during conflict, reversible attacks—besides being often easier and cheaper to execute—provide a wide spectrum of legitimate options to belligerents for proportional attacks against space architectures. The cases of Starlink, Viasat, and others suggest that commercial space actors are already experiencing reversible attacks in their day-to-day operations.

Summary Assessment

The international legal context today supports a consensus that commercial assets supporting military operations are legitimate military targets—and DoD and the U.S. government need to plan for this eventuality. DoD and USSPACECOM policies are clear in their intention to use commercial integration on a wide-ranging and adjustable scale for space support to military activities, which risks making the entire U.S. commercial space infrastructure a legitimate military target.[255] What is lacking is a common understanding and rules of engagement about what constitutes a legitimate adversary military attack and a legitimate military response and how to protect commercial space operators providing vital services to the military.

---

[252] Defense Intelligence Agency, 2022, p. 3.

[253] Steer, 2022, p. 6. Also, for example, International Committee of the Red Cross (2022, p. 5) notes:

> All foreseeable direct and indirect incidental harm . . . attacking, destroying, removing or rendering useless objects indispensable to the survival of the civilian population is prohibited, these rules apply to . . . kinetic and non-kinetic . . . including operations that would disable them without damaging them physically . . . including when targeting dual-use space object that has become a military objective.

[254] Jack Beard, "The Principle of Proportionality in an Era of High Technology," in Willian C. Winston and Christopher M. Ford, eds., *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, Vol. 1, Oxford University Press, 2018, pp. 283–288.

[255] DoD Directive 3100.10, "Space Policy," Office of the Under Secretary Defense for Policy, August 30, 2022, p. 6. See also USSPACECOM, "Commercial Integration Strategy Overview," April 1, 2022.

Chapter 8

Commercial Awareness of Threats and Insurance Coverage Schemes

U.S. adversaries are likely to target commercial space systems that support armed forces operations. This reality presents a challenge for both DoD and the commercial space industry. Given the increasingly important role that commercial space systems will play in supporting armed forces operations, potential attacks on commercial systems are a major concern for the defense and intelligence communities. Commercial satellite owners and operators are wary of this risk because of the potential devastating impact that an attack on their assets could have on their businesses, depending on the severity of the attack.[256] In light of this emerging risk, defense and intelligence communities are holding close discussions with the commercial space industry to explore what actions the U.S. government could and should take to protect commercial satellite systems. The following two topics of interest to Congress are highly relevant to the protection of commercial space assets:

- whether owners and operators of satellites are aware that they may be targeted by potential adversaries
- what insurance schemes exist for commercial satellites that support armed forces operations.

Commercial Satellite Operator Awareness That They May Be Targeted

Commercial satellite operators are generally aware that they may be the targets of potential attacks by U.S. adversaries. Their awareness has become more heightened in recent years because of the attacks on Viasat's and SpaceX's communications systems in the Russia-Ukraine conflict and Russian and Chinese officials' public statements indicating that they would target commercial satellites (as discussed in Chapter 7). Following the cyberattack on Viasat, many companies began disclosing potential risks from foreign actors, particularly potential risks associated with purposeful electromagnetic interference and cyber and data management.[257]

[256] See Chapter 2 for a discussion on a range of anti-satellite weapons that can potentially be used against commercial satellites. Commercial space operators who may not be supporting armed forces operations may still be targeted because most commercial satellites can be dual use (see Chapter 7), and thus, U.S. adversaries are likely to assume they are supporting DoD missions.

[257] Our review of financial disclosure annual reports from 2019 through 2023 for eight commercial space companies (Inmarsat, Iridium, SES, Viasat, Intelsat, SKY Perfect JSAT, Mynaric, and Maxar) revealed that these commercial satellite operators often highlighted financial and supply chain risks to investors, including risks of relying significantly on the U.S. government for revenue, but they did not discuss potential risks of being targeted by a foreign actor until 2022 reports after the Viasat attack occurred.

However, the degrees of awareness that commercial satellite operators have about whether, how, or when their own assets might be specifically targeted, depends on the level and timeliness of their access to threat information. Threat information can vary in scope (breadth and depth) and time horizon (e.g., threat trends versus indications and warning), and not all commercial space operators have access to more-specific, -actionable, and -timely threat information. We summarize in Table 8.1 the most common information channels that are available to commercial operators to increase their awareness of being potentially targeted. This list of information channels is not intended to be comprehensive.

Table 8.1. Threat Information-Sharing Channels Available to Commercial Satellite Operators

Awareness Level	Examples of Threat Information Channel	Access Level
General awareness	Report in public domain on space threats (e.g., a Defense Intelligence Agency report, news media)	All
	Industry Day	All
	Space Information Sharing and Analysis Center	Paid subscription
	CIC	Contract with Combined Force Space Component Command
	Wargame (e.g., Schriever Wargame)	Invitation only
Near real time	Conjunction data message	All
	Notice to space operators	JCO distribution list
	CIC	Contract with Combined Force Space Component Command

SOURCE: Authors' analysis based on discussions with selected military organizations and commercial space operators from January 2023 through August 2023.

As shown in Table 8.1, information about general threat trends is widely available and there are no access restrictions. Publicly available reports, such as those released by the Defense Intelligence Agency, often describe antisatellite weapons that adversaries are developing (e.g., uplink and downlink jamming).[258] Such reports are not intended to provide specific threat information that would require a specific action from an operator. That said, understanding of counterspace capabilities could inform satellite operators' future capability development plans to mitigate their risks of being targeted (e.g., implementing resilience and cybersecurity measures).[259] Satellite operators and other space industry partners who are cleared to access classified information could also gain more detailed information about threats at Industry Day events hosted by government agencies, such as Space Systems Command and the Space Warfighting Analysis Center. Commercial satellite operators can also pay

[258] Defense Intelligence Agency, 2022.

[259] CIC member, discussion with authors, June 9, 2023.

for a membership in the Space Information Sharing and Analysis Center to gain general awareness about threats to satellite systems.
Commercial satellite operators may also gain access to additional threat information through other relationships they may have with DoD (e.g., participating in wargames, supporting a particular DoD contract).

There is also a variety of information channels for commercial satellite operators to access near-real-time threat information. All satellite operators (commercial, government, foreign) receive spaceflight safety-related warnings (i.e., conjunction data messages from USSPACECOM's Combined Space Operations Center if their on-orbit asset is at risk of collision with another space object).[260] They receive a warning in a timely manner to enable operators to mitigate a potential collision (e.g., maneuvering their satellite). Additionally, USSPACECOM's JCO sends near-real-time warnings via email about events in the space domain that can potentially be a threat to satellite operators. These alerts, referred to as Notice to Space Operators, include such events as satellite maneuvers, launch, possible breakup, signature changes, conjunctions, RPO, and other types of activities that could potentially be a hazard or a threat.[261] However, Notices to Space Operators, by themselves, may be insufficient for operators to determine whether any of these events are an indication that they may be targeted.

Commercial satellite operators that are members of the CIC—a component of the Combined Space Operations Center—have the most exclusive access to threat information, including near-real-time indications and warning and frequent threat briefings.[262] CIC members also share potential threat information with the Combined Space Operations Center and, sometimes, with other CIC members as they identify potential threats (e.g., anomalies or potential cyber intrusion) during their operations. As of 2023, the CIC contains ten participants that comprise nine SATCOM companies and one imagery company.

The CIC arrangement, however, presents challenges in information-sharing and increasing threat awareness. Although all CIC participants are either a U.S. company or U.S. subsidiary, companies with a foreign parent company might find it difficult to leverage classified information to inform their own operations centers—because their operations centers may be foreign-based and managed by foreign personnel who are not cleared.[263] Even companies whose operations centers are U.S.-based with cleared personnel may face barriers in receiving timely threat information because of lack of classified infrastructure (e.g., lack of access to classified email or voice systems). In these cases, CIC participants need to provide a more generalized message to inform their company's operations center.

---

260 USSPACECOM staff, discussion with authors, April 4, 2023.

261 USSPACECOM staff, email correspondence with authors, April 24, 2023. Any entity can request to be on the JCO distribution list to receive Notices to Space Operators.

262 The CIC was established in 2016 with six members and has grown since. Recognizing the important role of commercial satellite operators in supporting DoD missions, CIC was established to increase real-time information flow between the Combined Space Operations Center and commercial satellite operators to increase SDA and enable coordinated time-sensitive responses to critical space activities, such as anomaly resolutions. Each CIC member has a bilateral Cooperative Research and Development Agreement with USSPACECOM's Combined Force Space Component Command to enable information-sharing. As of May 2023, the CIC members are Eutelsat America Corp., Hughes, Inmarsat, Intelsat, Iridium, Maxar, SES Space & Defense, SpaceX, Viasat, and XTAR (CIC official, discussion with authors, May 11, 2023; USSPACECOM, "Commercial Integration Cell Fact Sheet," June 2021).

263 CIC official, discussion with authors, May 11, 2023.

Additionally, commercial satellite operators may not be forthcoming when it comes to sharing information with other commercial operators because of concerns about sharing proprietary information. Commercial satellite operators routinely review technical and operational data for their respective constellations to gain insights into potential interference activities or cyberattacks, which some operators may treat as proprietary information.[264] As a result, how much and what type of information CIC members share with other members varies.[265] That said, CIC members or other commercial satellite operators may have one-on-one information exchanges with other satellite operators with nondisclosure agreements in place or based on trusted relationships.

As the number of innovations and entrants of satellite operations increases, several operators expressed a desire to increase their awareness of potential threats. To do so, DoD would likely need to expand access to near-real-time classified threat information to operators. Expanding the amount of information many operators receive may mitigate risks to both commercial operators and DoD by allowing operators to better protect their satellites and allowing DoD to increase the number of satellites it may be able to rely on for operations.

Efforts to this end are already being taken for commercial imagery providers. In late August 2023, the NGA, NRO, and USSPACECOM signed the Commercial Space Protection Tri-Seal Strategic Framework, which acknowledges the increased role of commercial satellites in U.S. government intelligence and defense and the need to improve commercial satellite protection. It discusses coordination among the three parties for threat information-sharing, anomaly reporting, and strategies for commercial imagery collection. Development of this framework toward commercial protection is continuing.[266]

Increased access to information could also be accomplished by expanding the CIC or through another contracting mechanism. Operators may need to demonstrate certain minimum performance requirements to be able to enter into these contractual relationships. Another option may be to decrease the levels of classification of information to increase commercial operator awareness. This option would require DoD to perform an overall risk assessment to determine the appropriate classification levels for various information. The potential benefit of declassifying some threat information would be that more commercial operators could gain access, while not necessarily requiring a new contractual relationship.

Insurance Schemes for Commercial Satellites

For anything of high value, insurance often offers protection from loss or damage, with plenty of choices and options available to the buyer for purchase. This is the case for space assets, with a variety of space insurance coverage schemes addressing different facets of pre-launch, launch, and in-orbit operations. Satellite owners and operators, users, manufacturers, launch service providers, and others

---

[264] Space insurance subject-matter expert, discussion with authors, May 10, 2023; CIC official, discussion with authors, May 11, 2023.

[265] The CIC does have a bilateral Cooperative Research and Development Agreement in place allowing for companies to share proprietary information with the government. The CIC attempts to remove proprietary information but has CIC participants sign nondisclosure agreements to prevent participants from gaining a potential advantage.

[266] NGA, "NGA, NRO, USSPACECOM Plan for Threats to Commercial Satellites," press release, August 31, 2023.

involved with a satellite or space mission can obtain a variety of types of insurance to cover activities throughout the life cycle of a satellite or launch vehicle, such as integration and test, launch, and in-orbit operations. Table 8.2 summarizes insurance options available to satellite owners and operators.

Typically, satellite owners or operators are the entities that seek insurance. They seek coverage for the asset, any associated liability with an accident, or potential damage one might cause.[267] Many commercial operators hold pre-launch and launch coverage, but a smaller portion also have in-orbit coverage.[268]

Table 8.2. Overview of General Space Insurance Coverage Schemes Available to Satellite Owners or Operators

Type of Coverage	Asset	Liability
Pre-launch	X	
Launch	X	
In-orbit	X	X
Re-entry	X	X
Business interruption (available in pre-launch, launch, and in-orbit)	X	

SOURCE: Modified from Kunstadter, 2023.
NOTE: This table includes only broad categories of coverage available to satellite owners and operators. Types of coverage listed in the first column include offerings that can be obtained independently or in combination with other types of coverage, depending on the insurance company. These categories may also contain other sub-categories of coverage. For example, launch coverage may include coverage for just the duration of the flight on the launch vehicle or post-separation from the vehicle. Other types of space insurance coverage available on the market include human spaceflight, testing, and more. Space insurance coverage is also available to satellite users, manufacturers, and launch service providers.

Although insurance exists for business interruption, the loss of the asset is the primary focus of satellite owners' or operators' insurance policies because of the high capital costs associated with satellites and high reliability required for a long service life (though this trend is changing with the development of smaller satellites with a shorter life). If a service is disrupted because of the loss of a single satellite, operators may have flexibility to quickly adjust between payloads and utilize additional capacity on one of their other satellites until the lost satellite is replaced. Therefore, such operators do not generally see the need for business interruption insurance. That said, if operators do not have excess capacity on their satellites, they would likely have to make some adjustment by prioritizing customers (perhaps offloading customers temporarily or reducing quality of service for certain

[267] Licensed or permitted commercial launch and re-entry operators are required by 51 U.S.C. 50914 and 14 CFR 440.3 to obtain liability insurance or demonstrate financial responsibility to cover third-party claims in accordance with the Maximum Probable Loss determination, as calculated by the Federal Aviation Administration Office of Commercial Space Transportation. See U.S. Code, Title 51, National and Commercial Space Programs; Section 50914, Liability Insurance and Financial Responsibility Requirements; and Code of Federal Regulations, Title 14, Aeronautics and Space; Part 440, Financial Responsibility; Section 440.3, Definitions.

[268] Christopher T. W. Kunstadter, "Space Risk Update: 2022 Year-End Review," briefing slides, AXA XL, January 2023.

customers). This approach is unlikely to be feasible for a long-term loss of service without losing customers.

Loss of service that results from a faulty satellite hardware component would be covered by insurance for the asset. Denial of service may also be caused by an adversary in an electronic warfare attack or cyberattack, and it may be a temporary, reversible, non-kinetic attack, which is typically not covered by insurance. However, satellite users, such as satellite television or satellite radio users, may choose to be insured for interruptions to their business.

One of the most notable differences in the satellite insurance market is the difference in the use of insurance between GEO operators and pLEO operators. A much larger percentage of satellites in GEO (and in MEO and HEO) are insured, and for a higher value, than the percentage of LEO satellites that are insured. There are approximately 7,000 satellites in all orbits (the majority being pLEO satellites). Approximately 40 percent of GEO, HEO, and MEO satellites are insured, compared with approximately 1 percent of the satellites in LEO (for a total insurance value of $24.7 billion in higher orbits and $3.1 billion in LEO).[269] The difference in these separate orbital regimes is due in part to the bias of expensive and exquisite satellites operating in GEO compared with the increase of relatively smaller and cheaper satellites in LEO. The increase and proliferation of smaller, cheaper, commercial-off-the-shelf-based constellations can add a level of redundancy to many owners' and operators' architectures, causing them to evaluate whether insurance would be worth it when the assets are relatively easy to replace and when the loss of one or two would not have an impact on their ability to continue their mission.[270] As a result, the rise of pLEO constellations is having a notable impact in the space insurance market.

Exclusions for War and Cyberattacks

Satellite insurance policies normally follow an *all-risks* approach, which means that all causes of loss are covered except for those explicitly named in the policy—referred to as *exclusions*.[271] Common exclusions are for acts of war and cyberattacks.[272] As discussed in Chapter 7, commercial entities working with or supporting the U.S. armed forces could be presented with these or other threats. As the space insurance industry and commercial satellite operators are wrangling with this reality, there are many complications associated with determining whether a potential attack on commercial satellites would be covered because of the uncertainties about what constitutes an act of war in the context of the space domain and difficulties in determining whether an attack took place.

There are few historical examples of acts of war in space, and the definition could be open for interpretation in the future. It is still yet to be determined whether the clause would likely cover physical damage to satellites resulting from an attack by another entity during a conflict or war. Questions remain regarding which hostile acts would be covered outside a conflict or war. Given

---

[269] Kunstadter, 2023.

[270] Insurance during launch of a partial constellation (where a portion of the satellites comprising the constellation is on board) is more common than on-orbit insurance for operators with pLEO constellations because there is a greater risk of loss of a large portion of the constellation during launch.

[271] Space insurance subject-matter expert, discussion with authors, May 10, 2023.

[272] Acts of terrorism is another common exclusion.

current insurance schemes that provide coverage for damage to physical assets, actions we typically identify as kinetic physical space warfare actions resulting in physical damage (such as attacks by direct-ascent or co-orbital antisatellite weapons) would likely not be covered under insurance.[273]

Commercial satellite owners and operators view cyberattacks as an increasing threat. Commercial operators and government experts we met with said that, should they be attacked by U.S. adversaries, they anticipate cyber-related activities as a most likely means of attack and perhaps a precursor to broader or larger-scale attacks on their satellites or other U.S. interests.[274] Citing observations from the war in Ukraine, Secure World Foundation notes, "They are not blowing up satellites. They're going after the interference and denial of service."[275]

Insurance providers need to know the cause of satellite damage (known as anomaly attribution) to determine whether they should provide coverage or not, but often attribution is not easy to prove.[276] For instance, cyberattacks are notoriously hard to attribute.[277] Without attribution, insurance companies are unable to determine whether the damage (if physical to the asset) would be an exclusion. Similarly, acts of interference or denial of service that occur today, such as electromagnetic interference and radio frequency interference, are typically temporary and do not result in damage to the satellite itself and, therefore, are typically not covered by the insurance. If electromagnetic interference or radio frequency interference were to cause damage to a satellite, insurance companies may have to cover those damages, but it depends on the scenario and whether there is active conflict. Still, as with cyberattacks, attribution would be necessary to determine whether the interference was purposeful or was the result of natural causes.[278]

One concern among commercial satellite operators we spoke with is that insurance coverage does not extend to acts of war. There was also interest in coverage for cyberattacks—one of the most imminent threats they face. At present, insurance policies for cyber also typically have an act of war exclusion. However, there appears to be growing interest in cyber insurance to cover acts of war, a term of art that is also not clearly defined within cyber insurance.[279] Insurance providers recognize this potential demand for financial protections against emerging threats and are exploring various options.

---

[273] Space insurance subject-matter expert, discussion with authors, May 10, 2023.

[274] As discussed in Chapters 3 and 4, commercial space operators are constantly dealing with cyberattacks but have not reported significant intrusions or impacts to their operations during peacetime. They are generally concerned about cyberattacks during peacetime becoming larger damaging events and have been focused on improving cyber protections as cyber threats evolve.

[275] Sandra Erwin, "On National Security: Drawing Lessons from the First 'Commercial Space War,'" *SpaceNews*, May 20, 2022a.

[276] Space insurance subject-matter expert, discussion with authors, May 10, 2023.

[277] For more discussion on this issue, see John S. Davis II, Benjamin Boudreaux, Jonathan W. Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase, *Stateless Attribution: Toward International Accountability in Cyberspace*, RAND Corporation, RR-2081-MS, 2017; and William Banks, "Cyber Attribution and State Responsibility," *International Law Studies*, Vol. 97, 2021, pp. 1039–1072.

[278] Space insurance subject-matter expert, discussion with authors, May 10, 2023.

[279] For example, a 2017 malware attack on Merck by NotPetya was attributed to Russia's GRU agency (this agency is now known as the Main Directorate of the General Staff of the Armed Forces of the Russian Federation). Merck had several all-risks cyber insurance policies that excluded coverage for damages resulting from "hostile or warlike action." Insurers argued that the action met the definition of the exclusion. A New Jersey judge recently determined that the cyberattack was not a "warlike action" because it was a government action of ill will, not a military action. Under this conclusion, insurance payouts could be made to Merck. Lack of clear definitions could similarly result in court proceedings that affect the insurance and satellite industry while a determination is being made (Andrew S. Bowen, *Russian Cyber Units*, Version 4, Congressional Research Service, IF11718, February 2, 2022).

However, coverage for acts of war may not be realized in the insurance market without support from the government.

Possible Protection Options

With commercial owners and operators facing growing emerging threats, especially those threats to which they are susceptible as they support the armed forces, many of those with whom we met are interested in possible government-backed financial protections and are exploring a variety of options (to include self-insuring) based on their business models, relationship with DoD, and system architecture. DoD is also exploring various options and, in particular, an initiative modeled after the Civil Reserve Air Fleet. Figure 8.1 shows examples of potential financial and nonfinancial protections that a commercial satellite operator supporting U.S. armed forces may consider. This area is rapidly evolving, and none of these tools are intended to be suggestions for implementation nor are they mutually exclusive. Rather, we aim to identify a variety of options for further investigation, with implications for insurance that may be appropriate and conducive to a continued partnership between the commercial industry and DoD as its relationship with commercial industry evolves.

Figure 8.1. Potential Protection Options for Commercial Satellite Operators Supporting U.S. Armed Forces

Commercial insurance

- A combination of insurance coverages is purchased for satellite assets, cyberattacks, business interruption, and other potential losses (like today's insurance structure, but potentially increased coverage).
- Commercial coverage expands to include wartime insurance. Commercial assets would be covered for claims involving damages resulting from operations in direct support of DoD in conflict or war.

Government-based insurance

Government provides insurance options, including war risk insurance, and reimburses commercial space operators for claims resulting from support to DoD or U.S. government.

Indemnification/legislation-derived protection

Congressional action would call for indemnification of commercial satellite operators supporting DoD. A commercial operator supporting DoD that experiences loss of assets or service as a result of an attack would receive reimbursement from the government/DoD (e.g., direct financial compensation).

Commercial Augmentation Space Reserve initiative

U.S. government would provide support (including financial support), via tailored, contractual agreements with commercial operators agreeing to support DoD in peacetime, crisis, and/or significant conflict or war. Financial support could depend on level of commercial support, types of services provided, amount of risk assumed, or other factors negotiated with each contract.

DoD protect and defend of satellites

DoD extends on-orbit protect and defend operations to include commercial operators supporting the armed forces (e.g., commercial satellites placed on a Prioritized Critical Assets List (PCAL) to receive protections in line with DoD-owned assets).

Architecture TTP

Commercial operators/assets, as part of a hybrid architecture with DoD, are incorporated in TTP for information sharing, response to active and potential threats, and real-time actions and responses. The architecture considers and enables protection for all users.

SOURCE: Authors' analysis based on discussions with commercial satellites operators and government experts from January 2023 through August 2023.

Insurance

Commercial insurance or wartime insurance could expand to support commercial satellite operators that support U.S. armed forces. Commercial insurance could grow to include coverage unique to this scenario. For example, increased coverage could include a package of coverage for the satellite asset, business interruption, cyberattacks, or other potential losses. Insurance could also expand existing commercial satellite insurance to provide coverage for loss of a satellite asset in wartime. Commercial operators would be able to purchase these expanded satellite insurance policies or potentially negotiate the added costs associated with such coverage contractually when supporting DoD or the U.S. government.

Statutory-based, government-provided insurance programs, including war risk insurance, is another possibility that DoD could explore. Under U.S. Code Title 46 Chapter 539 and U.S. Code Title 49 Chapter 443, the Department of Transportation—through the Maritime Administration and FAA, respectively—can issue non-premium insurance options to maritime and air carriers supporting the U.S. government or DoD.[280] For any claims resulting from support of DoD, the Department of Transportation pays the contractor and is reimbursed by DoD. These insurance programs have supported the Civil Reserve Air Fleet and Voluntary Intermodal Sealift Agreement programs and could serve as a useful model for application in the space domain.[281]

Indemnification

One type of possible protection discussed in the trade literature and other forums is the concept of indemnification. Insurance-based indemnification, government-based indemnification, and/or having indemnification risk incorporated into service contracts could provide a form of protection to those commercial companies continuing or hoping to provide services to the armed forces.

Indemnification could be insurance-based, in which companies would be protected from any claims against them resulting from damages caused by their support to DoD missions. For example, unless accounted for within the contract, an agricultural company using remote sensing data could bring a claim against an Earth imaging company for not upholding its contractual obligations because of its work for DoD. Indemnity insurance that the Earth imaging company holds, however, would pay for the associated legal fees and settlements. Similarly, an indemnification construct could be government-backed—in which the U.S. government would provide financial coverage potentially up to a predetermined dollar amount or other unanticipated losses the commercial entity may incur because of its support of DoD (i.e., potential legal fees resulting from other third-party claims). Alternatively, without indemnification, these nuances could be added into contracts between DoD and the commercial operator, in which specific scenarios or types of loss could be identified explicitly.

Commercial Augmentation Space Reserve Initiative

Modeled off the Civil Reserve Air Fleet initiative, a Commercial Augmentation Space Reserve could be a mechanism for companies to seek financial or tactical protections from the U.S. government in exchange for support to DoD. The USSF recently developed a framework for a Commercial Augmentation Space Reserve in which the U.S. government and commercial satellite operators establish contracts to ensure that commercial satellite capabilities are accessible to the U.S. government in various phases of conflict.[282] This framework is contractually based to consider various levels of support under different threat scenarios (e.g., peacetime, major crisis, wartime). Such details as the specific services provided, availability, and technical specifications allotted to DoD or the U.S. government; integration and cybersecurity requirements; amount of risk to be assumed by the commercial entity; financial or tactical protections; and others could be worked out within each contract. Commercial operators and DoD could utilize a tailored approach that could address the

---

[280] U.S. Code Title 46, Chapter 539, War Risk Insurance; U.S. Code Title 49, Chapter 443, Insurance.

[281] Yool Kim and George Nacouzi, *A Framework for Building a Civil Reserve Space Program: Applicability of U.S. Transportation Command's Commercial Partnership Models*, RAND Corporation, PE-A980-1, November 2023.

[282] Richard Kniseley, "Commercial Augmentation Space Reserve Framework," briefing slides, Space Systems Command, July 2023; Sandra Erwin, "Space Force to Further Define Details of a 'Commercial Space Reserve,'" *SpaceNews*, July 25, 2023d; Courtney Albon, "Space Force Finalizes Plan for Commercial Surge Capacity During Crisis," *C4ISRNET*, October 19, 2023.

uniqueness of commercial satellite service types, potential risks, technical requirements, and financial risks.

Nonfinancial Protections

The U.S. government could place select satellite assets on the Prioritized Critical Assets List (PCAL) as a means of protecting commercial satellites. A PCAL designation would assign commercial satellite assets to a category of assets that could be encompassed under DoD's actions to protect and defend. Procedures for commercial space assets on a larger PCAL and the corresponding actions are still being developed.[283] However, not all commercial companies want to be on the PCAL because they feel it could affect their insurance policies or increase the likelihood of being identified as a critical target.

Additionally, commercial satellites could be included more deliberately in defense space architecture by integrating commercial services and data more wholly in U.S. armed forces operations. A hybrid space architecture that includes commercial space assets (similar to the SATCOM hybrid architecture discussed in Chapter 3) increases the resiliency of the overall architecture and hence provides protection for the commercial assets and other elements in the architecture. Integration of commercial space services in a hybrid architecture from the start (rather than into an existing architecture, which can be challenging) would enable a more holistic approach to information-sharing, responses to threats, and real-time actions and responses that account for protection of all assets that are part of the hybrid architecture.

Summary Assessment

Commercial satellite operators supporting DoD are well aware that they face threats from U.S. adversaries and that they might be targeted. However, the level of their awareness varies depending on the level of access they have to a wide variety of information sources. Different layers of threat warnings are available starting with public statements and documentation in the public domain U.S. government notices to space operators of potential conjunctions and/or threatening activities, classified information to cleared DoD commercial providers, and information disseminated by industry bodies. These notifications range from near-real-time to longer-term general awareness. However, changes should be made so that this information is available to a wider set of commercial satellite operators and the timeliness and specificity of such information are improved.

Satellite owners and operators obtain a variety of types of insurance to cover activities throughout the life cycle of a satellite. Each owner or operator makes choices about what type of insurance or coverage they seek based on their risk profile, which generally depends on their satellite technologies, architecture, business model, and other factors. Most insurance policies exclude losses occurring from acts of war and cyberattacks, and the latter is viewed as a growing threat by the industry.

---

[283] USSPACECOM has the mission of protecting and defending satellites on orbit, but that effort does not include an automatic extension for commercial satellites. The commander of USSPACECOM stated that specific direction to protect commercial satellite assets would need to come from the Secretary of Defense and the President. See Frank Wolfe, "US Space Command Does Not Provide Blanket Protection for Commercial Satellites, If Attacked," *Via Satellite*, July 20, 2023.

The commercial industry continues to support the U.S. armed forces using the existing insurance regime, and there are no glaring insurance obstacles that would drastically change that support in times of conflict, barring a catastrophic event. That said, commercial satellite operators, DoD, and the space insurance industry are exploring a variety of protection options to adapt to this dynamic space environment.

PART III. SUMMARY OF ASSESSMENT

Chapter 9

Findings and Conclusions

The commercial space sector is evolving rapidly with growing capacity and capability across a variety of space mission areas. It offers the opportunity to meet DoD's evolving mission requirements more responsively and increase resiliency of DoD's space architectures. As DoD moves in the direction of increasing its use and integration of commercial space services and data, there are many operational and policy considerations that the department needs to weigh and navigate, and we explored a subset of them in this report. This chapter contains a summary of our findings.

Operational Topics

Current Use of Commercial Satellites to Support Armed Forces Operations

From an overall DoD perspective, commercial SATCOM is a significant contributor to the department and a critical enabler to several high-value missions. Most military services use some level of commercial SATCOM in their daily operations. The level of dependence on this commercial service varies from exclusive (e.g., as for the Army's logistics and Blue force tracking operations, which reflects the criticality of DoD's reliance on commercial SATCOM) to high dependency (e.g., some of the USAF airborne ISR platforms) to optional (e.g., the Navy's fleet operations).

Although some commercial SDA companies have been operating for more than a decade, the commercial SDA services market is evolving, and DoD currently relies mostly on its own SDA capabilities to support its missions and uses commercial capabilities as an augmentation to its own. The USSF is the sole DoD user and provider of SDA services. The mission involves several tasks revolving around space safety and security. The use of commercial SDA services by DoD is coordinated by the JCO and centers around the protect and defend mission. Although the JCO operations are constrained because it is in a demonstration phase, it has made valuable contributions to the DoD SDA mission (e.g., observing the Chinese Shijian-21 high delta-V maneuvers and providing indications and warning of the November 2021 Russian antisatellite test).

DoD use of commercial services is limited for the remaining space missions we considered, such as remote sensing, environmental monitoring, PNT, and space logistics. DoD does leverage space-based commercial remote sensing data and information obtained and disseminated by the IC (i.e., NRO and NGA to support their missions). The commercial SBEM market is small and has received limited funding so far. Commercial space–based PNT services are currently limited and have negligible operational usage at this time. Space logistics is a relatively new mission, and DoD has not made any significant use of commercial capabilities in that area.

The Anticipated Increase in Use of Commercial Space Services During the Next Decade

The National Space Policy encourages the use of commercial space services when possible.[284] The degree to which DoD will use commercial services in the future will depend, in part, on how much DoD signals its future needs today or indicates its intentions to use such services in the coming years. Companies will use those demand signals to decide on future investments that will potentially expand capabilities of interest to DoD, thus increasing the use of these services. We did not make quantitative estimates about the change in DoD's use of commercial services because sufficient information to do so was not available and such estimates for a ten-year period would be fraught with large margins of error. Nevertheless, our analyses suggest that DoD is likely to increase its use of commercial services in many markets, including many emerging markets as those markets mature.

DoD will likely increase its use of commercial SATCOM. Commercial companies continue to deploy and offer new services, including pLEO and integrated multi-orbit communications services, incorporating such advanced features as beam forming that make these services more resilient to disruptions. DoD is also developing new and future concepts of operations that require ubiquitous, high-bandwidth communications capabilities, such as JADC2. Although government systems will meet some of these needs, commercial services will play an important role as part of a hybrid communications architecture consisting of more-interoperable government and commercial systems. Other DoD needs that are relying on lower-bandwidth government systems will use commercial systems as backup or as an augmentation to the department's current capabilities. DoD users of commercial services will likely increase their use of these services as their needs for communications increase.

DoD's use of commercial SDA is also likely to increase. The SDA needs will continue to grow in the future as space continues to become more congested and contested. This trend will drive a need for more timely coverage and more-exquisite capabilities. Companies are planning to expand their capabilities while new commercial SDA start-ups are developing and planning to deploy innovative capabilities that will be valuable to DoD, which is also expanding its ability to effectively leverage commercial SDA services, albeit at a relatively slow rate. The Department of Commerce and international governments appear to be increasing their reliance on commercial SDA providers, providing limited confidence in the growth of the market. Additionally, commercial satellite owners may need more-responsive and timely commercial SDA services to support (1) their future operations involving larger constellations, (2) the RPO, and (3) other activities that may involve the beyond GEO region.

The commercial remote sensing services will likely continue to grow as commercial capabilities, such as higher revisit rates from proliferated constellations and multi-phenomenology sensors, become more valuable to DoD. These commercial capabilities could augment DoD ISR systems and possibly alleviate the burden on exquisite government sensors to perform lower resolution observations and allow these systems to be more responsive to other critical missions.

It is not clear to us whether the use of commercial PNT and environmental monitoring services by DoD will grow significantly. The commercial market for these services is relatively limited and may

[284] Office of the President, 2020, p. 20.

not grow substantially given that government systems will continue to provide free PNT and weather information to the general public that may be sufficient for many commercial applications.

The use of commercial space logistics by DoD is very limited. We expect that DoD will leverage these capabilities in the future as they evolve and become more valuable in support of the department's missions. One of the major drivers will be how capable these commercial systems will be in the future and their ability to support the DoD's and the U.S. government's evolving missions.

Impact on Armed Forces Operations of Loss of Access

It is unlikely that DoD will lose access to all commercially operated space systems because of the inherent resilience of individual company services and DoD's access to multiple, independent providers. Given the competitive nature of commercial SATCOM services and the need to provide a reliable service to remain profitable, commercial SATCOM systems have become more resilient and able to mitigate the effect of disruptions. Additionally, given DoD's access to multiple independent providers, it is very unlikely that DoD will completely lose access to commercial SATCOM systems. However, this assessment is based on several assumptions, such as the following:

- Individual missions may rely solely on a single commercial provider. In such cases, the user would have contingency plans to quickly switch to a government system, a different provider, or an alternative means to execute the supported mission should a disruption occur.
- All elements of DOTmLPF-P would have been considered and addressed to ensure the ability to effectively use commercial SATCOM.

In the event of commercial SATCOM loss for a given mission, the impact will depend on the criticality of the mission and any contingency plans the user has in place. In some cases, the loss may result in a mission abort; in other cases, a loss may result in mission degradation. Additionally, operating in a bandwidth-limited environment could degrade the effectiveness of many missions that rely on bandwidth-intensive applications.

We also think it is unlikely that DoD will experience a complete loss of commercial SDA services. However, should such a loss occur, DoD will likely face some degradation in its ability to execute that mission, although that degradation will not be substantial given the organic capabilities DoD possesses.

Steps to Mitigate the Risk of Loss of Access

DoD can take various actions to mitigate the risk of loss. It can diversify its space architecture to include government, international partner, and commercial space capabilities to increase mission resilience. Also, DoD should consider leveraging a resilient commercial architecture by using different independent companies, multiple phenomenologies, proliferated commercial networks, and distributed basing—such as by using multiple orbital regimes enabled by compatible user equipment.

There are actions that DoD can take to further reduce the vulnerability of commercial space systems or the company to various threats, including performing due diligence (such as examining physical and cyber security considerations) of individual companies prior to awarding contracts, providing timely threat information, conducting assessments of company viability, and considering countermeasures to possible foreign influence.

Additional steps to mitigate loss of SATCOM given the considerable use of these commercial services include providing clear indications of DoD needs to encourage future planning and development by the commercial space industry and developing operational concepts, TTP, and user equipment that enable the seamless switching between different orbits and providers, as needed.

For SDA, additional considerations also include supporting a healthy and competitive commercial industry by (1) providing clear indications of DoD needs to encourage future planning and development and (2) developing C2 capabilities that make it possible to leverage multiple commercial providers in a tactically relevant manner—such as what is being achieved through JCO.

The Role of Commercial Systems in Increased Resiliency of DoD Space Architectures

The role of commercial services in increasing the resiliency of DoD space architectures is notable and potentially critical. The commercial services improve many of the resiliency characteristics of DoD's space architecture, including disaggregation, distribution, distribution, diversification, and proliferation. If appropriately implemented, commercial space services can significantly increase DoD's space mission resiliency. DoD is shifting to a hybrid SATCOM architecture that integrates commercial SATCOM with military SATCOM to increase resiliency. Although we posit that the commercial SDA services leveraged by the JCO increase the resiliency of the SDA enterprise, it is not clear to what extent DoD plans to leverage commercial SDA as an additional capability to increase its SDA mission resiliency.

Frequency of Third-Party Interference in the Past Decade

Our research indicated that the frequency of intentional interference with commercial services supporting DoD has been limited. Companies we spoke with indicated that the interference they have experienced in the past has been unintentional or natural (e.g., weather related). However, this perspective is based on a benign, historical period in which the United States did not experience direct armed conflicts with near peer adversaries. Therefore, this historical trend may not be indicative of what the future might hold, especially if the United States is involved in a conflict with a capable adversary. A notable example of potential interference with commercial services during a conflict has been the Ukraine war in which Russia has demonstrated its will and capability to interfere with commercial SATCOM services. Commercial operators have also observed that interference activities by third parties are increasing in sophistication.

Policy Topics

Leveraging commercial space assets to support DoD operations requires an operational architecture that is not only able to effectively leverage the commercial services through appropriate integration, C2, and contractual agreements but also support policy at the national and international levels. In actuality, all elements of DOTmLPF-P need to be considered and addressed.

International Agreements and Governing Organizations

The Outer Space Treaty regime represents the strongest set of hard law mechanisms that govern the behavior of commercial and government operators in space. The Outer Space Treaty makes participating host nations responsible for the behavior of their commercial space owners and operators; however, the regime has weak or no international enforcement mechanisms. Additionally, the Outer Space Treaty is dated, and current international governing efforts focus on developing and propagating norms of behavior that are voluntary. Another key set of regulations promulgated by the ITU (a branch of the United Nations) coordinates and assigns the millions of frequencies for the global radio network and designates orbital slots for GEO satellites. Absent clear international norms and guidance, commercial operators are working together to establish their own operational guidelines.

Whether a Commercial Satellite Is a Legitimate Military Target

The general consensus among policy, legal, and military experts is that a commercial satellite supporting military operations is a legitimate military target under international laws. However, what constitutes a necessary and proportional military attack against a satellite is an open question, and what types of attacks might be considered a violation by the international community is also unsettled.

Awareness That Commercial Satellites May Be Targeted by a Foreign Power

Commercial satellite operators supporting DoD are well aware that they face threats from U.S. adversaries. There are different layers of threat warnings, starting with public statements and documentation in the public domain U.S. government notices to space operators of potential conjunctions and/or threatening activities, classified information to cleared DoD commercial providers, and information disseminated by industry bodies. These notifications range from near-real-time to longer-term general awareness.

Insurance Coverage for Commercial Satellites That Support Armed Forces Operations

Satellite owners and operators obtain a variety of types of insurance to cover activities throughout the life cycle of a satellite. Each owner or operator makes choices about what type of insurance or coverage each seeks based on the individual risk profile, which could vary depending on satellite technologies, architecture, business model, and other factors. Many operators of pLEO constellations are choosing to self-insure because their low-cost satellites are replaced more frequently unlike traditional GEO satellites that are high cost and long-lived; only 1 percent of all satellites in LEO are insured compared with about 40 percent of satellites in higher orbits. Most insurance policies exclude losses occurring from acts of war and cyberattacks, and the latter is viewed as a growing threat by the industry. The space insurance industry is exploring potential products to adapt to this dynamic space environment.

Way Ahead for DoD

We observe that much work remains for DoD to operationalize integration of commercial space services into DoD's space architectures, even in SATCOM—a space mission area where DoD has the most experience working with the commercial sector. The reality that commercial satellites may be targeted by U.S. adversaries is further complicating the matter.

We identified various measures that DoD should consider to mitigate the risk of losing commercial space services that support critical DoD operations, especially in times of conflict. The feasibility and effectiveness of these measures will vary depending on the space mission, technical characteristics of commercial space services or systems, tasks or missions being supported, commanders' risk tolerance, and a host of other contextual factors. As a result, DoD needs to investigate the applicability of various mitigation measures based on the specific context in which commercial space services or systems is being used.

The principal mitigation measure is to increase the resiliency of DoD's space architecture, which involves integrating a diverse set of commercial space capabilities from multiple providers. Operationalizing such a hybrid architecture will be a long journey. To ensure successful implementation, DoD should determine the roles of commercial space services early in the capability and architecture development process and follow through by allocating corresponding budget based on the expected commercial contribution. Additionally, DoD should concurrently address all dimensions of DOTmLPF-P, which will include developing a C2 construct and associated ground infrastructure, putting contractual agreements in place, and drafting policies that facilitate the use of commercial services. In the near term, DoD should ensure that contingency plans are in place and develop TTP to enable continuity of operations if commercial space services are lost.

Another area that DoD needs to prioritize is the development and advancement of commercial space integration strategies and policies that are better aligned with the pace of commercial development and the growing threats to attaining national security objectives and sustaining U.S. leadership in commercial space. DoD should consider various options for protecting commercial space entities by leveraging different tools at its disposal (e.g., contractual mechanisms, insurance, information-sharing, TTP). Each commercial space company has a different system architecture, business model, and risk profile; thus, it will be essential to draw from a variety of tools to support all types of commercial space companies and the multitude of ways they support DoD operations.

Implementing these measures will require synchronization of activities across the U.S. government and DoD components—including the possibility of legislative and regulatory actions. It will also require a concerted effort by DoD to further strengthen its partnership with the commercial space industry by communicating its evolving needs, investing in emerging technologies, and expanding information exchange.

Appendix

Overview of Commercial SATCOM and SDA Companies

In this appendix, we summarize relevant information for companies in two sectors of the commercial space industry—SATCOM and SDA. The companies in Tables A.1 and A.2 include major service providers in the United States and allied countries, particularly those foreign companies with subsidiary branches for U.S. business; the tables are not a comprehensive survey of all service providers in each market. For SATCOM companies, Table A.1 contains corporate information, the inventory of active assets available, and broadband service provision. Revenue is provided based on public documentation, but several companies are private or have been privatized, so estimates are based on the most recent documentation available. For SDA companies, Table A.2 contains corporate information, available assets, and technical capabilities. Many of the companies in this sector are private companies and much newer compared with SATCOM providers; consequently, less information about revenue is available.

Table A.1. SATCOM Companies

Company	Founded	Headquarters	Estimated Revenue (billions $USD, year)	Active Assets	Frequency	Orbit
Astranis	2015	United States		1 satellite	Ka-band, Ku-band	GEO
Echostar*	2008	United States	2 (2022)	10 satellites	Ka-band	GEO
Eutelsat*	1977	France	1.31 (2022)	36 satellites	Ku-band, C-band	GEO
Globalstar	1991	United States	0.124 (2022)	24 satellites	L-band, S-band, C-band	LEO
Inmarsat*	1979	United Kingdom	1.352 (2020)	15 satellites	L-band, Ka-band, Ku-band, C-band, S-band, (X-band via Cobra terminals)	GEO
Intelsat*	1964	Luxembourg	1.9 (2021)	52 satellite	C-band, Ku-band, Ka-band	GEO
Iridium Communications*	2000	United States	0.721 (2022)	75 satellites	L-band	LEO
Ligado Networks	2015	United States		1 satellite	L-band	GEO
Lynk Global	2017	United States		3 satellites	Ka-band, S-band	LEO
OHB	1958	Germany	1.1 (2022)	3 satellites	L-band, Ka-Band	GEO
Oneweb	2012	United Kingdom	0.096 (2022)	633 satellites	Ku-band, Ka-band	LEO
Optus	1981	Australia		5 satellites	Ku-band	GEO
Orbcomm	1993	United States	0.248 (2020)	~30 satellites	Very high frequency	LEO
SES*	1985	Luxembourg	1.782 (2021)	~70 satellites	Ka-band, Ku-band, C-band	GEO, MEO
Sky-Perfect JSAT	2007	Japan	0.811 (2021)	16 satellites	Ku-band, C-band	GEO
SpaceX*	2002	United States		~4,000 satellites	Ka-band, Ku-band	LEO
Telesat	1969	Canada	0.759 (2022)	17 satellites	C-band, Ku-band, Ka-band	GEO
Viasat*	1986	United States	2.6 (2022)	6 satellites	Ka-band	GEO
XTAR*	2001	United States		1 satellite, 1 hosted payload	X-band	LEO

SOURCE: Authors compiled this table from analysis conducted between June 2023 and August 2023 of company webpages, company annual financial disclosures, and media sources, such as *SpaceNews*, *Satellite Today*, and *Space.com*. Searches were supplemented with reports from LexisNexis, which yielded reports on finances from the companies listed in the table.
NOTE: Estimated revenue (column 3) is accurate as of the years indicated in parentheses. Empty entries in estimated revenue (column 3) indicate private companies that do not publicize their annual revenue.
* Indicates a company that is a member of the CIC.

Table A.2. SDA Companies

Company	Founded	Headquarters	Active Assets	Phenomenology
LeoLabs	2016	United States	6 ground stations, 10 radars	S-band and UHF radar
ExoAnalytic Solutions	2008	United States	350 telescopes	Electro-optical
Slingshot Aerospace	2017	United States	20 ground stations, 30 telescopes and 200 sensors	Electro-optical
Kratos Defense & Security Solutions	1994	United States	20 ground stations and 150 sensors	Passive radio frequency sensing (L-, S-, C-, X- and Ku-bands)
Elecnor Deimos	2001	Spain	4 telescopes	Electro-optical
Maxar Technologies	2017	United States	4 satellites	Electro-optical
Scout Space	2019	United States	Planned	Electro-optical, multispectral, and visible and near-infrared
Privateer Space	2021	United States		Radio frequency sensors
TrueAnomaly	2022	United States	Planned	
Safran	2005	France		Radio frequency sensors
Electro Optic Systems	1983	Australia		Passive and active optical sensors
NorthStar Earth & Space	2015	Canada	Planned	

SOURCE: Authors compiled this table from analysis conducted between June 2023 and August 2023 of company webpages, company factsheets, and media sources, such as *SpaceNews*, *Satellite Today*, and *Space.com*.
NOTE: Empty cells indicate that information is not available.

Abbreviations

AEHF	Advanced Extremely High Frequency
AFATDS	Advanced Field Artillery Tactical Data System
C2	command and control
C3	command, control, and communications
CIC	Commercial Integration Cell
CSCO	Commercial Satellite Communications Office
CSS VSAT	Combat Service Support Very Small Aperture Terminal
DoD	U.S. Department of Defense
DOTmLPF-P	doctrine, organizations, training, materiel, leadership and education, personnel, facilities, and policy
EO/IR	electro-optical/infrared
EOCL	Electro-Optical Commercial Layer
FFRDC	federally funded research and development center
FY	fiscal year
GCCS-A	Global Command and Control System-Army
GEO	geosynchronous earth orbit
GNSS	Global Navigation Satellite System
GNSS-RO	Global Navigation Satellite System Radio Occultation
GPS	Global Positioning System
HEO	highly elliptical orbit
IC	intelligence community
ISR	intelligence, surveillance, and reconnaissance
ITU	International Telecommunications Union
JADC2	Joint All Domain Command and Control
JCO	Joint Task Force-Space Defense Commercial Operations
JREAP	Joint Range Extension Applications Protocol
JTF-SD	Joint Task Force-Space Defense
LEO	low earth orbit
MEO	medium earth orbit
MUOS	Mobile User Objective System
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NDAA	National Defense Authorization Act
NGA	National Geospatial-Intelligence Agency

NIPR	Non-classified Internet Protocol Router
NMESIS	Navy Marine Corps Expeditionary Ship Interdiction System
NOAA	National Oceanic and Atmospheric Administration
NRO	National Reconnaissance Office
PACE	primary, alternate, contingency, and emergency
pLEO	proliferated low earth orbit
PLI	position and location information
PNT	positioning, navigation, and timing
RPO	rendezvous and proximity operations
SAF/SQ	Assistant Secretary of the Air Force for Space Acquisition and Integration
SATCOM	satellite communications
SBEM	space-based environmental monitoring
SDA	space domain awareness
SIPR	Secret Internet Protocol Router
SSA	space situational awareness
SSN	Space Surveillance Network
TTP	tactics, techniques, and procedures
UHF	Ultra High Frequency
USAF	U.S. Air Force
USSF	U.S. Space Force
USSPACECOM	U.S. Space Command
WGS	Wideband Global SATCOM

References

9th Communication Battalion, "I MEF Agile and Assured C5ISRT Overview," U.S. Marine Corps, May 1, 2023.

Air Force Doctrine Note 1-21, *Agile Combat Employment*, U.S. Air Force, August 23, 2022.

Air Force Doctrine Publication 1-1, *Mission Command*, U.S. Air Force, August 14, 2023.

Albon, Courtney, "Space Force Finalizes Plan for Commercial Surge Capacity During Crisis," *C4ISRNET*, October 19, 2023. As of November 22, 2023: https://www.c4isrnet.com/battlefield-tech/space/2023/10/19/space-force-finalizes-plan-for-commercial-surge-capacity-during-crisis/

Almalhodaei, Aria, "Orbit Fab Closes $28.5M Series A for On-Orbit Refueling Capabilities," *TechCrunch*, April 17, 2023.

American Institute of Aeronautics and Astronautics, "AIAA Space Logistics Technical Committee," webpage, undated. As of November 27, 2023: https://www.aiaa-sltc.org/

Austin, Lloyd J. III, "Tenets of Responsible Behavior in Space," memorandum from the Secretary of Defense to the secretaries of the military departments, July 7, 2021.

Banks, William, "Cyber Attribution and State Responsibility," *International Law Studies*, Vol. 97, 2021.

Beard, Jack, "The Principle of Proportionality in an Era of High Technology," in Willian C. Winston and Christopher M. Ford, eds., *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, Vol. 1, Oxford University Press, 2018.

Bowen, Andrew S., *Russian Cyber Unit*s, Version 4, Congressional Research Service, IF11718, February 2, 2022.

Cardillo, Robert, transcript of remarks at the 2017 GEOINT Symposium, National Geospatial-Intelligence Agency, June 5, 2017. As of May 16, 2023: https://www.nga.mil/news/GEOINT_2017_Symposium.html

Chaplain, Cristina T., *Space Situational Awareness Efforts and Planned Budgets*, U.S. Government Accountability Office, GAO-16-6R, October 2015.

Chaplain, Cristina T., *Defense Space Acquisitions: Too Early to Determine If Recent Changes Will Resolve Persistent Fragmentation in Management and Oversight*, U.S. Government Accountability Office, GAO-16-592R, July 27, 2016.

Chevli, K. R., P. Y. Kim, A. A. Kagel, D. W. Moy, R. S. Pattay, R. A. Nichols, and A. D. Goldfinger, "Blue Force Tracking Network Modeling and Simulation," *MILCOM 2006: 2006 IEEE Military Communications Conference*, 2006.

Clark, Stephen, "Live Coverage: SpaceX Launches Rideshare Mission, Lands Another Falcon Booster," *Spaceflight Now*, May 25, 2022.

Code of Federal Regulations, Title 14, Aeronautics and Space.

Code of Federal Regulations, Title 14, Aeronautics and Space; Part 440, Financial Responsibility; Section 440.3; Definitions.

Combined Space Operations Center/SATCOM Integrated Operations Division, "SATCOM Electromagnetic Interference (EMI), Trending Report: CY 2013-2022," undated, Not available to the general public.

Cox, Matthew, "Future Army Brigades Will Fight for a Week Without Resupply, General Says," Military.com, November 6, 2018.

Davenport, Christian, "Commercial Satellites Test the Rules of War in Russia-Ukraine Conflict," *Washington Post*, March 10, 2022a.

Davenport, Christian, "Russia Threatens Commercial Satellites That Pentagon Sees as Its Future," *Washington Post*, October 28, 2022b.

Davidson, Philip, "Advance Policy Questions for Admiral Philip Davidson, USN Expected Nominee for Commander, U.S. Pacific Command," Senate Armed Services Committee, April 18, 2018.

Davis, John S., II, Benjamin Boudreaux, Jonathan W. Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase, *Stateless Attribution: Toward International Accountability in Cyberspace*, RAND Corporation, RR-2081-MS, 2017. As of July 15, 2023: https://www.rand.org/pubs/research_reports/RR2081.html

Defense Intelligence Agency, *2022 Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion*, 2022.

Department of Defense Chief Information Officer, *Department of Defense Enterprise SATCOM Management and Control (ESC-MC) Implementation Plan*, October 20, 2022.

Department of Defense Directive 3100.10, *Space Policy*, Office of the Under Secretary of Defense for Policy, August 30, 2022.

DoD—*See* U.S. Department of Defense.

DoD Chief Information Officer—*See* Department of Defense Chief Information Officer.

DoD Directive—*See* Department of Defense Directive.

Duffy, Kate, "Elon Musk Says Russia Has Stepped Up Efforts to Jam SpaceX's Starlink in Ukraine," *Business Insider*, May 11, 2022.

Edwards, Jane, "DARPA's Robotic GEO Satellite Servicing Tech on Schedule for 2024 Launch," *ExecutiveGov*, November 9, 2022.

Edwards, Jane, "NASA Releases Solicitation for $476M Commercial SmallSat Data Acquisition Vehicle," *GovConWire*, March 22, 2023.

Erwin, Sandra, "Air Force: SSA Is No More; It's 'Space Domain Awareness,'" *SpaceNews*, November 14, 2019.

Erwin, Sandra, "Military Commanders Could Use More Satellites for Tactical Surveillance," *SpaceNews*, September 16, 2020.

Erwin, Sandra, "Bluestaq Wins $280 Million Space Force Contract to Expand Space Data Catalog," *SpaceNews*, March 23, 2021a.

Erwin, Sandra, "A Race Against Time to Replace Aging Military Weather Satellites," *SpaceNews*, May 24, 2021b.

Erwin, Sandra, "On National Security: Drawing Lessons from the First 'Commercial Space War,'" *SpaceNews*, May 20, 2022a.

Erwin, Sandra, "Russia Escalates Rhetoric on Commercial Satellites, Calls Them 'Legitimate Targets for Retaliation," *SpaceNews*, October 27, 2022b.

Erwin, Sandra, "New Space Force Procurement Shop Subscribes to the Space-as-a-Service Model," *SpaceNews*, November 21, 2022c.

Erwin, Sandra, "Report: Space Force Could Benefit from Commercial Data to Monitor Satellites and Debris," *SpaceNews*, April 2023a.

Erwin, Sandra, "Space Force Eager to Harness Satellite-Servicing Technologies," *SpaceNews*, June 13, 2023b.

Erwin, Sandra, "Space Force Selects Vendors for Low Earth Orbit Satellite Services," *SpaceNews*, July 25, 2023c.

Erwin, Sandra, "Space Force to Further Define Details of a 'Commercial Space Reserve,'" *SpaceNews*, July 25, 2023d.

Erwin, Sandra, "SpaceX Providing Starlink Services to DoD Under 'Unique Terms and Conditions,'" *SpaceNews*, October 3, 2023e.

Farrar, Michael, and Adam DeMarco, "Air Force Space-Based Environmental Monitoring (SBEM) Update," briefing, Headquarters, U.S. Air Force, Directorate of Weather, February 28, 2020.

Feldscher, Jacqueline, "Space Force Will Be One of the First Customers of a New Gas Station in Space," *Fast Company*, October 13, 2022.

Flick, Ridge R., "Winning the Counterland Battle by Enabling Sensor-to-Shooter Automation," *960th Cyberspace Wing*, October 6, 2021.

Fortinsky, Sarah, "Bipartisan Bill Designates Space as Critical Infrastructure Sector," *The Hill* blog, July 27, 2023. As of October 6, 2023: https://thehill.com/homenews/space/4123413-bipartisan-bill-designates-space-as-critical-infrastructure-sector/

Frederick, Bryan, and David E. Johnson, *The Continued Evolution of U.S. Law of Armed Conflict Implementation*, RAND Corporation, RR-1122-OSD, 2015. As of September 13, 2023: https://www.rand.org/pubs/research_reports/RR1122.html

Global Geodetic Observing System, "GNSS Radio Occultation," webpage, undated. As of June 23, 2023: https://ggos.org/item/gnss-radio-occultation/

Goehring, John, "The Legality of Intermingling Military and Civilian Capabilities in Space," Lieber Institute at West Point, October 17, 2022.

Goodman, Adam, "Beyond Pixels: How NGA is Integrating Commercial Analytic Services into Agency Workflows," *NGA News*, January 30, 2023.

Hague Convention, (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, October 18, 1907.

The Hague Institute for Global Justice, *The Washington Compact on Norms of Behavior for Commercial Space Operations*, July 4, 2022.

Harrison, Todd, and Matthew Strohmeyer, *Commercial Space Remote Sensing and Its Role in National Security*, Center for Strategic and International Studies, February 2, 2022.

Headquarters Marine Corps, Combat Development and Integration, *Navy Marine Corps Expeditionary Ship Interdiction System (NMESIS) Concept of Employment*, August 5, 2021, Not available to the general public.

Hitchens, Theresa, "NRO Keeps 3 Vendors for Commercial Imagery with New 10-Year Contracts," *Breaking Defense*, May 25, 2022a.

Hitchens, Theresa, "First Joint Pentagon-Intel Community Space ISR Needs Assessment Nears Completion," *Breaking Defense*, June 3, 2022b.

Hitchens, Theresa, "Space Force Wraps Initial Plan for Building 'Hybrid' Commercial/Military 'Outernet,'" *Breaking Defense*, April 26, 2023.

Holt, Brian, "SpaceWERX Awards 124 Orbital Prime Contracts," Air Force Research Laboratory, November 4, 2022.

Howard, Karen, and Jon Ludwigson, *Defense Navigation Capabilities: DOD is Developing Positioning, Navigation, and Timing Technologies to Complement GPS*, U.S. Government Accountability Office, GAO-21-320SP, May 10, 2021b.

Inmarsat, "U.S. Navy Commercial Broadband Satellite Program Services Contract Worth up to $980m Awarded to Inmarsat Government," October 11, 2022.

Insinna, Valerie, "Lockheed, Northrop, Invest in a Startup That Wants to Refuel Satellites in Space," *Defense News*, September 7, 2021.

International Committee of the Red Cross, Convention (IV) Relative to the Protection of Civilian Persons in Time of War, August 12, 1949.

International Committee of the Red Cross, "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)," June 8, 1977.

International Committee of the Red Cross, *Constraints Under International Law on Military Operations in, or in Relation to, Outer Space During Armed Conflicts*, May 3, 2022.

Jakhu, Ram S., and Steven Freeland, eds., *McGill Manual on International Law Applicable to Military Uses of Outer Space:* Vol. I, *Rules*, Centre for Research in Air and Space Law, 2022.

Jewett, Rachel, "Xona Broadcasts Demo PNT Signals, Certifies Constellation Simulator with Spirent," *Satellite Today*, May 31, 2023.

Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, February 2022.

Joint Doctrine Note 1-19, *Competition Continuum*, Joint Chiefs of Staff, June 3, 2019.

Joint Publication 3-09, *Joint Fire Support*, Joint Chiefs of Staff, April 10, 2019.

Joint Publication 3-14, *Space Operations*, Joint Chiefs of Staff, August 23, 2023.

Joint Task Force-Space Defense, "18th Space Defense Squadron," fact sheet, May 2, 2022.

Joseph, Christine, and Sandy Magnus, "Overview of NOAA's Office of Space Commerce: A Presentation to the NOAA Science Advisory Board," briefing, April 27, 2023.

"JTF-SD Commercial Ops (JCO)," briefing presented by Joe Gerber, KBR, Inc., March 2023.

Kassas, Zaher (Zak) M., "Navigation from Low-Earth Orbit: Part 2: Models, Implementation, and Performance," *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, Vol. 2, 1st ed., Wiley-IEEE Press, 2020.

Kim, Yool, George Nacouzi, Mary Lee, Brian Dolan, Krista Romita Grocholski, Emmi Yonekura, Moon Kim, Thomas Light, and Raza Khan, *Leveraging Commercial Space Capabilities to Enhance the Space Architecture of the U.S. Department of Defense*, RAND Corporation, RR-A578-1, 2022, Not available to the general public.

Kim, Yool, and George Nacouzi, *A Framework for Building a Civil Reserve Space Program: Applicability of U.S. Transportation Command's Commercial Partnership Models*, RAND Corporation, PE-A980-1, November 2023. As of February 19, 2024:
https://www.rand.org/pubs/perspectives/PEA980-1.html

Kniseley, Richard, "Commercial Augmentation Space Reserve Framework," briefing slides, Space Systems Command, July 2023.

Koller, Josef S., *The Future of Ubiquitous, Realtime Intelligence: A GEOINT Singularity*, The Aerospace Corporation, August 2019.

Koplow, David A., "Reverse Distinction: A U.S. Violation of the Law of Armed Conflict in Space," *Harvard National Security Journal*, Vol. 13, January 7, 2022.

Kramer, Miriam, "Commercial Satellites Are the Next Front in Space War," Axios, November 1, 2022.

Kunstadter, Christopher T. W., "Space Risk Update: 2022 Year-End Review," briefing slides, AXA XL, January 2023.

L3Harris, "L3Harris Awarded $81 Million Contract to Connect Multi-Orbit Satellite Constellations," press release, June 6, 2023.

Lee, Mary, Brien Alkire, Jim Dimarogonas, Jeff Hagen, Christian Johnson, Moon Kim, Abbie Tingstad, Kristin Warren, and Michael Wilson, *Reliable Communications in a Contested Environment:* Vol. 1—*Policy Findings*, RAND Corporation, 2022, Not available to the general public.

Ligor, Douglas C., and Bruce McClintock, "Nasty, Brutish, and Short—The Future of Space Operations in the Absence of the Rule of Law: Addressing Congestion, Contestation, and Competitiveness in the New Space Era," *NATO Legal Gazette*, No. 42, December 2021.

Lopez, C. Todd, "Allies, Partners Central to U.S. Integrated Deterrence Effort," *DOD News*, March 1, 2023.

Luccio, Matteo, "PNT by Other Means: Xona Space Systems," *GPS World*, July 5, 2023.

Ludwigson, Jon, *Satellite Communications: DoD Should Explore Options to Meet Needs for Narrowband Capabilities*, U.S. Government Accountability Office, GAO-21-105283, September 2021.

Ludwigson, Jon, and Alissa H. Czyz, *Space Situational Awareness, DoD Should Evaluate How It Can Use Commercial Data*, U.S. Government Accountability Office, GAO-23-105565, April 2023.

Manson, Katrina, "The Russian Hack Everyone Is Finally Talking About," *Bloomberg Businessweek*, March 6, 2023.

Manzanec, Brian, *National Security Space: Actions Needed to Better Use Commercial Satellite Imagery and Analytics*, U.S. Government Accountability Office, GAO-22-106106, September 2022.

Maurer, Diana, *Defense Logistics: Army Should Ensure New System Operates in All Situations and Soldiers Complete Training*, U.S. Government Accountability Office, GAO-21-313, April 2021a.

McClintock, Bruce, Katie Feistel, Douglas C. Ligor, and Kathryn O'Connor, *Responsible Space Behavior for the New Space Era: Preserving the Province of Humanity*, RAND Corporation, PE-A887-2, April 2021. As of July 15, 2023:
https://www.rand.org/pubs/perspectives/PEA887-2.html

Miller, Amanda, and Aaron M. U. Church, "Air Force & Space Force Almanac 2022: Equipment," *Air & Space Forces Magazine*, July 1, 2022.

Moore, Roscoe M. III, "Business-Driven Negotiations for Satellite System Coordination: Reforming the International Telecommunication Union to Increase Commercially Oriented Negotiations over Scarce Frequency Spectrum," *Journal of Air Law and Commerce*, Vol. 65, No. 1, 1999.

Morgan, Daniel, *Commercial Space: Federal Regulation, Oversight, and Utilization*, Congressional Research Service, R45416, November 29, 2018.

Morgenstern, Wendy, "Episode 91: OSAM-1," *Small Steps, Giant Leaps*, podcast, August 24, 2022.

Muon Space, "Muon Space Awarded Additional Funding for Space Weather Data Collection," press release, July 11, 2023.

NASA—*See* National Aeronautics and Space Administration.

National Geospatial-Intelligence Agency, "NGA, NRO, USSPACECOM Plan for Threats to Commercial Satellites," press release, August 31, 2023.

National Oceanic and Atmospheric Administration, Office of Space Commerce, "Commercial Data Program (CDP)," webpage, undated. As of June 23, 2023:
https://www.space.commerce.gov/business-with-noaa/commercial-weather-data-pilot-cwdp/

National Reconnaissance Office, "NRO Announces Largest Award of Commercial Imagery Contracts," press release, May 25, 2022.

NATO—*See* North Atlantic Treaty Organization.

NGA—*See* National Geospatial-Intelligence Agency.

North Atlantic Treaty Organization, "NATO Joint Civil/Military Frequency Agreement (NJFA)," Extract for Public Disclosure 2014, February 14, 2017.

Northrop Grumman, "SpaceLogistics," webpage, undated. As of May 12, 2023:
https://www.northropgrumman.com/space/space-logistics-services/

Novelly, Thomas, "Citing Growing Threat from China, Space Force Leaders Say They Need More Money," *Military.com*, October 28, 2022.

Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America*, 2019.

Office of the President, *National Space Policy of the United States of America*, December 9, 2020.

"OneWeb Technologies Demos Seamless LEO and GEO Multi-Orbit Services for the U.S.M.C.," *SatNews*, July 28, 2023.

Ortega, Almudena Azcarate, "'Reducing Space Threats Through Norms, Rules, and Principles of Responsible Behaviours,' Topic 3: Current and Future Space-to-Space Threats by States to Space Systems," working paper, Open-Ended Working Group, United Nations, Office of Disarmament Affairs, September 14, 2022.

Permanent Mission of the People's Republic of China to the United Nations Office at Geneva and other International Organizations in Switzerland, "Remarks by H. E. Amb. Li Song on Topic 2 (Earth-to-Space Threats) at the Second Substantive Session of the Open-Ended Working Group on Reducing Space Threats," Open-Ended Working Group, United Nations, Office of Disarmament Affairs, September 14, 2022.

Planet, "PlanetScope," webpage, May 4, 2023. As of May 9, 2023: https://developers.planet.com/docs/data/planetscope/

Priebe, Miranda, Laurinda L. Rohn, Alyssa Demus, Bruce McClintock, Derek Eaton, Sarah Harting, and Maria McCollester, *Promoting Joint Warfighting Proficiency: The Role of Doctrine in Preparing Airmen for Joint Operations*, RAND Corporation, RR-2472-AF, 2018. As of August 3, 2023: https://www.rand.org/pubs/research_reports/RR2472.html

Priebe, Miranda, Alan J. Vick, Jacob L. Heim, and Meagan L. Smith, *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation*, RAND Corporation, RR-2959-AF, 2019. As of August 2, 2023: https://www.rand.org/pubs/research_reports/RR2959.html

Psiaki, Mark L., "Navigation Using Carrier Doppler Shift from a LEO Constellation: TRANSIT on Steroids," *NAVIGATION: Journal of the Institute of Navigation*, September 2021, Vol. 68, No. 3.

Public Law 116-181, Promoting Research and Observations of Space Weather to Improve the Forecasting of Tomorrow Act, October 21, 2020.

Public Law 117-81, National Defense Authorization Act for Fiscal Year 2022, Section 1607, Programs of Record of Space Force and Commercial Capabilities, December 27, 2021.

Radvanyi, Richard A., *Operations Eagle Claw—Lessons Learned*, United States Marine Corps Command and Staff College, AY 2000-01, 2002.

Rauenzahn, Brianna, Jasmine Wang, Jamison Chung, Peter Jacobs, Aaron Kaufman, and Hannah Pugh, "Regulating Commercial Space Activity," *Regulatory Review*, June 6, 2020.

Raymond, Jay, *United States Space Force Vision for Satellite Communications (SATCOM)*, January 20, 2020.

Riley, Heather, "Micrometeoroids and Orbital Debris (MMOD)," National Aeronautics and Space Administration, June 14, 2016.

Satelles, "Global Coverage," webpage, undated. As of September 23, 2023: https://satelles.com/technology/stl-provides-global-coverage-timing-synchronization/

Satellite Industry Association, *State of the Satellite Industry Report*, 2022.

Schmidt, Johannes, "The Corps' Newest SATCOM Terminal Adds Lethality Through Speed," Marine Corps Systems Command Office of Public Affairs and Communications, January 26, 2023.

Schradin, Ryan, "The Role of COMSATCOM in Army Communications and the WIN-T Increment 2," *Government Satellite Report*, October 18, 2016.

Space Systems Command, Commercial Satellite Communications Office, *Fiscal Year 22 Commercial Satellite Communications Expenditures and Usage Report*, August 2023, Not available to the general public.

Space Systems Command, CSCO—*See* Space Systems Command, Commercial Satellite Communications Office.

SpaceWERX, "Orbital Prime," briefing slides, undated.

Steer, Cassandra, "Application of International Humanitarian Law/Laws of Armed Conflict in Space: Civilians and Neutral States," 5th Session of the Open-Ended Working Group, United Nations, Office for Disarmament Affairs, May 11, 2022.

Suciu, Peter, "How the Space Force Is Planning to Use Commercial Satellites," *National Interest*, February 19, 2022. As of May 12, 2023:
https://nationalinterest.org/blog/buzz/how-space-force-planning-use-commercial-satellites-200697

Taverney, Thomas D., "The Evolution of Space-Based ISR," *Air & Space Forces Magazine*, August 10, 2022.

Thibault, Jennifer, "JTF-SD Awards Space Domain Awareness Contract via Marketplace," Joint Task Force-Space Defense Public Affairs, undated.

Triplett, Neal L., *Evolution of Air Weather Service with Emphasis on Enlisted Participation*, research paper, Air University, August 1991. As of June 23, 2023:
https://www.airuniversity.af.edu/Portals/10/AFEHRI/documents/EnlistedHistory/triplett.pdf

True Anomaly, homepage, undated. As of August 18, 2023:
https://www.trueanomaly.space

UK Mission to the WTO, UN and Other International Organisations (Geneva), "Exchange of Views on the Outcome of the First Session and Outlook Towards the Second Session," United Nations, Office of Disarmament Affairs, May 13, 2022.

United Nations, Charter of the United Nations, 1 UNTS XVI, October 24, 1945.

United Nations, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 18 UST 2410, January 27, 1967.

United Nations, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 610 UNTS 205, January 27, 1967.

United Nations, Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 672 UNTS 119, April 22, 1968.

United Nations, Convention on International Liability for Damage Caused by Space Objects, 961 UNTS 187, March 29, 1972.

United Nations, Convention on Registration of Objects Launched into Outer Space, 1023 UNTS 15, January 14, 1975.

United Nations, Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, 1363 UNTS 3, December 18, 1979.

United Nations, "Reducing Space Threats Through Norms, Rules, and Principles of Responsible Behaviours," A/RES/76/231, adopted December 24, 2021.

United Nations, Office for Outer Space Affairs, *Status of International Agreements Relating to Activities in Outer Space*, A/AC.105/C.2/2022/CRP.10, January 1, 2022.

USAF—*See* U.S. Air Force.

U.S. Air Force, *Department of Defense Plan to Meet Joint Requirements Oversight Council Meteorological and Oceanographic Collection Requirements*, report to congressional committees, August 2016.

U.S. Air Force, *Global Vigilance, Global Reach, Global Power for America*, 2013.

U.S. Air Force, "Tactical Employment: Distributed Common Ground System," Air Force Tactics, Techniques, and Procedures 3-1, DCGS, June 2015, Not available to the general public.

U.S. Army, Program Executive Office Command Control Communications-Tactical, "Satellite Communications: FOT," webpage, undated. As of September 16, 2023: https://peoc3t.army.mil/tn/fot.php

U.S. Code Title 46, Chapter 539, War Risk Insurance.

U.S. Code Title 49, Chapter 443, Insurance.

U.S. Code, Title 51, National and Commercial Space Programs.

U.S. Code, Title 51, National and Commercial Space Programs; Section 50903, General Authority.

U.S. Code, Title 51, National and Commercial Space Programs; Section 50914, Liability Insurance and Financial Responsibility Requirements.

U.S. Department of Defense, *Department of Defense Law of War Manual*, Office of General Counsel, last updated July 2023.

U.S. Marine Corps, *Tentative Manual for Expeditionary Advanced Base Operations,* 2nd ed., May 2023.

U.S. Marine Corps, *Force Design 2030 Annual Update*, June 2023.

U.S. Mission to International Missions in Geneva, "U.S. Statement to the Open-Ended Working Group on Reducing Space Threats," January 30, 2023.

U.S. Senate, National Defense Authorization Act for Fiscal Year 2022, Bill 2792, Section 1513, Study on Commercial Systems Integration into, and Support of, Armed Forces Space Operations, September 22, 2021.

U.S. Space Command, "Commercial Integration Cell Fact Sheet," June 2021.

U.S. Space Command, "Commercial Integration Strategy Overview," April 1, 2022.

"US Space Force Boosts Resilience with Capella Federal's Satellite Services Contract," *Space War,* August 20, 2023.

USSF—*See* U.S. Space Force.

USSPACECOM—*See* U.S. Space Command.

U.S. Space Force, *Spacepower: Doctrine for Space Forces*, Space Capstone Publication, June 2020.

U.S. Space Force, "Global Broadcast Service," fact sheet, October 2020.

Viasat, "Blue Force Tracking with Viasat L-Band Terminals," webpage, undated. As of October 27, 2023: https://www.viasat.com/products/terminals-and-radios/l-band-terminals/

Vorontsov, Konstantin, "Statement by Mr. Konstantin Vorontsov, Deputy Head of the Delegation of the Russian Federation, Deputy Director of the Department for Non-Proliferation and Arms Control of the Ministry of Foreign Affairs of the Russian Federation, at the Thematic Discussion on Outer Space (Disarmament Aspects) in the First Committee of the 77th Session of the UN General Assembly," unofficial translation, *Journal of the United Nations*, October 26, 2022.

Werner, Debra, "Startups Map Out Strategies to Augment or Backup GPS," *SpaceNews*, August 4, 2021a.

Werner, Debra, "Tomorrow.io Wins Air Force Funding for Weather Satellite Constellation," *SpaceNews*, October 1, 2021b.

Werner, Debra, "Orbital Micro Systems and Thomas Keating Forge Weather Data Pact," *SpaceNews*, October 5, 2021c.

Werner, Debra, "GeoOptics Wins NASA Commercial SmallSat Data Contract," *SpaceNews*, November 15, 2022.

Werner, Debra, "TrustPoint Launches First PNT Cubesat," *SpaceNews*, April 15, 2023.

Welser, William IV, "The Democratization of Space," *RAND Blog*, March 28, 2016. As of July 20, 2023: https://www.rand.org/blog/2016/03/the-democratization-of-space.html

White House, "Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space," presidential memorandum, May 24, 2018.

White House, "Memorandum of Space Policy Directive-5—Cybersecurity Principles for Space Systems," presidential memorandum, September 4, 2020.

Wolfe, Frank, "US Space Command Does Not Provide Blanket Protection for Commercial Satellites, If Attacked," *Via Satellite*, July 20, 2023.

Wong, Jonathan P., Yool Kim, Krista Langeland, George Nacouzi, Krista Romita Grocholski, Jonathan Balk, Karishma V. Patel, and Barbara Bicksler, *Leveraging Commercial Space Services: Opportunities and Risks for the Department of the Air Force*, RAND Corporation, RR-A1724-1, 2023. As of September 15, 2023: https://www.rand.org/pubs/research_reports/RRA1724-1.html

Yonekura, Emmi, Brian Dolan, Moon Kim, Krista Romita Grocholski, Raza Khan, and Yool Kim, *Commercial Space Capabilities and Market Overview: The Relationship Between Commercial Space Developments and the U.S. Department of Defense*, RAND Corporation, RR-A578-2, 2022. As of April 27, 2023: https://www.rand.org/pubs/research_reports/RRA578-2.html

RAND PROJECT AIR FORCE

The U.S. Department of Defense (DoD) and the military services rely on a wide variety of space capabilities to carry out many of their missions—but the degree of use differs depending on the mission. The space industry is rapidly evolving with continual changes to markets, companies, and their offerings, and these market dynamics influence DoD decisions about the use of commercial space services, which is expected to increase in the next decade. Technological advances make these services increasingly capable of supporting DoD needs and providing valuable augmentation to the department's own systems and capabilities. Despite the benefits that commercial services can bring, DoD must consider the vulnerability of these commercial space services to adversary attack when determining how much to rely on them and what missions they should support. The research team explored six commercial space markets—satellite communications; space domain awareness; remote sensing; environmental monitoring; positioning, navigation, and timing; and space logistics—in this congressionally directed report, which focuses on the implications of these increasing demands for commercial space services on space operations and the national and international policy environment.

$49.95

ISBN-10 1-9774-1487-7
ISBN-13 978-1-9774-1487-8

54995

9 781977 414878

www.rand.org

RR-A2562-2